Number Theory Revealed: An Introduction

Andrew Granville

AMS American Mathematical Society

Number Theory Revealed: An Introduction

Number Theory Revealed: An Introduction

Andrew Granville

AMS American Mathematical Society
Providence, Rhode Island

Cover design by Marci Babineau.

Front cover image of Srinivasa Ramanujan in the playing card: Oberwolfach Photo Collection, https://opc.mfo.de/; licensed under Creative Commons Attribution Share Alike 2.0 Germany, https://creativecommons.org/licenses/by-sa/2.0/de/deed.en.

Front cover image of Andrew Wiles in playing card, credit: Alain Goriely.

2010 *Mathematics Subject Classification.* Primary 11-01, 11A05, 11A07, 11A15, 11A41, 11A51, 11B39, 11D04, 11D07.

For additional information and updates on this book, visit
www.ams.org/bookpages/mbk-126

Library of Congress Cataloging-in-Publication Data

Cataloging-in-Publication Data has been applied for by the AMS.
See http:www.loc.gov/publish/cip/.

---

10 9 8 7 6 5 4 3 2 1 24 23 22 21 20 19

Dedicated to my beloved wife, Marci.

Writing this book has had its challenges.
Being the spouse of the author, while writing
this book, has also had its challenges.

The enchanting charms of this sublime science
reveal themselves only to those who have the
courage to go deeply into it.

Carl Friedrich Gauss, 1807

Contents

Preface

This is a modern introduction to number theory, aimed at several different audiences: students who have little experience of university level mathematics, students who are completing an undergraduate degree in mathematics, as well as students who are completing a mathematics teaching qualification. Like most introductions to number theory, our contents are largely inspired by Gauss's *Disquisitiones Arithmeticae* (1801), though we also include many modern developments. We have gone back to Gauss to borrow several excellent examples to highlight the theory.

There are many different topics that might be included in an introductory course in number theory, and others, like the law of quadratic reciprocity, that surely must appear in any such course. The first dozen chapters of the book therefore present a "standard" course. In the *masterclass* version of this book we flesh out these topics, in copious appendices, as well as adding five additional chapters on more advanced themes. In the *introductory* version we select an appendix for each chapter that might be most useful as supplementary material.[1] A "minimal" course might focus on the first eight chapters and at least one of chapters 9 and 10.[2]

Much of modern mathematics germinated from number-theoretic seed and one of our goals is to help the student appreciate the connection between the relatively simply defined concepts in number theory and their more abstract generalizations in other courses. For example, our appendices allow us to highlight how modern algebra stems from investigations into number theory and therefore serve as an introduction to algebra (including rings, modules, ideals, Galois theory, p-adic numbers,...). These appendices can be given as additional reading, perhaps as student projects, and we point the reader to further references.

Following Gauss, we often develop examples *before* giving a formal definition and a theorem, firstly to see how the concept arises naturally, secondly to conjecture a theorem that describes an evident pattern, and thirdly to see how a proof of the theorem emerges from understanding some non-trivial examples.

[1] In the main text we occasionally refer to appendices that only appear in the *masterclass* version.
[2] Several sections might be discarded; their headings are in ***bold italics.***

Why study number theory? Questions arise when studying any subject, sometimes fascinating questions that may be difficult to answer precisely. Number theory is the study of the most basic properties of the integers, literally taking integers apart to see how they are built, and there we find an internal beauty and coherence that encourages many of us to seek to understand more. Facts are often revealed by calculations, and then researchers seek proofs. Sometimes the proofs themselves, even more than the theorems they prove, have an elegance that is beguiling and reveal that there is so much more to understand. With good reason, Gauss called number theory the "*Queen of Mathematics*", ever mysterious, but nonetheless graciously sharing with those that find themselves interested. In this first course there is much that is accessible, while at the same time natural, easily framed, questions arise which remain open, stumping the brightest minds.

Once celebrated as one of the more abstract subjects in mathematics, today there are scores of applications of number theory in the real world, particularly to the theory and practice of computer algorithms. Best known is the use of number theory in designing cryptographic protocols (as discussed in chapter 10), hiding our secrets behind the seeming difficulty of factoring large numbers which only have large prime factors.

For some students, studying number theory is a life-changing experience: They find themselves excited to go on to penetrate more deeply, or perhaps to pursue some of the fascinating applications of the subject.

Why give proofs? We give proofs to convince ourselves and others that our reasoning is correct. Starting from agreed upon truths, we try to derive a further truth, being explicit and precise about each step of our reasoning. A proof must be readable by people besides the author. It is a way of communicating ideas and needs to be persuasive, not just to the writer but also to a mathematically literate person who cannot obtain further clarification from the writer on any point that is unclear. It is not enough that the writer believes it; it must be clear to others. The burden of proof lies with the author.

The word "proof" can mean different things in different disciplines. In some disciplines a "proof" can be several different examples that justify a stated hypothesis, but this is inadequate in mathematics: One can have a thousand examples that work as predicted by the hypothesis, but the thousand and first might contradict it. Therefore to "prove" a theorem, one must build an incontrovertible argument up from first principles, so that the statement must be true in every case, assuming that those first principles are true.

Occasionally we give more than one proof of an important theorem, to highlight how inevitably the subject develops, as well as to give the instructor different options for how to present the material. (Few students will benefit from seeing *all* of the proofs on their first time encountering this material.)

Motivation. Challenging mathematics courses, such as point-set topology, algebraic topology, measure theory, differential geometry, and so on, tend to be dominated at first by formal language and requirements. Little is given by way of motivation. Sometimes these courses are presented as a prerequisite for topics that will come later. There is little or no attempt to explain what all this theory is good

for or why it was developed in the first place. Students are expected to subject themselves to the course, motivated primarily by trust.

How boring! Mathematics surely should not be developed only for those few who already know that they wish to specialize and have a high tolerance for boredom. We should help our students to appreciate and cherish the beauty of mathematics. Surely courses should be motivated by a series of interesting questions. The right questions will highlight the benefits of an abstract framework, so that the student will wish to explore even the most rarified paths herself, as the benefits become obvious. Number theory does not require much in the way of formal prerequisites, and there are easy ways to justify most of its abstraction.

In this book, we hope to capture the attention and enthusiasm of the reader with the right questions, guiding her as she embarks for the first time on this fascinating journey.

Student expectations. For some students, number theory is their first course that formulates abstract statements of theorems, which can take them outside of their "comfort zone". This can be quite a challenge, especially as high school pedagogy moves increasingly to training students to learn and use sophisticated techniques, rather than appreciate how those techniques arose. We believe that one can best use (and adapt) methods if one fully appreciates their genesis, so we make no apologies for this feature of the elementary number theory course. However this means that some students will be forced to adjust their personal expectations. Future teachers sometimes ask why they need to learn material, and take a perspective, so far beyond what they will be expected to teach in high school. There are many answers to this question; one is that, in the long term, the material in high school will be more fulfilling if one can see its long-term purpose. A second response is that every teacher will be confronted by students who are bored with their high school course and desperately seeking harder intellectual challenges (whether they realize it themselves or not); the first few chapters of this book should provide the kind of intellectual stimulation those students need.

Exercises. Throughout the book, there are a lot of problems to be solved. Easy questions, moderate questions, hard questions, exceptionally difficult questions. No one should do them all. The idea of having so many problems is to give the teacher options that are suitable for the students' backgrounds:

An unusual feature of the book is that exercises appear embedded in the text.[3] This is done to enable the student to complete the proofs of theorems as one goes along.[4] This does not require the students to come up with new ideas but rather to follow the arguments given so as to fill in the gaps. For less experienced students it helps to write out the solutions to these exercises; more experienced students might just satisfy themselves that they can provide an appropriate proof.

[3]Though they can be downloaded, as a separate list, from `www.ams.org/granville-number-theory`.

[4]Often students have little experience with proofs and struggle with the level of sophistication required, at least without adequate guidance.

Other questions work through examples. There are more challenging exercises throughout, indicated by the symbol † next to the question numbers, in which the student will need to independently bring together several of the ideas that have been discussed. Then there are some really tough questions, indicated by the symbol ‡, in which the student will need to be creative, perhaps even providing ideas not given, or hinted at, in the text.

A few questions in this book are open-ended, some even phrased a little misleadingly. The student who tries to develop those themes her- or himself, might embark upon a rewarding voyage of discovery. Once, after I had set the exercises in section 9.2 for homework, some students complained how unfair they felt these questions were but were silenced by another student who announced that it was so much fun for him to work out the answers that he now knew what he wanted to do with his life!

At the end of the book we give hints for many of the exercises, especially those that form part of a proof.

Special features of our syllabus. Number theory sometimes serves as an introduction to "proof techniques". We give many exercises to practice those techniques, but to make it less boring, we do so while developing certain themes as the book progresses, for examples, the theory of recurrence sequences, and properties of binomial coefficients. We dedicate a preliminary chapter to induction and use it to develop the theory of sums of powers. Here is a list of the main supplementary themes which appear in the book:

Special numbers: Bernoulli numbers; binomial coefficients and Pascal's triangle; Fermat and Mersenne numbers; and the Fibonacci sequence and general second-order linear recurrences.

Subjects in their own right: Algebraic numbers, integers, and units; computation and running times: Continued fractions; dynamics; groups, especially of matrices; factoring methods and primality testing; ideals; irrationals and transcendentals; and rings and fields.

Formulas for cyclotomic polynomials, Dirichlet L-functions, the Riemann zeta-function, and sums of powers of integers.

Interesting issues: Lifting solutions; polynomial properties; resultants and discriminants; roots of polynomials, constructibility and pre-Galois theory; square roots (mod n); and tests for divisibility.

Fun and famous problems like the *abc*-conjecture, Catalan's conjecture, Egyptian fractions, Fermat's Last Theorem, the Frobenius postage stamp problem, magic squares, primes in arithmetic progressions, tiling with rectangles and with circles.

Our most unconventional choice is to give a version of Rousseau's proof of the law of quadratic reciprocity, which is directly motivated by Gauss's proof of Wilson's Theorem. This proof avoids Gauss's Lemma so is a lot easier for a beginning student than Eisenstein's elegant proof (which we give in section 8.10 of appendix 8A). Gauss's original proof of quadratic reciprocity is more motivated by the introductory material, although a bit more complicated than these other two proofs.

We include Gauss's original proof in section 8.14 of appendix 8C, and we also understand $(2/n)$ in his way, in the basic course, to interest the reader. We present several other proofs, including a particularly elegant proof using Gauss sums in section 14.7.

Further exploration of number theory. There is a tremendous leap in the level of mathematical knowledge required to take graduate courses in number theory, because curricula expect the student to have taken (and appreciated) several other relevant courses. This is a shame since there is so much beautiful advanced material that is easily accessible after finishing an introductory course. Moreover, it can be easier to study other courses, if one already understands their importance, rather than taking it on trust. Thus this book, *Number Theory Revealed*, is designed to lead to two subsequent books, which develop the two main thrusts of number theory research:

In *The distribution of primes: Analytic number theory revealed*, we will discuss how number theorists have sought to develop the themes of chapter 5 (as well as chapters 4 and 13). In particular we prove the prime number theorem, based on the extraordinary ideas of Riemann. This proof rests heavily on certain ideas from complex analysis, which we will outline in a way that is relevant for a good understanding of the proofs.

In *Rational points on curves: Arithmetic geometry revealed*, we look at solutions to Diophantine equations, especially those of degree two and three, extending the ideas of chapter 12 (as well as chapters 14 and 17). In particular we will prove Mordell's Theorem (developed here in special cases in chapter 17) and gain a basic understanding of modular forms, outlining some of the main steps in Wiles's proof of Fermat's Last Theorem. We avoid a deep understanding of algebraic geometry, instead proceeding by more elementary techniques and a little complex analysis (which we explain).

References. There is a list of great number theory books at the end of our book and references that are recommended for further reading at the end of many chapters and appendices. Unlike most textbooks, I have chosen to not include a reference to every result stated, nor necessarily to most relevant articles, but rather focus on a smaller number that might be accessible to the reader. Moreover, many readers are used to searching online for keywords; this works well for many themes in mathematics.[5] However the student researching online should be warned that Wikipedia articles are often out of date, sometimes misleading, and too often poorly written. It is best to try to find relevant articles published in expository research journals, such as the *American Mathematical Monthly*,[6] or posted at arxiv.org which is "open access", to supplement the course material.

The cover (designed by Marci Babineau and the author)**.**

In 1675, Isaac Newton explained his extraordinary breakthroughs in physics and mathematics by claiming, "*If I have seen further it is by standing on the shoulders*

[5] Though getting just the phrasing to find the right level of article can be challenging.

[6] Although this is behind a paywall, it can be accessed, like many journals, by logging on from most universities, which have paid subscriptions for their students and faculty.

of Giants." Science has always developed this way, no more so than in the theory of numbers. Our cover represents five giants of number theory, in a fan of cards, each of whose work built upon the previous luminaries.

Modern number theory was born from PIERRE DE FERMAT's readings of the ancient Greek texts (as discussed in section 6.1) in the mid-17th century, and his enunciation of various results including his tantalizingly difficult to prove "Last Theorem." His "Little Theorem" (chapter 7) and his understanding of sums of two squares (chapter 9) are part of the basis of the subject.

The first modern number theory book, Gauss's *Disquisitiones Arithmeticae*, on which this book is based, was written by CARL FRIEDRICH GAUSS at the beginning of the 19th century. As a teenager, Gauss rethought many of the key ideas in number theory, especially the law of quadratic reciprocity (chapter 8) and the theory of binary quadratic forms (chapter 12), as well as inspiring our understanding of the distribution of primes (chapter 5).

Gauss's contemporary SOPHIE GERMAIN made perhaps the first great effort to attack Fermat's Last Theorem (her effort is discussed in appendix 7F). Developing her work inspired my own first research efforts.

SRINIVASA RAMANUJAN, born in poverty in India at the end of the 19th century, was the most talented untrained mathematician in history, producing some extraordinary results before dying at the age of 32. He was unable to satisfactorily explain many of his extraordinary insights which penetrated difficult subjects far beyond the more conventional approaches. (See appendix 12F and chapters 13, 15, and 17.) Some of his identities are still inspiring major developments today in both mathematics and physics.

ANDREW WILES sits atop our deck. His 1994 proof of Fermat's Last Theorem built on the ideas of the previous four mentioned mathematicians and very many other "giants" besides. His great achievement is a testament to the success of science building on solid grounds.

Thanks. I would like to thank the many inspiring mathematicians who have helped me shape my view of elementary number theory, most particularly Bela Bollobas, Paul Erdős, D. H. Lehmer, James Maynard, Ken Ono, Paulo Ribenboim, Carl Pomerance, John Selfridge, Dan Shanks, and Hugh C. Williams as well as those people who have participated in developing the relatively new subject of "additive combinatorics" (see sections 15.3, 15.4, 15.5, and 15.6). Several people have shared insights or new works that have made their way into this book: Stephanie Chan, Leo Goldmakher, Richard Hill, Alex Kontorovich, Jennifer Park, and Richard Pinch. The six anonymous reviewers added some missing perspectives and Olga Balkanova, Stephanie Chan, Patrick Da Silva, Tristan Freiberg, Ben Green, Mariah Hamel, Jorge Jimenez, Nikoleta Kalaydzhieva, Dimitris Koukoulopoulos, Youness Lamzouri, Jennifer Park, Sam Porritt, Ethan Smith, Anitha Srinivasan, Paul Voutier, and Max Wenqiang Xu kindly read subsections of the near-final draft, making valuable comments.

Gauss's *Disquisitiones Arithmeticae*

In July 1801, Carl Friedrich Gauss published *Disquisitiones Arithmeticae*, a book on number theory, written in Latin. It had taken five years to write but was immediately recognized as a great work, both for the new ideas and its accessible presentation. Gauss was then widely considered to be the world's leading mathematician, and today we rate him as one of the three greatest in history, alongside Archimedes and Sir Isaac Newton.

The first four chapters of *Disquisitiones Arithmeticae* consist of essentially the same topics as our course today (with suitable modifications for advances made in the last two hundred years). His presentation of ideas is largely the model upon which modern mathematical writing is based. There follow several chapters on quadratic forms and then on the rudiments of what we would call Galois theory today, most importantly the constructibility of regular polygons. Finally, the publisher felt that the book was long enough, and several further chapters did not appear in the book (though Dedekind published Gauss's disorganized notes, in German, after Gauss's death).

One cannot overestimate the importance of *Disquisitiones* to the development of 19th-century mathematics. It led, besides many other things, to Dirichlet's formulation of ideals (see sections 3.19, 3.20 of appendix 3D, 12.8 of appendix 12A, and 12.10 of appendix 12B), and the exploration of the geometry of the upper half-plane (see Theorem 1.2 and the subsequent discussion).

As a young man, Dirichlet took his copy of *Disquisitiones* with him wherever he went. He even slept with it under his pillow. As an old man, it was his most prized possession even though it was in tatters. It was translated into French in 1807, German in 1889, Russian in 1959, English only in 1965, Spanish and Japanese in 1995, and Catalan in 1996!

Disquisitiones is no longer read by many people. The notation is difficult. The assumptions about what the reader knows do not fit today's reader (for example, neither linear algebra nor group theory had been formulated by the time Gauss wrote his book, although *Disquisitiones* would provide some of the motivation for developing those subjects). Yet, many of Gauss's proofs are inspiring, and some have been lost to today's literature. Moreover, although the more advanced two-thirds of *Disquisitiones* focus on binary quadratic forms and have led to many of today's developments, there are several themes there that are not central to today's research. In the fourth book in our trilogy (!), *Gauss's* Disquisitiones Arithmeticae *revealed*, we present a reworking of Gauss's classic, rewriting it in modern notation, in a style more accessible to the modern reader. We also give the first English version of the missing chapters, which include several surprises.

Notation

$\mathbb{N}$ – The *natural numbers*, $1, 2, 3, \ldots$.

$\mathbb{Z}$ – The *integers*, $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$.

Throughout, all variables are taken to be integers, unless otherwise specified.

Usually p, and sometimes q, will denote prime numbers.

$\mathbb{Q}$ – The *rational numbers*, that is, the fractions a/b with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$.

$\mathbb{R}$ – The *real numbers*.

$\mathbb{C}$ – The *complex numbers*.

$$\sum_{\substack{\text{Some variables:}\\ \text{Certain conditions hold}}} \text{summand} \qquad \text{and} \qquad \prod_{\substack{\text{Some variables:}\\ \text{Certain conditions hold}}} \text{summand}$$

mean that we sum, or product, the summand over the integer values of some variable, satisfying certain conditions.

Brackets and parentheses: There are all sorts of brackets and parentheses in mathematics. It is helpful to have protocols with them that take on meaning, so we do not have to repeat ourselves too often, as we will see in the notation below. But we also use them in equations; usually we surround an expression with "(" and ")" to be clear where the expression begins and ends. If too many of these are used in one line, then we might use different sizes or even "{" and "}" instead. If the brackets have a particular meaning, then the reader will be expected to discern that from the context.

$A[x]$ — The set of *polynomials* with coefficients from the set A, that is, $f(x) = \sum_{i=0}^{d} a_i x^i$ where each $a_i \in A$. Mostly we work with $A = \mathbb{Z}$.

$A(x)$ —The set of *rational functions* with coefficients from the set A, in other words, functions $f(x)/g(x)$ where $f(x), g(x) \in A[x]$ and $g(x) \neq 0$.

$[t]$ — The *integer part of* t, that is, the largest integer $\leq t$.

$\{t\}$ — The *fractional part of* (real number) t, that is, $\{t\} = t - [t]$. Notice that $0 \le \{t\} < 1$.

(a, b) — The greatest common divisor of a and b.

$[a, b]$ — The least common multiple of a and b.

$b|a$ — Means b divides a.

$p^k \| a$ — Means p^k divides a, but not p^{k+1} (where p is prime). In other words, k is the "exact power" of p dividing a.

$I(a, b)$ — The set $\{am + bn : \ m, n \in \mathbb{Z}\}$, which is called the *ideal* generated by a and b over $\mathbb{Z}$.

log — The logarithm in base e, the natural logarithm, which is often denoted by "ln" in earlier courses.

Parity – The *parity* of an integer is either even (if it is divisible by 2) or odd (if it is not divisible by 2).

The language of mathematics

"By a *conjecture* we mean a proposition that has not yet been proven but which is favored by some serious evidence. It may be a significant amount of computational evidence, or a body of theory and technique that has arisen in the attempt to settle the conjecture.

An *open question* is a problem where the evidence is not very convincing one way or the other.

A *theorem*, of course, is something that has been proved. There are important theorems, and there are unimportant (but perhaps curious) theorems.

The distinction between open question and conjecture is, it is true, somewhat subjective, and different mathematicians may form different judgements concerning a particular problem. We trust that there will be no similar ambiguity concerning the theorems."

—— Dan Shanks [**Sha85**, p. 2]

Today we might add to this a *heuristic* argument, in which we explore an open question with techniques that help give us a good idea of what to conjecture, even if those techniques are unlikely to lead to a formal proof.

Prerequisites

The reader should be familiar with the commonly used sets of numbers $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$, as well as polynomials with integer coefficients, denoted by $\mathbb{Z}[x]$. Proofs will often use the *principle of induction*; that is, if $S(n)$ is a given mathematical assertion, dependent on the integer n, then to prove that it is true for all $n \in \mathbb{N}$, we need only prove the following:

- $S(1)$ is true.
- $S(k)$ is true implies that $S(k+1)$ is true, for all integers $k \geq 1$.

The example that is usually given to highlight the principle of induction is the statement "$1+2+3+\cdots+n = \frac{n(n+1)}{2}$" which we denote by $S(n)$.[1] For $n = 1$ we check that $1 = \frac{1\cdot 2}{2}$ and so $S(1)$ is true. For any $k \geq 1$, we assume that $S(k)$ is true and then deduce that

$$\begin{aligned} 1+2+3+\cdots+(k+1) &= (\underbrace{1+2+3+\cdots+k}) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \quad \text{as } S(k) \text{ is true} \\ &= \frac{(k+1)(k+2)}{2}\,; \end{aligned}$$

that is, $S(k+1)$ is true. Hence, by the principle of induction, we deduce that $S(n)$ is true for all integers $n \geq 1$.

To highlight the technique of induction with more examples, we develop the theory of sums of powers of integers (for example, we prove a statement which gives a formula for $1^2 + 2^2 + \cdots + n^2$ for each integer $n \geq 1$) in section 0.1 and give formulas for the values of the terms of recurrence sequences (like the Fibonacci numbers) in section 0.2.

[1] There are other, easier, proofs of this assertion, but induction will be the only viable technique to prove some of the more difficult theorems in the course, which is why we highlight the *technique* here.

Induction and the least counterexample: Induction can be slightly disguised. For example, sometimes one proves that a statement $T(n)$ is true for all $n \geq 1$, by supposing that it is false for some n and looking for a contradiction. If $T(n)$ is false for some n, then there must be a least integer m for which $T(m)$ is false. The trick is to use the assumption that $T(m)$ is false to prove that there exists some smaller integer k, $1 \leq k < m$, for which $T(k)$ is also false. This contradicts the minimality of m, and therefore $T(n)$ must be true for all $n \geq 1$. Such proofs are easily reformulated into an induction proof:

Let $S(n)$ be the statement that $T(1), T(2), \ldots, T(n)$ all hold. The induction proof then works for if $S(m-1)$ is true, but $S(m)$ is false, then $T(m)$ is false and so, by the previous paragraph, $T(k)$ is false for some integer k, $1 \leq k \leq m-1$, which contradicts the assumption that $S(m-1)$ is true.

A beautiful example is given by the statement, "*Every integer* > 1 *has a prime divisor.*" (A *prime* number is an integer > 1, such that the only positive integers that divide it are 1 and itself.) Let $T(n)$ be the statement that n has a prime divisor, and let $S(n)$ be the statement that $T(2), T(3), \ldots, T(n)$ all hold. Evidently $S(2) = T(2)$ is true since 2 is prime. We suppose that $S(k)$ is true (so that $T(2), T(3), \ldots, T(k)$ all hold). Now:

Either $k+1$ is itself a prime number, in which case $T(k+1)$ holds and therefore $S(k+1)$ holds.

Or $k+1$ is not prime, in which case it has a divisor d which is not equal to either 1 or $k+1$, and so $2 \leq d \leq k$. But then $S(d)$ holds by the induction hypothesis, and so there is some prime p, which divides d, and therefore divides $k+1$. Hence $T(k+1)$ holds and therefore $S(k+1)$ holds.

(The astute reader might ask whether certain "facts" that we have used here deserve a proof. For example, if a prime p divides d, and d divides $k+1$, then p divides $k+1$. We have also assumed the reader understands that when we write "d divides $k+1$" we mean that when we divide $k+1$ by d, the remainder is zero. One of our goals at the beginning of the course is to make sure that everyone interprets these simple facts in the same way, by giving as clear definitions as possible and outlining useful, simple deductions from these definitions.)

Preliminary Chapter on Induction

Induction is an important proof technique in number theory. This preliminary chapter gives the reader the opportunity to practice its use, while learning about some intriguing number-theoretic concepts.

0.1. Fibonacci numbers and other recurrence sequences

The *Fibonacci numbers*, perhaps the most famous sequence of integers, begin with

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233, \ldots.$$

The Fibonacci numbers appear in many places in mathematics and its applications.[1] They obey a rule giving each term of the Fibonacci sequence in terms of the recent history of the sequence:

$$F_n = F_{n-1} + F_{n-2} \quad \text{for all integers } n \geq 2.$$

We call this a *recurrence relation*. It is not difficult to find a formula for F_n:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) \quad \text{for all integers } n \geq 0, \tag{0.1.1}$$

where $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$ each satisfy the equation $x+1 = x^2$. Having such an explicit formula for the Fibonacci numbers makes them easy to work with, but there is a problem. It is not obvious from this formula that every Fibonacci number is an integer; however that does follow easily from the original recurrence relation.[2]

[1] Typically when considering a biological process whose current state depends on its past, such as evolution, and brain development.

[2] It requires quite sophisticated ideas to decide whether a given complicated formula like (0.1.1) is an integer or not. Learn more about this in appendix 0F on symmetric polynomials.

Exercise 0.1.1. (a) Use the recurrence relation for the Fibonacci numbers, and induction to prove that every Fibonacci number is an integer.
(b) Prove that (0.1.1) is correct by verifying that it holds for $n = 0, 1$ and then, for all larger integers n, by induction.

Exercise 0.1.2. Use induction on $n \geq 1$ to prove that
(a) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$ and
(b) $1 + F_2 + F_4 + \cdots + F_{2n} = F_{2n+1}$.

The number $\phi = \frac{1+\sqrt{5}}{2}$ is called the *golden ratio*; one can show that F_n is the nearest integer to $\phi^n/\sqrt{5}$.

Exercise 0.1.3. (a) Prove that ϕ satisfies $\phi^2 = \phi + 1$.
(b) Prove that $\phi^n = F_n\phi + F_{n-1}$ for all integers $n \geq 1$, by induction.

Any sequence $x_0,\ x_1,\ x_2, \ldots$, for which the terms x_n, with $n \geq 2$, are defined by the equation

$$\boxed{x_n = ax_{n-1} + bx_{n-2} \ \text{ for all } n \geq 2,} \tag{0.1.2}$$

where a, b, x_0, x_1 are given, is called a *second-order linear recurrence sequence*. Although this is a vast generalization of the Fibonacci numbers one can still prove a formula for the general term, x_n, analogous to (0.1.1): We begin by factoring the polynomial

$$x^2 - ax - b = (x - \alpha)(x - \beta)$$

for the appropriate $\alpha, \beta \in \mathbb{C}$ (we had $x^2 - x - 1 = (x - \frac{1+\sqrt{5}}{2})(x - \frac{1-\sqrt{5}}{2})$ for the Fibonacci numbers). If $\alpha \neq \beta$, then there exist coefficients c_α, c_β for which

$$x_n = c_\alpha\alpha^n + c_\beta\beta^n \ \text{ for all } n \geq 0. \tag{0.1.3}$$

(In the case of the Fibonacci numbers, we have $c_\alpha = 1/\sqrt{5}$ and $c_\beta = -1/\sqrt{5}$.) Moreover one can determine the values of c_α and c_β by solving the simultaneous equations obtained by evaluating the formula (0.1.3) at $n = 0$ and $n = 1$, that is,

$$c_\alpha + c_\beta = x_0 \quad \text{and} \quad c_\alpha\alpha + c_\beta\beta = x_1.$$

Exercise 0.1.4. (a) Prove (0.1.3) is correct by verifying that it holds for $n = 0, 1$ (with x_0 and x_1 as in the last displayed equation) and then by induction for $n \geq 2$.
(b) Show that c_α and c_β are uniquely determined by x_0 and x_1, provided $\alpha \neq \beta$.
(c) Show that if $\alpha \neq \beta$ with $x_0 = 0$ and $x_1 = 1$, then $x_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ for all integers $n \geq 0$.
(d) Show that if $\alpha \neq \beta$ with $y_0 = 2, y_1 = a$ with $y_n = ay_{n-1} + by_{n-2}$ for all $n \geq 2$, then $y_n = \alpha^n + \beta^n$ for all integers $n \geq 0$.

The $\{x_n\}_{n\geq 0}$ in (c) is a *Lucas sequence*, and the $\{y_n\}_{n\geq 0}$ in (d) its *companion sequence*

Exercise 0.1.5.[3] (a) Prove that $\alpha = \beta$ if and only if $a^2 + 4b = 0$.
(b)† Show that if $a^2 + 4b = 0$, then $\alpha = a/2$ and $x_n = (cn + d)\alpha^n$ for all integers $n \geq 0$, for some constants c and d.
(c) Deduce that if $\alpha = \beta$ with $x_0 = 0$ and $x_1 = 1$, then $x_n = n\alpha^{n-1}$ for all $n \geq 0$.

Exercise 0.1.6. Prove that if $x_0 = 0$ and $x_1 = 1$, if (0.1.2) holds, and if α is a root of $x^2 - ax - b$, then $\alpha^n = \alpha x_n + bx_{n-1}$ for all $n \geq 1$.

[3] In this question, and from here on, induction should be used at the reader's discretion.

0.2. Formulas for sums of powers of integers

When Gauss was ten years old, his mathematics teacher aimed to keep his class quiet by asking them to add together the integers from 1 to 100. Gauss did this in a few moments, by noting if one adds that list of numbers to itself, but with the second list in reverse order, then one has

$$1 + 100 = 2 + 99 = 3 + 98 = \cdots = 99 + 2 = 100 + 1 = 101.$$

That is, twice the asked-for sum equals 100 times 101, and so

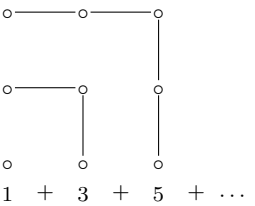
$$1 + 2 + \cdots + 100 \;=\; \frac{1}{2} \times 100 \times 101.$$

This argument generalizes to adding up the natural numbers less than any given N, yielding the formula[4]

$$\sum_{n=1}^{N-1} n \;=\; \frac{(N-1)N}{2}. \tag{0.2.1}$$

The sum on the left-hand side of this equation varies in length with N, whereas the right-hand side does not. The right-hand side is a formula whose value varies but has a relatively simple structure, so we call it a *closed form* expression. (In the prerequisite section, we gave a less interesting proof of this formula, by induction.)

Exercise 0.2.1. (a) Prove that $1 + 3 + 5 + \cdots + (2N-1) = N^2$ for all $N \geq 1$ by induction.
(b) Prove the formula in part (a) by the young Gauss's method.
(c) Start with a single dot, thought of as a 1-by-1 array of dots, and extend it to a 2-by-2 array of dots by adding an appropriate row and column. You have added 3 dots to the original dot and so $1 + 3 = 2^2$.



In general, draw an N-by-N array of dots, and add an additional row and column of dots to obtain an $(N+1)$-by-$(N+1)$ array of dots. By determining how many dots were added to the number of dots that were already in the array, deduce the formula in (a).

Let $S = \sum_{n=1}^{N-1} n^2$. Using exercise 0.2.1 we can write each square, n^2, as the sum of the odd positive integers $\leq 2n$. Therefore $2m-1$ appears $N-m$ times in the sum for S, and so

$$S = \sum_{m=1}^{N-1} (2m-1)(N-m) = -N \sum_{m=1}^{N-1} 1 + (2N+1) \sum_{m=1}^{N-1} m - 2S.$$

[4]This same idea appears in the work of Archimedes, from the third century B.C. in ancient Greece.

Using our closed formula for $\sum_m m$, we deduce, after some rearrangement, that

$$\sum_{n=1}^{N-1} n^2 = \frac{(N-1)N(2N-1)}{6},$$

a closed formula for the sum of the squares up to a given point. There is also a closed formula for the sum of the cubes:

$$\sum_{n=1}^{N-1} n^3 = \left(\frac{(N-1)N}{2}\right)^2. \tag{0.2.2}$$

This is the square of the closed formula (0.2.1) that we obtained for $\sum_{n=0}^{N-1} n$. Is this a coincidence or the first hint of some surprising connection?

Exercise 0.2.2. Prove these last two formulas by induction.

These three examples suggest that there are closed formulas for the sums of the kth powers of the integers, for every $k \geq 1$, but it is difficult to guess exactly what those formulas might look like. Moreover, to hope to prove a formula by induction, we need to have the formula at hand.

We will next find a closed formula in a simpler but related question and use this to find a closed formula for the sums of the kth powers of the integers in appendix 0A. We will go on to investigate, in section 7.34 of appendix 7I, whether there are other amazing identities for sums of different powers, like

$$\sum_{n=1}^{N-1} n^3 = \left(\sum_{n=1}^{N-1} n\right)^2.$$

0.3. The binomial theorem, Pascal's triangle, and the binomial coefficients

The *binomial coefficient* $\binom{n}{m}$ is defined to be the number of different ways of choosing m objects from n. (Therefore $\binom{n}{m} = 0$ whenever $m < 0$ or $m > n$.) From this definition we see that the binomial coefficients are all integers. To determine $\binom{5}{2}$ we note that there are 5 choices for the first object and 4 for the second, but then we have counted each pair of objects twice (since we can select them in either order), and so $\binom{5}{2} = \frac{5\times 4}{2}$. It is arguably nicer to write 5×4 as $\frac{5\times4\times3\times2\times1}{3\times2\times1} = \frac{5!}{3!}$ so that $\binom{5}{2} = \frac{5!}{3!2!}$. One can develop this proof to show that, for any integers $0 \leq m \leq n$, one has the very neat formula[5]

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}, \text{ where } r! = r \cdot (r-1) \cdots 2 \cdot 1. \tag{0.3.1}$$

From this formula alone it is not obvious that the binomial coefficients are integers.

Exercise 0.3.1. (a) Prove that $\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}$ for all integers m, and all integers $n \geq 0$.
(b) Deduce from (a) that each $\binom{n}{m}$ is an integer.

[5] We prefer to work with the closed formula 27!/(15!12!) rather than to evaluate it as 17383860, since the three factorials are easier to appreciate and to manipulate in subsequent calculations, particularly when looking for patterns.

Pascal's triangle is a triangular array in which the $(n+1)$st row contains the binomial coefficients $\binom{n}{m}$, with m increasing from 0 to n, as one goes from left to right:

$$\begin{array}{c} 1 \\ 1\ \ 1 \\ 1\ \ 2\ \ 1 \\ 1\ \ 3\ \ 3\ \ 1 \\ 1\ \ 4\ \ 6\ \ 4\ \ 1 \\ 1\ \ 5\ \ 10\ \ 10\ \ 5\ \ 1 \\ 1\ \ 6\ \ 15\ \ 20\ \ 15\ \ 6\ \ 1 \\ \ldots \text{ etc.} \end{array}$$

The addition formula in exercise 0.3.1(a) yields a rule for obtaining a row from the previous one, by adding any two neighboring entries to give the entry immediately below. For example the third entry in the bottom row is immediately below 5 and 10 (to either side) and so equals $5 + 10 = 15$. The next entry is $10 + 10 = 20$, etc.

The *binomial theorem* states that if n is an integer ≥ 1, then

$$\boxed{(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^{n-m} y^m.}$$

Exercise 0.3.2.† Using exercise 0.3.1(a) and induction on $n \geq 1$, prove the binomial theorem.

Notice that one can read off the coefficients of $(x+y)^n$ from the $(n+1)$st row of Pascal's triangle; for example, reading off the bottom row above (which is the 7th row down of Pascal's triangle), we obtain

$$(x+y)^6 = x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6.$$

In the previous section we raised the question of finding a closed formula for the sum of n^k, over all positive integers $n < N$. We can make headway in a related question in which we replace n^k with a different polynomial in n of degree k, namely the binomial coefficient

$$\binom{n}{k} \;=\; \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

This is a polynomial of degree k in n. For example, we have $\binom{n}{3} = \frac{n^3}{6} - \frac{n^2}{2} + \frac{n}{3}$, a polynomial in n of degree 3. We can identify a closed formula for the sum of these binomial coefficients, over all positive integers $n < N$, namely:

$$\sum_{n=0}^{N-1} \binom{n}{k} \;=\; \binom{N}{k+1} \tag{0.3.2}$$

for all N and $k \geq 0$. For $k = 2, N = 6$, this can be seen in the following diagram:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & (1) & & 2 & & 1 & & & \\
 & & 1 & & (3) & & 3 & & 1 & & \\
 & 1 & & 4 & & (6) & & 4 & & 1 & \\
1 & & 5 & & 10 & & (10) & & 5 & & 1 \\
 & 1 & & 6 & & 15 & & \mathbf{(20)} & & 15 & & 6 & & 1
\end{array}$$

so that $1 + 3 + 6 + 10$ equals 20.

Exercise 0.3.3. Prove (0.3.2) for each fixed $k \geq 1$, for each $N \geq k + 1$, using induction and exercise 0.3.1. You might also try to prove it by induction using the idea behind the illustration in the last diagram.

If we instead display Pascal's triangle by lining up the initial 1's and then summing the diagonals,

$$\begin{array}{ccccccc}
1 & & & & & & \\
1 & & 1 & & & & \\
1 & & 2 & & 1 & & \\
1 & & 3 & & 3 & & (1) \\
1 & & 4 & & (6) & & 4 & & 1 \\
1 & & (5) & & 10 & & 10 & & \dots \\
(1) & & 6 & & 15 & & \dots
\end{array}$$

the sums are $1, 1, 1 + 1, 1 + 2, 1 + 3 + 1, 1 + 4 + 3, 1 + 5 + 6 + 1, \dots$ which equal $1, 1, 2, 3, 5, 8, 13, \dots$, the Fibonacci numbers. It therefore seems likely that

$$F_n = \sum_{k=0}^{n-1} \binom{n-1-k}{k} \text{ for all } n \geq 1. \tag{0.3.3}$$

Exercise 0.3.4. Prove (0.3.3) for each integer $n \geq 1$, by induction using exercise 0.3.1(a).

Articles with further thoughts on factorials and binomial coefficients

[1] Manjul Bhargava, *The factorial function and generalizations*, Amer. Math. Monthly **107** (2000), 783–799 (preprint).

[2] John J. Watkins, chapter 5 of *Number theory. A historical approach*, Princeton University Press, 2014.

Additional exercises

Exercise 0.4.1. (a) Prove that for all $n \geq 1$ we have

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

(b) Deduce that $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ for all $n \geq 1$.
(c) Deduce that $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ for all $n \geq 0$.

Exercise 0.4.2.† Deduce from (0.1.1) that the Fibonacci number F_n is the nearest integer to $\phi^n/\sqrt{5}$, for each integer $n \geq 0$, where the constant $\phi := \frac{1+\sqrt{5}}{2}$. This *golden ratio* appears in art and architecture when attempting to describe "perfect proportions".

Exercise 0.4.3. Prove that $F_n^2 + F_{n+3}^2 = 2(F_{n+1}^2 + F_{n+2}^2)$ for all $n \geq 0$.

Exercise 0.4.4. Prove that for all $n \geq 1$ we have

$$F_{2n-1} = F_{n-1}^2 + F_n^2 \quad \text{and} \quad F_{2n} = F_{n+1}^2 - F_{n-1}^2.$$

Exercise 0.4.5. Use (0.1.1) to prove the following:
(a) For every r we have $F_n^2 - F_{n+r}F_{n-r} = (-1)^{n-r}F_r^2$ for all $n \geq r$.
(b) For all $m \geq n \geq 0$ we have $F_mF_{n+1} - F_{m+1}F_n = (-1)^nF_{m-n}$.

Exercise 0.4.6. Let $u_0 = b$ and $u_{n+1} = au_n$ for all $n \geq 0$. Give a formula for all u_n with $n \geq 0$.

The expression 011010 is a *string of* 0*'s and* 1*'s*. There are 2^n strings of 0's and 1's of length n as there are two possibilities for each entry. Let A_n be the set of strings of 0's and 1's of length n which contain no two consecutive 1's. Our example 011010 does not belong to A_6 as the second and third characters are consecutive 1's, whereas 01001010 is in A_8. Calculations reveal that $|A_1| = 2$, $|A_2| = 3$, and $|A_3| = 5$, data which suggests that perhaps $|A_n| = F_{n+2}$, the Fibonacci number.

Exercise 0.4.7.† (a) If $0w$ is a string of 0's and 1's of length n, prove that $0w \in A_n$ if and only if $w \in A_{n-1}$.
(b) If $10w$ is a string of 0's and 1's of length n, prove that $10w \in A_n$ if and only if $w \in A_{n-2}$.
(c) Prove that $|A_n| = F_{n+2}$ for all $n \geq 1$, by induction on n.

Exercise 0.4.8.† Prove that every positive integer other than the powers of 2 can be written as the sum of two or more consecutive integers.

Exercise 0.4.9. Prove that $\binom{n}{m}\binom{n-m}{a-m} = \binom{a}{m}\binom{n}{a}$ for any integers $n \geq a \geq m \geq 0$.

Exercise 0.4.10.† Suppose that a and b are integers and $\{x_n : n \geq 0\}$ is the second-order linear recurrence sequence given by (0.1.2) with $x_0 = 0$ and $x_1 = 1$.
(a) Prove that for all non-negative integers m we have

$$x_{m+k} = x_{m+1}x_k + bx_mx_{k-1} \text{ for all integers } k \geq 1.$$

(b) Deduce that

$$x_{2n+1} = x_{n+1}^2 + bx_n^2 \quad \text{and} \quad x_{2n} = x_{n+1}x_n + bx_nx_{n-1} \quad \text{for all natural numbers } n.$$

Exercise 0.4.11. Suppose that the sequences $\{x_n : n \geq 0\}$ and $\{y_n : n \geq 0\}$ both satisfy (0.1.2) and that $x_0 = 0$ and $x_1 = 1$, whereas y_0 and y_1 might be anything. Prove that

$$y_n = y_1x_n + by_0x_{n-1} \text{ for all } n \geq 1.$$

Exercise 0.4.12. Suppose that $x_0 = 0$, $x_1 = 1$, and $x_{n+2} = ax_{n+1} + bx_n$. Prove that for all $n \geq 1$ we have
(a) $(a + b - 1)\sum_{j=1}^{n} x_j = x_{n+1} + bx_n - 1$;
(b) $a(b^nx_0^2 + b^{n-1}x_1^2 + \cdots + bx_{n-1}^2 + x_n^2) = x_nx_{n+1}$;
(c) $x_n^2 - x_{n-1}x_{n+1} = (-b)^{n-1}$.

Exercise 0.4.13. Suppose that $x_{n+2} = ax_{n+1} + bx_n$ for all $n \geq 0$.
(a) Show that

$$\begin{pmatrix} x_{n+2} & x_{n+1} \\ x_{n+1} & x_n \end{pmatrix} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} x_2 & x_1 \\ x_1 & x_0 \end{pmatrix} \text{ for all } n \geq 0.$$

(b) Deduce that $x_{n+2}x_n - x_{n+1}^2 = c(-b)^n$ for all $n \geq 0$ where $c := x_2x_0 - x_1^2$.
(c) Deduce that $x_{n+1}^2 - ax_{n+1}x_n - bx_n^2 = -c(-b)^n$.

Other number-theoretic sequences can be obtained from linear recurrences or other types of recurrences. Besides the Fibonacci numbers, there is another sequence of integers that is traditionally denoted by $(F_n)_{n\geq 0}$: These are the *Fermat numbers*, $F_n = 2^{2^n} + 1$ for all $n \geq 0$ (see sections 3.11 of appendix 3A, 5.1, 5.25 of appendix 5H, etc.).

Exercise 0.4.14. Show that if $F_0 = 3$ and $F_{n+1} = F_n^2 - 2F_n + 2$, then $F_n = 2^{2^n} + 1$ for all $n \geq 0$.

Exercise 0.4.15. (a) Show that if $M_0 = 0$, $M_1 = 1$, and $M_{n+2} = 3M_{n+1} - 2M_n$ for all integers $n \geq 0$, then $M_n = 2^n - 1$ for all integers $n \geq 0$. The integer M_n is the nth *Mersenne number* (see exercise 2.5.16 and sections 4.2, 5.1, etc.).

(b) Show that if $M_0 = 0$ with $M_{n+1} = 2M_n + 1$ for all $n \geq 0$, then $M_n = 2^n - 1$.

Exercise 0.4.16.‡ We can reinterpret exercise 0.4.3 as giving a recurrence relation for the sequence $\{F_n^2\}_{n\geq 0}$, where F_n is the nth Fibonacci number; that is,

$$F_{n+3}^2 = 2F_{n+2}^2 + 2F_{n+1}^2 - F_n^2 \text{ for all } n \geq 0.$$

Here F_{n+3}^2 is described in terms of the last three terms of the sequence; this is called a *linear recurrence of order* 3. Prove that for any integer $k \geq 1$, the sequence $\{F_n^k\}_{n\geq 0}$ satisfies a linear recurrence of order $k + 1$.

How to proceed through this book. It can be challenging to decide what proof technique to try on a given question. There is no simple guide—practice is what best helps decide how to proceed. Some students find Zeitz's book [**Zei17**] helpful as it exhibits all of the important techniques in context. I like Conway and Guy's [**CG96**] since it has lots of great questions, beautifully discussed with great illustrations, and introduces quite a few of the topics from this book.

A paper that questions one's assumptions is

[1] Richard K. Guy *The strong law of small numbers*, Amer. Math. Monthly, **95** (1988), 697–712.

Appendices. The short version of this book will offer an appendix at the end of most chapters. Sometimes this will add a little more insight or will present a proof that is a little more difficult than what is normal for this course. The long version of the book will include many appendices after each chapter, highlighting directions one might use to develop the material for that chapter. For example, the extended version of chapter 0 contains the following appendices:

Appendix 0A. *A closed formula for sums of powers* develops the ideas of section 0.2 to obtain a closed formula for the sum of n^k for all positive integers $n < N$.

Appendix 0B. *Generating functions*, which gives a more elegant proof of the closed formula for sums of kth powers using Bernoulli numbers and then discusses the generating function for Fibonacci numbers and other recurrence sequences.

Appendix 0C. *Finding roots of polynomials* shows how to determine the roots of cubic and quartic polynomials and discusses surds.

Appendix 0D. *What is a group?* introduces the notion of a group and looks in detail at the commutativity of 2-by-2 matrices.

Appendix 0E. *Rings and fields* explains the point of developing these notions in number-theoretic settings and goes on to define and study algebraic numbers.

Appendix 0F. *Symmetric polynomials* explains and sketches the proof of Newton's *fundamental theorem of symmetric polynomials*, which is the elementary way mathematicians used to obtain information about properties of fixed fields before Galois invented Galois theory! It allows one to further develop algebraic numbers and number fields.

Appendix 0G. *Constructibility* introduces the ancient Greek questions of drawing a square that has area equal to that of a given circle, constructing a cube that has twice the volume of a given cube, and constructing an angle which is one third the size of a given angle, explaining what these questions have to do with constructing number fields.

The Euclidean algorithm

1.1. Finding the gcd

Most readers will know the Euclidean algorithm, used to find the greatest common divisor (gcd) of two given integers. For example, to determine the greatest common divisor of 85 and 48, we begin by subtracting the smaller from the larger, 48 from 85, to obtain $85 - 48 = 37$. Now $\gcd(85, 48) = \gcd(48, 37)$, because the common divisors of 48 and 37 are precisely the same as those of 85 and 48, and so we apply the algorithm again to the pair 48 and 37. So we subtract the smaller from the larger to obtain $48 - 37 = 11$, so that $\gcd(48, 37) = \gcd(37, 11)$. Next we should subtract 11 from 37, but then we would only do so again, and a third time, so let's do all that in one go and take $37 - 3 \times 11 = 4$, to obtain $\gcd(37, 11) = \gcd(11, 4)$. Similarly we take $11 - 2 \times 4 = 3$, and then $4 - 3 = 1$, so that the gcd of 85 and 48 is 1. This is the Euclidean algorithm that you might already have seen,[1] but did you ever prove that it really works?

To do so, we will first carefully define terms that we have implicitly used in the above paragraph, perhaps mathematical terms that you have used for years (such as "divides", "quotient", and "remainder") without a formal definition. This may seem pedantic but the goal is to make sure that the rules of basic arithmetic are really established on a sound footing.

Let a and b be given integers. We say that a *is divisible by* b, or that b divides a,[2] if there exists an integer q such that $a = qb$. For convenience we write "$b \mid a$".[3,4] We now set an exercise for the reader to check that the definition allows one to manipulate the notion of division in several familiar ways.

Exercise 1.1.1. In this question, and throughout, we assume that a, b, and c are integers.
(a) Prove that if b divides a, then either $a = 0$ or $|a| \geq |b|$.

[1] There will be a formal discussion of the Euclidean algorithm in appendix 1A.
[2] One can also say a *is a multiple of* b or b *is a divisor of* a or b *is a factor of* a.
[3] And if b does not divide a, we write "$b \nmid a$".
[4] One reason for giving a precise mathematical definition for division is that it allows us to better decide how to interpret questions like, "What is 1 divided by 0?" or "What is 0 divided by 0?"

(b) Deduce that if $a|b$ and $b|a$, then $b = a$ or $b = -a$ (which, in future, we will write as "$b = \pm a$").
(c) Prove that if a divides b and c, then a divides $bx + cy$ for all integers x, y.
(d) Prove that a divides b if and only if a divides $-b$ if and only if $-a$ divides b.
(e) Prove that if a divides b, and b divides c, then a divides c.
(f) Prove that if $a \neq 0$ and ac divides ab, then c divides b.

Next we formalize the notion of "dividing with remainder".

Lemma 1.1.1. *If a and b are integers, with $b \geq 1$, then there exist unique integers q and r, with $0 \leq r \leq b-1$, such that $a = qb + r$. We call q the "*quotient*", and r the "*remainder*".*

Proof by induction. We begin by proving the existence of q and r. For each $b \geq 1$, we proceed by induction on $a \geq 0$. If $0 \leq a \leq b-1$, then the result follows with $q = 0$ and $r = a$. Otherwise assume that the result holds for $0, 1, 2, \ldots, a-1$, where $a \geq b$. Then $a - 1 \geq a - b \geq 0$ so, by the induction hypothesis, there exist integers Q and r, with $0 \leq r \leq b-1$, for which $a - b = Qb + r$. Therefore $a = qb + r$ with $q = Q + 1$.

If $a < 0$, then $-a > 0$ so we have $-a = Qb + R$, for some integers Q and R, with $0 \leq R \leq b-1$, by the previous paragraph. If $R = 0$, then $a = qb$ where $q = -Q$ (and $r = 0$). Otherwise $1 \leq R \leq b-1$ and so $a = qb + r$ with $q = -Q - 1$ and $1 \leq r = b - R \leq b - 1$, as required.

Now we show that q and r are unique. If $a = qb + r = Qb + R$, then b divides $(q - Q)b = R - r$. However $0 \leq r, R \leq b-1$ so that $|R - r| \leq b-1$, and $b \mid R - r$. Therefore $R - r = 0$ by exercise 1.1.1(a), and so $Q - q = 0$. In other words $q = Q$ and $r = R$; that is, the pair q, r is unique. □

An easier, but less intuitive, proof. We can add a multiple of b to a to get a positive integer. That is, there exists an integer n such that $a + nb \geq 0$; any integer $n \geq -a/b$ will do. We now subtract multiples of b from this number, as long as it remains positive, until subtracting b once more would make it negative. In other words we now have an integer $a - qb \geq 0$, which we denote by r, such that $r - b < 0$; in other words $0 \leq r \leq b - 1$. □

Exercise 1.1.2. Suppose that $a \geq 1$ and $b \geq 2$ are integers. Show that we can write a in base b; that is, show that there exist integers $a_0, a_1, \ldots \in [0, b-1]$ for which $a = a_d b^d + a_{d-1} b^{d-1} + a_1 b + a_0$.

We say that d is a *common divisor* of integers a and b if d divides both a and b. We are mostly interested in the *greatest common divisor* of a and b, which we denote by $\gcd(a, b)$, or more simply as (a, b).[5,6]

We say that a is *coprime* with b, or that a and b are *coprime integers*, or that a and b are *relatively prime*, if $(a, b) = 1$.

[5] In the UK this is known as the *highest common factor* of a and b and is written $\mathrm{hcf}(a, b)$.

[6] When $a = b = 0$, every integer is a divisor of 0, so there is no greatest divisor, and therefore $\gcd(0, 0)$ is undefined. There are often one or two cases in which a generally useful mathematical definition does not give a unique value. Another example is 0 divided by 0, which we explore in exercise 1.7.1. For aesthetic reasons, some authors choose to assign a value which is consistent with the theory in one situation but perhaps not in another. This can lead to artificial inconsistencies which is why we choose to leave such function-values undefined.

Corollary 1.1.1. *If $a = qb + r$ where a, b, q, and r are integers, then*

$$\gcd(a, b) = \gcd(b, r).$$

Proof. Let $g = \gcd(a, b)$ and $h = \gcd(r, b)$. Now g divides both a and b, so g divides $a - qb = r$ (by exercise 1.1.1(c)). Therefore g is a common divisor of both r and b, and therefore $g \leq h$. Similarly h divides both b and r, so h divides $qb + r = a$ and hence h is a common divisor of both a and b, and therefore $h \leq g$. We have shown that $g \leq h$ and $h \leq g$, which together imply that $g = h$. □

Corollary 1.1.1 justifies the method used to determine the gcd of 85 and 48 in the first paragraph of section 1.1 and indeed in general:

Exercise 1.1.3. Use Corollary 1.1.1 to prove that the Euclidean algorithm indeed yields the greatest common divisor of two given integers. (You might prove this by induction on the smallest of the two integers.)

Exercise 1.1.4. Prove that $(F_n, F_{n+1}) = 1$ by induction on $n \geq 0$.

1.2. Linear combinations

The Euclidean algorithm can also be used to determine a linear combination[7] of a and b, over the integers, which equals $\gcd(a, b)$; that is, one can always use the Euclidean algorithm to find integers u and v such that

$$au + bv = \gcd(a, b). \tag{1.2.1}$$

Let us see how to do this in an example, by finding integers u and v such that $85u + 48v = 1$; remember that we found the gcd of 85 and 48 at the beginning of section 1.1. We retrace the steps of the Euclidean algorithm, but in reverse: The final step was that $1 = 1 \cdot 4 - 1 \cdot 3$, a linear combination of 4 and 3. The second to last step used that $3 = 11 - 2 \cdot 4$, and so substituting $11 - 2 \cdot 4$ for 3 in $1 = 1 \cdot 4 - 1 \cdot 3$, we obtain

$$1 = 1 \cdot 4 - 1 \cdot 3 = 1 \cdot 4 - 1 \cdot (11 - 2 \cdot 4) = 3 \cdot 4 - 1 \cdot 11,$$

a linear combination of 11 and 4. This then implies, since we had $4 = 37 - 3 \cdot 11$, that

$$1 = 3 \cdot (37 - 3 \cdot 11) - 1 \cdot 11 = 3 \cdot 37 - 10 \cdot 11,$$

a linear combination of 37 and 11. Continuing in this way, we successively deduce, using that $11 = 48 - 37$ and then that $37 = 85 - 48$,

$$\begin{aligned} 1 = \ & 3 \cdot 37 - 10 \cdot (48 - 37) \ = 13 \cdot 37 - 10 \cdot 48 \\ = \ & 13 \cdot (85 - 48) - 10 \cdot 48 \ = 13 \cdot 85 - 23 \cdot 48; \end{aligned}$$

that is, we have the desired linear combination of 85 and 48.

To prove that this method always works, we will use Lemma 1.1.1 again: Suppose that $a = qb + r$ so that $\gcd(a, b) = \gcd(b, r)$ by Corollary 1.1.1, and that we have $bu - rv = \gcd(b, r)$ for some integers u and v. Then

$$\gcd(a, b) = \gcd(b, r) = bu - rv = bu - (a - qb)v = b(u + qv) - av, \tag{1.2.2}$$

[7] A *linear combination* of two given integers a and b, over the integers, is a number of the form $ax + by$ where x and y are integers. This can be generalized to yield a linear combination $a_1x_1 + \cdots + a_nx_n$ of any finite set of integers, $a_1, \ldots, a_n$. Linear combinations are a key concept in linear algebra and appear (without necessarily being called that) in many courses.

the desired linear combination of a and b. This argument forms the basis of our proof of (1.2.1), but to give a complete proof we proceed by induction on the smaller of a and b:

Theorem 1.1. *If a and b are positive integers, then there exist integers u and v such that*

$$au + bv = \gcd(a, b).$$

Proof. Interchanging a and b if necessary we may assume that $a \geq b \geq 1$. We shall prove the result by induction on b. If $b = 1$, then b only has the divisor 1, so that

$$\gcd(a, 1) = 1 = 0 \cdot a + 1 \cdot 1.$$

We now prove the result for $b > 1$: If b divides a, then

$$\gcd(b, a) = b = 0 \cdot a + 1 \cdot b.$$

Otherwise b does not divide a and so Lemma 1.1.1 implies that there exist integers q and r such that $a = qb + r$ and $1 \leq r \leq b - 1$. Since $1 \leq r < b$ we know, by the induction hypothesis, that there exist integers u and v for which $bu - rv = \gcd(b, r)$. The result then follows by (1.2.2). □

We now establish various useful properties of the gcd:

Exercise 1.2.1. (a) Prove that if d divides both a and b, then d divides $\gcd(a, b)$.
(b) Deduce that d divides both a and b *if and only if* d divides $\gcd(a, b)$.
(c) Prove that $1 \leq \gcd(a, b) \leq |a|$ and $|b|$.
(d) Prove that $\gcd(a, b) = |a|$ if and only if a divides b.

Exercise 1.2.2. Suppose that a divides m, and b divides n.
(a) Deduce that $\gcd(a, b)$ divides $\gcd(m, n)$.
(b) Deduce that if $\gcd(m, n) = 1$, then $\gcd(a, b) = 1$.

Exercise 1.2.3. Show that Theorem 1.1 holds for any integers a and b that are not both 0. (It is currently stated and proved only for positive integers a and b.)

Corollary 1.2.1. *If a and b are integers for which $\gcd(a, b) = 1$, then there exist integers u and v such that*

$$au + bv = 1.$$

This is one of the most useful results in mathematics and has applications in many areas, including in safeguarding today's global communications. For example, we will see in section 10.3 that to implement RSA, a key cryptographic protocol that helps keep important messages safe in our electronic world, one uses Corollary 1.2.1 in an essential way. More on that later, after developing more basic number theory.

Exercise 1.2.4. (a) Use exercise 1.1.1(c) to show that if $au + bv = 1$, then $(a, b) = (u, v) = 1$.
(b) Prove that $\gcd(u, v) = 1$ in Theorem 1.1.

Corollary 1.2.2. *If $\gcd(a, m) = \gcd(b, m) = 1$, then $\gcd(ab, m) = 1$.*

Proof. By Theorem 1.1 there exist integers r, s, u, v such that

$$au + mv = br + ms = 1.$$

Therefore

$$ab(ur) + m(bvr + aus + msv) = (au + mv)(br + ms) = 1,$$

and the result follows from exercise 1.2.4(a). □

Corollary 1.2.3. *We have* $\gcd(ma, mb) = m \cdot \gcd(a, b)$ *for all integers* $m \geq 1$.

Proof. By Theorem 1.1 there exist integers u, v such that $au+bv = \gcd(a, b)$. Now $\gcd(ma, mb)$ divides ma and mb so it divides $mau + mbv = m \cdot \gcd(a, b)$. Similarly $\gcd(a, b)$ divides a and b, so that $m \cdot \gcd(a, b)$ divides ma and mb, and therefore $\gcd(ma, mb)$ by exercise 1.2.1(a). The result follows from exercise 1.1.1(b), since the gcd is always positive. □

Exercise 1.2.5. (a) Show that if A and B are given integers, not both 0, with $g = \gcd(A, B)$, then $\gcd(A/g, B/g) = 1$.

(b) Prove that any rational number u/v where $u, v \in \mathbb{Z}$ with $v \neq 0$ may be written as r/s where r and s are coprime integers with $s > 0$. This is called a *reduced fraction*.

1.3. The set of linear combinations of two integers

Theorem 1.1 states that the greatest common divisor of two integers is a linear combination of those two integers. This suggests that it might be useful to study *the set of linear combinations*

$$I(a, b) := \{am + bn : \ m, n \in \mathbb{Z}\}$$

of two given integers a and b.[8] We see that $I(a, b)$ contains $0,\ a,\ b,\ a + b,\ a + 2b,\ 2b + a,\ a - b,\ b - a, \ldots$ and any sum of integer multiples of a and b, so that $I(a, b)$ is closed under addition. Let $I(a) := I(a, 0) = \{am : \ m \in \mathbb{Z}\}$, the set of integer multiples of a. We now prove that $I(a, b)$ can be described as the set of integer multiples of $\gcd(a, b)$, a set which is easier to understand:

Corollary 1.3.1. *For any given non-zero integers* a *and* b*, we have*

$$\{am + bn : \ m, n \in \mathbb{Z}\} = \{gk : \ k \in \mathbb{Z}\}$$

where $g := \gcd(a, b)$*; that is,* $I(a, b) = I(g)$*. In other words, there exist integers* m *and* n *with* $am + bn = c$ *if and only if* $\gcd(a, b)$ *divides* c*.*

Proof. By Theorem 1.1 we know that there exist $u, v \in \mathbb{Z}$ for which $au + bv = g$. Therefore $a(uk)+b(vk) = gk$ so that $gk \in I(a, b)$ for all $k \in \mathbb{Z}$; that is, $I(g) \subset I(a, b)$. On the other hand, as g divides both a and b, there exist integers A, B such that $a = gA$, $b = gB$, and so any $am+bn = g(Am+Bn) \in I(g)$. That is, $I(a, b) \subset I(g)$. The result now follows from the two inclusions. □

It is instructive to see how this result follows directly from the Euclidean algorithm: In our example, we are interested in $\gcd(85, 48)$, so we will study $I(85, 48)$, that is, the set of integers of the form

$$85m + 48n.$$

[8] This is usually called the *ideal* generated by a and b in $\mathbb{Z}$ and denoted by $\langle a, b\rangle_{\mathbb{Z}}$. The notion of an ideal is one of the basic tools of modern algebra, as we will discuss in appendix 3D.

The first step in the Euclidean algorithm was to write $85 = 1 \cdot 48 + 37$. Substituting this in above yields

$$85m + 48n = (1 \cdot 48 + 37)m + 48n = 48(m + n) + 37m,$$

and so $I(85, 48) \subset I(48, 37)$. In the other direction, any integer in $I(48, 37)$ can be written as

$$48a + 37b = 48a + (85 - 48)b = 85b + 48(a - b),$$

and so belongs to $I(85, 48)$. Combining these last two statements yields that

$$I(85, 48) = I(48, 37).$$

Each step of the Euclidean algorithm leads to a similar equality, and so we get

$$I(85, 48) = I(48, 37) = I(37, 11) = I(11, 4) = I(4, 3) = I(3, 1) = I(1, 0) = I(1).$$

To truly justify this we need to establish an analogous result to Corollary 1.1.1:

Lemma 1.3.1. *If $a = qb+r$ where a, b, q, and r are integers, then $I(a, b) = I(b, r)$.*

Proof. We begin by noting that

$$am + bn = (qb + r)m + bn = b(qm + n) + rm$$

so that $I(a, b) \subset I(b, r)$. In the other direction

$$bu + rv = bu + (a - qb)v = av + b(u - qv)$$

so that $I(b, r) \subset I(a, b)$. The result follows by combining the two inclusions. □

We have used the Euclidean algorithm to find the gcd of any two given integers a and b, as well as to determine integers u and v for which $au + bv = \gcd(a, b)$. The price for obtaining the actual values of u and v, rather than merely proving the existence of u and v (which is all that was claimed in Theorem 1.1), was our somewhat complicated analysis of the Euclidean algorithm. However, if we *only wish to prove* that such integers *u and v exist*, then we can do so with a somewhat easier proof: [9]

Non-constructive proof of Theorem 1.1. Let h be the smallest positive integer that belongs to $I(a, b)$, say $h = au + bv$. Then $g := \gcd(a, b)$ divides h, as g divides both a and b.

Now $a = a \cdot 1 + b \cdot 0$ so that $a \in I(a, b)$, and $1 \le h \le a$ by the definition of h. Therefore Lemma 1.1.1 implies that there exist integers q and r, with $0 \le r \le h-1$, for which $a = qh + r$. Therefore

$$r = a - qh = a - q(au + bv) = a(1 - qu) + b(-qv) \in I(a, b),$$

which contradicts the minimality of h, unless $r = 0$; that is, h divides a. An analogous argument reveals that h divides b, and so h divides g by exercise 1.2.1(a).

[9] We will now prove the *existence* of u and v by showing that their non-existence would lead to a contradiction. We will develop other instances, as we proceed, of both constructive and non-constructive proofs of important theorems.

Which type of proof is preferable? This is somewhat a matter of taste. The non-constructive proof is often shorter and more elegant. The constructive proof, on the other hand, is practical—that is, it *gives* solutions. It is also "richer" in that it develops more than is (immediately) needed, though some might say that these extras are irrelevant.

Which type of proof has the greatest clarity? That depends on the *algorithm* devised for the constructive proof. A compact algorithm will often cast light on the subject. But a cumbersome one may obscure it. In this case, the Euclidean algorithm is remarkably simple and efficient ([**Sha85**, p. 11]).

Hence g divides h, and h divides g, and g and h are both positive, so that $g = h$ as desired. □

We say that the integers a, b, and c are *relatively prime* if $\gcd(a, b, c) = 1$. We say that they are *pairwise coprime* if $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$. For example, $6, 10, 15$ are relatively prime, but they are not pairwise coprime (since each pair of integers has a common factor > 1).

Exercise 1.3.1. Suppose that a, b, and c are non-zero integers for which $a + b = c$.
(a) Show that a, b, c are relatively prime if and only if they are pairwise coprime.
(b) Show that $(a, b) = (a, c) = (b, c)$.
(c) Show that the analogy to (a) is false for integer solutions a, b, c, d to $a + b = c + d$ (perhaps by constructing a counterexample).

1.4. The least common multiple

The *least common multiple*[10] of two given integers a and b is defined to be the smallest positive integer that is a multiple of both a and b. We denote this by $\operatorname{lcm}[a, b]$ (or simply $[a, b]$). We now prove the counterpart to exercise 1.2.1(a):

Lemma 1.4.1. $\operatorname{lcm}[a, b]$ *divides integer* m *if and only if* a *and* b *both divide* m.

Proof. Since a and b divide $\operatorname{lcm}[a, b]$, if $\operatorname{lcm}[a, b]$ divides m, then a and b both divide m, by exercise 1.1.1(e).

On the other hand suppose a and b both divide m, and write $m = q \operatorname{lcm}[a, b] + r$ where $0 \le r < \operatorname{lcm}[a, b]$. Now a and b both divide m and $\operatorname{lcm}[a, b]$ so they both divide $m - q \operatorname{lcm}[a, b] = r$. However $\operatorname{lcm}[a, b]$ is defined to be the smallest positive integer that is divisible by both a and b, which implies that r must be 0. Therefore $\operatorname{lcm}[a, b]$ divides m. □

The analogies to exercise 1.2.1(d) and Corollary 1.2.3 for lcms are given by the following two exercises:

Exercise 1.4.1. Prove that $\operatorname{lcm}[m, n] = n$ if and only if m divides n.

Exercise 1.4.2. Prove that $\operatorname{lcm}[ma, mb] = m \cdot \operatorname{lcm}[a, b]$ for any positive integer m.

1.5. *Continued fractions*

Another way to write Lemma 1.1.1 is that for any given integers $a \ge b \ge 1$ with $b \nmid a$, there exist integers q and r, with $b > r \ge 1$, for which

$$\frac{a}{b} \;=\; q + \frac{r}{b} \;=\; q + \frac{1}{\frac{b}{r}}.$$

This is admittedly a strange way to write things, but repeating this process with the pair of integers b and r, and then again, will eventually lead us to an interesting representation of the original fraction a/b. Working with our original example, in which we found the gcd of 85 and 48, we can represent $85 = 48 + 37$ as

$$\frac{85}{48} = 1 + \frac{1}{\frac{48}{37}},$$

[10] Sometimes called the *lowest common multiple*.

and the next step, $48 = 37 + 11$, as

$$\frac{48}{37} = 1 + \frac{1}{\frac{37}{11}}, \text{ so that } \frac{85}{48} = 1 + \frac{1}{\frac{48}{37}} = 1 + \frac{1}{1 + \frac{1}{\frac{37}{11}}}.$$

The remaining steps of the Euclidean algorithm may be rewritten as

$$\frac{37}{11} = 3 + \frac{1}{\frac{11}{4}}, \quad \frac{11}{4} = 2 + \frac{1}{\frac{4}{3}}, \quad \text{and} \quad \frac{4}{3} = 1 + \frac{1}{3},$$

so that

$$\frac{85}{48} = 1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3}}}}}.$$

This is the *continued fraction* for $\frac{85}{48}$ and is conveniently written as $[1, 1, 3, 2, 1, 3]$. Notice that this is the sequence of quotients a_i from the various divisions; that is,

$$\frac{a}{b} \;=\; [a_0,\ a_1,\ a_2,\ \ldots,\ a_k] := \; a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots + \frac{1}{a_k}}}}.$$

The a_i's are called the *partial quotients* of the continued fraction.

Exercise 1.5.1. (a) Show that if $a_k > 1$, then $[a_0,\ a_1, \ldots,\ a_k] = [a_0,\ a_1, \ldots,\ a_k - 1, 1]$.
(b) Prove that the set of positive rational numbers are in 1-1 correspondence with the finite length continued fractions that do not end in 1.

We now list the rationals that correspond to the first few entries in our continued fraction $[1, 1, 3, 2, 1, 3]$. We have $[1] = 1, [1, 1] = 2$, and

$$1 + \frac{1}{1 + \frac{1}{3}} = \frac{7}{4}, \qquad 1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{2}}} = \frac{16}{9}, \qquad 1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{2 + \frac{1}{1}}}} = \frac{23}{13}.$$

These yield increasingly good approximations to $85/48 = 1.770833\ldots$, that is, in decimal notation,

$$1,\ 2,\ 1.75,\ 1.777\ldots,\ 1.7692\ldots.$$

We call these p_j/q_j, $j \geq 1$, the *convergents* for the continued fraction, defined by

$$\frac{p_j}{q_j} = [a_0,\ a_1,\ a_2,\ \ldots,\ a_j],$$

since they converge to $a/b = p_k/q_k$ for some k. Do you notice anything surprising about the convergents for 85/48? In particular the previous one, namely 23/13? When we worked through the Euclidean algorithm we found that $13 \cdot 85 - 23 \cdot 48 = 1$ — could it be a coincidence that these same numbers show up again in this new context? In section 1.8 of appendix 1A we show that this is no coincidence; indeed we always have

$$p_j q_{j-1} - p_{j-1} q_j = (-1)^{j-1},$$

so, in general, if $u = (-1)^{k-1} q_{k-1}$ and $v = (-1)^k p_{k-1}$, then

$$au + bv = 1.$$

When one studies this in detail, one finds that the continued fraction is really just a convenient reworking of the Euclidean algorithm (as we explained it above)

for finding u and v. Bachet de Meziriac[11] introduced this method to Renaissance mathematicians in the second edition of his brilliantly named book *Pleasant and delectable problems which are made from numbers* (1624). Such methods had been known from ancient times, certainly to the Indian scholar Āryabhata in 499 A.D., probably to Archimedes in Syracuse (Greece) in 250 B.C., and possibly to the Babylonians as far back as 1700 B.C.[12]

1.6. *Tiling a rectangle with squares*[13]

Given a 48-by-85 rectangle we will tile it, greedily, with squares. The largest square that we can place inside a 48-by-85 rectangle is a 48-by-48 square. This 48-by-48 square goes from top to bottom of the rectangle, and if we place it at the far right, then we are left with a 37-by-48 rectangle to tile, on the left.

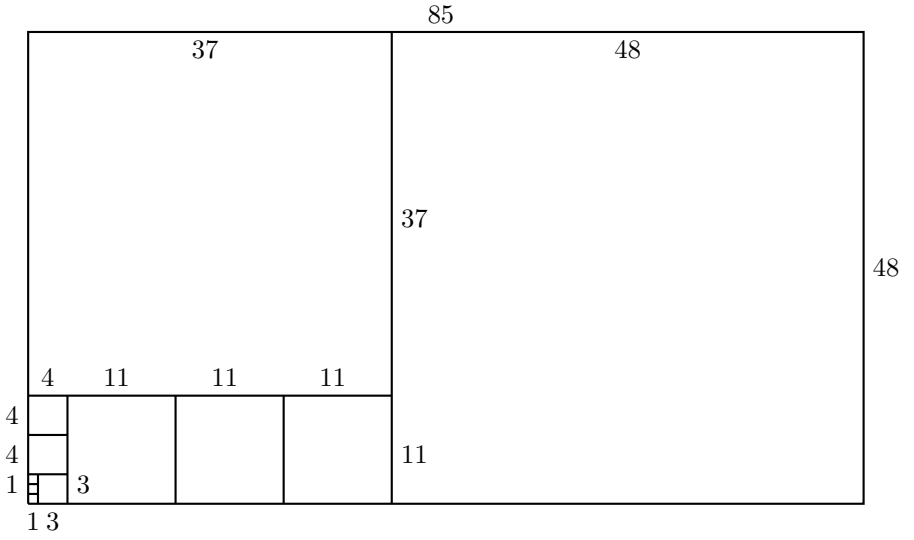


Figure 1.1. Partitioning a rectangle into squares, using the Euclidean algorithm.

If we place a 37-by-37 square at the top of this rectangle, then we are left with an 11-by-37 rectangle in the bottom left-hand corner. We can now place three 11-by-11 squares inside this, leaving a 4-by-11 rectangle. We finish this off with two 4-by-4 squares, one 3-by-3 square, and finally three 1-by-1 squares.

[11] The celebrated editor and commentator on Diophantus, whom we will meet again in chapter 6.

[12] There are Cuneiform clay tablets from this era that contain related calculations. It is known that after conquering Babylon in 331 B.C., Alexander the Great ordered his archivist Callisthenes and his tutor Aristotle to supervise the translation of the Babylonian astronomical records into Greek. It is therefore feasible that Archimedes was introduced to these ideas from this source. Indeed, Pythagoras's Theorem may be misnamed as the Babylonians knew of integer-sided right-angled triangles like $3, 4, 5$ and $5, 12, 13$ more than one thousand years before Pythagoras (570–495 B.C.) was born.

[13] Thanks to Dusa MacDuff and Dylan Thurston for bringing my attention to this beautiful application.

The area of the rectangle can be computed in terms of the areas of each of the squares; that is,

$$85 \cdot 48 = 1 \cdot 48^2 + 1 \cdot 37^2 + 3 \cdot 11^2 + 2 \cdot 4^2 + 1 \cdot 3^2 + 3 \cdot 1^2.$$

What has this to do with the Euclidean algorithm? Hopefully the reader has recognized the same sequence of numbers and quotients that appeared above, when we computed the $\gcd(85, 48)$. This is no coincidence. At a given step we have an a-by-b rectangle, with $a \geq b \geq 1$, and then we can remove q b-by-b squares, where $a = qb + r$ with $0 \leq r \leq a - 1$ leaving an r-by-b rectangle, and so proceed by induction.

Exercise 1.6.1. Given an a-by-b rectangle show how to write $a \cdot b$ as a sum of squares, as above, in terms of the partial quotients and convergents of the continued fraction for a/b.

Exercise 1.6.2. (a) Use this to show that $F_{n+1}F_n = F_n^2 + F_{n-1}^2 + \cdots + F_0^2$, where F_n is the nth Fibonacci number (see section 0.1 for the definition and a discussion of Fibonacci numbers and exercise 0.4.12(b) for a generalization of this exercise).
(b)† Find the correct generalization to more general second-order linear recurrence sequences.

Additional exercises

Exercise 1.7.1. (a) Does 0 divide 0? (Use the definition of "divides".)
(b) Show that there is no unique meaning to $0/0$.
(c) Prove that if b divides a and $b \neq 0$, then there is a unique meaning to a/b.

Exercise 1.7.2. Prove that if a and b are not both 0, then $\gcd(a, b)$ is a positive integer.

Exercise 1.7.3.† Prove that if m and n are coprime positive integers, then $\frac{(m+n-1)!}{m!n!}$ is an integer.

Exercise 1.7.4. Suppose that $a = qb + r$ with $0 \leq r \leq b - 1$.
(a) Let $[t]$ be the *integer part* of t, that is, the largest integer $\leq t$. Prove that $q = [a/b]$.
(b) Let $\{t\}$ to be the *fractional part* of t, that is, $\{t\} = t - [t]$. Prove that $r = b\{r/b\} = b\{a/b\}$.

(Beware of these functions applied to negative numbers: e.g., $[-3.14] = -4$ *not* -3, and $\{-3.14\} = .86$ *not* $.14$.)

Exercise 1.7.5.† (a) Show that if n is an integer, then $\{n + \alpha\} = \{\alpha\}$ and $[n + \alpha] = n + [\alpha]$ for all $\alpha \in \mathbb{R}$.
(b) Prove that $[\alpha + \beta] - [\alpha] - [\beta] = 0$ or 1 for all $\alpha, \beta \in \mathbb{R}$, and explain when each case occurs.
(c) Deduce that $\{\alpha\} + \{\beta\} - \{\alpha + \beta\} = 0$ or 1 for all $\alpha, \beta \in \mathbb{R}$, and explain when each case occurs.
(d) Show that $\{\alpha\} + \{-\alpha\} = 1$ unless α is an integer in which case it equals 0.
(e) Show that if $a \in \mathbb{Z}$ and $r \in \mathbb{R} \setminus \mathbb{Z}$, then $[r] + [a - r] = a - 1$.

Exercise 1.7.6. Suppose that d is a positive integer and that $N, x > 0$.
(a) Show that there are exactly $[x]$ positive integers $\leq x$.
(b) Show that kd is the largest multiple of d that is $\leq N$, where $k = [N/d]$.
(c) Deduce that there are exactly $[N/d]$ positive integers $n \leq N$ which are divisible by d.

Exercise 1.7.7. Prove that $\sum_{k=0}^{n-1} [a + \frac{k}{n}] = [na]$ for any real number a and integer $n \geq 1$.

Exercise 1.7.8. Suppose that $a + b = c$ and let $g = \gcd(a, b)$. Prove that we can write $a = gA$, $b = gB$, and $c = gC$ where $A + B = C$, where A, B, and C are pairwise coprime integers.

Exercise 1.7.9. Prove that if $(a, b) = 1$, then $(a + b, a - b) = 1$ or 2.

Exercise 1.7.10.† Prove that for any given integers $b > a \geq 1$ there exists an integer solution u, w to $au - bw = \gcd(a, b)$ with $0 \leq u \leq b - 1$ and $0 \leq w \leq a - 1$.

Exercise 1.7.11.† Show that if $\gcd(a,b)=1$, then $\gcd(a^k,b^\ell)=1$ for all integers $k,\ell\geq 1$.

Exercise 1.7.12. Let m and n be positive integers. What fractions do the two lists $\frac{1}{m},\dots,\frac{m-1}{m}$ and $\frac{1}{n},\dots,\frac{n-1}{n}$ have in common (when the fractions are reduced)?

Exercise 1.7.13. Suppose m and n are coprime positive integers. When the fractions $\frac{1}{m},\frac{2}{m},\dots,\frac{m-1}{m},\frac{1}{n},\dots,\frac{n-1}{n}$ are put in increasing order, what is the shortest distance between two consecutive fractions?

Given a 7-liter jug and a 5-liter jug one can measure 1 liter of water as follows: Fill the 5-liter jug, and pour the contents into the 7-liter jug. Fill the 5-liter jug again, use this to fill the 7-liter jug, so we are left with 3 liters in the 5-liter jug and the 7-liter jug is full. Empty the 7-liter jug, pour the contents of the 5-liter jug into the 7-liter jug, and refill the 5-liter jug. We now have 3 liters in the 7-liter jug. Fill the 7-liter jug using the 5-liter jug; we have poured 4 liters from the 5-liter jug into the 7-liter jug, so that there is just 1 liter left in the 5-liter jug! Notice that we filled the 5-liter jug 3 times and emptied the 7-liter jug twice, and so we used here that $3\times 5-2\times 7=1$. We have wasted 2×7 liters of water in this process.

Exercise 1.7.14. (a) Since $3\times 7-4\times 5=1$ describe how we can proceed by filling the 7-liter jug each time rather than filling the 5-liter jug.
(b) Can you measure 1 liter of water using a 25-liter jug and a 17-liter jug?
(c)† Prove that if m and n are positive coprime integers then you can measure one liter of water using an m liter jug and an n liter jug?
(d) Prove that one can do this wasting less than mn liters of water.

Exercise 1.7.15. Can you weigh 1 lb of tea using scales with 25-lb and 17-lb weights?

The definition of a set of linear combinations can be extended to an arbitrary set of integers (in place of the set $\{a,b\}$); that is,

$$I(a_1,\dots,a_k):=\{a_1m_1+a_2m_2+\cdots+a_km_k:\ m_1,m_2,\dots,m_k\in\mathbb{Z}\}.$$

Exercise 1.7.16. Show that $I(a_1,\dots,a_k)=I(g)$ for any non-zero integers $a_1,\dots,a_k$, where we have $g=\gcd(a_1,\dots,a_k)$.

Exercise 1.7.17.† Deduce that if we are given integers $a_1,a_2,\dots,a_k$, not all zero, then there exist integers $m_1,m_2,\dots,m_k$ such that

$$m_1a_1+m_2a_2+\cdots+m_ka_k=\gcd(a_1,a_2,\dots,a_k).$$

We say that the integers $a_1,a_2,\dots,a_k$ are *relatively prime* if $\gcd(a_1,a_2,\dots,a_k)=1$. We say that they are *pairwise coprime* if $\gcd(a_i,a_j)=1$ whenever $i\neq j$. Note that $6,10,15$ are relatively prime, but not pairwise coprime (since each pair of integers has a common factor >1).

Exercise 1.7.18. Prove that if $g=\gcd(a_1,a_2,\dots,a_k)$, then $\gcd(a_1/g,a_2/g,\dots,a_k/g)=1$.

Exercise 1.7.19.† (a) Prove that $abc=[a,b,c]\cdot\gcd(ab,bc,ca)$.
(b)‡ Prove that if $r+s=n$, then

$$a_1\cdots a_n=\operatorname{lcm}\left[\prod_{i\in I}a_i:\ I\subset\{1,\dots,n\},\ |I|=r\right]\cdot\gcd\left(\prod_{j\in J}a_j:\ J\subset\{1,\dots,n\},\ |J|=s\right).$$

Throughout this book we will present more challenging exercises in the final part of each chapter. If some of the questions are part of a consistent subject, then they will be presented as a separate subsection:

Divisors in recurrence sequences

We begin by noting that for any integer $d \geq 1$ we have the polynomial identity

$$x^d - y^d = (x-y)(x^{d-1} + x^{d-2}y + \cdots + xy^{d-2} + y^{d-1}). \tag{1.7.1}$$

Hence if r and s are integers, then $r - s$ divides $r^d - s^d$. (This also follows from Corollary 2.3.1 in the next chapter.)

Exercise 1.7.20. (a) Prove that if $m|n$, then $2^m - 1$ divides $2^n - 1$.
(b)† Prove that if $n = qm + r$ with $0 \leq r \leq m-1$, then there exists an integer Q such that

$$2^n - 1 = Q(2^m - 1) + (2^r - 1) \qquad \text{(and note that } 0 \leq 2^r - 1 < 2^m - 1\text{)}.$$

(c)† Use the Euclidean algorithm to show that $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(n,m)} - 1$.
(d) What is the value of $\gcd(N^a - 1, N^b - 1)$ for arbitrary integer $N \neq -1, 0,$ or 1?

In exercise 0.4.15(a) we saw that the Mersenne numbers $M_n = 2^n - 1$ (of the previous exercise) are an example of a second-order linear recurrence sequence. We will show that an analogous result holds for *any* second-order linear recurrence sequence that begins $0, 1, \ldots$. For the rest of this section we assume that a and b are coprime integers with $x_0 = 0,\ x_1 = 1$ and that $x_n = ax_{n-1} + bx_{n-2}$ for all $n \geq 2$.

Exercise 1.7.21. Use exercise 0.4.10(a) to show that $\gcd(x_m, x_n) = \gcd(x_m, x_{m+1}x_{n-m})$ whenever $n \geq m$.

Exercise 1.7.22.† Prove that if $m|n$, then $x_m|x_n$; that is, $\{x_n : n \geq 0\}$ is a *division sequence*.

Exercise 1.7.23.† Assume that $(a, b) = 1$.
(a) Prove that $\gcd(x_n, b) = 1$ for all $n \geq 1$.
(b) Prove that $\gcd(x_n, x_{n-1}) = 1$ for all $n \geq 1$.
(c) Prove that if $n > m$, then $(x_n, x_m) = (x_{n-m}, x_m)$.
(d) Deduce that $(x_n, x_m) = x_{(n,m)}$.

Exercise 1.7.24.† For any given integer $d \geq 2$, let $m = m_d$ be the smallest positive integer for which d divides x_m. Prove that d divides x_n if and only if m_d divides n.

It is sometimes possible to reverse the direction in the defining recurrence relation for a recurrence sequence; that is, if $b = 1$, then (0.1.2) can be rewritten as $x_{n-2} = -ax_{n-1} + x_n$. So if $x_0 = 0$ and $x_1 = 1$, then $x_{-1} = 1, x_{-2} = -a, \ldots$. We now try to understand the terms x_{-n}.

Exercise 1.7.25. Let us suppose that $x_n = ax_{n-1} + x_{n-2}$ for all integers n, both positive and negative, with $x_0 = 0$ and $x_1 = 1$. Prove, by induction on $n \geq 1$, that $x_{-n} = (-1)^{n-1}x_n$ for all $n \geq 2$.

Appendix 1A. Reformulating the Euclidean algorithm

In section 1.5 we saw that the Euclidean algorithm may be usefully reformulated in terms of continued fractions. In this appendix we reformulate the Euclidean algorithm in two further ways: firstly, in terms of matrix multiplication, which makes many of the calculations easier; and secondly, in terms of a dynamical system, which will be useful later when we develop similar ideas in a more general context.

1.8. Euclid matrices and Euclid's algorithm

In discussing the Euclidean algorithm we showed that $\gcd(85, 48) = \gcd(48, 37)$ from noting that $85 - 1 \cdot 48 = 37$. In this we changed our attention from the pair $85, 48$ to the pair $48, 37$. Writing this down using matrices, we performed this change via the map

$$\begin{pmatrix} 85 \\ 48 \end{pmatrix} \to \begin{pmatrix} 48 \\ 37 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 85 \\ 48 \end{pmatrix}.$$

Next we went from the pair $48, 37$ to the pair $37, 11$ via the map

$$\begin{pmatrix} 48 \\ 37 \end{pmatrix} \to \begin{pmatrix} 37 \\ 11 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 48 \\ 37 \end{pmatrix}$$

and then from the pair $37, 11$ to the pair $11, 4$ via the map

$$\begin{pmatrix} 37 \\ 11 \end{pmatrix} \to \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 37 \\ 11 \end{pmatrix}.$$

We can compose these maps so that

$$\begin{pmatrix} 85 \\ 48 \end{pmatrix} \to \begin{pmatrix} 48 \\ 37 \end{pmatrix} \to \begin{pmatrix} 37 \\ 11 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 48 \\ 37 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 85 \\ 48 \end{pmatrix}$$

and then

$$\begin{pmatrix}85\\48\end{pmatrix} \to \begin{pmatrix}11\\4\end{pmatrix} = \begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}37\\11\end{pmatrix} = \begin{pmatrix}0&1\\1&-3\end{pmatrix}\cdot\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}85\\48\end{pmatrix}.$$

Continuing on to the end of the Euclidean algorithm, via $11 = 2\cdot 4+3$, $4 = 1\cdot 3+1$, and $3 = 3\cdot 1+0$, we have

$$\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}85\\48\end{pmatrix}.$$

Since $\begin{pmatrix}0&1\\1&-x\end{pmatrix}\begin{pmatrix}x&1\\1&0\end{pmatrix} = I$ for any x, we can invert to obtain

$$\begin{pmatrix}85\\48\end{pmatrix} = M\begin{pmatrix}1\\0\end{pmatrix}$$

where

$$M = \begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}3&1\\1&0\end{pmatrix}\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}3&1\\1&0\end{pmatrix}.$$

Here we used that the inverse of a product of matrices is the product of the inverses of those matrices, in reverse order. If we write

$$M := \begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}$$

where $\alpha, \beta, \gamma, \delta$ are integers (since the set of integer matrices are closed under multiplication), then

$$\alpha\delta - \beta\gamma = \det M = (-1)^6 = 1,$$

since M is the product of six matrices, each of determinant -1, and the determinant of the product of matrices equals the product of the determinants. Now

$$\begin{pmatrix}85\\48\end{pmatrix} = M\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\alpha\\\gamma\end{pmatrix}$$

so that $\alpha = 85$ and $\gamma = 48$. This implies that

$$85\,\delta - 48\,\beta = 1;$$

that is, the matrix method gives us the solution to (1.2.1) without extra effort.

If we multiply the matrices defining M together in order, we obtain the sequence

$$\begin{pmatrix}1&1\\1&0\end{pmatrix},\ \begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix} = \begin{pmatrix}2&1\\1&1\end{pmatrix},\ \begin{pmatrix}2&1\\1&1\end{pmatrix}\begin{pmatrix}3&1\\1&0\end{pmatrix} = \begin{pmatrix}7&2\\4&1\end{pmatrix}$$

and then

$$\begin{pmatrix}16&7\\9&4\end{pmatrix},\ \begin{pmatrix}23&16\\13&9\end{pmatrix},\ \begin{pmatrix}85&23\\48&13\end{pmatrix}.$$

We notice that the columns give us the numerators and denominators of the convergents of the continued fraction for 85/48, as discussed in section 1.5.

We can generalize this discussion to formally explain the Euclidean algorithm:

Let $u_0 := a \geq u_1 := b \geq 1$. Given $u_j \geq u_{j+1} \geq 1$:

- Let $a_j = [u_j/u_{j+1}]$, an integer ≥ 1.
- Let $u_{j+2} = u_j - a_j u_{j+1}$ so that $0 \leq u_{j+2} \leq u_{j+1} - 1$.
- If $u_{j+2} = 0$, then $g := \gcd(a, b) = u_{j+1}$, and terminate the algorithm.
- Otherwise, repeat these steps with the new pair u_{j+1}, u_{j+2}.

The first two steps work by Lemma 1.1.1, the third by exercise 1.1.3. We end up with the continued fraction

$$a/b = [a_0, a_1, \ldots, a_k]$$

for some $k \geq 0$. The convergents $p_j/q_j = [a_0, a_1, \ldots, a_j]$ are most easily calculated by matrix arithmetic as

$$\begin{pmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \tag{1.8.1}$$

so that $a/g = p_k$ and $b/g = q_k$, where $g = \gcd(a, b)$.

Exercise 1.8.1. Prove that this description of the Euclidean algorithm really works.

Exercise 1.8.2. (a) Show that $p_j q_{j-1} - p_{j-1} q_j = (-1)^{j+1}$ for all $j \geq 0$.
(b) Explain how to use the Euclidean algorithm, along with (1.8.1), to determine, for given positive integers a and b, an integer solution u, v to the equation $au + bv = \gcd(a, b)$.

Exercise 1.8.3. With the notation as above, show that $[a_k, \ldots, a_0] = a/c$ for some integer c for which $0 < c < a$ and $bc \equiv (-1)^k \pmod{a}$.

Exercise 1.8.4. Prove that for every $n \geq 1$ we have

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n,$$

where F_n is the nth Fibonacci number.

My favorite open question in this area is Zaremba's conjecture: He conjectured that there is an integer $B \geq 1$ such that for every integer $n \geq 2$ there exists a fraction m/n, where m is an integer, $1 \leq m \leq n - 1$, coprime with n, for which the continued fraction $m/n = [a_0, a_1, \ldots, a_k]$ has each partial quotient $a_k \leq B$. Calculations suggest one can take $B = 5$.

1.9. Euclid matrices and ideal transformations

In section 1.3 we used Euclid's algorithm to transform the basis of the ideal $I(85, 48)$ to $I(48, 37)$, and so on, until we showed that it equals $I(1, 0) = I(1)$. The transformation rested on the identity

$$85m + 48n = 48m' + 37n', \text{ where } m' = m + n \text{ and } n' = n;$$

a transformation we can write as

$$(m, n) \to (m', n') = (m, n) \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

The transformation of linear forms can then be seen by

$$48m' + 37n' = (m', n') \begin{pmatrix} 48 \\ 37 \end{pmatrix} = (m, n) \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 48 \\ 37 \end{pmatrix} = (m, n) \begin{pmatrix} 85 \\ 48 \end{pmatrix} = 85m + 48n.$$

The inverse map can be found simply by inverting the matrix:

$$\begin{pmatrix} m' \\ n' \end{pmatrix} \to \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} m' \\ n' \end{pmatrix}.$$

These linear transformations can be composed by multiplying the relevant matrices, which are the same matrices that arise in the previous section, section 1.8. For example, after three steps, the change is

$$(m, n) \to (m_3, n_3) = (m, n) \begin{pmatrix} 7 & 2 \\ 4 & 1 \end{pmatrix},$$

so that $11m_3 + 4n_3 = 85m + 48n$.

Exercise 1.9.1. (a) With the notation of section 1.8, establish that $xu_j + yu_{j+1} = ma + nb$ where the variables x and y are obtained from the variables m and n by a linear transformation.

(b) Deduce that $I(u_j, u_{j+1}) = I(a, b)$ for $j = 0, \ldots, k$.

1.10. The dynamics of the Euclidean algorithm

We now explain a dynamical perspective on the Euclidean algorithm, by focusing on each individual transformation of the pair of numbers with which we work. In our example, we began with the pair of numbers $(85, 48)$, subtracted the smaller from the larger to get $(37, 48)$, and then swapped the order to obtain $(48, 37)$. Now we begin with the fraction $x := 85/48$; the first step transforms $x \to y := x - 1 = 37/48$, and the second transforms $y \to 1/y = 48/37$. The Euclidean algorithm can easily be broken down into a series of steps of this form:

$$\begin{aligned} \frac{85}{48} \to \frac{37}{48} \to \frac{48}{37} \to \frac{11}{37} \to \frac{37}{11} \to \frac{26}{11} \to \frac{15}{11} \to \frac{4}{11} \\ \to \frac{11}{4} \to \frac{7}{4} \to \frac{3}{4} \to \frac{4}{3} \to \frac{1}{3} \to \frac{3}{1} \to \frac{2}{1} \to \frac{1}{1} \to \frac{0}{1}. \end{aligned}$$

It is possible that the map $x \to x - 1$ is repeated several times consecutively (for example, as we went from $37/11$ to $4/11$), the number of times corresponding to the quotient, $[x]$. On the other hand, the map $y \to 1/y$ is not immediately repeated, since repeating this map sends y back to y, which corresponds to swapping the order of a pair of numbers twice, sending the pair back to their original order.

These two linear maps correspond to our matrix transformations:

$$x \to x - 1 \text{ corresponds to } \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \text{ so that } \begin{pmatrix} 37 \\ 48 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 85 \\ 48 \end{pmatrix};$$

$$\text{and } y \to 1/y \text{ corresponds to } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ so that } \begin{pmatrix} 48 \\ 37 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 37 \\ 48 \end{pmatrix}.$$

The Euclidean algorithm is therefore a series of transformations of the form $x \to x - 1$ and $y \to 1/y$ and defines a finite sequence of these transformations that begins with any given positive rational number and ends with 0. One can invert

that sequence of transformations, to transformations of the form $x \to x+1$ and $y \to 1/y$, to begin with 0 and to end at any given rational number.

Determinant 1 transformations. Foreshadowing later results, it is more useful to develop a variant on the Euclidean algorithm in which the matrices of all of the transformations have determinant 1. To begin with, we break each transformation down into the two steps:

- Beginning with the pair $85, 48$ the first step is to subtract 1 times 48 from 85, and in general we subtract q times b from a. This transformation is therefore given by
$$\begin{pmatrix} a \\ b \end{pmatrix} \to \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \text{ and notice that } \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-q}.$$
- The second step swaps the roles of $37 (= 85-48)$ and 48, corresponding to a matrix of determinant -1. Here we do something unintuitive which is to change 48 to -48, so that the matrix has determinant 1:
$$\begin{pmatrix} 37 \\ 48 \end{pmatrix} \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 37 \\ 48 \end{pmatrix}, \text{ and more generally } \begin{pmatrix} a \\ b \end{pmatrix} \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$
One then sees that if $g = \gcd(a,b)$ and $a/b = [a_0, \dots, a_k]$, then
$$\begin{pmatrix} 0 \\ g \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-a_k} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-a_{k-1}} \cdots \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-a_0} \begin{pmatrix} a \\ b \end{pmatrix}.$$

We write $S := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Taking inverses here we get

$$\begin{pmatrix} a \\ b \end{pmatrix} = S^{a_0} T S^{a_1} T \cdots S^{a_{k-1}} T S^{a_k} \begin{pmatrix} 0 \\ g \end{pmatrix}.$$

If a and b are coprime, then this implies that

$$S^{a_0} T S^{a_1} T \cdots S^{a_{k-1}} T S^{a_k} = \begin{pmatrix} c & a \\ d & b \end{pmatrix} \tag{1.10.1}$$

for some integers c and d. The left-hand side is the product of determinant one matrices, and so the right-hand side also has determinant one; that is, $cb - ad = 1$. This is therefore an element of $\mathrm{SL}(2,\mathbb{Z})$, the subgroup (under multiplication) of 2-by-2 integer matrices of determinant one; more specifically

$$\mathrm{SL}(2,\mathbb{Z}) := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \ \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \ \alpha\delta - \beta\gamma = 1 \right\}.$$

Theorem 1.2. *Each matrix in* $\mathrm{SL}(2,\mathbb{Z})$ *can be represented as* $S^{e_1} T^{f_1} \cdots S^{e_r} T^{f_r}$ *for integers* $e_1, f_1, \dots, e_r, f_r$.

Proof. Suppose that we are given $\begin{pmatrix} x & a \\ y & b \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. Taking determinants we see that $bx - ay = 1$. Therefore $\gcd(a,b) = 1$, and so above we saw how to construct an element of $\mathrm{SL}(2,\mathbb{Z})$ with the same last column. In Theorem 3.5 we will show

that every other integer solution to $bx - ay = 1$ is given by $x = c - ma, y = d - mb$ for some integer m. Therefore

$$\begin{pmatrix} x & a \\ y & b \end{pmatrix} = \begin{pmatrix} c & a \\ d & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix}.$$

One can easily verify that

$$T^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ so that } T^{-1}ST = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

and therefore

$$\begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix} = (T^{-1}ST)^m = T^{-1}S^mT.$$

Combining these last two statements together with (1.10.1) completes the proof of the theorem. □

Appendices. The extended version of chapter 1 has the following additional appendices:

Appendix 1B. *Computational aspects of the Euclidean algorithm*, which discusses how to speed up the Euclidean algorithm, how to determine how long it takes, and asks what a "fast" algoirthm is.

Appendix 1C. *Magic squares* is a basic introduction to constructing different types of magic and Latin squares of arbitrary dimension.

Appendix 1D. *The Frobenius postage stamp problem* introduces the question of what amounts of postage can be made up of stamps of given costs.

Appendix 1E. *Egyptian fractions* discusses what rational numbers are a sum of distinct fractions of the form $1/n$.

Congruences

The key step in understanding the Euclidean algorithm, Lemma 1.1.1, shows that $\gcd(a, b)$ equals $\gcd(r, b)$, *because* b divides $a - r$. Inspired by how useful this observation is, Gauss developed the theory of when two given integers, like a and r, differ by a multiple of b:

2.1. Basic congruences

If m, b, and c are integers for which m divides $b - c$, then we write

$$b \equiv c \pmod{m}$$

and say that b and c are *congruent modulo* m, where m is the *modulus*.[1] The numbers involved should be integers, not fractions, and the modulus can be taken in absolute value; that is, $b \equiv c \pmod{m}$ if and only if $b \equiv c \pmod{|m|}$, by definition.

For example, $-10 \equiv 15 \pmod{5}$, and $-7 \equiv 15 \pmod{11}$, but $-7 \not\equiv 15 \pmod{3}$. Note that $b \equiv b \pmod{m}$ for all integers m and b.

The integers $\equiv a \pmod{m}$ are precisely those of the form $a + km$ where k is an integer, that is, $a, a + m, a + 2m, \ldots$ as well as $a - m, a - 2m, a - 3m, \ldots$. We call this set of integers a *congruence class* or *residue class* mod m, and any particular element of the congruence class is a *residue*.[2]

For any given integers a and $m > 0$, there exists a unique pair of integers q and r with $0 \le r \le m - 1$, for which $a = qm + r$, by Lemma 1.1.1. Therefore there exists a unique integer $r \in \{0, 1, 2, \ldots, m - 1\}$ for which $a \equiv r \pmod{m}$. Moreover, if two integers are congruent mod m, then they leave the same remainder, r, when

[1] Gauss proposed the symbol $\equiv$ because of the analogies between equality and congruence, which we will soon encounter. To avoid ambiguity he made a minor distinction by adding the extra bar.

[2] The sequence of numbers $a, a + m, a + 2m, \ldots$, in which we add m to the last number in the sequence to obtain the next one, is an *arithmetic progression*.

divided by m. We now prove a generalization of these last remarks:

Theorem 2.1. *Suppose that m is a positive integer. Exactly one of any m consecutive integers is $\equiv a \pmod m$.*

Two proofs.[3] Suppose we have the m consecutive integers $x, x+1, \dots, x+m-1$.

Analytic proof: An integer n in the range $x \le n < x+m$ is of the form $a+km$, for some integer k, if and only if there exists an integer k for which

$$x \le a + km < x + m.$$

Subtracting a from each term here and dividing through by m, we find that this holds if and only if

$$\frac{x-a}{m} \le k < \frac{x-a}{m} + 1.$$

Hence k must be an integer from an interval of length one which has just one endpoint included in the interval. Such an integer k exists and is unique; it is the smallest integer that is $\ge \frac{x-a}{m}$.

Exercise 2.1.1. Prove that for any real number t there is a unique integer in the interval $[t, t+1)$.

Number-theoretic proof: By Lemma 1.1.1 there exist integers q and r with $0 \le r \le m-1$, for which $a - x = qm + r$, with $0 \le r \le m-1$. Then $x \le x + r \le x + m - 1$ and $x + r = a - qm \equiv a \pmod m$, and so $x + r$ is the integer that we are looking for. We still need to prove that it is unique:

If $x + i \equiv a \pmod m$ and $x + j \equiv a \pmod m$, where $0 \le i < j \le m-1$, then $i \equiv a - x \equiv j \pmod m$, so that m divides $j - i$, which is impossible as $1 \le j - i \le m - 1$. □

Exercise 2.1.2. Prove that m divides $(n-1)(n-2)\cdots(n-m)$ for every integer n and every integer $m \ge 1$.

Theorem 2.1 implies that any m consecutive integers yield a *complete set of residues* $\pmod m$; that is, every congruence class $\pmod m$ is represented by exactly one element of the given set of m integers. For example, every integer has a unique residue amongst

$$\textit{the least non-negative residues } \pmod m: \quad 0,\ 1,\ 2,\ \dots, (m-1),$$

as well as amongst

$$\textit{the least positive residues } \pmod m: \quad 1,\ 2,\ \dots, m,$$

and also amongst

$$\textit{the least negative residues } \pmod m: \quad -(m-1),\ -(m-2),\ \dots,\ -2,\ -1,\ 0.$$

For example, 2 is the least positive residue of $-13 \pmod 5$, whereas -3 is the least negative residue; and 5 is its own least positive residue mod 7, whereas -2 is the least negative residue. Notice that if the residue is not $\equiv 0 \pmod m$, then these residues occur in pairs, one positive and the other negative, and at least one of each

[3] Why give two proofs? Throughout this book we will frequently take the opportunity to give more than one proof of a key result. The idea is to highlight different aspects of the theory that are, or will become, of interest. Here we find both an analytic proof (meaning that we focus on the size or quantity of the objects involved) as well as a number-theoretic proof (in which we use their algebraic properties). Sometimes the interplay between these two perspectives can take us much further than either one alone.

pair is $\le m/2$ in absolute value. We call this the *absolutely least* residue (mod m) (and we select $m/2$, rather than $-m/2$, when m is even).[4] For example if $m = 5$, we can pair up the least positive residues and the least negative residues as

$$1 \equiv -4 \pmod 5,\ 2 \equiv -3 \pmod 5,\ 3 \equiv -2 \pmod 5,\ 4 \equiv -1 \pmod 5,$$

as well as the exceptional $5 \equiv 0 \pmod 5$. Hence the absolutely least residues (mod 5) are $-2, -1, 0, 1, 2$. Similarly the the absolutely least residues (mod 6) are $-2, -1, 0, 1, 2, 3$. More generally if $m = 2k + 1$ is odd, then the absolutely least residues (mod $2k + 1$) are $-k, \dots, -1, 0, 1 \dots, k$; and if $m = 2k$ is even, then the absolutely least residues (mod $2k$) are $-(k - 1), \dots, -1, 0, 1 \dots, k$.

We defined a *complete set of residues* to be any set of representatives for the residue classes mod m, one for each residue class. A *reduced set of residues* has representatives only for the residue classes that are coprime with m. For example $\{0, 1, 2, 3, 4, 5\}$ is a complete set of residues (mod 6), whereas $\{1, 5\}$ is a reduced set of residues, as 0, 2, and 4 are divisible by 2, and 0 and 3 are divisible by 3 and so are excluded.

Exercise 2.1.3. Suppose that $a_1, \dots, a_m$ is a complete set of residues mod m. Prove that m divides $(n - a_1) \cdots (n - a_m)$ for every integer n.

Exercise 2.1.4. (a) Explain how "a number of the form $3n - 1$" means the same thing as "a number of the form $3n + 2$", using the language of congruences.

(b) Prove that the set of integers in the congruence class $a \pmod d$ can be partitioned into the set of integers in the congruence classes $a \pmod{kd}$, $a + d \pmod{kd}, \dots$ and $a + (k - 1)d \pmod{kd}$.

Exercise 2.1.5. Show that if $a \equiv b \pmod m$, then $(a, m) = (b, m)$.

Exercise 2.1.6. Prove that if $a \equiv b \pmod m$, then $a \equiv b \pmod d$ for any divisor d of m.

Exercise 2.1.7. Satisfy yourself that addition and multiplication mod m are commutative.[5]

Exercise 2.1.8. Prove that the property of congruence modulo m is an *equivalence relation* on the integers. To prove this, one must establish

(i) $a \equiv a \pmod m$;
(ii) $a \equiv b \pmod m$ implies $b \equiv a \pmod m$;
(iii) $a \equiv b \pmod m$ and $b \equiv c \pmod m$ imply $a \equiv c \pmod m$.

The equivalence classes are therefore the congruence classes mod m.

One consequence of this is that integers that are congruent modulo m have the same least residues modulo m, whereas integers that are not congruent modulo m have different least residues.

The main use of congruences is that it simplifies arithmetic when we are looking into questions about remainders. This is because the usual rules for addition, subtraction, and multiplication work for congruences. However, division is a little more complicated, as we will see in the next section.

[4] This is often called the *least residue in absolute value*.

[5] A mathematical operation is *commutative* if you get the same result no matter what order you take the input variables in. Thus, in $\mathbb{C}$, we have $x + y = y + x$ and $xy = yx$. There are common operations that are not commutative; for example $a - b \neq b - a$ in $\mathbb{C}$, unless $a = b$. Moreover multiplication in different settings might not be commutative, for example when we multiply 2-by-2 matrices, as we discovered, in detail, in section 0.12 of appendix 0D.

Lemma 2.1.1. *If* $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$, *then*

$$a + c \equiv b + d \pmod m,$$
$$a - c \equiv b - d \pmod m,$$
$$\text{and} \quad ac \equiv bd \pmod m.$$

Proof. By hypothesis there exist integers u and v for which $a - b = um$ and $c - d = vm$. Therefore

$$(a + c) - (b + d) = (a - b) + (c - d) = um + vm = (u + v)m$$

so that $a + c \equiv b + d \pmod m$;

$$(a - c) - (b - d) = (a - b) - (c - d) = um - vm = (u - v)m$$

so that $a - c \equiv b - d \pmod m$; and

$$ac - bd = a(c - d) + d(a - b) = a \cdot vm + d \cdot um = (av + du)m$$

so that $ac \equiv bd \pmod m$. □

These are the rules of *modular arithmetic*.

Exercise 2.1.9. Under the hypothesis of Lemma 2.1.1, show that $ka + lc \equiv kb + ld \pmod m$ for any integers k and l.

Exercise 2.1.10. If $p|m$ and $m/p \equiv a \pmod q$, then prove that $m \equiv ap \pmod q$.

2.2. The trouble with division

Although the rules for addition, subtraction, and multiplication work for congruences as they do for the integers, reals, and most other mathematical objects we have encountered, the rule for division is more subtle. In the complex numbers, if we are given numbers a and $b \neq 0$, then there exists a unique value of c for which $a = bc$ (so that $c = a/b$), and therefore there is no ambiguity in the definition of division. We now look at the multiplication tables mod 5 and mod 6 to see whether this same property holds for modular arithmetic:

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The multiplication table (mod 5).

Other than in the top row, we see that every congruence class mod 5 appears exactly once in each row of the table. For example, in the row corresponding to the multiples of 2, mod 5 we have 0, 2, 4, 1, 3, which implies that for each $a \pmod 5$

there exists a unique value of $c \pmod 5$ for which $a \equiv 2c \pmod 5$; that is, $c \equiv a/2 \pmod 5$. We read off

$$0/2 \equiv 0 \pmod 5,\ 1/2 \equiv 3 \pmod 5,\ 2/2 \equiv 1 \pmod 5,$$
$$3/2 \equiv 4 \pmod 5,\ \text{and}\ 4/2 \equiv 2 \pmod 5,$$

each division leading to a unique value. This is true in each row, so for every non-zero value of $b \pmod 5$ and every $a \pmod 5$, there exists a unique multiple of b, which equals $a \bmod 5$. Therefore division is well- (and uniquely) defined modulo 5.

However, the multiplication table mod 6 looks rather different.

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The multiplication table (mod 6).

The row corresponding to the multiples of 5, mod 6, is 0, 5, 4, 3, 2, 1, so that each $b/5 \pmod 6$ is well-defined.

However, the row corresponding to the multiples of 2, mod 6, reads $0, 2, 4, 0, 2, 4$. There is no solution to $1/2 \pmod 6$. On the other hand, for something as simple as $4/2 \pmod 6$, there are two different solutions: $5 \pmod 6$ as well as $2 \pmod 6$. Evidently it is more complicated to understand division mod 6 than mod 5.

We can obtain a hint of what is going on by applying exercise 2.1.4, which implies that the union of the sets of integers in the two arithmetic progressions $5 \pmod 6$ and $2 \pmod 6$ gives exactly the integers $\equiv 2 \pmod 3$. So we now have a unique solution to $4/2 \pmod 6$, albeit a congurence class belonging to a different modulus.

Exercise 2.2.1. Determine one congruence class which gives all solutions to 3 divided by 3 (mod 6). (In other words, find a congruence class $a \pmod m$ such that $3x \equiv 3 \pmod 6$ if and only if $x \equiv a \pmod m$.)

These issues with division arise when we try to solve equations by division: If we divide each side of $8 \equiv 2 \pmod 6$ by 2, we obtain the incorrect "$4 \equiv 1 \pmod 6$". We can correct this by dividing the modulus through by 2 also, so as to obtain $4 \equiv 1 \pmod 3$. Even this is not the whole story, for if we wish to divide both sides of $21 \equiv 6 \pmod 5$ through by 3, we cannot also divide the modulus, since 3 does not divide 5. However, in this case one does not need to divide the modulus through by 3, since $7 \equiv 2 \pmod 5$. So what is the general rule? We shall resolve all of these issues in Lemma 3.5.1, after we have developed a little more theory.

2.3. Congruences for polynomials

Let $\mathbb{Z}[x]$ denote the set of polynomials with integer coefficients. Using the above rules for congruences, one gets a very useful result for congruences involving polynomials:

Corollary 2.3.1. *If $f(x) \in \mathbb{Z}[x]$ and $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.*

Proof. Since $a \equiv b \pmod{m}$ we have $a^2 \equiv b^2 \pmod{m}$ by Lemma 2.1.1, and then

Exercise 2.3.1. Prove that $a^k \equiv b^k \pmod{m}$ for all integers $k \geq 1$, by induction.

Now, writing $f(x) = \sum_{i=0}^{d} f_i x^i$ where each f_i is an integer, we have

$$f(a) = \sum_{i=0}^{d} f_i a^i \equiv \sum_{i=0}^{d} f_i b^i = f(b) \pmod{m},$$

by Lemma 2.1.1. □

This result can be extended to polynomials in many variables.

Exercise 2.3.2. Deduce, from Corollary 2.3.1, that if $f(t) \in \mathbb{Z}[t]$ and $r, s \in \mathbb{Z}$, then $r - s$ divides $f(r) - f(s)$.

Therefore, for any polynomial $f(x) \in \mathbb{Z}[x]$, the sequence $f(0), f(1), f(2), \ldots$ modulo m is *periodic* of period m; that is, the values repeat every mth term in the sequence, repeating indefinitely. More precisely $f(n + m) \equiv f(n) \pmod{m}$ for all integers n.

Example. If $f(x) = x^3 - 8x + 6$ and $m = 5$, then we get the sequence

$$f(0), f(1), \ldots = 1, 4, 3, 4, 3, 1, 4, 3, 4, 3, 1 \ldots$$

and the first five terms $1, 4, 3, 4, 3$ repeat infinitely often. Moreover we get the same pattern if we run though the consecutive negative integer values for x.

Note that in this example $f(x)$ is never 0 or 2 (mod 5). Thus none of the equations

$$x^3 - 8x + 6 = 0, \qquad y^3 - 8y + 1 = 0, \qquad \text{and} \qquad z^3 - 8z + 4 = 0$$

can have solutions in integers x, y, or z.

Exercise 2.3.3. Let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(r) \not\equiv 0 \pmod{m}$ for all integers r in the range $0 \leq r \leq m - 1$. Deduce that there does not exist an integer n for which $f(n) = 0$.

2.4. *Tests for divisibility*

There are easy tests for divisibility based on ideas from this chapter. For example, writing an integer in decimal as[6]

$$a + 10b + 100c + \cdots,$$

[6] More precisely, $\sum_{i=0}^{d} a_i 10^i$ where each a_i is an integer in $\{0, 1, 2, \ldots, 9\}$ and $a_d \neq 0$. Why did we write the decimal expansion so informally in the text, when surely good mathematics is all about precision? While good mathematics is anchored by precision, mathematical writing also requires good communication—after all why shouldn't the reader understand with as little effort as possible?—and so we attempt to explain accurately with as little notation as possible.

we employ Corollary 2.3.1 with $f(x) = a + bx + cx^2 + \cdots$ and $m = 9$, so that

$$a + 10b + 100c + \cdots = f(10) \equiv f(1) = a + b + c + \cdots \pmod 9.$$

Therefore we can test whether the integer $a + 10b + 100c + \cdots$ is divisible by 9 by testing whether the much smaller integer $a + b + c + \cdots$ is divisible by 9. In other words, if an integer is written in decimal notation, then it is divisible by 9 if and only if the sum of its digits is divisible by 9. This same test works for divisibility by 3 (by exercise 2.1.6) since 3 divides 9. For example, to decide whether 7361842509 is divisible by 9, we need only decide whether $7+3+6+1+8+4+2+5+0+9 = 45$ is divisible by 9, and this holds if and only if $4 + 5 = 9$ is divisible by 9, which it obviously is.

One can test for divisibility by 11 in a similar way: Since $10 \equiv -1 \pmod{11}$, we deduce that $f(10) \equiv f(-1) \pmod{11}$ from Corollary 2.3.1, and so

$$a + 10b + 100c + \cdots \equiv a - b + c \cdots \pmod{11}.$$

Therefore 7361842509 is divisible by 11 if and only if $7-3+6-1+8-4+2-5+0-9 = 1$ is divisible by 11, which it is not.

One may determine similar (but slightly more complicated) rules to test for divisibility by *any* integer, though we will need to develop our theory of congruences. We return to this theme in section 7.7.

Exercise 2.4.1. (a) Invent tests for divisibility by 2 and 5 (easy).
(b) Invent tests for divisibility by 7 and 13 (similar to the above).
(c)† Create one test that tests for divisibility by 7, 11, and 13 simultaneously (assuming that one knows about the divisibility by 7, 11, and 13 of every non-negative integer up to 1000).

Additional exercises

Exercise 2.5.1. Prove that if a, b, and c are integers and $d = b^2 - 4ac$, then $d \equiv 0$ or $1 \pmod 4$.

Exercise 2.5.2. Prove that if $N = a^2 - b^2$, then either N is odd or N is divisible by 4.

Exercise 2.5.3. (a) Prove that 2 divides $n(3n + 101)$ for every integer n.
(b) Prove that 3 divides $n(2n + 1)(n + 10)$ for every integer n.
(c) Prove that 5 divides $n(n + 1)(2n + 1)(3n + 1)(4n + 1)$ for every integer n.

Exercise 2.5.4. (a) Prove that, for any given integer $k \geq 1$, exactly k of any km consecutive integers is $\equiv a \pmod m$.
(b)† Let I be an interval of length N. Prove that the number of integers in I that are $\equiv a \pmod m$ is between $N/m - 1$ and $N/m + 1$.
(c) By considering the number of even integers in $(0, 2)$ and then in $[0, 2]$, show that (b) cannot be improved, in general.

Exercise 2.5.5. The *Universal Product Code* (that is, the bar code used to identify items in the supermarket) has 12 digits, each between 0 and 9, which we denote by $d_1, \ldots, d_{12}$. The first 11 digits identify the product. The 12th is chosen to be the least residue of

$$3d_1 - d_2 + 3d_3 - d_4 - \cdots - d_{10} + 3d_{11} \pmod{10}.$$

(a) Deduce that $d_1 + 3d_2 + d_3 + \cdots + d_{11} + 3d_{12}$ is divisible by 10.
(b) Deduce that if the scanner does not read all the digits correctly, then either the sum in (a) will not be divisible by 10 or the scanner has misread at least two digits.

Exercise 2.5.6. (a) Take $f(x) = x^2$ in Corollary 2.3.1 to determine the squares modulo m, for $m = 3, 4, 5, 6, 7, 8, 9$, and 10. ("The squares modulo m" are those congruence classes (mod m) that are equivalent to the square of at least one congruence class (mod m).)

(b) Show that there are no solutions in integers x, y, z to $x^2 + y^2 = z^2$ with x and y odd.
(c) Show that if $x^2 + y^2 = z^2$, then 3 divides xy.
(d) Show that there are no solutions in integers x, y, z to $x^2 + y^2 = 3z^2$ with $(x, y) = 1$.
(e) Show that there are no solutions in integers x, y, z to $x^2 + y^2 = 666z^2$ with $(x, y) = 1$.
(f) Prove that no integer $\equiv 7 \pmod 8$ can be written as the sum of three squares of integers.

Exercise 2.5.7.† Show that if $x^3 + y^3 = z^3$, then 7 divides xyz.

Binomial coefficients modulo p

We will assume that p is prime for all of the next two sections.

Exercise 2.5.8. Use the formula for $\binom{p}{j}$ given in (0.3.1) to prove that p divides $\binom{p}{j}$ for all integers j in the range $1 \le j \le p-1$. This implies that $\frac{1}{p}\binom{p}{j}$ is an integer.

For $1 \le j \le p-1$ we can write $\binom{p-1}{j}$ as $\frac{p-1}{1}\frac{p-2}{2}\cdots\frac{p-j}{j}$. There is considerable cancelation when we reduce this latter expression mod p.

Exercise 2.5.9. (a) Prove that $\binom{p-1}{j} \equiv (-1)^j \pmod p$ for all $j,\ 0 \le j \le p-1$.
(b) Prove that $\frac{1}{p}\binom{p}{j} \equiv (-1)^{j-1}/j \pmod p$ for all $j,\ 1 \le j \le p-1$.

Exercise 2.5.10.† (a) Prove that $\binom{ap}{bp} \equiv \binom{a}{b} \pmod p$ whenever $a, b \ge 0$.
(b) Prove that $\binom{ap+c}{bp+d} \equiv \binom{a}{b}\cdot\binom{c}{d} \pmod p$ whenever $0 \le c, d \le p-1$. (Remember that $\binom{c}{d} = 0$ if $c < d$.)
(c) If $m = m_0 + m_1 p + m_2 p^2 + \cdots + m_k p^k$ and $n = n_0 + n_1 p + \cdots + n_k p^k$ are non-negative integers written in base p, deduce *Lucas's Theorem* (by induction on $k \ge 0$), that

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\cdots\binom{n_k}{m_k} \pmod p.$$

One can extend the notion of congruences to polynomials with integer coefficients: For $f(x), g(x) \in \mathbb{Z}[x]$ we have $f(x) \equiv g(x) \pmod m$ if and only if there exists a polynomial $h(x) \in \mathbb{Z}[x]$ for which $f(x) - g(x) = mh(x)$. This notion can be extended even further to polynomials in several variables.

The binomial theorem for $n = 3$ gives

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

Notice that the two middle coefficients here are both 3, and so

$$(x+y)^3 \equiv x^3 + y^3 \pmod 3.$$

Similarly

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5 \equiv x^5 + y^5 \pmod 5,$$

since all four of the middle coefficients are divisible by 5. This does not generalize to all exponents n, for example for $n = 4$ we have $(x+y)^4 \equiv x^4 + 2x^2y^2 + y^4 \pmod 4$ which is not congruent to $x^4 + y^4 \pmod 4$, but the above does generalize to all prime exponents, as we will see in the next exercise.

Exercise 2.5.11. Deduce from exercise 2.5.8 that $(x+y)^p \equiv x^p + y^p \pmod p$ for all primes p.[7]

Exercise 2.5.12. Prove that $(x+y)^{p-1} \equiv x^{p-1} - yx^{p-2} + \cdots - xy^{p-2} + y^{p-1} \pmod p$.

[7] This is sometimes called the *freshman's dream* or the *child's binomial theorem*, sarcastically referring to the unfortunately common mistaken belief that this works over $\mathbb{C}$, rather than the more complicated binomial theorem, as in section 0.3.

Exercise 2.5.13. Prove that $(x+y)^{p^k} \equiv x^{p^k} + y^{p^k} \pmod{p}$ for all primes p and integers $k \geq 1$.

Exercise 2.5.14. (a) Writing a positive integer $n = n_0 + n_1 p + n_2 p^2 + \cdots$ in base p, use exercise 2.5.13 to prove that

$$(x+y)^n \equiv (x+y)^{n_0}(x^p + y^p)^{n_1}(x^{p^2} + y^{p^2})^{n_2} \cdots \pmod{p}.$$

(b)† Reprove Lucas's Theorem (as in exercise 2.5.10(c)) by studying the coefficient of $x^m y^{n-m}$ in (a).

Exercise 2.5.15. (a) Prove that $(x+y+z)^p \equiv x^p + y^p + z^p \pmod{p}$.
(b) Deduce that $(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod{p}$ for all $n \geq 2$.

The Fibonacci numbers modulo d

The Fibonacci numbers mod 2 are

$$0,\ 1,\ 1,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1, \ldots.$$

We see that the Fibonacci numbers modulo 2 are periodic of period 3. The Fibonacci numbers mod 3 are

$$0,\ 1,\ 1,\ 2,\ 0,\ 2,\ 2,\ 1,\ 0,\ 1,\ 1,\ 2,\ 0,\ 2,\ 2,\ 1,\ \ldots$$

and so seem to be periodic of period 8. In exercise 1.7.24 we defined $m = m_d$ to be the smallest positive integer for which d divides F_m and showed that d divides F_n if and only if m_d divides n. In our two cases we therefore have $m_2 = 3$ which is the period and $m_3 = 4$ which is half the period.

In the next exercise we show that Fibonacci numbers (and other such sequences) are periodic mod d, for every integer $d > 1$, by using the *pigeonhole principle*. This states that if one puts $N+1$ letters into N pigeonholes, then, no matter how one does this, some pigeonhole will contain at least two letters.[8]

Exercise 2.5.16. (a) Prove that the pigeonhole principle is true.
We will now show that the Mersenne numbers $M_n := 2^n - 1$ are periodic mod d.
(b) Show that there exist two integers in the range $0 \leq r < s \leq d$ for which $M_r \equiv M_s \pmod{d}$.
(c) In exercise 0.4.15(b) we saw that the Mersenne numbers satisfy the recurrence $M_{n+1} = 2M_n + 1$. Use this to show that $M_{r+j} \equiv M_{s+j} \pmod{d}$ for all $j \geq 0$.
(d) Deduce that there exists a positive integer $p = p_d$, which is $\leq d$, such that $M_{n+p} \equiv M_n \pmod{d}$ for all $n \geq d$. That is, M_n is *eventually periodic* mod d with period $p_d \leq d$.

An analogous proof works for general second-order linear recurrence sequences, including Fibonacci numbers. For the rest of this section, we suppose a and b are integers and $\{x_n :\ n \geq 0\}$ is the second-order linear recurrence sequence given by

$$x_n = ax_{n-1} + bx_{n-2} \text{ for all } n \geq 2 \text{ with } x_0 = 0 \text{ and } x_1 = 1.$$

Exercise 2.5.17. (a) By using the pigeonhole principle creatively, prove that there exist two integers in the range $0 \leq r < s \leq d^2$ for which $x_r \equiv x_s \pmod{d}$ *and* $x_{r+1} \equiv x_{s+1} \pmod{d}$.
(b) Use the recurrence for the x_n to show that $x_{r+j} \equiv x_{s+j} \pmod{d}$ for all $j \geq 0$.
(c) Deduce that the x_n are eventually periodic mod d with period $\leq d^2$.
(d) Prove that m_d divides the period mod d.

[8] In French, this is the "principle of the drawers". What invocative metaphors are used to describe this principle in other languages?

We saw above that the Fibonacci numbers mod 3 have period 3^2-1, and further calculations reveal that the period mod d never seems to be larger than d^2-1, a small improvement over the bound that we obtained in exercise 2.5.17(c). In the next exercise we see how to obtain this bound, in general.

Exercise 2.5.18. (a) Show that if there exists a positive integer r for which $x_r \equiv x_{r+1} \equiv 0 \pmod{d}$, then $x_n \equiv 0 \pmod{d}$ for all $n \geq r$ so that the x_n are eventually periodic mod d with period 1.

(b) Now assume that there does not exist a positive integer r for which $x_r \equiv x_{r+1} \equiv 0 \pmod{d}$. Modify the proof of exercise 2.5.17 to prove that the x_n are eventually periodic mod d with period $\leq d^2-1$.

It is possible to get a more precise understanding of the Fibonacci numbers and other second-order recurrences, mod d:

Exercise 2.5.19. In order to understand $x_n \pmod{d}$, we take $m = m_d$ in the results of this exercise.

(a) Prove, by induction, that $x_{m+k} \equiv x_{m+1}x_k \pmod{x_m}$ for all $k \geq 0$.

(b) Deduce the same result from exercise 0.4.10.

(c) Deduce that if $n = qm + r$ with $0 \leq r \leq m-1$, then $x_n \equiv (x_{m+1})^q x_r \pmod{x_m}$.

We will return to this result in chapter 7 where we study the powers mod n.

In exercise 0.1.5 we saw the importance of the discriminant[9] $\Delta := a^2 + 4b$ of the quadratic polynomial $x^2 - ax - b$. The rule for the x_n mod Δ is a little easier:

Exercise 2.5.20. Prove by induction that

(a) $x_{2k} \equiv ka(-b)^{k-1} \pmod{\Delta}$ and $x_{2k+1} \equiv (2k+1)(-b)^k \pmod{\Delta}$ for all $k \geq 0$ and

(b) $x_{2k} \equiv kab^{k-1} \pmod{a^2}$ and $x_{2k+1} \equiv b^k \pmod{a^2}$ for all $k \geq 0$.

Exercise 2.5.21. Suppose that the sequence $(u_n)_{n\geq 1}$ satisfies a dth-order linear recurrence (as defined in appendix 0B). Prove that for any integer $m > 1$, the u_n are eventually periodic mod m with period $\leq m^d - 1$. (We prove that this bound is best possible when m is prime in exercise 7.25.5.)

[9] The colon ":" plays many roles in the grammar of mathematics. Here it means that "Henceforth we define Δ to be ...."

Appendix 2A. Congruences in the language of groups

2.6. Further discussion of the basic notion of congruence

Congruences can be rephrased in the language of groups. The integers, $\mathbb{Z}$, form a group,[10] in which addition is the group operation. In exercise 0.11.1 of appendix 0D we proved that the non-trivial, proper subgroups of $\mathbb{Z}$ all take the form $m\mathbb{Z} := \{mn : \ n \in \mathbb{Z}\}$ for some integer $m > 1$, that is, the set of integers divisible by m. The congruence classes (mod m) are simply the *cosets* of $m\mathbb{Z}$ inside $\mathbb{Z}$:

$$0 + m\mathbb{Z}, \ 1 + m\mathbb{Z}, \ 2 + m\mathbb{Z}, \ldots, \ (m-1) + m\mathbb{Z},$$

where

$$j + m\mathbb{Z} := \{j + mn : \ n \in \mathbb{Z}\},$$

which is the set of integers belonging to the congruence class $j \pmod m$. Notice that the m cosets of $m\mathbb{Z}$ are disjoint and their union gives all of $\mathbb{Z}$.

The group operation on $\mathbb{Z}$, namely addition, is inherited by the cosets of $m\mathbb{Z}$. For example, as $7 + 11 = 18$ in $\mathbb{Z}$, the same is true when we add together the relevant cosets of $m\mathbb{Z}$ in $\mathbb{Z}$; in other words,[11]

$$(7 + m\mathbb{Z}) + (11 + m\mathbb{Z}) \ = \ (18 + m\mathbb{Z}).$$

This new additive group is the *quotient group*

$$\mathbb{Z}/m\mathbb{Z}.$$

This is the beginning of the theory of quotient groups, which we develop in the next section.

[10] See appendix 0D for a discussion of the basic properties of groups.

[11] Throughout, we define the sum of two given sets A and B to be $A + B := \{a + b : \ a \in A, b \in B\}$, that is, the set of elements that can be represented as $a + b$ with $a \in A$ and $b \in B$. Note that an element may be represented more than once.

The reader should be aware that multiplication mod m (and, in particular, how its properties are inherited from $\mathbb{Z}$) does not fit into this discussion of additive quotient groups.

2.7. Cosets of an additive group

Suppose that H is a subgroup of an additive (and so abelian[12]) group G. A *coset* of H in G is given by the set

$$a + H := \{a + h : \ h \in H\}.$$

In Proposition 2.7.1 we will show, as in the example $m\mathbb{Z}$ of the previous section, that the cosets of H are all disjoint and their union gives G.

The *quotient group* G/H has as its elements the distinct cosets $a + H$ and inherits its group law from G, in this case addition, so that

$$(a + H) + (b + H) = (a + b) + H.$$

Proposition 2.7.1. *Let H be a subgroup of an additive group G. The cosets of H in G are disjoint, so that the elements of G/H are well-defined; and the addition law on G/H is also well-defined. If G is finite, then $|H|$ divides $|G|$ and $|G/H| = |G|/|H|$.*

Proof. If $a+H$ and $b+H$ have a common element c, then there exists $h_1, h_2 \in H$ such that $a + h_1 = c = b + h_2$. Therefore $b = a + h_1 - h_2 = a + h_0$ where $h_0 = h_1 - h_2 \in H$ since H is a group (and therefore closed under addition). Now if $h \in H$, then $b+h = a+(h_0+h) \in a+H$, as $h_0+h \in H$, so that $b+H \subset a+H$, and by the analogous argument $a+H \subset b+H$. We deduce that $a+H = b+H$. Hence the cosets of H are either identical or disjoint, which means that they partition G; therefore if G is finite, then $|H|$ divides $|G|$.

This also implies that if $c \in a+H$, then $c+H = a+H$. We wish to show that addition in G/H is well-defined. If $a + H,\ b + H$ are cosets of H, then we defined $(a+H)+(b+H) = (a+b)+H$, so we need to verify that the sum of the two cosets does not depend on the choice of representatives of the cosets. So, if $c \in a+H$ and $d \in b+H$, then there exists $h_1, h_2 \in H$ for which $c = a+h_1$ and $d = b+h_2$. Then $c+H = a+H$ and $d+H = b+H$. Moreover $c+d = a+b+(h_1+h_2) \in a+b+H$, as H is closed under addition, and so $c+d+H = a+b+H$, as desired. Hence G/H is well-defined, and $|G/H| = |G|/|H|$ when G is finite. □

Example. $\mathbb{Z}$ is a subgroup of the additive group $\mathbb{R}$, and the cosets $a+\mathbb{Z}$ are given by all real numbers r that differ from a by an integer. Every coset $a+\mathbb{Z}$ has exactly one representative in any given interval of length 1, in particular the interval $[0, 1)$ where the coset representative is $\{a\}$, the fractional part of a. These cosets are well-defined under addition and yield the quotient group $\mathbb{R}/\mathbb{Z}$.

The *exponential map* $e : \mathbb{R} \to U := \{z \in \mathbb{C} : \ |z| = 1\}$, from the real numbers to the unit circle, is defined by $e(t) = e^{2i\pi t}$. Since $e(1) = 1$, therefore $e(n) = e(1)^n = 1$ for every integer n. Therefore if $b \in a + \mathbb{Z}$ so that $b = a + n$ for some integer n, then $e(b) = e(a + n) = e(a)e(n) = e(a)$, so the value of $e(t)$ depends only what

[12] A group G is called *abelian* or *commutative* if $ab = ba$ for all elements $a, b \in G$.

coset t belongs to in $\mathbb{R}/\mathbb{Z}$. Therefore we can think of the exponential map as the concatenation of two maps: firstly the natural quotient map from $\mathbb{R} \to \mathbb{R}/\mathbb{Z}$ (that is, $a \to a + \mathbb{Z}$) and then the map $e : \mathbb{R}/\mathbb{Z} \to U$. Picking the representatives $[0, 1)$ for $\mathbb{R}/\mathbb{Z}$, we see that the restricted map $e : [0, 1) \to U$ is 1-to-1.

By a slight abuse of terminology, we let $a \equiv b \pmod 1$, for real numbers a and b, if and only if a and b belong to the same coset of $\mathbb{R}/\mathbb{Z}$.

Exercise 2.7.1. Prove that $a \equiv b \pmod m$ if and only if a/m and b/m belong to the same coset of $\mathbb{R}/\mathbb{Z}$.

Exercise 2.7.2. (a) Prove that $t \equiv \{t\} \pmod 1$ for all real numbers t.
(b) Prove that the usual rules of addition, subtraction, and multiplication hold mod 1.
(c) Show that division is not always well-defined mod 1, by finding a counterexample.

2.8. A new family of rings and fields

We have seen, in Lemma 2.1.1, that the congruence classes mod m support both an additive and multiplicative structure.

Exercise 2.8.1. Prove that $\mathbb{Z}/m\mathbb{Z}$ is a ring for all integers $m \geq 2$.

To be a field, all the non-zero congruence classes of $\mathbb{Z}/m\mathbb{Z}$ would need to have a multiplicative inverse, but this is not the case for all m. For example we claim that 3 does not have a multiplicative inverse mod 15. If it did, say $3m \equiv 1 \pmod{15}$, then multiplying through by 5 we obtain $5 \equiv 5 \cdot 1 \equiv 5 \cdot 3m \equiv 0 \pmod{15}$, which is evidently untrue.

We call 3 and 5 *zero divisors* since they non-trivially divide 0 in $\mathbb{Z}/15\mathbb{Z}$.

Exercise 2.8.2. (a) Prove that if m is a composite integer > 1, then $\mathbb{Z}/m\mathbb{Z}$ has zero divisors.
(b) Prove that $\mathbb{Z}/m\mathbb{Z}$ is not a field whenever m is a composite integer > 1.
(c) Prove that if R is any ring with zero divisors, then R cannot be a field.

An *integral domain* is a ring with no zero divisors. Note that $\mathbb{Z}$ is an integral domain (hence the name) but is not a field.

If R is a commutative ring and $m \in R$, then mR is an additive subgroup of R, and the cosets of mR support a multiplicative structure. To see this, note that if $x \in a + mR$ and $y \in b + mR$, then $x = a + mr_1$ and $y = b + mr_2$ for some $r_1, r_2 \in R$, and so $xy = ab + mr$ where $r = ar_2 + br_1 + mr_1r_2$ which belongs to R, as R is closed under both addition and multiplication. That is, $xy \in ab + mR$. Hence R/mR inherits the multiplicative and distributive properties of R, as well as the identity element $1 + mR$; and so R/mR is itself a commutative ring.

2.9. The order of an element

If g is an element of a given group G, we define the *order* of g to be the smallest integer $n \geq 1$ for which $g^n = 1$, where 1 is the identity element of G. If n does not exist, then we say that g has infinite order (for example, 1 in the additive group $\mathbb{Z}$). We shall explore the multiplicative order of a reduced residue mod m, in detail, in chapter 7.

There is a beautiful observation of Lagrange which restricts the possible order of an element in any finite abelian group.

Theorem 2.2 (Lagrange)**.** *If G is a finite abelian group, then the order of any element g of G divides $|G|$, the number of elements in G. Moreover, $g^{|G|} = 1$.*

Proof. Suppose that g has order n and let $H := \{1, g, g^2, \ldots, g^{n-1}\}$, a subgroup of G of order n. By Proposition 2.7.1 we deduce that $n = |H|$ divides $|G|$. Moreover if $|G| = mn$, then $g^{|G|} = g^{mn} = (g^n)^m = 1^m = 1$. □

Lagrange's Theorem actually holds for any finite group, non-abelian as well as abelian, as we will see in Corollary 7.23.1 of appendix 7D.

Appendices. The extended version of chapter 2 has the following additional appendix:

Appendix 2B. *The Euclidean algorithm for polynomials*, which shows that there is an analogous theory for polynomials.

Chapter 3

The basic algebra of number theory

A *prime number* is an integer $n > 1$ whose only positive divisors are 1 and n. Hence $2, 3, 5, 7, 11, \ldots$ are primes. An integer $n > 1$ is *composite* if it is not prime.[1]

Exercise 3.0.1. Suppose that p is a prime number. Prove that $\gcd(p, a) = 1$ if and only if p does not divide a.

3.1. The Fundamental Theorem of Arithmetic

Positive integers factor into primes, the basic building blocks out of which integers are made. Often, in school, one discovers this by factoring a given composite integer into two parts and then factoring each of those parts that are composite into two further parts, etc. For example $120 = 8 \times 15$, and then $8 = 2 \times 4$ and $15 = 3 \times 5$. Now 2, 3, and 5 are all primes, but $4 = 2 \times 2$ is not. Putting this altogether gives $120 = 2 \times 2 \times 2 \times 3 \times 5$. This can be factored no further since 2, 3, and 5 are all primes. It is not difficult to prove that this always works:

Exercise 3.1.1. Prove that any integer $n > 1$ can be factored into a product of primes.

We can factor 120 in other ways. For example $120 = 4 \times 30$, and then $4 = 2 \times 2$ and $30 = 5 \times 6$. Finally noting that $6 = 2 \times 3$, we eventually obtain the same factorization, $120 = 2 \times 2 \times 2 \times 3 \times 5$, of 120 into primes, even though we arrived at it in a different way. No matter how you go about splitting a positive integer up into its factors, you will always end up with the same factorization into primes.[2] If it is true that any two such factorizations are indeed the same and if we are given one factorization of n as $q_1 \cdots q_k$, then every prime factor p of n, found in any other way, must equal some q_i. This suggests that we will need to prove Theorem 3.1.

[1] Notice that 1 is neither prime nor composite, and the same is true of 0 and all negative integers.

[2] Recognizing that this claim needs a proof and then supplying a proof, is one of the great achievements of Greek mathematics. They developed an approach to mathematics which assures that theorems are established on a solid basis.

Theorem 3.1. *If prime p divides ab, then p must divide at least one of a and b.*

We will prove this in the next subsection. The necessity of such a result was appreciated by ancient Greek mathematicians, who went on to show that Theorem 3.1 is sufficient to establish that every integer has a unique factorization, as we will see. It is best to begin by making a simple deduction from Theorem 3.1:

Exercise 3.1.2. (a) Prove that if prime p divides $a_1a_2\cdots a_k$, then p divides a_j for some j, $1 \le j \le k$.
(b) Deduce that if prime p divides $q_1\cdots q_k$ where each q_i is prime, then $p = q_j$ for some j, $1 \le j \le k$.

With this preparation we are ready to prove the first great theorem of number theory, which appears in Euclid's "*Elements*":[3]

Theorem 3.2 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ can be written as a product of primes in a unique way (up to reordering).*

Proof. We first show that there is a factorization of n into primes and afterwards we will prove that it is unique. We prove this by induction on n: If n is prime, then we are done; since 2 and 3 are primes, this also starts our induction hypothesis. If n is composite, then it must have a divisor a for which $1 < a < n$, and so $b = n/a$ is also an integer for which $1 < b < n$. Then, by the induction hypothesis, both a and b can be factored into primes, and so $n = ab$ equals the product of these two factorizations. (For example, to prove the result for 1050, we note that $1050 = 15\times70$. We have already obtained the factorizations of 15 and 70, namely $15 = 3\times5$ and $70 = 2\times5\times7$, so that $1050 = 15\times70 = (3\times5)\times(2\times5\times7) = 2\times3\times5\times5\times7$.)

Now we prove that there is just one factorization for each $n \ge 2$. If this is not true, then let n be the smallest integer ≥ 2 that has two distinct factorizations,

$$p_1p_2\cdots p_r \;=\; q_1q_2\cdots q_s,$$

where the p_i and q_j are (not necessarily distinct) primes. Now prime p_r divides $q_1q_2\cdots q_s$, and so $p_r = q_j$ for some j, by exercise 3.1.2(b). Reordering the q_j if necessary we may assume that $j = s$, and if we divide through both factorizations by $p_r = q_s$, then we have two distinct factorizations of

$$n/p_r \;=\; p_1p_2\cdots p_{r-1} \;=\; q_1q_2\cdots q_{s-1}.$$

This contradicts the minimality of n unless $n/p_r = 1$. But then $n = p_r$ is prime, and by the definition (of primes) it can have no other factorization. □

The *Fundamental Theorem of Arithmetic* states that there is a unique way to break down an integer into its fundamental (i.e., irreducible) parts, and so every integer can be viewed simply in terms of these parts (i.e., its prime factors). On the other hand any finite product of primes equals an integer, so there is a 1-to-1 correspondence between positive integers and finite products of primes, allowing one to translate questions about integers into questions about primes and vice versa.

[3]When we write that a product of primes is "unique up to reordering" we mean that although one can write 12 as $2\times2\times3$ or $2\times3\times2$ or $3\times2\times2$, we think of all of these as the same product, since they involve the same primes, each the same number of times, differing only in the way that we order the prime factors.

It is useful to write the factorizations of natural numbers n in a standard form, like

$$n = 2^{n_2}3^{n_3}5^{n_5}7^{n_7}\dots,$$

where n_p denotes the exact number of times the prime p divides n. Since n is an integer, each $n_p \geq 0$, and only finitely many of the n_p are non-zero. Usually we write down only those prime powers where $n_p \geq 1$, for example $12 = 2^2 \cdot 3$ and $50 = 2 \cdot 5^2$. We will write $p^e \| n$ if p^e is the highest power of p that divides n; thus $5^2 \| 50$ and $11^1 \| 1001$.

Our proof of the *Fundamental Theorem of Arithmetic* is constructive but it does not provide an efficient way to find the prime factors of a given integer n. Indeed finding efficient techniques for factoring an integer is a difficult and important problem, which we discuss in chapter 10.[4]

In particular, the known difficulty of factoring large integers underlies the security of the RSA cryptosystem, which is discussed in section 10.3.

Exercise 3.1.3. (a) Prove that every natural number has a unique representation as $2^k m$ with $k \geq 0$ and m an odd natural number.
(b) Show that each integer $n \geq 3$ is either divisible by 4 or has at least one odd prime factor.
(c) An integer is *squarefree* if every prime in its factorization appears to the power 1. Prove that every non-zero integer can be written, uniquely, in the form mn^2 where m is a squarefree integer and n is a non-zero positive integer.
(d)† Deduce that every non-zero rational number can be written, uniquely, in the form mr^2 where m is a squarefree integer and r is a positive rational number.

Exercise 3.1.4. (a) Show that if all of the prime factors of an integer n are $\equiv 1 \pmod m$, then $n \equiv 1 \pmod m$. Deduce that if $n \not\equiv 1 \pmod m$ then n has a prime factor that is $\not\equiv 1 \pmod m$.
(b)† Show that if all of the prime factors of an integer n are $\equiv 1$ or $3 \pmod 8$, then $n \equiv 1$ or $3 \pmod 8$. Prove this with 3 replaced by 5 or 7.
(c)† Generalize this as much as you can to other moduli and other sets of congruence classes.

3.2. Abstractions

The ancient Greek mathematicians recognized that abstract lemmas allowed them to *prove* sophisticated theorems. For example, in the previous section we stated Theorem 3.1, a result whose formulation is not obviously relevant and yet was used to good effect. The archetypal lemma is known today as "Euclid's Lemma", an important result that first appeared in Euclid's "*Elements*" (Book VII, No. 32), and we will see that it is even more useful than Theorem 3.1:

Theorem 3.3 (Euclid's Lemma)**.** *If c divides ab and $\gcd(c, a) = 1$, then c must divide b.*

[4]It is easy enough to multiply together two given integers. If the integers each have 50 digits, then one can obtain the product in about 3,000 steps (digit-by-digit multiplications) and this can be accomplished within a second on a computer. On the other hand, given the 100-digit product, how do we factor it to find the original two 50-digit integers? Trial division is too slow ... if every atom in the universe were a computer as powerful as any supercomputer, then most such products would not be factored before the end of the universe! This is why we need more sophisticated factoring methods, and although the best ones known today, implemented on the best computers, can factor a 100-digit number in reasonable time, they are currently incapable of factoring typical 200-digit numbers. (See sections 10.4 and 10.6 for further discussion on this theme.)

Proof of Euclid's Lemma. Since $\gcd(c,a)=1$ there exist integers m and n such that $cm+an=1$ by Theorem 1.1. Now c divides both c and ab, so that

$$c \text{ divides } c\cdot bm+ab\cdot n=b(cm+an)=b,$$

by exercise 1.1.1(c). □

This proof surprisingly uses, inexplicitly, the complicated construction from Euclid's algorithm. Now that we have proved Euclid's Lemma we proceed to

Deduction of Theorem 3.1. Suppose that prime p does not divide a (or else we are done), and so $\gcd(p,a)=1$ (as seen in exercise 3.0.1). Taking $c=p$ in Euclid's Lemma, we deduce that p divides b. □

The hypothesis "$\gcd(c,a)=1$" in Euclid's Lemma is necessary, as may be seen from the example in which 4 divides $2\cdot 6$, but 4 does not divide either 2 or 6.

Now that we have completed the proof of the Fundamental Theorem of Arithmetic, we are ready to develop the basic number-theoretic properties of integers.[5] We begin by noting one further important consequence of Euclid's Lemma:

Corollary 3.2.1. *If $am=bn$, then $a/\gcd(a,b)$ divides n.*

Proof. Let $a/\gcd(a,b)=A$ and $b/\gcd(a,b)=B$ so that $(A,B)=1$ by exercise 1.2.5(a) and $Am=Bn$. Therefore $A|Bn$ with $(A,B)=1$, and so $A|n$ by Euclid's Lemma, as desired. We also observe that if we write $n=Ak$ for some integer k, then $m=Bn/A=Bk$. □

One consequence is a simple way to determine the least common multiple of two integers from knowing their greatest common divisor.

Corollary 3.2.2. *For any positive integers a and b we have $ab=\gcd(a,b)\cdot\operatorname{lcm}(a,b)$.*

Proof. By definition, there exist integers m and n for which $am=bn=\operatorname{lcm}[a,b]$. By Corollary 3.2.1 we know that $a/\gcd(a,b)$ divides n and so $L:=b\cdot a/\gcd(a,b)$ divides $bn=\operatorname{lcm}[a,b]$. Therefore $L\le\operatorname{lcm}[a,b]$. On the other hand L is a multiple of b, by definition, and of a, since $L=a\cdot b/\gcd(a,b)$. Therefore L is a common multiple of a and b, and so $L\ge\operatorname{lcm}[a,b]$ by the definition of lcm. These two inequalities imply that $L=\operatorname{lcm}[a,b]$, and the result follows by multiplying through by the denominator. □

We will see an easier proof of this elegant result in exercise 3.3.2.

Exercise 3.2.1. Suppose that $(a,b)=1$. Prove that if a and b both divide m, then ab divides m.

[5] However if we wish to develop the analogy of this theory for more complicated sets of numbers, for example the numbers of the form $\{a+b\sqrt{d}:\ a,b\in\mathbb{Z}\}$ for some fixed large integer d, then Euclid's Lemma generalizes in a straightforward way, but the Fundamental Theorem of Arithmetic does not. We discuss this further in appendix 3F.

3.3. Divisors using factorizations

Suppose that[6]

$$n = \prod_{p \text{ prime}} p^{n_p}, \quad a = \prod_{p} p^{a_p}, \quad \text{and} \quad b = \prod_{p} p^{b_p}.$$

If $n = ab$, then

$$2^{n_2}3^{n_3}5^{n_5}\cdots \;=\; 2^{a_2}3^{a_3}5^{a_5}\cdots 2^{b_2}3^{b_3}5^{b_5}\cdots \;=\; 2^{a_2+b_2}3^{a_3+b_3}5^{a_5+b_5}\cdots .$$

As there is only one factorization into primes of a given positive integer, by the Fundamental Theorem of Arithmetic, we can equate the exact power of prime p dividing each side of the last equation, to deduce that

$$n_p = a_p + b_p \;\text{ for each prime } p.$$

As $a_p, b_p \geq 0$ for each prime p, therefore

$$0 \leq a_p,\; b_p \leq n_p \;\text{ for each prime } p.$$

On the other hand if $a = 2^{a_2}3^{a_3}5^{a_5}\cdots$ with each $0 \leq a_p \leq n_p$, then a divides n since we can construct the integer

$$b = 2^{n_2-a_2}3^{n_3-a_3}5^{n_5-a_5}\cdots$$

for which $n = ab$. We have therefore classified all of the possible (positive integer) divisors a of n.

This classification allows us to easily count the number of divisors a of n, since this is equal to the number of possibilities for the exponents a_p; and we have that each a_p is any integer in the range $0 \leq a_p \leq n_p$. There are, therefore, $n_p + 1$ possibilities for the exponent a_p, for each prime p, making

$$(n_2 + 1)(n_3 + 1)(n_5 + 1)\cdots$$

possible divisors in total. Hence if we write $\tau(n)$ for the number of divisors of n, then

$$\tau(n) = \prod_{\substack{p \text{ prime} \\ p^{n_p} \| n}} \tau(p^{n_p});$$

and $\tau(p^k) = k + 1$ for all integers $k \geq 0$. A function whose value at n equals the product of the values of the function at the exact prime powers that divide n is called a *multiplicative function* (which will be explored in detail in the next chapter).

As an example, we see that the divisors of $175 = 5^2 7^1$ are given by

$$5^0 7^0 = 1,\; 5^1 7^0 = 5,\; 5^2 7^0 = 25,\; 5^0 7^1 = 7,\; 5^1 7^1 = 35,\; 5^2 7^2 = 175;$$

in other words, they can all be factored as

$$5^0, 5^1, \text{ or } 5^2 \;\text{ times }\; 7^0 \text{ or } 7^1.$$

Therefore the number of divisors is $(2 + 1) \times (1 + 1) = 3 \times 2 = 6$.

Use the Fundamental Theorem of Arithmetic in all of the remaining exercises in this section.

[6] We suppress writing "prime" in the subscript of $\prod$, for convenience, at least when it should be obvious, from the context, that the parameter is only taking prime values.

Exercise 3.3.1. Use the description of the divisors of a given integer to prove the following: If $m = \prod_p p^{m_p}$ and $n = \prod_p p^{n_p}$ are positive integers, then (a) $\gcd(m,n) = \prod_p p^{\min\{m_p,n_p\}}$ and (b) $\operatorname{lcm}[m,n] = \prod_p p^{\max\{m_p,n_p\}}$.

The method in exercise 3.3.1(a) for finding the gcd of two integers appears to be much simpler than the Euclidean algorithm. However, in order to make this method work, one needs to be able to factor the integers involved. We have not yet discussed techniques for factoring integers (though we will in chapter 10). Factoring is typically difficult for large integers. This difficulty limits when we can, in practice, use exercise 3.3.1 to determine gcds and lcms. On the other hand, the Euclidean algorithm is very efficient for finding the gcd of two given integers (as discussed in appendix 1B) without needing to know anything about those numbers.

Exercise 3.3.2. Deduce that $mn = \gcd(m,n) \cdot \operatorname{lcm}[m,n]$ for all pairs of natural numbers m and n using exercise 3.3.1. (The proof in Corollary 3.2.2 is more difficult.)

In combination with the Euclidean algorithm, the result in exercise 3.3.2 allows us to quickly and easily calculate the lcm of any two given integers. For example, to determine $\operatorname{lcm}[12,30]$, we first use the Euclidean algorithm to show that $\gcd(12,30) = 6$, and then $\operatorname{lcm}[12,30] = 12 \cdot 30/\gcd(12,30) = 360/6 = 60$.

Although we have already proved the results in the next exercise (exercise 1.2.1(a), Lemma 1.4.1, exercise 1.2.5(a), and Corollary 1.2.2), we can now reprove them more easily by using our description of the divisors of a given integer.

Exercise 3.3.3. (a) Prove that d divides $\gcd(a,b)$ if and only if d divides both a and b.
(b) Prove that $\operatorname{lcm}[a,b]$ divides m if and only if a and b both divide m.
(c) Prove that if $(a,b) = g$, then $(a/g, b/g) = 1$.
(d) Prove that if $(a,m) = (b,m) = 1$, then $(ab,m) = 1$.
(e) Prove that if $(a,b) = 1$, then $(ab,m) = (a,m)(b,m)$.
(f)† Show that the hypothesis $(a,b) = 1$ is necessary in part (e), by constructing a counterexample to the conclusion when $(a,b) > 1$.

One can obtain the gcd and lcm for any number of integers by means similar to exercise 3.3.1:

Example. If $A = 504 = 2^3 \cdot 3^2 \cdot 7$, $B = 2880 = 2^6 \cdot 3^2 \cdot 5$, and $C = 864 = 2^5 \cdot 3^3$, then the greatest common divisor is $2^3 \cdot 3^2 = 72$ and the least common multiple is $2^6 \cdot 3^3 \cdot 5 \cdot 7 = 60480$. That is, if the powers of prime p that divide A, B, and C are a_p, b_p, and c_p, respectively, then the powers of p that divide the gcd and lcm are $\min\{a_p, b_p, c_p\}$ and $\max\{a_p, b_p, c_p\}$, respectively.

Exercise 3.3.4. Prove that $\gcd(a,b,c) = \gcd(a, \gcd(b,c))$ and $\operatorname{lcm}[a,b,c] = \operatorname{lcm}[a, \operatorname{lcm}[b,c]]$.

Exercise 3.3.5. Prove that if each of $a, b, c, \ldots$ is coprime with m, then so is $abc\ldots$.

The representation of an integer in terms of its prime power factors can be useful when considering powers of integers:

Exercise 3.3.6. Prove that if prime p divides a^n, then p^n divides a^n.

Exercise 3.3.7. (a) Prove that a positive integer A is the square of an integer if and only if the exponent of each prime factor of A is even.
(b) Prove that if $a, b, c, \ldots$ are pairwise coprime, positive integers and their product is a square, then they are each a square.

(c) Prove that if ab is a square, then either $a = gA^2$ and $b = gB^2$, or $a = -gA^2$ and $b = -gB^2$, where $g = \gcd(a, b)$, for some coprime integers A and B.

Exercise 3.3.8. (a) Prove that a positive integer A is the nth power of an integer if and only if n divides the exponent of all of the prime power factors of A.

(b) Prove that if $a, b, c, \ldots$ are pairwise coprime, positive integers and their product is an nth power, then they are each an nth power.

3.4. Irrationality

One of the most beautiful applications of the Fundamental Theorem of Arithmetic is its use in showing that there are real irrational numbers,[7] the easiest example being $\sqrt{2}$:

Proposition 3.4.1. *The real number $\sqrt{2}$ is irrational. That is, there is no rational number a/b for which $\sqrt{2} = a/b$.*

Proof. We will assume that $\sqrt{2}$ is rational and find a contradiction. If $\sqrt{2}$ is rational, then we can write $\sqrt{2} = a/b$ where a and $b \geq 1$ are coprime integers by exercise 1.2.5(b). We have $a = b\sqrt{2} > 0$.

Now $a = b\sqrt{2}$ and so $a^2 = 2b^2$. If we factor

$$a = \prod_p p^{a_p} \quad \text{and} \quad b = \prod_p p^{b_p}, \quad \text{then} \quad \prod_p p^{2a_p} = a^2 = 2b^2 = 2\prod_p p^{2b_p},$$

where the a_p's and b_p's are all integers. The exponent of the prime 2 in the factorization of $a^2 = 2b^2$ is $2a_2 = 1 + 2b_2$ which is impossible (mod 2), giving a contradiction. Hence $\sqrt{2}$ cannot be rational. □

More generally we have, by a different proof,

Proposition 3.4.2. *If d is an integer for which $\sqrt{d}$ is rational, then $\sqrt{d}$ is an integer. Therefore if integer d is not the square of an integer, then $\sqrt{d}$ is irrational.*

Proof. We may write $\sqrt{d} = a/b$ where a and b are coprime positive integers, so that $a^2 = db^2$. Now $(a^2, b^2) = 1$ and a^2 divides db^2, which implies that a^2 divides d, by Euclid's Lemma. But then $d \leq db^2 = a^2 \leq d$, implying that $d = a^2$; that is, d is the square of an integer as claimed. □

Exercise 3.4.1. Give a proof of Proposition 3.4.2, which is analogous to the proof of Proposition 3.4.1 above.

Exercise 3.4.2.† Prove that $17^{1/3}$ is irrational (using the ideas of the proof of Proposition 3.4.1).

The proof of Proposition 3.4.2 generalizes to give a nice application of Euclid's Lemma to rational roots of arbitrary polynomials with integer coefficients:

Theorem 3.4 (The rational root criterion)**.** *Suppose $f(x)$ is a polynomial with integer coefficients, with leading coefficient a_d and last coefficient a_0. If $f(m/n) = 0$ where m and n are coprime integers, then m divides a_0 and n divides a_d.*

[7] That is, real numbers that are not rational.

Proof. Writing $f(x) = \sum_{j=0}^{d} a_j x^j$ where each $a_j \in \mathbb{Z}$ we have

$$a_d m^d + a_{d-1} m^{d-1} n + \cdots + a_1 m n^{d-1} + a_0 n^d = n^d f(m/n) = 0.$$

Reducing this equation mod n gives $a_d m^d \equiv 0 \pmod{n}$ as every other term on the left-hand side is divisible by n. This can be restated as n divides $a_d m^d$. By the hypothesis, we have $(n, m) = 1$ and so $(n, m^d) = 1$ by exercise 1.7.11. Therefore n divides $a_d m^d$ and $(n, m^d) = 1$, which implies that n divides a_d by Euclid's Lemma. We complete the proof by establishing

Exercise 3.4.3. Prove that m divides a_0 by reducing the above equation mod m. □

Corollary 3.4.1. *If a monic polynomial $f(x) \in \mathbb{Z}[x]$ has a rational root, then that root must be an integer.*

Proof. We have $a_d = 1$ as f is monic. Therefore $n = \pm 1$ in the rational root criterion, which implies that $m/n = \pm m$, an integer. □

We can apply Corollary 3.4.1 to the rational roots of the polynomial $x^n - d$, and so we deduce that if $d^{1/n}$ is rational, then $d^{1/n}$ is an integer (and therefore if $d^{1/n}$ is not an integer, then it is irrational), generalizing Proposition 3.4.2.

We have now proved that there exist infinitely many irrational numbers, the numbers $\sqrt{d}$ when d is not the square of an integer. This caused important philosophical conundrums for the early Greek mathematicians.[8]

Exercise 3.4.4. Prove that the polynomial $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$.

3.5. Dividing in congruences

We are now ready to return to the topic of dividing both sides of a congruence through by a given divisor, resolving the conundrums raised in section 2.2.

Lemma 3.5.1. *If d divides both a and b and $a \equiv b \pmod{m}$, then*

$$a/d \equiv b/d \pmod{m/g} \quad \text{where} \quad g = \gcd(d, m).$$

[8] Ancient Greek mathematicians did not think of numbers as an abstract concept, but rather as units of measurement. That is, one starts with fixed length measures and determines what lengths can be measured by a combination of those original lengths: A stick of length a can be used to measure any length that is a positive integer multiple of a (by measuring out k copies of length a, one after another). Theorem 1.1 can be interpreted as stating that if one has measuring sticks of length a and b, then one can measure length $\gcd(a, b)$ by measuring out u copies of length a and then v copies of length b, to get total length $au + bv = \gcd(a, b)$. One can then measure out any multiple of $\gcd(a, b)$ by copying the above construction that many times.

Pythagoras ($\approx$ 570–495 B.C.) traveled to Egypt and perhaps India in his youth on his quest for understanding. In 530 B.C. he founded a mystical sect in Croton, a Greek colony in southern Italy, which developed influential philosophical theories. Pythagoreans believed that numbers must be constructible in a finite number of steps from a finite given set of lengths and so erroneously concluded that no irrational number could be constructed in this way. However an isosceles right-angled triangle with two sides of length 1 has a hypotenuse of length $\sqrt{2}$, and so the Pythagoreans believed that $\sqrt{2}$ must be a rational number. When one of them proved Proposition 3.4.1 it contradicted their whole philosophy and so was suppressed, "*for the unspeakable should always be kept secret*"!

We looked at what types of lengths are "constructible" using only a compass and a straight edge in section 0.18 of appendix 0G. In fact, although the constructible lengths are quite restricted, they are, nonetheless, a far richer set of numbers than just the rational numbers.

The Pythagoreans similarly associated the four regular polygons that were then known (the *Platonic solids* after Plato) with the four "elements"—the tetrahedron with fire, the cube with earth, the octahedron with air, and the icosahedron with water—and so believed that there could be no others. They also suppressed their discovery of a fifth regular polygon, the dodecahedron.

Proof. As d divides both a and b, we may write $a = dA$ and $b = dB$ for some integers A and B, so that $dA \equiv dB \pmod{m}$. Hence m divides $d(A-B)$ and therefore $\frac{m}{g}$ divides $\frac{d}{g}(A-B)$. Now $\gcd(\frac{m}{g}, \frac{d}{g}) = 1$ by exercise 1.2.5(a), and so $\frac{m}{g}$ divides $A-B$ by Euclid's Lemma. This is the result that was claimed. □

For example, $14 \equiv 91 \pmod{77}$. Now $14 = 7 \times 2$ and $91 = 7 \times 13$, and so we divide 7 out from 77 to obtain $2 \equiv 13 \pmod{11}$. More interestingly $12 \equiv 42 \pmod{15}$, and 6 divides both 12 and 42. However 6 does not divide 15, so we cannot divide this out from 15, but rather we divide out by $\gcd(15, 6) = 3$ to obtain $2 \equiv 7 \pmod{5}$.

Corollary 3.5.1. *Suppose that* $(a, m) = 1$.

(i) $u \equiv v \pmod{m}$ *if and only if* $au \equiv av \pmod{m}$.

(ii) *The residues*

$$a.0,\ a.1,\ \ldots,\ a.(m-1) \tag{3.5.1}$$

form a complete set of residues $\pmod{m}$.

Proof. (i) The third congruence of Lemma 2.1.1 implies that if $u \equiv v \pmod{m}$, then $au \equiv av \pmod{m}$. In the other direction, we take a, b, d in Lemma 3.5.1 to equal au, av, a, respectively. Then $g = (a, m) = 1$, and so $au \equiv av \pmod{m}$ implies that $u \equiv v \pmod{m}$ by Lemma 3.5.1.

(ii) By part (i) we know that the residues in (3.5.1) are distinct mod m. Since there are m of them, they must form a complete set of residues $\pmod{m}$. □

Corollary 3.5.1(ii) states that the residues in (3.5.1) form a complete set of residues $\pmod{m}$. In particular one of them is congruent to $1 \pmod{m}$; and so we deduce the following:

Corollary 3.5.2. *If* $(a, m) = 1$, *then there exists an integer* r *such that* $ar \equiv 1 \pmod{m}$. *We call* r *the* inverse *of* $a \pmod{m}$. *We denote this by* $1/a \pmod{m}$, *or* $a^{-1} \pmod{m}$; *some authors write* $\overline{a} \pmod{m}$.

Third proof of Theorem 1.1. [*For any positive integers* a, b, *there exist integers* u *and* v *such that* $au + bv = \gcd(a, b)$.] Let $g = \gcd(a, b)$ and write $a = gA, b = gB$ so that $(A, B) = 1$. By Corollary 3.5.2, there exists an integer r such that $Ar \equiv 1 \pmod{B}$, and so there exists an integer s such that $Ar - 1 = Bs$; that is, $Ar - Bs = 1$. Therefore $ar - bs = g(Ar - Bs) = g \cdot 1 = g = \gcd(a, b)$, as desired. □

This also goes in the other direction:

Second proof of Corollary 3.5.2. By Theorem 1.1 there exist integers u and v such that $au + mv = 1$, and so

$$au \equiv au + mv = 1 \pmod{m}.$$

Therefore u is the inverse of $a \pmod{m}$. □

Exercise 3.5.1. Assume that $(a, m) = 1$.
(a) Prove that if b is an integer, then $a.0 + b,\ a.1 + b,\ \ldots,\ a(m-1) + b$ form a complete set of residues (mod m).
(b) Deduce that for all given integers b and c, there is a unique value of x (mod m) for which $ax + b \equiv c \pmod{m}$.

If $(a, m) = 1$, then we can (unambiguously) express the root of $ax \equiv c \pmod{m}$ as $ca^{-1} \pmod{m}$, or $c/a \pmod{m}$; we take this to mean the residue class mod m which contains the unique value from exercise 3.5.1(b). For example $19/17 \equiv 11 \pmod{12}$. Such quotients share all the properties described in Lemma 2.1.1.

Exercise 3.5.2. Prove that if $\{r_1, \ldots, r_k\}$ is a reduced set of residues mod m and $(a, m) = 1$, then $\{ar_1, \ldots, ar_k\}$ is also a reduced set of residues mod m

Exercise 3.5.3. (a) Show that there exists $r \pmod{b}$ for which $ar \equiv c \pmod{b}$ if and only if $\gcd(a, b)$ divides c.
(b)† Prove that the solutions r are precisely the elements of a residue class mod $b/\gcd(a, b)$.

Exercise 3.5.4. Prove that if $(a, m) > 1$, then there does not exist an integer r such that $ar \equiv 1 \pmod{m}$. (And so Corollary 3.5.2 could have been phrased as an "if and only if" condition.)

Exercise 3.5.5. Explain how the Euclidean algorithm may be used to efficiently determine the inverse of $a \pmod{m}$ whenever $(a, m) = 1$. (Calculating the inverse of $a \pmod{m}$ is an essential part of the RSA algorithm discussed in section 10.3.)

3.6. Linear equations in two unknowns

Given integers a, b, c, can we determine all of the integer solutions m, n to

$$am + bn = c\ ?$$

Example. To find all integer solutions to $4m + 6n = 10$, we begin by noting that we can divide through by 2 to get $2m + 3n = 5$. There is clearly a solution, $2 \cdot 1 + 3 \cdot 1 = 5$. Therefore

$$2m + 3n = 5 = 2 \cdot 1 + 3 \cdot 1,$$

so that $2(m-1) = 3(1-n)$. We therefore need to find all integer solutions u, v to

$$2u = 3v$$

and then the general solution to our original equation is given by $m = 1 + u,\ n = 1 - v$, as we run over the possible pairs u, v. Now $2|3v$ and $(2, 3) = 1$ so that $2|v$. Hence we may write $v = 2\ell$ for some integer ℓ and then deduce that $u = 3\ell$. Therefore all integer solutions to $4m + 6n = 10$ take the form

$$m = 1 + 3\ell,\ n = 1 - 2\ell, \text{ for some integer } \ell.$$

We can imitate this procedure to establish a general result:

Theorem 3.5. *Let a, b, c be given integers. There are solutions in integers m, n to $am + bn = c$ if and only if (a, b) divides c. Given a first solution, say r, s (which can be found using the Euclidean algorithm), all integer solutions to $am + bn = c$ are then given by the formula*

$$m = r + \frac{b}{(a,b)}\ell, \quad n = s - \frac{a}{(a,b)}\ell \quad \textit{for some integer } \ell.$$

The full set of *real* solutions to $ax + by = c$ is given by

$$x = r + kb,\ y = s - ka, \text{ where } k \text{ is an arbitrary real number.}$$

By Theorem 3.5 these are integer solutions exactly when $k = \ell/(a, b)$ for some $\ell \in \mathbb{Z}$.

In the discussion above we saw that it is best to "reduce" this to the case when $(a, b) = 1$.

Corollary 3.6.1. *Let a, b, c be given integers with $(a, b) = 1$. Given a first solution in integers r, s to $ar + bs = c$, all integer solutions to $am + bn = c$ are then given by the formula*

$$m = r + b\ell, \quad n = s - a\ell \quad \textit{for some integer } \ell.$$

Deduction of Theorem 3.5 from Corollary 3.6.1. If there is a solution in integers m, n to $am + bn = c$, then $g := (a, b)$ divides a, b and $am + bn = c$, so we can write $a = Ag$, $b = Bg$, $c = Cg$ for some integers A, B, C with $(A, B) = 1$. We now determine the integer solutions to $Am + Bn = C$, where $(A, B) = 1$ by Corollary 3.6.1. □

Proof #1 of Corollary 3.6.1. If

$$am + bn = c = ar + bs,$$

then

$$a(m - r) = b(s - n).$$

We therefore need to find all integer solutions u, v to

$$au = bv.$$

In any given solution a divides v by Euclid's Lemma as $(a, b) = 1$, and so we may write $v = a\ell$ for some integer ℓ and deduce that $u = b\ell$. We then deduce the claimed parametrization of integer solutions to $am + bn = c$. □

Exercise 3.6.1. Show that if there exists a solution in integers m, n to $am+bn = c$ with $(a, b) = 1$, then there exists a solution with $0 \le m < b$.

Proof #2 of Corollary 3.6.1. There is an inverse to $a \pmod b$, as $(a, b) = 1$; call it r. Let m be any integer $\equiv rc \pmod b$, so that $am \equiv arc \equiv c \pmod b$, and therefore there exists an integer n for which $am + bn = c$. The result follows. □

Exercise 3.6.2. (a) Find all solutions in integers m, n to $7m + 5n = 1$.
(b) Find all solutions in integers u, v to $7v - 5u = 3$.
(c) Find all solutions in integers j, k to $3j - 9k = 1$.
(d) Find all solutions in integers r, s to $5r - 10s = 15$.

Exercise 3.6.3. Show that a linear equation $am + bn = c$ where a, b, and c are given integers, cannot have exactly one solution in integers m, n.

An equation involving a congruence is said to be *solved* when integer values can be found for the variables so that the congruence is satisfied. For example $6x + 5 \equiv 13 \pmod{11}$ has the unique solution $x \equiv 5 \pmod{11}$, that is, all integers of the form $11k + 5$.

There is another way to interpret Theorem 3.5, which will prove to be the best reformulation to understand what happens with quadratic equations:

Exercise 3.6.4 (The local-global principle for linear equations)**.** Let a, b, c be given non-zero integers. There are solutions in integers m, n to $am + bn = c$ if and only if there exist residue classes $u, v \pmod b$ such that $au + bv \equiv c \pmod b$.

"Global" refers to looking over the infinite number of possibilities for integer solutions, "local" to looking through the finite number of possibilities mod b. This exercise will be revisited in exercise 3.9.13.

3.7. Congruences to several moduli

What are the integers that satisfy given congruences to two different moduli?

Lemma 3.7.1. *Suppose that a, A, b, B are integers. There exists an integer x such that both $x \equiv a \pmod A$ and $x \equiv b \pmod B$ if and only if $b \equiv a \pmod{\gcd(A, B)}$. If there is such an integer x, then the two congruences hold simultaneously for all integers x belonging to a unique residue class $\pmod{\operatorname{lcm}[A, B]}$.*

Proof. The integers x for which $x \equiv a \pmod A$ may be written in the form $x = Ay + a$ for some integer y. We are therefore seeking solutions to $Ay + a = x \equiv b \pmod B$, which is the same as $Ay \equiv b - a \pmod B$. By exercise 3.5.3(a), this has solutions if and only $\gcd(A, B)$ divides $b - a$. Moreover exercise 3.5.3(b) implies that y is a solution if and only if it is of the form $u + n \cdot B/(A, B)$ for some initial solution u and any integer n. Therefore x must be of the form

$$x = Ay + a = A(u + n \cdot B/(A, B)) + a = v + n \cdot \operatorname{lcm}[A, B],$$

where $v = Au + a$ and since $A \cdot B/(A, B) = [A, B]$ by Corollary 3.2.2. □

The generalization of this last result is most elegant when we restrict to moduli that are pairwise coprime. We prepare with the following exercises:

Exercise 3.7.1. Determine all integers n for which $n \equiv 101 \pmod{7^{11}}$ and $n \equiv 101 \pmod{13^{17}}$, in terms of one congruence.

Exercise 3.7.2. Suppose that $a, b, c, \dots$ are pairwise coprime integers.
(a) Prove that if $a, b, c, \dots$ each divide m, then $abc\dots$ divides m.
(b) Deduce that if $m \equiv n \pmod a$ and $m \equiv n \pmod b$ and $m \equiv n \pmod c$, $\dots$, then $m \equiv n \pmod{abc\dots}$.

Theorem 3.6 (The Chinese Remainder Theorem)**.** *Suppose that $m_1, \dots, m_k$ are a set of pairwise coprime positive integers. For any set of residue classes*

$$a_1 \pmod{m_1},\ a_2 \pmod{m_2}, \dots, a_k \pmod{m_k},$$

there exists a unique residue class $x \pmod m$ where $m = m_1 m_2 \dots m_k$, for which

$$x \equiv a_j \pmod{m_j} \quad \text{for each } j.$$

Proof. We can map $x \pmod m$ to the vector $(x \pmod{m_1},\ x \pmod{m_2}, \dots, x \pmod{m_k})$. There are $m_1 m_2 \dots m_k$ different such vectors and each different x mod m maps to a different one, for if $x \equiv y \pmod{m_j}$ for each j, then $x \equiv y \pmod m$ by exercise 3.7.2(b). Hence there is a suitable 1-to-1 correspondence between residue classes mod m and vectors, which implies the result. □

This is known as the *Chinese Remainder Theorem* because of the ancient Chinese practice (as discussed in Sun Tzu's 4th-century *Classic Calculations*) of counting the number of soldiers in a platoon by having them line up in three columns and seeing how many are left over, then in five columns and seeing how many are left over, and finally in seven columns and seeing how many are left over, etc. For instance, if there are a hundred soldiers, then there should be 1, 0, and 2 soldiers left over, respectively;[9] and the next smallest number of soldiers one would need for this to be true is 205 (since 205 is the next smallest positive integer $\equiv 100 \pmod{105}$). Presumably an experienced commander can eyeball the difference between 100 soldiers and 205! Primary school children in China learn a song that celebrates this contribution.

We can make the Chinese Remainder Theorem a practical tool by giving a formula to determine x, given $a_1, a_2, \dots, a_k$: Since $(m/m_j, m_j) = 1$ there exists an integer b_j such that $b_j \cdot \frac{m}{m_j} \equiv 1 \pmod{m_j}$ for each j, by Corollary 3.5.2. Then

$$\boxed{x \equiv a_1 b_1 \cdot \frac{m}{m_1} + a_2 b_2 \cdot \frac{m}{m_2} + \cdots + a_k b_k \cdot \frac{m}{m_k} \pmod{m}.} \tag{3.7.1}$$

This works because m_j divides m/m_i for each $i \neq j$ and so

$$x \equiv 0 + \cdots + 0 + a_j \cdot b_j \frac{m}{m_j} + 0 + \cdots + 0 \equiv a_j \cdot 1 \equiv a_j \pmod{m_j}$$

for each j. The b_j can all be determined using the Euclidean algorithm, so x can be determined rapidly in practice.

Exercise 3.7.3.† Use this method to give a general formula for $x \pmod{1001}$ when $x \equiv a \pmod 7$, $x \equiv b \pmod{11}$, and $x \equiv c \pmod{13}$.

Exercise 3.7.4.† Find the smallest positive integer n which can be written as $n = 2a^2 = 3b^3 = 5c^5$ for some integers a, b, c.

There is more discussion of the Chinese Remainder Theorem in section 3.14 of appendix 3B, in particular in the more difficult case in which the m_i's have common factors:

Exercise 3.7.5.† Given residue classes $a_1 \pmod{m_1}, \dots, a_k \pmod{m_k}$ let $m = \text{lcm}[m_1, \dots, m_k]$. Prove that there exists a residue class $b \pmod m$ for which $b \equiv a_j \pmod{m_j}$ for each j if and only if $a_i \equiv a_j \pmod{(m_i, m_j)}$ for all $i \neq j$.

Moreover in appendix 3C we explain how the Chinese Remainder Theorem can be extended to, and understood in, the more general and natural context of group theory.

Exercise 3.7.6. (a) Prove that each of $a, b, c, \dots$ divides m if and only if $\text{lcm}[a, b, c, \dots]$ divides m.
(b) Deduce that if $m \equiv n \pmod a$ and $m \equiv n \pmod b$ and $\dots$, then $m \equiv n \pmod{\text{lcm}[a, b, \dots]}$.
(c) Prove that if $b \pmod m$ in exercise 3.7.5 exists, then it is unique.

Exercise 3.7.7.† Let M, N, g be positive integers with $(M, N, g) = 1$. Prove that the set of residues $\{aN + bM \pmod g : 0 \leq a, b \leq g - 1\}$ is precisely g copies of the complete set of residues mod g.

[9] Since $100 \equiv 1 \pmod 3, \equiv 0 \pmod 5$, and $\equiv 2 \pmod 7$.

Exercise 3.7.8. (a) Prove that for any odd integer m there are infinitely many integers n for which $(n, m) = (n + 1, m) = 1$.
(b) Why is this false if m is even?
(c) Prove that for any integer m there are infinitely many integers n for which $(n, m) = (n + 2, m) = 1$.
(d)‡ Let $a_1 < a_2 < \cdots < a_k$ be given integers. Give an "if and only if" criterion in terms of the $a_i \pmod p$, for each prime p dividing m, to determine whether there are infinitely many integers n for which $(n + a_1, m) = (n + a_2, m) = \cdots = (n + a_k, m) = 1$.

Exercise 3.7.9. Prove that there exist one million consecutive integers, each of which is divisible by the cube of an integer > 1.

3.8. Square roots of $1 \pmod n$

We begin by noting

Lemma 3.8.1. *If p is an odd prime, then there are exactly two square roots of* $1 \pmod p$*, namely* 1 *and* -1.

Proof. If $x^2 \equiv 1 \pmod p$, then $p|(x^2 - 1) = (x - 1)(x + 1)$ and so p divides either $x - 1$ or $x + 1$ by Theorem 3.1. Hence $x \equiv 1$, or $-1 \pmod p$. □

There can be more than two square roots of 1 if the modulus is composite. For example, 1, 3, 5, and 7 are all roots of $x^2 \equiv 1 \pmod 8$, while $1, 4, -4$, and -1 are all roots of $x^2 \equiv 1 \pmod{15}$, and $\pm 1, \pm 29, \pm 34, \pm 41$ are all square roots of 1 (mod 105). How can we find all of these solutions?

By the Chinese Remainder Theorem, x is a root of $x^2 \equiv 1 \pmod{15}$ if and only if $x^2 \equiv 1 \pmod 3$ and $x^2 \equiv 1 \pmod 5$. But, by Lemma 3.8.1, this happens if and only if $x \equiv 1$ or $-1 \pmod 3$ and $x \equiv 1$ or $-1 \pmod 5$. There are therefore four possibilities for $x \pmod{15}$, given by making the choices

$$\begin{aligned}
x \equiv 1 \pmod 3 \quad &\text{and} \quad x \equiv 1 \pmod 5, \quad \text{which imply } x \equiv 1 \pmod{15};\\
x \equiv -1 \pmod 3 \quad &\text{and} \quad x \equiv -1 \pmod 5, \quad \text{which imply } x \equiv -1 \pmod{15};\\
x \equiv 1 \pmod 3 \quad &\text{and} \quad x \equiv -1 \pmod 5, \quad \text{which imply } x \equiv 4 \pmod{15};\\
x \equiv -1 \pmod 3 \quad &\text{and} \quad x \equiv 1 \pmod 5, \quad \text{which imply } x \equiv -4 \pmod{15},
\end{aligned}$$

the last two giving the less obvious solutions. This proof generalizes in a straightforward way:

Proposition 3.8.1. *If m is an odd integer with k distinct prime factors, then there are exactly 2^k solutions $x \pmod m$ to the congruence $x^2 \equiv 1 \pmod m$.*

Proof. Lemma 3.8.1 proves the result for m prime. What if $m = p^e$ is a power of an odd prime p? If $x^2 \equiv 1 \pmod{p^e}$, then $p|(x^2 - 1) = (x - 1)(x + 1)$ and so p divides either $x - 1$ or $x + 1$ by Theorem 3.1. However p cannot divide both, or else p divides their difference, which is 2. Now suppose that p does not divide $x + 1$. Since $p^e|(x^2 - 1) = (x - 1)(x + 1)$ we deduce that $p^e|(x - 1)$ by Euclid's Lemma. Similarly, if p does not divide $x - 1$, then $p^e|(x + 1)$. Therefore $x \equiv -1$ or $1 \pmod{p^e}$.

Now, suppose that a is an integer for which

$$a^2 \equiv 1 \pmod m,$$

where $m = p_1^{e_1} \dots p_k^{e_k}$ where the p_j are distinct odd primes and the $e_j \geq 1$. By the Chinese Remainder Theorem, this is equivalent to a satisfying

$$a^2 \equiv 1 \pmod{p_j^{e_j}} \text{ for } j = 1, 2, \dots, k.$$

By the first paragraph, this is, in turn, equivalent to

$$a \equiv 1 \text{ or } -1 \pmod{p_j^{e_j}} \text{ for } j = 1, 2, \dots, k.$$

By the Chinese Remainder Theorem, each choice of $a \pmod{p_1^{e_1}}, \dots, a \pmod{p_k^{e_k}}$ gives rise to a different value of $a \pmod{m}$ that will satisfy the congruence $a^2 \equiv 1 \pmod{m}$. Therefore there are exactly 2^k distinct solutions. □

Proposition 3.8.1 is, in effect, an algorithm for finding all of the square roots of 1 (mod m), provided one knows the factorization of m. Conversely, in section 10.1, we will see that if we are able to find square roots mod m, then we are able to factor m.

Exercise 3.8.1. Prove that if $(x, 6) = 1$, then $x^2 \equiv 1 \pmod{24}$ *without working mod* 24. You are allowed to work mod 8 and mod 3.

Exercise 3.8.2. (a)† What are the roots of $x^2 \equiv 1 \pmod{2^e}$ for each integer $e \geq 1$? (This must be different from the odd prime case since $x^2 \equiv 1 \pmod 8$ has four solutions, $1, 3, 5, 7 \pmod 8$.)

(b)† Prove that if m has k distinct prime factors, there are exactly $2^{k+\delta}$ solutions $x \pmod m$ to the congruence $x^2 \equiv 1 \pmod m$, where, if $2^e \| m$, then $\delta = 0$ if $e = 0$ or 2, $\delta = -1$ if $e = 1$, and $\delta = 1$ if $e \geq 3$.

(c) Deduce that the product of the square roots of 1 $\pmod{2^e}$ equals 1 $\pmod{2^e}$ if $e \geq 3$.

Exercise 3.8.3.† Prove that the product of the square roots of 1 (mod m) equals 1 (mod m), unless $m = 4$ or $m = p^e$ or $m = 2p^e$ for some power p^e of an odd prime p, in which case it equals $-1 \pmod m$.

In Gauss's 1801 book he gives an explicit practical example of the Chinese Remainder Theorem. Before pocket watches and cheap printing, people were more aware of solar cycles and the moon's phases than what year it actually was. Moreover, from Roman times to Gauss's childhood, taxes were hard to collect since travel was difficult and expensive and so were not paid annually but rather on a multiyear cycle. Gauss explained how to use the Chinese Remainder Theorem to deduce the year in the Julian calendar from these three pieces of information:

• The *indiction* was used from 312 to 1806 to specify the position of the year in a 15-year taxation cycle. The indiction is $\equiv \text{year} + 3 \pmod{15}$.

• The moon's phases and the days of the year repeat themselves every 19 years.[10] The *golden number*, which is $\equiv \text{year} + 1 \pmod{19}$, indicates where one is in that cycle of 19 years (and is still used to calculate the correct date for Easter).

• The days of the week and the dates of the year repeat in cycles of 28 years in the Julian calender.[11] The *solar cycle*, which is $\equiv \text{year} + 9 \pmod{28}$, indicates where one is in this cycle of 28 years.

[10] Meton of Athens, in the 5th century BC, observed that 19 (solar) years is less than two hours out from being a whole number of lunar months.

[11] Since there are seven days in a week and leap years occur every four years.

Taking $m_1 = 15,\ m_2 = 19,\ m_3 = 28$, we observe that

$$b_1 \equiv \frac{1}{19\cdot 28} \equiv \frac{1}{4\cdot(-2)} \equiv -2 \pmod{15} \text{ and } b_1 \cdot \frac{m}{m_1} = -2\cdot 19\cdot 28 = -1064,$$
$$b_2 \equiv \frac{1}{15\cdot 28} \equiv \frac{1}{(-4)\cdot 9} \equiv \frac{1}{2} \equiv 10 \pmod{19} \text{ and } b_2 \cdot \frac{m}{m_2} = 10\cdot 15\cdot 28 = 4200,$$
$$b_3 \equiv \frac{1}{15\cdot 19} = \frac{1}{(14+1)\cdot 19} \equiv \frac{1}{14+19} \equiv \frac{1}{5} \equiv -11 \pmod{28} \text{ and } b_3 \cdot \frac{m}{m_3} = -3135.$$

Therefore if the indiction is a, the golden number is b, and the solar cycle is c, then the year is

$$\equiv -1064a + 4200b - 3135c \pmod{7980}.$$

Additional exercises

Exercise 3.9.1. Prove that if $2^n - 1$ is prime, then n must be prime.

Exercise 3.9.2. Suppose that $0 \le x_0 \le x_1 \le \cdots$ is a division sequence (that is, $x_m | x_n$ whenever $m|n$; see exercise 1.7.22), with $x_{n+1} > x_n$ whenever $n \ge n_0$ (≥ 1). Prove that if x_n is prime for some integer $n > n_0^2$, then n is prime.

We can apply exercise 3.9.2 to the Mersenne numbers $M_n = 2^n - 1$, with $n_0 = 1$, so that if M_n is prime, then n is prime; and to the Fibonacci numbers with $n_0 = 2$, so that if F_n is prime, then n is prime or $n = 4$.

Exercise 3.9.3. We introduced the companion sequence $(y_n)_{n\ge 0}$ of the Lucas sequence $(x_n)_{n\ge 0}$ in exercise 0.1.4. Note that $y_1 = a$ does not necessarily divide $y_2 = a^2 + 2b$.

(a)‡ Prove that y_m divides y_n whenever m divides n and n/m is odd.

(b) Assume that $a > 1$ and $b > 0$. Deduce that if y_n is prime, then n must be a power of 2.

(c) Deduce that if $2^n + 1$ is prime, then it must be a Fermat number.

Exercise 3.9.4.‡ Prove that the Fundamental Theorem of Arithmetic implies that for any finite set of primes $\mathcal{P}$, the numbers $\log p,\ p \in \mathcal{P}$, are linearly independent[12] over $\mathbb{Q}$.

Exercise 3.9.5.† Prove that $\gcd(a,b,c)\cdot \operatorname{lcm}[a,b,c] = abc$ if and only if a, b, and c are pairwise coprime.

Exercise 3.9.6.† Prove that if a and b are positive integers whose product is a square and whose difference is a prime p, then $a + b = (p^2+1)/2$.

Exercise 3.9.7. Let p be an odd prime and x, y, and z pairwise coprime, positive integers.

(a)† Prove that $\frac{z^p - y^p}{z-y} \equiv py^{p-1} \pmod{z-y}$.

(b) Deduce that $\gcd(\frac{z^p-y^p}{z-y}, z-y) = 1$ or p.

(This problem is continued in exercise 7.10.6.)

Exercise 3.9.8. Suppose that $f(x) \in \mathbb{Z}[x]$ is monic and $f(0) = 1$. Prove that if $r \in \mathbb{Q}$ and $f(r) = 0$, then $r = 1$ or -1.

Exercise 3.9.9 (Another proof that $\sqrt{2}$ is irrational)**.** Suppose that $\sqrt{2} = a/b$ where a and b are coprime integers, so that $a^2 = 2b^2$.

(a) Prove that 3 cannot divide b, and so let $c \equiv a/b \pmod 3$.

(b) Prove that $c^2 \equiv 2 \pmod 3$, and therefore obtain a contradiction.

[12] $x_1, \ldots, x_k$ are *linearly dependent* over $\mathbb{Q}$ if there exist rational numbers $a_1, \ldots, a_k$, which are not all zero, such that $a_1x_1 + \cdots + a_kx_k = 0$. They are *linearly independent* over $\mathbb{Q}$ if they are not linearly dependent over $\mathbb{Q}$.

Exercise 3.9.10.‡ (a) Prove that $\sqrt{2}+\sqrt{3}$ is irrational.
(b) Prove that $\sqrt{a}+\sqrt{b}$ is irrational unless a and b are both squares of integers.

Exercise 3.9.11. Suppose that d is an integer and $\sqrt{d}$ is rational.
(a) Show that there exists an integer m such that $\sqrt{d}-m = p/q$ where $0 \le p < q$ and $(p,q)=1$.
(b) If $p \neq 0$, show that $\sqrt{d}+m = Q/p$ for some integer Q.
(c) Use (a) and (b) to establish a contradiction when $p \neq 0$.
(d) Deduce that $d = m^2$.

Reference on the many proofs that $\sqrt{2}$ is irrational

[1] John H. Conway and Joseph Shipman, *Extreme proofs I: The irrationality of* $\sqrt{2}$, Math. Intelligencer **35** (2013), 2–7.

We say that N can be represented by the linear form $ax+by$, if there exist integers m and n such that $am+bn = N$. The representation is *proper* if $(m,n)=1$.

Exercise 3.9.12.† In this question we prove that if N can be represented by $ax+by$, then it can be represented properly. Let $A = a/(a,b)$ and $B = b/(a,b)$. Theorem 3.5 states that if $N = ar+bs$, then all solutions to $am+bn = N$ take the form $m = r+kB, n = s-kA$ for some integer k.
(a) Prove that $\gcd(m,n)$ divides N.
(b) Prove that at least one of A and B is not divisible by p, for each prime p.
(c) Prove that if $p \nmid A$, then there exists a residue class $k_p \pmod p$ such that $p|s-kA$ if and only if $k \equiv k_p \pmod p$. Therefore deduce that $p \nmid s-kA$ if $k \equiv k_p+1 \pmod p$. Note an analogous result if $p|A$ (in which case $p \nmid B$).
(d) Deduce that there exists an integer k such that, for all primes p dividing N, either p does not divide $r+kB$ or p does not divide $s-kA$ (or both).
(e) Deduce that if $m = r+kB$ and $n = s-kA$, then N is properly represented by $am+bn$.

Exercise 3.9.13. Prove the following version of the local-global principle for linear equations (exercise 3.6.4): Let a,b,c be given integers. There are solutions in integers m,n to $am+bn = c$ if and only if for all prime powers p^e (where p is prime and e is an integer ≥ 1) there exist residue classes $u,v \pmod{p^e}$ for which $au+bv \equiv c \pmod{p^e}$.

Exercise 3.9.14. Find all solutions to $5a+7b = 211$ where a and b are positive integers.

Exercise 3.9.15. Suppose that $f(x) \in \mathbb{Z}[x]$ and m and n are coprime integers.
(a) Prove that there exist integers a and b for which $f(a) \equiv 0 \pmod m$ and $f(b) \equiv 0 \pmod n$ if and only if there exists an integer c for which $f(c) \equiv 0 \pmod{mn}$, and show that we may take $c \equiv a \pmod m$ and $c \equiv b \pmod n$.
(b) Suppose that $p_1 < p_2 < \cdots < p_k$ are primes. Prove that there exist integers $a_1,\dots,a_k$ such that $f(a_i) \equiv 0 \pmod{p_i}$ for $1 \le i \le k$ if and only if there exists an integer a such that $f(a) \equiv 0 \pmod{p_1p_2\dots p_k}$.

Adding reduced fractions. A *reduced fraction* takes the form a/b where a and $b>0$ are coprime integers. We wish to better understand adding reduced fractions.

Exercise 3.9.16.† Suppose that m and n are coprime integers.
(a) Prove that for any integer c there exist integers a and b for which $\frac{c}{mn} = \frac{a}{m}+\frac{b}{n}$.
(b) Prove that there are (unique) positive integers a and b for which $\frac{1}{mn} = \frac{a}{m}+\frac{b}{n}-1$.

Exercise 3.9.17. Let m and n be given positive integers.

(a) Prove that for any integers a and b there exists an integer c for which $\frac{a}{m} + \frac{b}{n} = \frac{c}{L}$ where $L = \text{lcm}[m, n]$.

For the denominators 3 and 6, with $L = 6$, we have the example $\frac{1}{3} + \frac{1}{6} = \frac{1}{2}$, a case in which the sum has a denominator smaller than L when written as a reduced fraction. However $\frac{1}{3} + \frac{5}{6} = \frac{7}{6}$ so there are certainly examples with these denominators for which the sum has denominator L.

(b)† Show that $\text{lcm}[m, n]$ is the smallest positive integer L such that for all integers a and b we can write $\frac{a}{m} + \frac{b}{n}$ as a fraction with denominator L. (This is why $\text{lcm}[m, n]$ is sometimes called the *lowest* (or *least*) *common denominator* of the fractions $1/m$ and $1/n$.)

(c)† Show that if $\frac{a}{m}$ and $\frac{b}{n}$ are reduced fractions whose sum has denominator less than L, then there must exist a prime power p^e such that $p^e \| m$ and $p^e \| n$ for which p^{e+1} divides $an + bm$.

Appendix 3A. Factoring binomial coefficients and Pascal's triangle modulo p

3.10. The prime powers dividing a given binomial coefficient

Lemma 3.10.1. *The power of prime p that divides $n!$ is $\sum_{k\geq 1}[n/p^k]$. In other words*

$$n! = \prod_{p \ prime} p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots}.$$

Proof. We wish to determine the power of p dividing $n! = 1\cdot 2\cdot 3\cdots(n-1)\cdot n$. If p^k is the power of p dividing m, then we will count 1 for p dividing m, then 1 for p^2 dividing m,..., and finally 1 for p^k dividing m. Therefore the power of p dividing $n!$ equals the number of integers $m,\ 1\leq m\leq n$, that are divisible by p, plus the number of integers $m,\ 1\leq m\leq n$, that are divisible by p^2, plus .... The result follows as there are $[n/p^j]$ integers $m,\ 1\leq m\leq n$, that are divisible by p^j for each $j\geq 1$, by exercise 1.7.6(c). □

Exercise 3.10.1. Write $n = n_0 + n_1 p + \cdots + n_d p^d$ in base p so that each $n_j \in \{0, 1, \ldots, p-1\}$.

(a) Prove that $[n/p^k] = (n - (n_0 + n_1 p + \cdots + n_{k-1}p^{k-1}))/p^k$.

The *sum of the digits of n in base p* is defined to be $s_p(n) := n_0 + n_1 + \cdots + n_d$.

(b) Prove that the exact power of prime p that divides $n!$ is $\frac{n-s_p(n)}{p-1}$.

Theorem 3.7 (Kummer's Theorem)**.** *The largest power of prime p that divides the binomial coefficient $\binom{a+b}{a}$ is given by the number of carries when adding a and b in base p.*

Example. To recover the factorization of $\binom{14}{6}$ we add 6 and 8 in each prime base ≤ 14:

0101	020	11	06	06	06
$\underline{1000_2}$	$\underline{022_3}$	$\underline{13_5}$	$\underline{11_7}$	$\underline{08_{11}}$	$\underline{08_{13}}$
1101	112	24	20	13	11

We see that there are no carries in base 2, 1 carry in base 3, no carries in base 5, 1 carry in base 7, 1 carry in base 11, and 1 carry in base 13, so we deduce that $\binom{14}{6} = 3^1 \cdot 7^1 \cdot 11^1 \cdot 13^1$.

Proof. For given integer $k \ge 1$, let $q = p^k$. Then let A and B be the least non-negative residue of a and $b \pmod q$, respectively, so that $0 \le A, B \le q-1$. Note that A and B give the first k digits (from the right) of a and b in base p. If C is the first k digits of $a+b$ in base p, then C is the least non-negative residue of $a+b \pmod q$, that is, of $A+B \pmod q$. Now $0 \le A+B < 2q$:

• If $A+B < q$, then $C = A+B$ and there is no carry in the kth digit when we add a and b in base p.

• If $A+B \ge q$, then $C = A+B-q$ and so there is a carry of 1 in the kth digit when we add a and b in base p.

We need to relate these observations to the formula in Lemma 3.10.1. The trick comes in noticing that $A = a - p^k \left[\frac{a}{p^k}\right]$, and similarly $B = b - p^k \left[\frac{b}{p^k}\right]$ and $C = a+b-p^k \left[\frac{a+b}{p^k}\right]$. Therefore

$$\left[\frac{a+b}{p^k}\right] - \left[\frac{a}{p^k}\right] - \left[\frac{b}{p^k}\right] = \frac{A+B-C}{p^k} = \begin{cases} 1 & \text{if there is a carry in the } k\text{th digit,} \\ 0 & \text{if not,} \end{cases}$$

and so

$$\sum_{k\ge 1} \left(\left[\frac{a+b}{p^k}\right] - \left[\frac{a}{p^k}\right] - \left[\frac{b}{p^k}\right] \right)$$

equals the number of carries when adding a and b in base p. However Lemma 3.10.1 implies that this also equals the exact power of p dividing $\frac{(a+b)!}{a!b!} = \binom{a+b}{a}$, and the result follows. □

Exercise 3.10.2. State, with proof, the analogy to Kummer's Theorem for trinomial coefficients $n!/(a!b!c!)$ where $a+b+c=n$.

Corollary 3.10.1. *If p^e divides the binomial coefficient $\binom{n}{m}$, then $p^e \le n$.*

Proof. There are $k+1$ digits in the base p expansion of n when $p^k \le n < p^{k+1}$. When adding m and $n-m$ there can be carries in every digit except the $(k+1)$st (which corresponds to the number of multiples of p^k). Therefore there are no more than k carries when adding m to $n-m$ in base p, so that $p^e \le p^k \le n$ by Kummer's Theorem. □

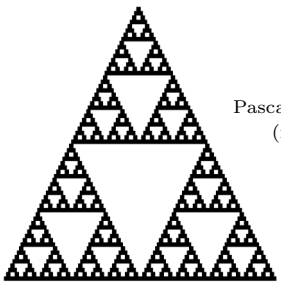
Exercise 3.10.3. Prove that if $0 \le k \le n$, then $\binom{n}{k}$ divides $\operatorname{lcm}[m : m \le n]$.

3.11. Pascal's triangle modulo 2

In section 0.3 we explained the theory and practice of constructing Pascal's triangle. We are now interested in constructing Pascal's triangle modulo 2, mod 3, mod 4, etc. To do so one can either reduce the binomial coefficients mod m (for $m = 2, 3, 4, \ldots$) or one can rework Pascal's triangle, starting with a 1 in the top row and then obtaining a row from the previous one by adding the two entries immediately above the given entry, modulo m. For example, Pascal's triangle mod 2 starts with the rows

$$
\begin{array}{ccccccccccccccc}
 & & & & & & 1 & & & & & & & & \\
 & & & & & 1 & & 1 & & & & & & & \\
 & & & & 1 & & 0 & & 1 & & & & & & \\
 & & & 1 & & 1 & & 1 & & 1 & & & & & \\
 & & 1 & & 0 & & 0 & & 0 & & 1 & & & & \\
 & 1 & & 1 & & 0 & & 0 & & 1 & & 1 & & & \\
1 & & 0 & & 1 & & 0 & & 1 & & 0 & & 1 & &
\end{array}
$$

It is perhaps easiest to visualize this by replacing 1 (mod 2) by a dark square and, otherwise, a white square, as in the following fascinating diagram:[13]



Pascal's triangle (mod 2)

One can see patterns emerging. For example the rows corresponding to $n = 1, 3, 7, 15, \ldots$ are all 1's, and the next rows, $n = 2, 4, 8, 16, \ldots$, start and end with a 1 and have all 0's in between. Even more: The two 1's at either end of row $n = 4$ seem to each be the first entry of a (four-line) triangle, which is an exact copy of the first four rows of Pascal's triangle mod 2, similarly the two 1's at either end of row $n = 8$ and the eight-line triangles beneath (and including) them. In general if T_k denotes the top 2^k rows of Pascal's triangle mod 2, then T_{k+1} is given by a triangle of copies of T_k, with an inverted triangle of zeros in the middle, as in the

[13] This and other images in this section reproduced with kind permission of Bill Cherowitzo.

following diagram:

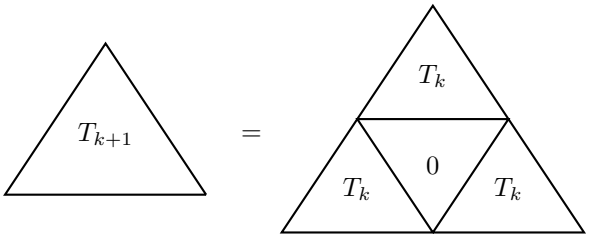


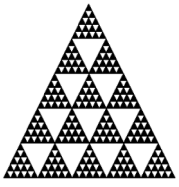
Figure 3.1. The top 2^{k+1} rows of Pascal's triangle mod 2, in terms of the top 2^k rows.

This is called *self-similarity*. One immediate consequence is that one can determine the number of 1's in a given row: If $2^k \le n < 2^{k+1}$, then row n consists of two copies of row m $(:= n - 2^k)$ with some 0's in between.

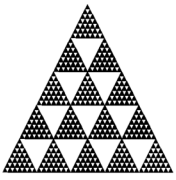
Exercise 3.11.1. Deduce that there are 2^k odd entries in the nth row of Pascal's triangle, where $k = s_2(n)$, the number of 1's in the binary expansion of n.

This self-similarity generalizes nicely for other primes p, where we again replace integers divisible by p by a white square, and those not divisible by p by a black square.

Pascal's triangle (mod 3)



Pascal's triangle (mod 5)



Pascal's triangle (mod 7)

The top p rows are all black since the entries $\binom{n}{m}$ with $0 \le m \le n \le p-1$ are never divisible by p. Let T_k denote the top p^k rows of Pascal's triangle. Then T_{k+1} is given by an array of p rows of triangles, in which the nth row contains n copies of T_k, with inverted triangles of 0's in between.

Pascal's triangle modulo primes p is a bit more complicated; we wish to color in the black squares with one of $p-1$ colors, each representing a different reduced residue class mod p. Call the top row the 0th row, and the leftmost entry of each row its 0th entry. Therefore the mth entry of the nth row is $\binom{n}{m}$. By Lucas's Theorem (exercise 2.5.10) the value of $\binom{rp^k+s}{ap^k+b} \pmod p$, which is the bth entry of the sth row of the copy of T_k which is the ath entry of the rth row of the copies of T_k that make up T_{k+1}, is $\equiv \binom{r}{a}\binom{s}{b} \pmod p$. In other words, the values in the copy of T_k which is the ath entry of the rth row of the copies of T_k are $\binom{r}{a}$ times the values in T_k.

The odd entries in Pascal's triangle mod 4 make even more interesting patterns, but this will take us too far afield; see [**1**] for a detailed discussion.

Reading each row of Pascal's triangle mod 2 as the binary expansion of an integer, we obtain the numbers

$$1,\ 11_2 = 3,\ 101_2 = 5,\ 1111_2 = 15,\ 10001_2 = 17,\ 110011_2 = 51,\ 1010101_2 = 85, \ldots.$$

Do you recognize these numbers? If you factor them, you obtain

$$1, \quad F_0, \quad F_1, \quad F_0F_1 \quad F_2, \quad F_0F_2, \quad F_1F_2, \quad F_0F_1F_2, \ldots$$

where $F_m = 2^{2^m} + 1$ are the Fermat numbers (introduced in exercise 0.4.14). It appears that all are products of Fermat numbers, and one can even guess at which Fermat numbers. For example the 6th row is F_2F_1 and $6 = 2^2+2^1$ in base 2, whereas the 7th row is $F_2F_1F_0$ and $7 = 2^2+2^1+2^0$ in base 2, and our other examples follow this same pattern. This leads to the following challenging problem:

Exercise 3.11.2.† Show that the nth row of Pascal's triangle mod 2, considered as a binary number, is given by $\prod_{j=0}^{k} F_{n_j}$, where $n = 2^{n_0} + 2^{n_1} + \cdots + 2^{n_k}$, with $0 \le n_0 < n_1 < \cdots < n_k$ (i.e., the binary expansion of n).[14]

References for this chapter

[1] Andrew Granville, *Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle*, Amer. Math. Monthly **99** (1992), 318–331.

[2] Kathleen M. Shannon and Michael J. Bardzell, *Patterns in Pascal's Triangle - with a Twist - First Twist: What is It?*, Convergence (December 2004).

Appendices. The extended version of chapter 3 has the following additional appendices:

Appendix 3B. *Solving linear congruences.* We develop Gauss's methods for solving linear congruences in several variables with composite moduli. We then prove the general form of the Chinese Remainder Theorem.

Appendix 3C. *Groups and rings.* We present some of the basics of groups and rings and show how the multiplicative and additive groups mod m can be viewed in this more abstract way. We also prove the Fundamental Theorem of Abelian Groups.

Appendix 3D. *Unique factorization revisited.* We discuss various situations in which unique factorization works and situations in which it does not. This leads us to a discussion of the properties of ideals which allows us to recover a notion of unique factorization in all situations.

Appendix 3E. *Gauss's approach.* We review Gauss's approach to unique factorization.

[14] An m-sided regular polygon with m odd is constructible with ruler and compass (see section 0.18 of appendix 0G) if and only if m is the product of distinct Fermat primes. Therefore the integers m created here include all of the odd m-sided, constructible, regular polygons.

Appendix 3F. *The Fundamental theorems and factoring* states that a polynomial of degree d, with coefficients in $\mathbb{C}$, has exactly d roots, counted with multiplicity. We indicate how to prove this and go on to better understand polynomials and their reductions mod m, as well as how resultants tell us how polynomials factor mod m.

Appendix 3G. *Open problems*. Here we revisit the Frobenius postage stamp problem and Egyptian fractions and introduce the $3x + 1$ conjecture.

Chapter 4

Multiplicative functions

In the previous chapter we discussed $\tau(n)$, which counts the number of divisors of n. We discovered that $\tau(n)$ is a multiplicative function, which allowed us to calculate its value fairly easily. *Multiplicative functions*, so called since

$$f(mn) = f(m)f(n) \text{ for all pairwise coprime, positive integers } m \text{ and } n,$$

play a central role in number theory. (Moreover f is *totally multiplicative*, or *completely multiplicative*, if $f(mn) = f(m)f(n)$ for all integers $m, n \geq 1$.) Thus the divisor function, $\tau(n)$, is multiplicative but not totally multiplicative, since $\tau(p^a) = a + 1$, and so $\tau(p^2) = 3$ is not equal to $\tau(p)^2 = 2^2$. Common examples of totally multiplicative functions include $f(n) = 1$, $f(n) = n$, and $f(n) = n^s$ for a fixed complex number s. Also Liouville's function $\lambda(n)$ which equals -1 to the power of the total number of prime factors of n, counting repetitions of the same prime factor. For example $\lambda(2) = \lambda(3) = \lambda(12) = \lambda(32) = -1$ and $\lambda(4) = \lambda(6) = \lambda(10) = \lambda(60) = 1$.

What makes multiplicative functions central to number theory is that one can evaluate a multiplicative function $f(n)$ in terms of the $f(p^e)$ for the prime powers p^e dividing n.

Exercise 4.0.1. Show that if f is multiplicative and $n = \prod_{p \text{ prime}} p^{e_p}$, then

$$f(n) = \prod_{p \text{ prime}} f(p^{e_p}).$$

Deduce that if f is totally multiplicative, then $f(n) = \prod_p f(p)^{e_p}$.

Exercise 4.0.2. Prove that if f is a multiplicative function, then either $f(n) = 0$ for all $n \geq 1$ or $f(1) = 1$.

Exercise 4.0.3. Prove that if f and g are multiplicative functions, then so is h, where $h(n) = f(n)g(n)$ for all $n \geq 1$.

Exercise 4.0.4. Prove that if f is completely multiplicative and $d|n$, then $f(d)$ divides $f(n)$.

Exercise 4.0.5. Prove that if f is multiplicative and a and b are any two positive integers, then

$$f((a,b))f([a,b]) = f(a)f(b).$$

In this chapter we will focus on two multiplicative functions of great interest.

4.1. Euler's ϕ-function

There are

$$\phi(n) := \#\{m : \ 1 \le m \le n \text{ and } (m,n) = 1\}$$

elements in any reduced system of residues mod n. Obviously $\phi(1) = 1$.

Lemma 4.1.1. *$\phi(n)$ is a multiplicative function.*

Proof. Suppose that $n = mr$ where $(m,r) = 1$. By the Chinese Remainder Theorem (Theorem 3.6) there is a natural bijection between the integers $a \pmod n$ with $(a,n) = 1$ and the pairs of integers $(b \pmod m, c \pmod r)$ with $(b,m) = (c,r) = 1$. Since there are $\phi(m)\phi(r)$ such pairs (b,c) we deduce that $\phi(n) = \phi(m)\phi(r)$. □

Hence to evaluate $\phi(n)$ for all n we simply need to evaluate it on the prime powers, by exercise 4.0.1. This is straightforward because $(m,p^e) = 1$ if and only if $(m,p) = 1$; and $(m,p) = 1$ is not satisfied if and only if p divides m. Therefore

$$\begin{aligned}\phi(p^e) &= \#\{m : \ 1 \le m \le p^e \text{ and } (m,p) = 1\}\\ &= \#\{m : \ 1 \le m \le p^e\} - \#\{m : \ 1 \le m \le p^e \text{ and } p|m\}\\ &= p^e - p^{e-1}\end{aligned}$$

by exercise 1.7.6(c). We deduce the following:

Theorem 4.1. *If $n = \prod_{p \ prime} p^{e_p}$, then*

$$\phi(n) = \prod_{\substack{p \ prime\\ p|n}} (p^{e_p} - p^{e_p-1}) = \prod_{\substack{p \ prime\\ p|n}} p^{e_p}\left(1 - \frac{1}{p}\right) = n \prod_{\substack{p \ prime\\ p|n}} \left(1 - \frac{1}{p}\right).$$

Example. $\phi(60) = 60 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16$, the least positive residues being

$$1, 7, 11, 13, \ 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, \text{ and } 59.$$

We give an alternative proof of Theorem 4.1, based on the inclusion-exclusion principle, in section 4.5.

Studying the values taken by $\phi(n)$, one makes a surprising observation:

Proposition 4.1.1. *We have $\sum_{d|n} \phi(d) = n$.*

Example. For $n = 30$, we have

$$\begin{aligned}\phi(1) + \phi(2) + \phi(3) + \phi(5) + \phi(6) + \phi(10) + \phi(15) + \phi(30)\\ = \ 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = \ 30.\end{aligned}$$

Proof. Given any integer m with $1 \le m \le n$, let $d = n/(m,n)$, which divides n. Then $(m,n) = n/d$ so one can write $m = an/d$ with $(a,d) = 1$ and $1 \le a \le d$. Now, for each divisor d of n the number of integers m for which $(m,n) = n/d$ equals the number of integers a for which $(a,d) = 1$ and $1 \le a \le d$, which is $\phi(d)$ by definition. We have therefore shown that

$$\begin{aligned} n = \#\{m:\ 1 \le m \le n\} &= \sum_{d|n} \#\{m:\ 1 \le m \le n \text{ and } (m,n) = n/d\} \\ &= \sum_{d|n} \#\{m:\ m = a(n/d),\ 1 \le a \le d \text{ and } (a,d) = 1\} \\ &= \sum_{d|n} \#\{a:\ 1 \le a \le d \text{ and } (a,d) = 1\} = \sum_{d|n} \phi(d), \end{aligned}$$

which is the result claimed. □

Exercise 4.1.1. Prove that if $d|n$, then $\phi(d)$ divides $\phi(n)$.

Exercise 4.1.2. Prove that if n is odd and $\phi(n) \equiv 2 \pmod 4$, then n has exactly one prime factor (perhaps repeated several times).

Exercise 4.1.3. Prove that $\sum_{1\le m\le n,\ (m,n)=1} m = n\phi(n)/2$ and $\prod_{d|n} d = n^{\tau(n)/2}$.

Exercise 4.1.4. (a) Prove that $\phi(n^2) = n\phi(n)$.
(b) Prove that if $\phi(n)|n-1$, then n is squarefree.
(c) Find all integers n for which $\phi(n)$ is odd.

Exercise 4.1.5.† Suppose that n has exactly k prime factors, each of which is $> k$. Prove that $\phi(n) \ge n/2$.

4.2. Perfect numbers. *"The whole is equal to the sum of its parts."*

The number 6 is a *perfect number* since it is the sum of its *proper* divisors (the *proper divisors* of m are those divisors d of m for which $1 \le d < m$); that is,

$$6 = 1 + 2 + 3.$$

> *Six is a number perfect in itself, and not because God created all things in six days; rather, the converse is true. God created all things in six days because the number is perfect.*
>
> — from *The City of God* by Saint Augustine (354–430)

The next perfect number is $28 = 1 + 2 + 4 + 7 + 14$ which is the number of days in a lunar month. However the next, $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$, appears to have little obvious cosmic relevance. Nonetheless, we will be interested in trying to classify all perfect numbers. To create an equation we will add n to both sides to obtain that n is perfect if and only if

$$2n = \sigma(n), \text{ where } \sigma(n) := \sum_{d|n} d.$$

Exercise 4.2.1. Show that $\sigma(n) = \sum_{d|n} n/d$, and so deduce that n is perfect if and only if $\sum_{d|n} \frac{1}{d} = 2$.

Exercise 4.2.2. (a) Prove that each divisor d of ab can be written as ℓm where $\ell|a$ and $m|b$.
(b) Show that if $(a,b)=1$, then there is a unique such pair ℓ, m for each divisor d.

By this last exercise we see that if $(a,b)=1$, then

$$\sigma(ab)=\sum_{d|ab} d=\sum_{\ell|a,\ m|b} \ell m=\sum_{\ell|a}\ell\cdot\sum_{m|b} m=\sigma(a)\sigma(b),$$

proving that σ is a multiplicative function. Now

$$\sigma(p^k)=1+p+p^2+\cdots+p^k=\frac{p^{k+1}-1}{p-1}$$

by definition, and so

$$\boxed{\text{If } n=\prod_p p^{k_p},\ \text{then } \sigma(n)=\prod_p \frac{p^{k_p+1}-1}{p-1}.}$$

For example $\sigma(2^5\cdot 3^3\cdot 5^2\cdot 7)=\frac{2^6-1}{2-1}\cdot\frac{3^4-1}{3-1}\cdot\frac{5^3-1}{5-1}\cdot\frac{7^2-1}{7-1}$.

Euclid observed that the first perfect numbers factor as $6=2\cdot 3$ where $3=2^2-1$ is prime, and $28=2^2\cdot 7$ where $7=2^3-1$ is prime, and then that this pattern persists:

Proposition 4.2.1 (Euclid)**.** *If 2^p-1 is a prime number, then $2^{p-1}(2^p-1)$ is a perfect number.*

The cases $p=2,\ 3,\ 5$ correspond to the Mersenne primes $2^2-1=3,\ 2^3-1=7,\ 2^5-1=31$ and therefore yield the three smallest perfect numbers 6, 28, 496 (and the next smallest examples are given by $p=7$ and $p=13$).

Proof. Since σ is multiplicative we have, for $n=2^{p-1}(2^p-1)$,

$$\sigma(n)=\sigma(2^{p-1})\cdot\sigma(2^p-1)=\frac{2^p-1}{2-1}\cdot(1+(2^p-1))=(2^p-1)\cdot 2^p=2n. \qquad \square$$

After extensive searching one finds that perfect numbers of the form $2^{p-1}(2^p-1)$ with 2^p-1 prime appear to be the only perfect numbers. Euler succeeded in proving that these are the only *even* perfect numbers, and we believe (but don't know) that there are no *odd* perfect numbers. If there are no odd perfect numbers, as claimed, then we would achieve our goal of classifying all the perfect numbers.

Theorem 4.2 (Euclid)**.** *If n is an even perfect number, then there exists a prime number of the form 2^p-1 such that $n=2^{p-1}(2^p-1)$.*

In exercise 3.9.1 we showed that if 2^p-1 is prime, then p must itself be prime. Now, although $2^2-1, 2^3-1, 2^5-1$, and 2^7-1 are all prime, $2^{11}-1=23\times 89$ is not, so we do not know for sure whether 2^p-1 is prime, even if p is prime. However it is conjectured that there are infinitely many Mersenne primes $M_p=2^p-1$,[1] which would imply that there are infinitely many even perfect numbers.

[1]It is known that 2^p-1 is prime for $p=2,3,5,7,13,17,19,\ldots,82589933$, a total of 51 values as of September 2019 (and this last is currently the largest prime explicitly known). There is a long history of the search for Mersenne primes, from the first serious computers to the first great distributed computing project, GIMPS (Great Internet Mersenne Prime Search).

Proof. Any even integer can be written as $n = 2^{k-1}m$ where m is odd and $k \geq 2$, so that if n is perfect, then

$$2^k m = 2n = \sigma(n) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

Now $(2^k - 1, 2^k) = 1$ and so $2^k - 1$ divides m. Writing $m = (2^k - 1)M$ we find that $\sigma(m) = 2^k M = m + M$. That is, $\sigma(m)$, which is the sum of all of the divisors of m, equals the sum of just two of its divisors, namely m and M (and note that these are different integers since $m = (2^k - 1)M \geq (2^2 - 1)M > M$). This implies that m and M are the only divisors of m. The only integers with just two divisors are the primes, so that m is a prime and $M = 1$, and the result follows. □

It is widely believed that the only perfect numbers were those identified by Euclid, that is, that there are no odd perfect numbers. It has been proved that if there is an odd perfect number, then it must be $> 10^{1500}$, and it would have to have more than 100 (not necessarily distinct) prime factors.

Exercise 4.2.3. (a) Prove that if p is odd and k is odd, then $\sigma(p^k)$ is even.
(b)† Deduce that if n is an odd perfect number, then $n = p^\ell m^2$ where p is a prime that does not divide the integer $m \geq 1$ and $p \equiv \ell \equiv 1 \pmod 4$.

Exercise 4.2.4. Fix integer $m > 1$. Show that there are only finitely many integers n for which $\sigma(n) = m$.

Exercise 4.2.5.† (a) Prove that for all integers $n > 1$ we have the inequalities

$$\prod_{p|n} \frac{p+1}{p} \leq \frac{\sigma(n)}{n} < \prod_{p|n} \frac{p}{p-1}.$$

(b) We have seen that every even perfect number has exactly two distinct prime factors. Prove that every odd perfect number has at least three distinct prime factors.

Additional exercises

Exercise 4.3.1. Suppose that $f(n) = 0$ if n is even, $f(n) = 1$ if $n \equiv 1 \pmod 4$, and $f(n) = -1$ if $n \equiv -1 \pmod 4$. Prove that $f(.)$ is a multiplicative function.

Exercise 4.3.2.† Suppose that $r(.)$ is a multiplicative function taking values in $\mathbb{C}$. Let $f(n) = 1$ if $r(n) \neq 0$, and $f(n) = 0$ if $r(n) = 0$. Prove that $f(.)$ is also a multiplicative function.

Exercise 4.3.3.† Suppose that f is a multiplicative function, such that the value of $f(n)$ depends only on the value of $n \pmod 3$. What are the possibilities for f?

Exercise 4.3.4.‡ Suppose that f is a multiplicative function, such that the value of $f(n)$ depends only on the value of $n \pmod 8$. What are the possibilities for f?

Exercise 4.3.5. How many of the fractions a/n with $1 \leq a \leq n - 1$ are reduced?

Looking at the values of $\phi(m)$, Carmichael conjectured that for all integers m there exists an integer $n \neq m$ such that $\phi(n) = \phi(m)$.

Exercise 4.3.6.† (a) Find all integers n for which $\phi(2n) = \phi(n)$.
(b) Find all integers n for which $\phi(3n) = \phi(2n)$.
(c) Can you find other classes of m for which Carmichael's conjecture is true?

Carmichael's conjecture is still an open problem but it is known that if it is false, then the smallest counterexample is $> 10^{10^{10}}$.

Exercise 4.3.7.† (a) Given a polynomial $f(x) \in \mathbb{Z}[x]$ let $N_f(m)$ denote the number of $a \pmod m$ for which $f(a) \equiv 0 \pmod m$. Show that $N_f(m)$ is a multiplicative function.
(b) Be explicit about $N_f(m)$ when $f(x) = x^2 - 1$. (You can use section 3.8.)

Exercise 4.3.8.‡ Given a polynomial $f(x) \in \mathbb{Z}[x]$ let $R_f(m)$ denote the number of $b \pmod m$ for which there exists $a \pmod m$ with $f(a) \equiv b \pmod m$. Show that $R_f(m)$ is a multiplicative function. Can you be more explicit about $R_f(m)$ for $f(x) = x^2$, the example of exercise 2.5.6?

Exercise 4.3.9. Let $\tau(n)$ denote the number of divisors of n (as in section 3.3), and let $\omega(n)$ and $\Omega(n)$ be the number of prime divisors of n not counting and counting repeated prime factors, respectively. Therefore $\tau(12) = 6, \omega(12) = 2$, and $\Omega(12) = 3$. Prove that

$$2^{\omega(n)} \le \tau(n) \le 2^{\Omega(n)} \text{ for all integers } n \ge 1.$$

Exercise 4.3.10. Let $\sigma_k(n) = \sum_{d|n} d^k$. Prove that $\sigma_k(n)$ is multiplicative.

Exercise 4.3.11. (a) Prove that $\tau(ab) \le \tau(a)\tau(b)$ for all positive integers a and b, with equality if and only if $(a, b) = 1$,
(b) Prove that $\sigma_k(ab) \le \sigma_k(a)\sigma_k(b)$ for all positive integers a, b, and k.
(c) Prove that $\sigma_{k+\ell}(n) \le \sigma_k(n)\sigma_\ell(n)$ for all positive integers k, ℓ, and n.

Exercise 4.3.12. Give closed formulas for (a)† $\sum_{m=1}^{n} \gcd(m, n)$ and (b)‡ $\sum_{m=1}^{n} \operatorname{lcm}(m, n)$ in terms of the prime power factors of n.

Exercise 4.3.13. n is *multiplicatively perfect* if it equals the product of its proper divisors.
(a) Show that n is multiplicatively perfect if and only if $\tau(n) = 4$.
(b) Classify exactly which integers n satisfy this.

The integers m and n are *amicable* if the sum of the proper divisors of m equals n and the sum of the proper divisors of n equals m. For example, 220 and 284 are amicable, as are 1184 and 1210.[2]

Exercise 4.3.14. (a) Show that m and n are amicable if and only if $\sigma(m) = \sigma(n) = m + n$.
(b) Verify Thâbit ibn Qurrah's 9th-century claim that if $p = 3 \times 2^{n-1} - 1$, $q = 3 \times 2^n - 1$, and $r = 9 \times 2^{2n-1} - 1$ are each odd primes, then $2^n pq$ and $2^n r$ are amicable.[3]
(c) Find an example (other than the two given above) using the construction in (b).

An integer n is *abundant* if the sum of its proper divisors is $> n$, for example $n = 12$; and n is *deficient* if the sum of its proper divisors is $< n$, for example $n = 8$. Each positive integer is either deficient, perfect, or abundant, a classification that goes back to antiquity.[4]

Exercise 4.3.15. (a) Prove that every prime number is deficient.
(b) Prove that every multiple of 6 is abundant.
(c) How do these concepts relate to the value of $\sigma(n)/n$?
(d) Prove that every multiple of an abundant number is abundant.
(e)† Prove that if n is the product of k distinct primes that are each $> k$, then n is deficient.
(f) Prove that every divisor of a deficient number is deficient.

[2]The 14th-century scholar Ibn Khladun claimed: "Experts on talismans assure me that these numbers have a special influence in establishing strong bonds of friendship between individuals ... A bond so close that they cannot be separated. The author of the Ghaia, and other great masters in this art, swear that they have seen this happen again and again."

[3]This was rediscovered by Descartes in the 17th century.

[4]Specifically a book by Nichomachus from A.D. 100. Another interesting reference is the 10th-century German nun Hrotsvitha who depicts the heroine of her play "*Sapientia*" challenging Emperor Hadrian while he is persecuting Christians, to surmise the ages of her children from information about this classification and the number of Olympic games that each has been alive for!

Carl André is a controversial minimalist artist, his most infamous work being his *Equivalent I–VIII* series exhibited at several of the world's leading museums. Each of the eight sculptures involves 120 bricks arranged in a different rectangular formation. In *Equivalent VIII*, at the Tate Modern in London, the bricks are stacked 2 deep, 6 wide, and 10 long. (See http://thesingleroad.blogspot.co.uk/2011/01/test-post.html for a photo of the original eight formations.)

Exercise 4.3.16. (a) How many different 2-deep, 120-brick, rectangular formations are there? (b) What if there must be at least three bricks along the width and along the length?

Appendix 4A. More multiplicative functions

4.4. Summing multiplicative functions

We have already seen that the functions 1, n, $\phi(n)$, $\sigma(n)$, and $\tau(n)$ are all multiplicative. In Proposition 4.1.1 we saw the surprising connection that n is the sum of the multiplicative function $\phi(d)$, summed over the divisors d of n. Similarly $\tau(n)$ is the sum of 1, and $\sigma(n)$ is the sum of d, summed over the divisors d of n. This suggests that there might be a general such phenomenon.

Theorem 4.3. *For any given multiplicative function f, the function*

$$F(n) := \sum_{d|n} f(d)$$

is also multiplicative.

Proof. Suppose that $n = ab$ with $(a, b) = 1$. In exercise 4.2.2 we showed that the divisors of n can be written as ℓm where $\ell|a$ and $m|b$. Note that $(\ell, m) = 1$ since (ℓ, m) divides $(a, b) = 1$ and so $f(\ell m) = f(\ell)f(m)$. Therefore

$$F(ab) = \sum_{d|ab} f(d) = \sum_{\substack{\ell|a \\ m|b}} f(\ell m) = \sum_{\ell|a} f(\ell) \sum_{m|b} f(m) = F(a)F(b),$$

as desired. □

It is worth noting that if we write $m = n/d$, then Theorem 4.3 becomes

$$F(n) := \sum_{m|n} f(n/m).$$

Above we have the examples $\{F(n), f(d)\} = \{n, \phi(d)\}$, $\{\tau(n), 1\}$, $\{\sigma(n), d\}$; but what about for other $F(n)$? For $F(n) = 1$ we have $1 = \sum_{d|n} \delta(d)$ where

$\delta(d) = 1$ if $d = 1$, and $= 0$ otherwise. Finding f when $F(n) = \delta(n)$ looks more complicated. This leads us to two questions: For every multiplicative F, does there exist a multiplicative f for which $F(n) := \sum_{d|n} f(d)$? And, if so, is f unique? To answer these questions we begin by defining another multiplicative function which arises in a rather different context.

Exercise 4.4.1. Prove that $\frac{n}{\phi(n)} = \sum_{\substack{d|n \\ d \text{ squarefree}}} \frac{1}{\phi(d)}$.

4.5. Inclusion-exclusion and the Möbius function

In the proof of Theorem 4.1 we saw that if $n = p^a$ is a prime power, then $\phi(n)$ is the total number of integers up to n, minus the number of those that are divisible by p. This leads to the formula

$$\phi(n) \;=\; n - \frac{n}{p} \;=\; n\left(1 - \frac{1}{p}\right).$$

Similarly if $n = p^a q^b$, then we wish to count the number of positive integers up to n that are not divisible by either p or q. To do so we take the n integers up to n, subtract the n/p that are divisible by p and the n/q that are divisible by q. This is not quite right as we have twice subtracted the n/pq integers divisible by both p and q, and so we need to add them back in. This leads to the formula

$$\phi(n) \;=\; n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq} \;=\; n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

This argument generalizes to arbitrary n, though we need to keep track of the terms of the form $\pm n/d$. In our examples so far, we see that each such d is a divisor of n, but the term n/d only has a non-zero coefficient if d is squarefree. When d is squarefree the coefficient is given by $(-1)^{\omega(d)}$ where

$$\omega(d) := \sum_{p \text{ prime},\ p|d} 1$$

is the number of distinct prime factors of d. One therefore deduces that the coefficient of n/d is always given by the *Möbius* function, $\mu(d)$, a multiplicative function defined by

$$\mu(p) = -1, \text{ with } \mu(p^k) = 0 \text{ for all } k \geq 2, \text{ for every prime } p.$$

For example $\mu(1) = 1$, $\mu(2) = \mu(3) = -1$, $\mu(4) = 0$, $\mu(6) = \mu(10) = 1$, and $\mu(1001) = -1$ as $1001 = 7 \times 11 \times 13$.

The argument for general n uses the *inclusion-exclusion principle*, which we formulate here to fit well with the topic of multiplicative functions.

Corollary 4.5.1. *We have*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The result for $n = 1$ is trivial. If n is a prime power p^a with $a \geq 2$, then $\sum_{d|p^a} \mu(d) = 1 + (-1) + 0 + \cdots + 0 = 0$ by definition.

The result for general n then follows from Theorem 4.3. □

Exercise 4.5.1. (a) Show that if m is squarefree, then

$$(1+x)^{\omega(m)} = \sum_{d|m} x^{\omega(d)}.$$

(b) Deduce Corollary 4.5.1.

A proof of Theorem 4.1 using the inclusion-exclusion principle. We want a function that counts 1 if $(a,n)=1$ and 0 otherwise. This counting function can be given by Corollary 4.5.1:

$$\sum_{d|a \ \& \ d|n} \mu(d) = \begin{cases} 1 & \text{if } (a,n)=1, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned} \phi(n) &= \sum_{a=1}^{n} \begin{cases} 1 & \text{if } (a,n)=1, \\ 0 & \text{otherwise.} \end{cases} \\ &= \sum_{a=1}^{n} \sum_{d|a \ \& \ d|n} \mu(d) \\ &= \sum_{d|n} \mu(d) \sum_{\substack{1\le a\le n \\ d|a}} 1 = \sum_{d|n} \mu(d) \, \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}. \end{aligned}$$

The last line comes from first swapping the order of summation and then using exercise 1.7.6(c) as $[n/d] = n/d$ since each d divides n. Exercise 4.5.2 completes the proof. □

Exercise 4.5.2. Prove that for any positive integer n we have

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{\substack{p \text{ prime} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

Exercise 4.5.3. Prove that $\mu(n)^2$ is the characteristic function for the squarefree integers, and deduce that $\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu(d)^2}{\phi(d)}$.

4.6. Convolutions and the Möbius inversion formula

In the proof of Theorem 4.1 in the last section we saw that

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

If we let $r = n/d$, then the sum is over all factorizations of n into two positive integers $n = dr$, and so

$$\phi(n) = \sum_{\substack{d,r\ge 1 \\ n=dr}} \mu(d) r.$$

This can be compared to Proposition 4.1.1 which yielded

$$n = \sum_{d|n} \phi(d) = \sum_{\substack{d,r\ge 1 \\ n=dr}} \phi(d) 1(r),$$

where $1(r)$ is the function that is always 1 (which is a multiplicative function). Something similar happens for the sum of any function f defined on the positive integers.

Theorem 4.4 (The Möbius inversion formula)**.** *For any two arithmetic functions f and g we have*

$$g(n) = \sum_{ab=n} f(b) \text{ for all integers } n \geq 1$$

if and only if

$$f(m) = \sum_{cd=m} \mu(c)g(d) \text{ for all integers } m \geq 1.$$

This can be rewritten as

$$g(n) = \sum_{d|n} f(d) \text{ for all } n \geq 1 \text{ if and only if } f(m) = \sum_{d|m} \mu(m/d)g(d) \text{ for all } m \geq 1.$$

Proof. If $f(m) = \sum_{cd=m} \mu(c)g(d)$ for all integers $m \geq 1$, then

$$\sum_{ab=n} f(b) = \sum_{ab=n} \sum_{cd=b} \mu(c)g(d) = \sum_{acd=n} \mu(c)g(d) = \sum_{d|n} g(d) \cdot \sum_{ac=n/d} \mu(c) = g(n),$$

since this last sum is 0 unless $n/d = 1$, that is, unless $d = n$. Similarly if $g(n) = \sum_{ab=n} f(b)$ for all integers $n \geq 1$, then

$$\sum_{cd=m} \mu(c)g(d) = \sum_{cd=m} \mu(c) \sum_{ab=d} f(b) = \sum_{abc=m} \mu(c)f(b) = \sum_{b|m} f(b) \sum_{ac=\frac{m}{b}} \mu(c) = f(m),$$

as desired. □

In the discussion above we saw several examples of the *convolution* $f * g$ of two multiplicative functions f and g, which we define by

$$(f * g)(n) := \sum_{ab=n} f(a)g(b).$$

Note that $f * g = g * f$. We saw that if $I(n) = n$, then $\phi * 1 = I$ and $\mu * I = \phi$, as well as $1 * \mu = \delta$.

Exercise 4.6.1. Prove that $\delta * f = f$ for all f, $\tau = 1 * 1$, and $\sigma(n) = 1 * I$.

Proposition 4.6.1. *For any two multiplicative functions f and g, the convolution $f * g$ is also multiplicative.*

Exercise 4.6.2. Prove that if $ab = mn$, then there exist integers r, s, t, u with $a = rs$, $b = tu$, $m = rt$, $n = su$ with $(s, t) = 1$.

Proof. Suppose that $(m, n) = 1$. For $h = f * g$, we have

$$h(mn) = \sum_{ab=mn} f(a)g(b).$$

We use exercise 4.6.2 and note that (r,s) and (t,u) both divide $(m,n)=1$ and so both equal 1. Therefore $f(a)=f(rs)=f(r)f(s)$ and $g(b)=g(tu)=g(t)g(u)$. This implies that

$$h(mn)=\sum_{\substack{rt=m,\\ su=n}} f(rs)g(tu)=\sum_{rt=m} f(r)g(t)\sum_{su=n} f(s)g(u)=h(m)h(n). \qquad \square$$

In this new language, Theorem 4.3, which states that $1*f$ is multiplicative whenever f is, is the special case $g=1$ of Proposition 4.6.1. Corollary 4.5.1 states that $1*\mu=\delta$. The Möbius inversion formula states that $F=1*f$ if and only if $f=\mu*F$. It is also easy to prove the Möbius inversion formula with this notation since if $F=1*f$, then $\mu*F=\mu*1*f=\delta*f=f$; and if $f=\mu*F$, then $1*f=1*\mu*F=\delta*F=F$.

Exercise 4.6.3. Prove that $(\mu*\sigma)(n)=n$ for all integers $n\geq 1$.

Exercise 4.6.4. (a) Show that $(a*f)+(b*f)=(a+b)*f$.
(b) Let $f(n)\geq 0$ for all integers $n\geq 1$. Prove that $(1*f)(n)+(\mu*f)(n)\geq 2f(n)$ for all integers $n\geq 1$.
(c) Prove that $\sigma(n)+\phi(n)\geq 2n$ for all integers $n\geq 1$.

Exercise 4.6.5. Suppose that $g(n)=\prod_{d|n} f(d)$. Deduce that $f(n)=\prod_{d|n} g(d)^{\mu(n/d)}$.

4.7. The Liouville function

The number of prime factors of a given integer $n=\prod_{i=1}^{k} p_i^{e_i}$ can be interpreted in two different ways:

$$\omega(n):=\sum_{p|n} 1=\#\{\text{distinct primes that divide } n\}=k$$

and

$$\Omega(n):=\sum_{\substack{p \text{ prime},\ k\geq 1\\ p^k|n}} 1=\#\{\text{distinct prime powers that divide } n\}=\sum_{i=1}^{k} e_i.$$

In other words, $\Omega(n)$ counts the number of primes when one factors n into primes without using exponents, so $\Omega(12)=3$ as $12=2\times 2\times 3$, while $\omega(n)$ counts the number of primes when one factors n into primes using exponents, so $\omega(12)=2$ as $12=2^2\cdot 3$. For other examples, $\omega(27)=1$ with $\Omega(27)=3$, and $\omega(36)=2$ with $\Omega(36)=4$, while $\Omega(105)=\omega(105)=3$.

Another interesting multiplicative function is Liouville's function, defined at the start of this chapter by $\lambda(n)=(-1)^{\Omega(n)}$ so that, for example, $\lambda(12)=(-1)^3=-1$. We notice that λ is the totally multiplicative function that agrees with μ on the squarefree integers. Liouville's function feels, intuitively, more natural, but Möbius's function fits better with the theory.

Exercise 4.7.1. Prove that $\Omega(n)\geq\omega(n)$ for all integers $n\geq 1$, with equality if and only if n is squarefree.

Exercise 4.7.2. Prove that $\lambda*\mu^2=\delta$.

Exercise 4.7.3. (a) Prove that

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases}$$

(b)† By summing the formula in (a) over all positive integers $n \le N$, deduce that for all integers $N \ge 1$ we have

$$\sum_{n \ge 1} \lambda(n) \left[\frac{N}{n} \right] = [\sqrt{N}].$$

Additional exercises

Exercise 4.8.1. Prove that $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$ for all integers $n \ge 1$.

Exercise 4.8.2. Prove that $\phi(n) + \sigma(n) = 2n$ if and only if $n = 1$ or n is a prime.

Exercise 4.8.3. (a) By summing the formula in Corollary 4.5.1 over all positive integers $n \le N$, deduce that

$$\sum_{n \ge 1} \mu(n) \left[\frac{N}{n} \right] = 1 \quad \text{for all } N \ge 1.$$

(b)† Deduce that

$$\left| \sum_{n \le N} \frac{\mu(n)}{n} \right| \le 1 \quad \text{for all } N \ge 1.$$

It is a much deeper problem to prove that $\sum_{n \le N} \mu(n)/n$ tends to a limit as $N \to \infty$.

Exercise 4.8.4. (a) Prove that if f is an arithmetic function, then

$$\sum_{n \ge 1} f(n) \frac{x^n}{1 - x^n} = \sum_{m \ge 1} (1 * f)(m) x^m,$$

without worrying about convergence.

(b) Write out explicitly the example $f = \mu$ as well as some other common multiplicative functions.

Appendices. The extended version of chapter 4 has the following additional appendices:

Appendix 4B. *Dirichlet series and multiplicative functions.* We discuss the construction of Dirichlet series, establishing that they have an Euler product if the coefficients are given by a multiplicative function. We discuss convergence issues, interesting Dirichlet series, and important identities.

Appendix 4C. *Irreducible polynomials mod p.* We develop, in part, the analogy to the theory of this chapter when working with polynomials mod p, giving a formula for the number of irreducibles.

Appendix 4D. *The harmonic sum and the divisor function.* We develop upper and lower bounds for the sum of $1/n$ over positive integers $n \le N$ and use these to determine a good estimate for the average number of divisors of an integer. We develop Dirichlet's hyperbola method to get a spectacularly accurate estimate for this average.

Appendix 4E. *Cyclotomic polynomials.* We introduce their properties which will come in useful in several areas, later on.

Chapter 5

The distribution of prime numbers

Once one begins to determine which integers are primes, one quickly finds that there are many. Are there infinitely many? One notices that the primes seem to make up a decreasing proportion of the positive integers. Can we explain this? Can we give a formula for how many primes there are up to a given point? Or at least give a good estimate?

When we write out the primes there seem to be patterns, though the patterns rarely persist for long. Can we find patterns that do persist? Is there a formula that describes all of the primes? Or at least some of them?

Is it possible to recognize prime numbers quickly and easily?

These questions motivate different parts of this chapter and of chapter 10.

5.1. Proofs that there are infinitely many primes

The first known proof appears in Euclid's *Elements*, Book IX, Proposition 20:

Theorem 5.1. *There are infinitely many primes.*

Proof #1.[1] Suppose that there are only finitely many primes, which we will denote by $2 = p_1 < p_2 = 3 < \cdots < p_k$. What are the prime factors of $p_1 p_2 \dots p_k + 1$? Since this number is > 1 it must have a prime factor by the Fundamental Theorem of Arithmetic, and this must be p_j for some j, $1 \le j \le k$, since *all* primes are contained amongst $p_1, p_2, \dots, p_k$. But then p_j divides both $p_1 p_2 \dots p_k$ and $p_1 p_2 \dots p_k + 1$, and hence p_j divides their difference, 1, by exercise 1.1.1(c), which is impossible. □

[1] Not until relatively recently has there been mathematical notation to describe a collection of objects, for example, $p_1, p_2, \dots, p_k$. Neither Euclid nor Fermat had subscripts or "..." or "etc." (Gauss used "&c"). So instead the reader had to infer from the context how many objects the author meant. In Euclid's *Elements*, he writes that he assumes α, β, γ denote all of the prime numbers and then gives, in terms of ideas, the same proof as here. The reader had to understand that in writing "α, β, γ", Euclid meant an arbitrary number of primes, not just three!

There are many variants on Euclid's proof. For example:

Exercise 5.1.1 (Proof #2)**.** Suppose that there are only finitely many primes, the largest of which is $n > 2$. Show that this is impossible by considering the prime factors of $n! - 1$.

Other variants include Furstenberg's curious proof using point-set topology (see appendix 5F). These all boil down to showing that there exists an integer $q > 1$ that is not divisible by any of a given finite set of primes $p_1, \dots, p_k$. If $m = p_1 p_2 \cdots p_k$, then we wish to show there exists an integer $q > 1$ with $(q, m) = 1$, and there are $\phi(m) - 1$ such integers up to m. There is therefore such an integer by the formula in Theorem 4.1 once $m > 2$.

Exercise 5.1.2. Prove that there are infinitely many composite numbers.

Euclid's proof that there are infinitely many primes is a "proof by contradiction", showing that it is impossible that there are finitely many, and so does not suggest how one might find infinitely many. We can use the following constructive technique to determine infinitely many primes:

Lemma 5.1.1. *Suppose that $a_1 < a_2 < \cdots$ is an infinite sequence of pairwise coprime positive integers, and let p_n be a prime factor of a_n for each $n \geq 2$. Then $p_2, p_3, \dots$ is an infinite sequence of distinct primes.*

Proof. If $p_m = p_n$ with $1 < m < n$, then p_m divides both a_m and a_n and so divides $(a_m, a_n) = 1$, which is impossible. □

By Lemma 5.1.1 we need only find an infinite sequence of pairwise coprime positive integers to obtain infinitely many primes. This can be achieved by modifying Euclid's construction. We define the sequence

$$a_1 = 2,\ a_2 = 3 \text{ and then } \ a_n = a_1 a_2 \dots a_{n-1} + 1 \text{ for each } n \geq 2.$$

Now if $m < n$, then $a_n \equiv 1 \pmod{a_m}$ and so $(a_m, a_n) = (a_m, 1) = 1$ by exercise 2.1.5, as desired. Therefore, by Lemma 5.1.1, we can take a prime factor p_n of each a_n with $n > 1$ to obtain an infinite sequence of prime numbers.

Fermat conjectured that the integers $F_n = 2^{2^n} + 1$ are primes for all $n \geq 0$. His claim starts off correct: $3, 5, 17, 257, 65537$ are all prime, but his conjecture is false for $F_5 = 641 \times 6700417$, as Euler famously noted. It is an open question as to whether there are infinitely many primes of the form F_n.[2] Using the identity

$$F_n = F_1 F_2 \dots F_{n-1} + 2 \text{ for each } n \geq 1 \tag{5.1.1}$$

we see that if $m < n$, then $F_n \equiv 2 \pmod{F_m}$ so that $(F_m, F_n) = (F_m, 2) = 1$, the last equality since each F_m is odd. Therefore, by Lemma 5.1.1, we can take a prime factor p_n of each F_n to obtain an infinite sequence of prime numbers.[3]

These proofs that there are infinitely many primes will be generalized using dynamical systems in appendix 5H.

[2] The only Fermat numbers known to be primes have $n \leq 4$. We know that the F_n are composite for $5 \leq n \leq 30$ and for many other n besides. It is always a significant moment when a Fermat number is factored for the first time. It could be that all F_n with $n > 4$ are composite or they might all be prime from some sufficiently large n onwards or some might be prime and some composite. Currently, we have no way of knowing which is true.

[3] This proof that there are infinitely many primes first appeared in a letter from Goldbach to Euler in July 1730.

Exercise 5.1.3. Prove (5.1.1).

Exercise 5.1.4. Suppose that $p_1 = 2 < p_2 = 3 < \cdots$ is the sequence of prime numbers. Use the fact that every Fermat number has a distinct prime divisor to prove that $p_n \le 2^{2^n} + 1$. What can one deduce about the number of primes up to x?

Exercise 5.1.5. (a) Show that if m is not a power of 2, then $2^m + 1$ is composite by showing that $2^a + 1$ divides $2^{ab} + 1$ whenever b is odd.
(b) Deduce that if $2^m + 1$ is prime, then there exists an integer n such that $m = 2^n$; that is, if $2^m + 1$ is prime, then it is a Fermat number $F_n = 2^{2^n} + 1$. (This also follows from exercise 3.9.3(b).)

Another interesting sequence is the *Mersenne numbers*,[4] which take the form $M_n = 2^n - 1$. After exercise 3.9.2 we observed that if M_n is prime, then n is prime and, in our discussion of perfect numbers (section 4.2) we observed that M_2, M_3, M_5, and M_7 are each prime but $M_{11} = 23 \times 89$ is not. The Lucas-Lehmer test provides a relatively quick and elegant way to test whether a given M_p is prime (see Corollary 10.10.1 in appendix 10C).

5.2. Distinguishing primes

We can determine whether a given integer n is prime in practice, by proving that it is not composite: If a given integer n is composite, then we can write it as ab, two integers both > 1. If we suppose that $a \le b$, then $a^2 \le ab = n$ and so $a \le \sqrt{n}$. Hence n must be divisible by some integer a in the range $1 < a \le \sqrt{n}$. Therefore we can test divide n by every integer a in this range, and we either discover a factor of n or, if not, we know that n must be prime. This process is called *trial division* and is too slow, in practice, except for relatively small integers n. We can slightly improve this algorithm by noting that if p is a prime dividing a, then p divides n, so we only need to test divide by the primes up to $\sqrt{n}$. This is still very slow, in practice.[5] We discuss more practical techniques in chapter 10.

Trial division is a very slow way of recognizing whether an *individual* integer is prime, but it can be organized to be a highly efficient way to determine *all* of the primes up to some given point, as observed by Eratosthenes around 200 B.C.[6]

The *sieve of Eratosthenes* provides an efficient method for finding all of the primes up to x. For example to find all the primes up to 100, we begin by writing down every integer between 2 and 100 and then deleting every composite even number; that is, one deletes (or *sieves out*) every second integer up to x after 2.

[4] In 1640, France was home to the great philosophers and mathematicians of the age, such as Descartes, Desargues, Fermat, and Pascal. From 1630 on, Father Marin Mersenne wrote letters to all of these luminaries, posting challenges and persuading them all to think about perfect numbers.

[5] How slow is "slow"? If we could test divide by one prime per second, for a year, with no rest, then we could determine the primality of 17-digit numbers but not 18-digit numbers. If we used the world's fastest computer in 2019, we could test divide 53-, but not 54-, digit numbers. In chapter 10 we will encounter much better methods that can test such a number for primality, in moments.

[6] Eratosthenes lived in Cyrene in ancient Greece, from 276 to 195 B.C. He created the grid system of latitude and longitude to draw an accurate map of the world incorporating parallels and meridians. He was the first to calculate the circumference of the earth, the tilt of the earth's axis, and the distance from the earth to the sun (and so invented the leap day). He even attempted to assign dates to what was then ancient history (like the conquest of Troy) using available evidence.

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

Deleting every even number > 2, between 2 and 100

The first undeleted integer > 2 is 3; one then deletes every composite integer divisible by 3; that is, one sieves out every third integer up to x after 3. The next undeleted integer is 5 and one sieves out every fifth integer after 5, and then every seventh integer after 7.

	2	**3**	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

	2	3	**5**	**7**	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	

Then delete remaining integers > 3 that are divisible by 3

and > 5 that are divisible by 5

and > 7 that are divisible by 7.

The sieve of Eratosthenes enables us to find all of the primes up to 100.

What's left are the primes up to 100. To obtain the primes up to any given limit x, one keeps on going like this, finding the next undeleted integer, call it p, which must be prime since it is undeleted, and then deleting every pth integer beyond p and up to x. We stop once $p > \sqrt{x}$ and then the undeleted integers are the primes $\leq x$. There are about $x \log\log x$ steps[7] in this algorithm, so it is a remarkably efficient way to find all the primes up to some given x,[8] but not for finding any particular prime.

Exercise 5.2.1. Use this method to find all of the primes up to 200.

The number of integers left after one removes the multiples of 2 is roughly $\frac{1}{2} \cdot x$, since about half of the integers up to x are divisible by 2. After one then removes

[7] How should one think about an expression like $\log\log x$? It goes to ∞ as x does, but it is a *very* slow growing function of x. For example, if $x = 10^{100}$, far more than the current estimate for the number of atoms in the universe, then $\log\log x < 5\frac{1}{2}$. Dan Shanks once wrote that "$\log\log x$ goes to infinity with great dignity."

[8] In practice, this algorithm determines which of the first x integers are prime in no more than $6x$ steps.

the multiples of 3, one expects that there are about $\frac{2}{3} \cdot \frac{1}{2} \cdot x$ integers left, since about a third of the odd integers up to x are divisible by 3. In general removing the multiples of p removes, we expect, about $1/p$ of the integers in our set and so leaves a proportion $1 - \frac{1}{p}$. Therefore we *expect* that the number of integers left unsieved in the sieve of Eratosthenes, up to x, after sieving by the primes up to y, is about

$$x \prod_{\substack{p \le y \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

The product $\prod_{p \le y}(1 - \frac{1}{p})$ is well-approximated by $e^{-\gamma}/\log y$, where γ is the Euler-Mascheroni constant discussed in section 4.14 of appendix 4D.[9] The logarithm, used here and elsewhere in this book, is the natural logarithm.

When we take $y = \sqrt{x}$, then only 1 and the primes up to x should be left in the sieve of Eratosthenes, and so one might guess from this analysis of sieve methods that the number of primes up to x is approximately

$$2e^{-\gamma} \frac{x}{\log x}. \tag{5.2.1}$$

This guess is not correct; the constant is off,[10] as we will discuss in section 5.4.

5.3. Primes in certain arithmetic progressions

How are the primes split between the arithmetic progressions modulo 3? Or modulo 4? Or modulo any given integer m? Evidently every integer in the arithmetic progression 0 (mod 3) (that is, integers of the form $3k$) is divisible by 3, so the only prime in that arithmetic progression is 3 itself. There are no such divisibility restrictions for the arithmetic progressions 1 (mod 3) and 2 (mod 3) and if we partition the primes up to 100 into these arithmetic progressions, we find:

$$\text{Primes} \equiv 1 \pmod 3 : \ 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, \ldots.$$
$$\text{Primes} \equiv 2 \pmod 3 : \ 2, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, \ldots.$$

There seem to be a lot of primes in each arithmetic progression, and they seem to be roughly equally split between the two. Let's see what we can prove. First let's deal, in general, with the analogy to the case 0 (mod 3). This includes not only 0 (mod m) but also cases like 2 (mod 4):

Exercise 5.3.1. (a) Prove that any integer $\equiv a \pmod m$ is divisible by (a, m).
(b) Deduce that if $(a, m) > 1$ and if there is a prime $\equiv a \pmod m$, then that prime is (a, m).
(c) Give examples of arithmetic progressions which contain exactly one prime and examples which contain none.
(d) Show that the arithmetic progression 2 (mod 6) contains infinitely many prime powers.

Therefore all but finitely many primes are distributed among the $\phi(m)$ arithmetic progressions $a \pmod m$ with $(a, m) = 1$. How are they distributed? If the $m = 3$ case is anything to go by, it appears that there are infinitely many in each

[9] This is a fact that is beyond the scope of this book but will be discussed in [**Graa**]. In fact $e^{-\gamma} = .56145948\ldots$.

[10] Though not by much. The correct constant is 1 whereas $2e^{-\gamma} = 1.12291896\ldots$.

such arithmetic progression, and maybe even roughly equal numbers of primes in each up to any given point.

We will prove that there are infinitely many primes in each of the two feasible residue classes mod 3 (see Theorems 5.2 and 7.7).

Theorem 5.2. *There are infinitely many primes* $\equiv -1 \pmod 3$.

Proof. Suppose that there are only finitely many primes $\equiv -1 \pmod 3$, say $p_1, p_2, \ldots, p_k$. The integer $N = 3p_1p_2 \ldots p_k - 1$ must have a prime factor $q \equiv -1 \pmod 3$, by exercise 5.3.2. However q divides both N and $N+1$ (since it must be one of the primes p_i), and hence q divides their difference, 1, which is impossible. □

Exercise 5.3.2. Use exercise 3.1.4(a) to show that if $n \equiv -1 \pmod 3$, then there exists a prime factor p of n which is $\equiv -1 \pmod 3$.

In 1837 Dirichlet showed that whenever $(a, q) = 1$ there are infinitely many primes $\equiv a \pmod q$. (We discuss this deep result in sections 8.17 of appendix 8D and 13.7.) In fact there are roughly equally many primes in each of these arithmetic progressions mod q. For example, half the primes are $\equiv 1 \pmod 3$ and half are $\equiv -1 \pmod 3$, as our data above suggested. Roughly 1% of the primes are $\equiv 69 \pmod{101}$ and indeed there are roughly 1% of the primes in each arithmetic progression a mod 101 with $1 \le a \le 100$. This is a deep result and will be discussed at length in our book [**Graa**].

Exercise 5.3.3. Prove that there are infinitely many primes $\equiv -1 \pmod 4$.

Exercise 5.3.4. Prove that there are infinitely many primes $\equiv 5 \pmod 6$.

Exercise 5.3.5.† Prove that at least two of the arithmetic progressions mod 8 contain infinitely many primes.

Exercise 5.8.6 generalizes these results considerably, using similar ideas.

5.4. How many primes are there up to x?

When people started to develop large tables of primes, perhaps looking for a pattern, they discovered no patterns but did find that the proportion of integers that are prime is gradually diminishing (which will be proved in section 5.13 of appendix 5B). In 1808 Legendre quantified this, suggesting that there are roughly $\frac{x}{\log x}$ primes up to x.[11] A few years earlier, aged 15 or 16, Gauss had already made a much better guess, based on studying tables of primes:

> *In 1792 or 1793 ... I turned my attention to the decreasing frequency of primes ... counting the primes in intervals of length* 1000. *I soon recognized that behind all of the fluctuations, this frequency is on average inversely proportional to the logarithm ....*
>
> — from a letter to Encke by K. F. Gauss (Christmas Eve, 1849)

[11] And even the more precise assertion that there exists a constant B such that $\pi(x)$, the number of primes up to x, is well-approximated by $x/(\log x - B)$ for large enough x. This turns out to be true with $B = 1$, though this was not the value for B suggested by Legendre (who presumably made a guess based on data for small values of x).

His observation may be best phrased as

About 1 in $\log x$ *of the integers near* x *are prime,*

which is (subtly) different from Legendre's assertion: Gauss's observation suggests that a good approximation to the number of primes up to x is $\sum_{n=2}^{x} \frac{1}{\log n}$. As $\frac{1}{\log t}$ does not vary much for t between n and $n+1$, Gauss deduced that $\pi(x)$ should be well-approximated by

$$\int_2^x \frac{dt}{\log t}. \tag{5.4.1}$$

We denote this quantity by $\mathrm{Li}(x)$ and call it *the logarithmic integral.*[12] The logarithm here is again the natural logarithm. Here is a comparison of Gauss's prediction with the actual count of primes up to various values of x:

x	$\pi(x) = \#\{\text{primes} \le x\}$	Overcount: $\mathrm{Li}(x) - \pi(x)$
10^3	168	10
10^4	1229	17
10^5	9592	38
10^6	78498	130
10^7	664579	339
10^8	5761455	754
10^9	50847534	1701
10^{10}	455052511	3104
10^{11}	4118054813	11588
10^{12}	37607912018	38263
10^{13}	346065536839	108971
10^{14}	3204941750802	314890
10^{15}	29844570422669	1052619
10^{16}	279238341033925	3214632
10^{17}	2623557157654233	7956589
10^{18}	24739954287740860	21949555
10^{19}	234057667276344607	99877775
10^{20}	2220819602560918840	222744644
10^{21}	21127269486018731928	597394254
10^{22}	201467286689315906290	1932355208
10^{23}	1925320391606803968923	7250186216
10^{24}	18435599767349200867866	17146907278
10^{25}	176846309399143769411680	55160980939

Primes up to various x *and the overcount in Gauss's prediction.*

Gauss's prediction is amazingly accurate. From the data, Gauss's prediction seems to overcount by a small amount, for all $x \ge 8$.[13] To quantify this "small amount", we observe that the last column (representing the overcount) is always about half the width of the central column (representing the number of primes up to x), so these data suggest that the difference is no bigger than a small multiple of $\sqrt{x}$.

[12] Some authors begin the integral defining $\mathrm{Li}(x)$ at $x = 0$. This adds complication since the integrand equals ∞ at $x = 1$; nonetheless this can be handled, and the difference between the two definitions is then the constant $1.045163\ldots$, which has little relevance to our discussion.

[13] It is not true that $\mathrm{Li}(x) > \pi(x)$ for all $x > 2$ but the first counterexample is far beyond where we can hope to calculate. Understanding how we know this is well beyond the scope of this book, but see [**Graa**].

This might be optimistic but, at the very least, the ratio of $\pi(x)$, the number of primes up to x, to Gauss's guess, $\mathrm{Li}(x)$, should tend to 1 as $x \to \infty$; that is,

$$\pi(x) \,/\, \mathrm{Li}(x) \to 1 \quad \text{as} \quad x \to \infty.$$

In exercise 5.8.11 we show that $\mathrm{Li}(x) \,\Big/\, \frac{x}{\log x} \to 1$ as $x \to \infty$, and combining these last two limits, we deduce that

$$\pi(x) \,\Big/\, \frac{x}{\log x} \to 1 \quad \text{as} \quad x \to \infty.$$

The notation of limits is cumbersome; it is easier to write

$$\boxed{\pi(x) \sim \frac{x}{\log x}} \tag{5.4.2}$$

as $x \to \infty$, "$\pi(x)$ *is asymptotic to* $x/\log x$".[14] This is different by a multiplicative constant from (5.2.1), our guesstimate based on the sieve of Eratosthenes. Our data makes it seem more likely that the constant 1 given here, rather than the $2e^{-\gamma}$ given in (5.2.1), is the correct constant.

The asymptotic (5.4.2) is called the *prime number theorem*. Its proof came in 1896, more than 100 years after Gauss's guess, involving several remarkable developments. It was a high point of 19th-century mathematics and there is still no straightforward approach. The main reason is that the prime number theorem can be shown to be equivalent to a statement about zeros of the analytic continuation of a function (the Riemann zeta-function which we discuss in appendices 4B, 5B, and 5D), which seems preposterous at first sight. Although proofs can be given that avoid mentioning these zeros, they are still lurking somewhere just beneath the surface.[15] A proof of the prime number theorem is beyond the scope of this book (but see [**Graa**] and [**GS**]).

Exercise 5.4.1.† Assume the prime number theorem.
(a) Show that there are infinitely many primes whose leading digit is a "1". How about leading digit "7"?
(b) Show that for all $\epsilon > 0$, if x is sufficiently large, then there are primes between x and $x + \epsilon x$.
(c) Deduce that $\mathbb{R}_{\geq 0}$ is the set of limit points of the set $\{p/q : \ p, q \text{ primes}\}$.
(d) Let $a_1, \ldots, a_d$ be any sequence of digits, that is, integers between 0 and 9, with $a_1 \neq 0$. Show that there are infinitely many primes whose first (leading) d digits are $a_1, \ldots, a_d$.

Exercise 5.4.2.† Let $p_1 = 2 < p_2 = 3 < \cdots$ be the sequence of primes. Assume the prime number theorem and prove that

$$p_n \sim n \ \log n \ \text{ as } n \to \infty.$$

Exercise 5.4.3.† (a) Show that the sum of primes and prime powers $\leq x$ is $\sim x^2/(2 \log x)$.
(b) Deduce that if the sum equals N, then $x \sim \sqrt{N \log N}$.

[14] In general, $A(x) \sim B(x)$, that is, $A(x)$ is asymptotic to $B(x)$, is equivalent to $\lim_{x\to\infty} A(x)/B(x) = 1$. It does *not* mean that "$A(x)$ is approximately equal to $B(x)$", which has no strict mathematical meaning, rather that for any $\epsilon > 0$, no matter how small, one has

$$(1 - \epsilon)B(x) < A(x) < (1 + \epsilon)B(x)$$

once x is sufficiently large (where how large is " sufficiently large" depends on ϵ). This definition concerns the ratio $A(x)/B(x)$, *not* their difference $A(x) - B(x)$. Therefore $n^2 + 1 \sim n^2$ and $n^2 + n^2/\log n \sim n^2$ are equally true, even though the first is a better approximation to n^2 than the second ([**Sha85**], p. 16),

[15] Including the so-called "elementary proof" of the prime number theorem.

Primes in arithmetic progressions. As we mentioned in section 5.3, Dirichlet showed in 1837 that if $(a, q) = 1$, then there are infinitely many primes $p \equiv a \pmod q$. Dirichlet's proof was combined in 1896 with the proof of the prime number theorem to establish that

$$\#\{p \le x : p \text{ is prime}, p \equiv a \pmod q\} \sim \frac{\pi(x)}{\phi(q)} \sim \frac{x}{\phi(q)\log x}.$$

The factor "$1/\phi(q)$" emerges as there are $\phi(q)$ reduced residues a modulo q.

Exercise 5.4.4.‡ Use the prime number theorem in arithmetic progressions to prove that for any integers $a_1, \dots, a_d, b_0, \dots, b_d \in \{0, \dots, 9\}$, with $a_1 \neq 0$ and $b_0 = 1$, 3, 7, or 9, there are infinitely many primes whose first d digits are $a_1, \dots, a_d$ and whose last d digits are $b_d, \dots, b_0$.

5.5. *Bounds on the number of primes*

The first quantitative lower bound proven on the number of primes is due to Euler in the mid-18th century who showed that

$$\sum_{p \text{ prime}} \frac{1}{p} \text{ diverges},$$

as we will prove in section 5.12 of appendix 5B. This gives some idea of how numerous the primes are in comparison to other sequences of integers. For example $\sum_{n\ge1} \frac{1}{n^2}$ converges, so the primes are, in this sense, more numerous than the squares. This implies that there are arbitrarily large values of x for which $\pi(x) > \sqrt{x}$.

Exercise 5.5.1.† Do better than this using Euler's result.

(a) Prove that $\sum_{n\ge1} \frac{1}{n(\log n)^2}$ converges.

(b) Deduce that there are arbitrarily large x for which $\pi(x) > x/(\log x)^2$.

Next we will prove upper and lower bounds for the number of primes up to x, of the form

$$c_1 \frac{x}{\log x} \le \pi(x) \le c_2 \frac{x}{\log x} \tag{5.5.1}$$

for some constants $0 < c_1 < 1 < c_2$, for all sufficiently large x. The prime number theorem is equivalent to being able to take $c_1 = 1 - \epsilon$ and $c_2 = 1 + \epsilon$ for any fixed $\epsilon > 0$ in (5.5.1). Instead we will prove Chebyshev's weaker 1850 result that one can take any $c_1 < \log 2$ and any $c_2 > \log 4$ in (5.5.1).

Theorem 5.3. *For all integers $n \ge 2$ we have*

$$(\log 2)\ \frac{n}{\log n} - 1 \le \pi(n) \le (\log 4)\frac{n}{\log n} + 4\frac{n}{(\log n)^2}.$$

Exercise 5.5.2. Fix $\epsilon > 0$ arbitrarily small. Deduce Chebyshev's bounds (5.5.1) with $c_1 = \log 2 - \epsilon$ and $c_2 = \log 4 + \epsilon$, for all sufficiently large x, from Theorem 5.3.

Proof. The binomial theorem states that $(x + y)^N = \sum_{j=0}^N \binom{N}{j} x^j y^{N-j}$. Taking $x = y = 1$ we get

$$\sum_{j=0}^{N} \binom{N}{j} = 2^N. \tag{5.5.2}$$

Lemma 5.5.1. *The product of the primes up to N is $\le 4^{N-1}$ for all $N \ge 1$.*

Proof. Each prime in $[n+1, 2n]$ appears in the numerator of the binomial coefficient $\binom{2n-1}{n}$ but not in the denominator, and so their product divides $\binom{2n-1}{n}$. Now if $N = 2n-1$ is odd, then $\binom{2n-1}{n-1} = \binom{2n-1}{n}$ so the value appears twice in the sum in (5.5.2). Therefore

$$\prod_{\substack{n<p\le 2n\\ p \text{ prime}}} p \le \binom{2n-1}{n} < \frac{1}{2}\sum_{j=0}^{2n-1}\binom{2n-1}{j} = 2^{2n-2} = 4^{n-1}. \tag{5.5.3}$$

We now prove the claimed result by induction on $N \ge 1$. The result is straightforward for $N = 1, 2$ by calculation. If $N = 2n$ or $2n-1$, then the product of the primes up to N is at most the product of the primes up to n times the product of the primes in $[n+1, 2n]$. The first product is $\le 4^{n-1}$ by the induction hypothesis, and the second $< 4^{n-1}$ by the previous paragraph. Combining these two upper bounds gives the upper bound $\le 4^{2n-2} \le 4^{N-1}$, as claimed. □

If we take logarithms in (5.5.3), we obtain

$$\sum_{\substack{p \text{ prime}\\ n<p\le 2n}} \log p < (n-1)\log 4. \tag{5.5.4}$$

As each term of the left side is $> \log n$ we deduce that

$$\pi(2n) - \pi(n) = \#\{p \text{ prime}: \ n < p \le 2n\} \le \frac{n-1}{\log n}\cdot \log 4. \tag{5.5.5}$$

We now use this to deduce the upper bound claimed in Theorem 5.3. We verify the bound by calculations for all $N \le 100$ and then proceed by induction for $N \ge 101$. If $N = 2n$ or $2n-1$ (so that $n \ge 51$), then by the induction hypothesis and (5.5.5)

$$\pi(N) \le \pi(2n) = \pi(n) + (\pi(2n) - \pi(n)) \le (\log 4)\frac{2n-1}{\log n} + 4\frac{n}{(\log n)^2},$$

and for all $n \ge 51$ this is

$$< (\log 4)\frac{2n-1}{\log 2n} + 4\frac{2n-1}{(\log 2n)^2} < (\log 4)\frac{N}{\log N} + 4\frac{N}{(\log N)^2},$$

as a careful calculation reveals. This yields the upper bound claimed in Theorem 5.3.

To obtain the lower bound claimed in Theorem 5.3 we begin by observing that the largest binomial coefficient $\binom{n}{m}$ occurs with $m = [n/2]$. All the other binomial coefficients are smaller, as is $\binom{n}{0} + \binom{n}{n}$, so that

$$2^n = \left(\binom{n}{0} + \binom{n}{n}\right) + \sum_{m=1}^{n-1}\binom{n}{m} \le n\binom{n}{[n/2]},$$

by (5.5.2). Now, all prime factors of any $\binom{n}{[n/2]}$ are $\le n$, and in fact if p^{e_p} divides $\binom{n}{[n/2]}$, then $p^{e_p} \le n$ by Corollary 3.10.1 to Kummer's Theorem. Therefore

$$2^n \le n\binom{n}{[n/2]} \le n \prod_{\substack{p \text{ prime} \\ p \le n}} p^{e_p} \le n^{\pi(n)+1}.$$

Taking logarithms we deduce the claimed result. □

Exercise 5.5.3. Use exercise 3.10.3 and the last displayed equation to prove that

$$\operatorname{lcm}[m : \ m \le n] \ge \frac{2^n}{n}. \tag{5.5.6}$$

5.6. *Gaps between primes*

Let $p_1 = 2 < p_2 = 3 < \cdots$ be the sequence of primes. We are interested in the possible gaps, $p_{n+1} - p_n$, between primes.

The prime number theorem tells us that there are about $x/\log x$ primes up to x, so that the average gap between primes $\le x$ is about $\log x$: If $N = \pi(x)$, then p_N is the largest prime $\le x$, and $p_N \sim x$ by exercise 5.4.1(b). This implies that the average gap between consecutive primes up to x is

$$\frac{1}{N-1}\sum_{n=1}^{N-1}(p_{n+1} - p_n) \ = \ \frac{p_N - 2}{N-1} \ \sim \ \frac{x}{x/\log x} \ = \ \log x,$$

by the prime number theorem.

Are there gaps between consecutive primes that are much smaller than the average? Much larger than the average? What is the largest that gaps between primes can be, and what is the smallest?

Exercise 5.6.1. (a) Prove that there are gaps between primes $\le x$ that are at least as large as the average gap between primes up to x.
(b) Prove that there are gaps between primes $\le x$ that are no bigger than the average gap between primes up to x.

Legendre conjectured that there are always primes between consecutive squares, that is, that there are primes in the interval $(n^2, (n+1)^2)$ for every integer n.

Exercise 5.6.2. (a) Show that if every interval $(x, x + 2\sqrt{x})$ contains a prime, then there are always primes between consecutive squares.
(b) Show that if there are always primes between consecutive squares, then every interval $(x, x + 4\sqrt{x} + 3]$ contains a prime.

At present we do not know how to prove every interval $(x, x + C\sqrt{x})$ contains primes, for any given $C > 0$. However it has been proven, by Baker, Harman, and Pintz, that any interval $(x, x + cx^{\frac{1}{2}+\frac{1}{40}}]$ contains a prime for c sufficiently large.

Exercise 5.6.3. Deduce from this that there is a prime between any consecutive, sufficiently large, cubes.

There is a simple way to construct a long interval which contains no primes:

Proposition 5.6.1. *For any integer m the interval $m!+2,\ m!+3,\dots,m!+m$ contains no primes. Therefore if p_n is the largest prime $\le m!+1$, then $p_{n+1}-p_n \ge m$.*

Proof. If $2 \le j \le m$, then j is included in the product for $m!$, and so j divides $m!+j$. Therefore $m!+j$ is composite as it is $> j$. Now $p_{n+1} \ne m!+j$ for each such j and so $p_{n+1} \ge m!+m+1 \ge p_n+m$. □

The gaps between primes constructed in this way are not quite as large as the average gaps. However one can extend this idea, creating a long interval of integers which each have a small prime factor, to prove that

$$\limsup_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = \infty.$$

Proving this is again beyond the scope of this book but a proof can be found in [**Graa**].

What about small gaps between primes?

Exercise 5.6.4. Prove that 2 and 3 are the only two primes that differ by 1.

There are plenty of pairs of primes that differ by two, namely 3 and 5, 5 and 7, 11 and 13, 17 and 19, etc., seemingly infinitely many, and this *twin prime conjecture* that there are infinitely many prime twins p, $p+2$ remains an open problem. Until recently, very little was proved about short gaps between primes, but that changed in 2009, when Goldston, Pintz, and Yildirim (see [**1**]) showed that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0.$$

In 2013, Yitang Zhang, until then a practically unknown mathematician,[16] showed that there are infinitely many pairs of primes that differ by at most a bounded amount. More precisely there exists a constant B such that there are infinitely many pairs of distinct primes that differ by at most B. This was soon improved by Maynard and Tao, though by a different method, so that we now know there are infinitely many pairs of consecutive primes p_n, p_{n+1} such that

$$p_{n+1}-p_n \le 246.$$

This is not quite the twin prime conjecture, but it is a very exciting development. (See [**2**] for a discussion.)

The proofs of Maynard and of Tao yield a further great result: For any integer $m \ge 3$ there are infinitely many intervals of length 2^{14m} which contain m primes. That is, there are infinitely many m-tuples of consecutive primes $p_n, p_{n+1}, \dots, p_{n+m-1}$ such that

$$p_{n+m-1}-p_n \le 2^{14m}.$$

[16] See the movie *Counting from Infinity* (Zala Films, 2015) for an account of his fascinating story.

Further reading on hot topics in this section

[1] K. Soundararajan, *Small gaps between prime numbers: The work of Goldston-Pintz-Yıldırım*, Bull. Amer. Math. Soc. (N.S.) 44 (2007), 1–18.

[2] Andrew Granville, *Primes in intervals of bounded length*, Bull. Amer. Math. Soc. (N.S.) 52 (2015), 171–222.

5.7. *Formulas for primes*

Are there polynomials (of degree ≥ 1) that only yield prime values? That is, is $f(n)$ prime for every integer n? The example $6n+5$ begins by taking the prime values $5, 11, 17, 23, 29$ before getting to $35 = 5 \times 7$. Continuing on, we get more primes $41, 47, 53, 59$ till we hit $65 = 5 \times 13$, another multiple of 5. So every fifth term of the arithmetic progression seems to be divisible by 5, which we verify as $6(5k) + 5 = 5(6k+1)$. More generally $qn + a$ is a multiple of a whenever n is a multiple of a, since $q(ak) + a = a(qk+1)$. A famous example of a polynomial that takes lots of prime values is $f(x) = x^2 + x + 41$. Indeed $f(n)$ is prime for $0 \leq n \leq 39$. However $f(40) = 41^2$ and $f(41k) = 41(41k^2 + k + 1)$. Therefore $f(41k)$ is composite for each integer k for which $41k^2 + k + 1 \neq -1$, 0, or 1.

We will develop this argument to work for all polynomials, but we will need the following result, which is a consequence of the Fundamental Theorem of Algebra and is proved in Theorem 3.11 of section 3.22 in appendix 3F.

Lemma 5.7.1. *A non-zero degree d polynomial has no more than d distinct roots in $\mathbb{C}$.*

The main consequence that we need is the following:

Corollary 5.7.1. *Suppose that $f(x) \in \mathbb{Z}[x]$ has degree $d \geq 1$. For any integer $B \geq 1$, there are no more than $(2B+1)d$ integers n for which $|f(n)| \leq B$.*

Proof. If n is an integer, then so is $f(n)$, and therefore if $|f(n)| \leq B$, then $f(n) = m$ for some integer m with $|m| \leq B$. Therefore n is a root of one of the $2B+1$ polynomials $f(x) - m$, each of which has no more than d roots by Lemma 5.7.1, and so the result follows. □

Proposition 5.7.1. *If $f(x) \in \mathbb{Z}[x]$ has degree $d \geq 1$, then there are infinitely many integers n for which $|f(n)|$ is composite.*

Proof. By Corollary 5.7.1 there are no more than $3d$ integers n for which $f(n) = -1$, 0, or 1, so there exists an integer a in the range $0 \leq a \leq 3d$ for which $|f(a)| > 1$. Let $m := |f(a)| > 1$. Now $km + a \equiv a \pmod{m}$ and so, by Corollary 2.3.1, we have

$$f(km + a) \equiv f(a) \equiv 0 \pmod{m}.$$

There are at most $3d$ values of k for which $km + a$ is a root of one of $f(x) - m$, $f(x)$, or $f(x) + m$, by Corollary 5.7.1. For any other k we have that $|f(km+a)| \neq 0$ or m, in which case $|f(km + a)|$ is divisible by m and $|f(km + a)| > m$, so that $|f(km + a)|$ is composite. □

Exercise 5.7.1. Show that if $f(x, y) \in \mathbb{Z}[x, y]$ has degree $d \geq 1$, then there are infinitely many pairs of integers m, n for which $|f(m, n)|$ is composite.

Nine of the first ten values of the polynomial $6n+5$ are primes. The polynomial n^2+n+41, discovered by Euler in 1772, is prime for $n = 0, 1, 2, \ldots, 39$ and the square of a prime for $n = 40$. However, in the proof of Proposition 5.7.1, we saw that n^2+n+41 is composite whenever n is a positive multiple of 41. See section 12.5 for more on such prime rich polynomials.

We discuss other places to look for primes in section 5.21 of appendix 5G.

It is not difficult to show that if a polynomial f takes on infinitely many prime values, then f must be irreducible. The next result indicates how many prime values f needs to take before we *know* that f is irreducible.

Theorem 5.4. *If $f(x) \in \mathbb{Z}[x]$ has degree $d \geq 1$ and $|f(n)|$ is prime for $\geq 2d+1$ integers n, then $f(x)$ is irreducible.*

Proof. Suppose that f is reducible; that is, $f = gh$ for polynomials $g(x)$, $h(x) \in \mathbb{Z}[x]$. If $|f(n)| = p$, a prime, then $g(n)h(n) = p$ or $-p$. Therefore one of $g(n)$ and $h(n)$ equals p or $-p$, the other 1 or -1. In particular n is a root of $(g(x)-1)(h(x)-1)(g(x)+1)(h(x)+1)$, a polynomial of degree $2d$. This has no more than $2d$ roots by Lemma 5.7.1, and so $|f(n)|$ can be prime for no more than $2d$ integers n. □

This is often more than we need, as we see in the following beautiful result:

Theorem 5.5. *Write a given prime p in base 10 as $p = a_0 + a_1 10 + \cdots + a_d 10^d$ (with each $a_i \in \{0, 1, 2, \ldots, 9\}$ and $a_d \neq 0$). Then $a_0 + a_1 x + \cdots + a_d x^d$ is an irreducible polynomial.*

Proof. Let $f(x) = a_0 x + \cdots + a_d x^d$ and suppose that $f = gh$. As $g(10)h(10)$ is prime, one of $g(10)$ and $h(10)$ equals 1 or -1. We will suppose that it is g (swapping g and h if necessary). As $g(x) \in \mathbb{Z}[x]$ it can be written in the form $g(x) = c\prod_{j=1}^{D}(x-\alpha_j)$ with $c \in \mathbb{Z}$, and so $\prod_{j=1}^{D}|10-\alpha_j| \leq |g(10)| = 1$. Therefore there is a root α of $g(x)$ for which $|\alpha - 10| \leq 1$. This implies that $\mathrm{Re}(\alpha) \in [9, 11]$ and so $\mathrm{Re}(1/\alpha) > 0$ and $|\alpha| \geq 9$.

As $f(\alpha) = 0$ we deduce that

$$0 = \mathrm{Re}\left(\frac{f(\alpha)}{\alpha^d}\right) = a_d + a_{d-1}\mathrm{Re}\left(\frac{1}{\alpha}\right) + \sum_{i=2}^{d} a_{d-i}\mathrm{Re}\left(\frac{1}{\alpha^i}\right).$$

As discussed above $\mathrm{Re}(1/\alpha) > 0$ and so $a_{d-1}\mathrm{Re}(1/\alpha) \geq 0$. On the other hand, $\mathrm{Re}(1/\alpha^i)$ might be negative and so $a_{d-i}\mathrm{Re}(1/\alpha^i) \geq -9/|\alpha|^i$. Therefore

$$0 \geq 1 + 0 - 9\sum_{i=2}^{d}\frac{1}{|\alpha|^i},$$

which implies that

$$1 < 9\sum_{i\geq 2}\frac{1}{|\alpha|^i} = \frac{9}{|\alpha|(|\alpha|-1)} \leq \frac{1}{8}$$

as $|\alpha| \geq 9$, which yields a contradiction. □

Exercise 5.7.2. Prove an analogous result for primes written in an arbitrary base $b \geq 3$.

Exercise 5.7.3.† Suppose that $f(x) = a_0x + \cdots + a_dx^d \in \mathbb{Z}[x]$ with each $|a_i| \le A$ and $a_d \neq 0$. Prove that if $f(n)$ is prime for some integer $n \ge A + 2$, then $f(x)$ is irreducible.

There are many books on the distribution of primes. My favorites for beginners are [**TMF00**] which explains the key ideas behind the prime number theorem and other important results in an accessible way, and [**Rib91**] which is more recreational but full of good stuff. The introductory book [**HW08**] proves quite a few of the easier theorems in the subject.

Additional exercises

Exercise 5.8.1. Let m be the product of the primes ≤ 1000. Prove that if n is an integer between 10^3 and 10^6, then n is prime if and only if $(n, m) = 1$.

Exercise 5.8.2. Show that if $p > 3$ and $q = p + 2$ are twin primes, then $p + q$ is divisible by 12.

Exercise 5.8.3. Show that there are infinitely many integers n for which each of $n, n+1, \dots, n+1000$ is composite.

Exercise 5.8.4. Fix integer $m > 1$. Show that there are infinitely many integers n for which $\tau(n) = m$.

Exercise 5.8.5.† Fix integer $k > 1$. Prove that there are infinitely many integers n for which $\mu(n) = \mu(n + 1) = \cdots = \mu(n + k)$.

Exercise 5.8.6. Let H be a proper subgroup[17] of $(\mathbb{Z}/m\mathbb{Z})^*$.

(a) Show that if a is coprime to m and q is a given non-zero integer, then there are infinitely many integers $n \equiv a \pmod m$ such that $(n, q) = 1$.

(b) Prove that if n is an integer coprime to m but which is not in a residue class of H, then n has a prime factor which is not in a residue class of H.

(c) Deduce there are infinitely many primes which do not belong to any residue class of H.

Exercise 5.8.7.† Suppose that for any coprime integers a and q there exists *at least one* prime $\equiv a \pmod q$. Deduce that for any coprime integers A and Q, there are *infinitely many* primes $\equiv A \pmod Q$.

Exercise 5.8.8. Prove that there are infinitely many primes p for which there exists an integer a such that $a^3 - a + 1 \equiv 0 \pmod p$.

Exercise 5.8.9. Prove that for any $f(x) \in \mathbb{Z}[x]$ of degree ≥ 1, there are infinitely many primes p for which there exists an integer a such that p divides $f(a)$.

Exercise 5.8.10. Let $\mathcal{L}(n) = \operatorname{lcm}[1, 2, \dots, n]$.

(a) Show that $\mathcal{L}(n)$ divides $\mathcal{L}(n + 1)$ for all $n \ge 1$.

(b) Express $\mathcal{L}(n)$ as a function of the prime powers $\le n$.

(c) Prove that for any integer k there exist integers n for which $\mathcal{L}(n) = \mathcal{L}(n+1) = \cdots = \mathcal{L}(n+k)$.

(d)‡ Prove that if k is sufficiently large, then there is such an integer n which is $< 3^k$.

Exercise 5.8.11.† Prove that

$$\operatorname{Li}(x) \Big/ \frac{x}{\log x} \to 1 \text{ as } x \to \infty.$$

Exercise 5.8.12. Prove that 1 is the best choice for B when approximating $\operatorname{Li}(x)$ by $x/(\log x - B)$.

Exercise 5.8.13.† Using the Maynard-Tao result, prove that there exists a positive integer $k \le 246$ for which there are infinitely many prime pairs $p, p + k$.

[17] H is a *proper* subgroup of G if it is a subgroup of G but not the whole of G

Exercise 5.8.14. Suppose that a and b are integers for which $g(a) = 1$ and $g(b) = -1$, where $g(x) \in \mathbb{Z}[x]$.

(a) Prove that $b = a-2$, $a-1$, $a+1$, or $a+2$.

(b)† Deduce that there are no more than four integer roots of $(g(x)-1)(g(x)+1) = 0$.

(c)† Show that if $g(x)$ has degree 2 and there are four integer roots of $(g(x)-1)(g(x)+1) = 0$, then $g(x) = \pm h(x-A)$ where $h(t) = t^2 - 3t + 1$, with roots A, $A+1$, $A+2$, and $A+3$.

(d)† Modify the proof of Theorem 5.4 to establish that if $f(x) \in \mathbb{Z}[x]$ has degree $d \geq 6$ and $|f(n)|$ is prime for $\geq d+3$ integers n, then $f(x)$ is irreducible.

Let $f(x) = h(x)h(x-4)$, which has degree 4. Note that $|f(n)|$ is prime for the eight values $n = 0, 1, \ldots, 7$, and so there is little room in which to improve (d).

One can show that there are reducible polynomials $f(x) \in \mathbb{Z}[x]$ of arbitrarily large degree d for which $|f(n)|$ takes on at least $d+1$ prime values: Let $p_1 < \cdots < p_m$ be distinct primes. Let $g(x) = \prod_{j=1}^{m}(p_j^2 - x^2)$ and $q = g(1)$. By Dirichlet's Theorem (section 5.3) we know that there are infinitely many primes $p_0 \equiv 1 \pmod{q}$.[18] We select one such prime and write $p_0 = 1 + \ell q$ for some positive integer ℓ. Now let $f(x) = x(1+\ell g(x))$ which has degree $d := 2m+1$. We have that $|f(\pm 1)| = 1+\ell q = p_0$ and $|f(\pm p_j)| = p_j$ for $j = 1, \ldots, m$, so there are $\geq 2m+2 = d+1$ integers n for which $|f(n)|$ is prime.

In the next exercise, assuming certain conjectures,[19] we construct reducible polynomials $f(x) \in \mathbb{Z}[x]$ of arbitrarily large degree d for which $|f(n)|$ takes on $d+2$ prime values. This implies that the result in exercise 5.8.14(d) is "best possible".

Exercise 5.8.15.† Assume that there are infinitely many positive integers n for which n^2-3n+1 is prime, and denote these integers by $n_1 < n_2 < \cdots$. Let $g_m(x) := (n_1 - x)\cdots(n_m - x)$. If ℓ is a positive integer for which $1 + \ell g_m(0), 1 + \ell g_m(1), 1 + \ell g_m(2), 1 + \ell g_m(3)$ are simultaneously prime, then prove that the polynomial $f(x) := (x^2 - 3x + 1)(1 + \ell g_m(x))$ has degree $d := m + 2$ and that there are exactly $d + 2$ integers n for which $|f(n)|$ is prime.

[18] We will prove this later, in Theorem 7.8.

[19] These conjectures follows from the *Polynomial prime values conjecture* stated in the bonus section of this chapter.

Appendix 5A. Bertrand's postulate and beyond

5.9. Bertrand's postulate

In 1845 Bertrand conjectured, on the basis of calculations up to a million:

Theorem 5.6 (Bertrand's postulate)**.** *For every integer $n \geq 1$, there is a prime number between n and $2n$.*

Bertrand's postulate was proved in 1850 by Chebyshev. We will follow the 19-year-old Erdős's proof, or, as N. J. Fine put it (in the voice of Erdős):

Chebyshev said it, but I'll say it again:
There's always a prime between n and $2n$.

Exercise 5.9.1. Show that prime p does not divide $\binom{2n}{n}$ when $2n/3 < p \leq n$.

Proof of Bertrand's postulate. Let p^{e_p} be the exact power of prime p dividing $\binom{2n}{n}$. We know that

- $e_p = 1$ if $n < p \leq 2n$ by Kummer's Theorem (Theorem 3.7),
- $e_p = 0$ if $2n/3 < p \leq n$ by exercise 5.9.1,
- $e_p \leq 1$ if $\sqrt{2n} < p \leq 2n$ by Corollary 3.10.1,
- $p^{e_p} \leq 2n$ if $p \leq 2n$ by Corollary 3.10.1.

Combining these gives

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n} = \prod_{p \leq 2n} p^{e_p} \leq \prod_{n < p \leq 2n} p \prod_{p \leq 2n/3} p \prod_{p \leq \sqrt{2n}} 2n$$

$$\leq \left(\prod_{n < p \leq 2n} p \right) \times 4^{2n/3-1} \times (2n)^{(\sqrt{2n}+1)/2},$$

using Lemma 5.5.1 to bound $\prod_{p\le 2n/3} p$ and the bound $\pi(\sqrt{2n}) \le \frac{1}{2}(\sqrt{2n}+1)$ (as neither 1 nor any even integer > 2 is prime). Taking logarithms we deduce that

$$\sum_{\substack{p \text{ prime} \\ n<p\le 2n}} \log p > \frac{\log 4}{3}\, n - \frac{\sqrt{2n}+3}{2}\, \log(2n).$$

This implies that

$$\sum_{\substack{p \text{ prime} \\ n<p\le 2n}} \log p \ge \frac{1}{3}\, n \tag{5.9.1}$$

for all $n \ge 2349$, which implies Bertrand's postulate in this range. (This lower bound should be compared to the upper bound (5.5.4).)

If $1 \le n \le 5000$, then the interval $(n, 2n]$ contains at least one of the primes 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, and 5003. □

Exercise 5.9.2. Use Bertrand's postulate to prove that there are infinitely many primes with first digit "1".

Exercise 5.9.3. Use Bertrand's postulate to show, by induction, that every integer $n > 6$ can be written as the sum of distinct primes.

Exercise 5.9.4. Goldbach conjectured that every even integer ≥ 6 can be written as the sum of two primes. Deduce Bertrand's postulate from Goldbach's conjecture.

Exercise 5.9.5. Use Bertrand's postulate to prove that $\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}$ is never an integer.

Exercise 5.9.6. Prove that for every $n \ge 1$ one can partition the set of integers $\{1, 2, \dots, 2n\}$ into pairs $\{a_1, b_1\}, \dots, \{a_n, b_n\}$ such that each sum $a_j + b_j$ is a prime.

Exercise 5.9.7.† (a) Prove that prime p divides $\binom{2n}{n}$ when $n/2 < p \le 2n/3$.
(b) Prove that the product of the primes in $(3m, 12m]$ divides $\binom{12m}{6m}\binom{6m}{4m}$.
(c)† Deduce that we can take any constant $c_2 > \frac{2}{9}\log(432)$ in (5.5.1).
(Note that $\frac{2}{9}\log(432) = 1.3485\ldots < \log 4 = 1.3862\ldots$.)
(d) Now deduce Bertrand's postulate for all sufficiently large x from (5.5.1).

5.10. The theorem of Sylvester and Schur

Bertrand's postulate can be rephrased to state that at least one of the integers $k+1, k+2, \dots, 2k$ has a prime factor $> k$. This can be generalized as follows:

Theorem 5.7 (Sylvester-Schur Theorem)**.** *For any integers $n \ge k \ge 1$, at least one of the integers $n+1, n+2, \dots, n+k$ is divisible by a prime $p > k$.*

Proposition 5.10.1. *If, for given integers $n \ge k \ge 1$, we have*

$$\binom{n+k}{k} > (n+k)^{\pi(k)}, \tag{5.10.1}$$

then at least one of the integers $n+1, n+2, \dots, n+k$ is divisible by a prime $p > k$. If (5.10.1) holds for $n_1(k)$, then it holds for all $n \ge n_1(k)$.

Proof. If the prime factors of $n+1, n+2, \dots, n+k$ are all $\le k$, then all of the prime factors p of $\binom{n+k}{k}$ are $\le k$. If $p^e \| \binom{n+k}{k}$, then $p^e \le n+k$ by Corollary 3.10.1. Therefore

$$\binom{n+k}{k} \le \prod_{p \le k} (n+k) = (n+k)^{\pi(k)}, \tag{5.10.2}$$

contradicting (5.10.1). This proves the first part of the result.

We prove the second part by induction on $n \ge n_1(k)$ using the following result.

Exercise 5.10.1. Prove that $\left(1+\frac{1}{x+k}\right)^k \le \left(1+\frac{k}{x+1}\right)$ for all $x \ge k \ge 1$.

The result holds for $n = n_1(k)$, so now suppose that (5.10.1) holds for some given n. Then

$$\binom{n+1+k}{k} = \left(1+\frac{k}{n+1}\right)\binom{n+k}{k} > \left(1+\frac{1}{n+k}\right)^k (n+k)^{\pi(k)} > (n+1+k)^{\pi(k)},$$

by exercise 5.10.1 and the induction hypothesis, and so (5.10.1) holds for $n+1$. The result follows. □

Proof of the Sylvester-Schur Theorem for all $k \le 1500$. Calculations give some value for $n_1(k)$ in Proposition 5.10.1 for all $k \le 1500$, and so the Sylvester-Schur Theorem follows for these k and all $n \ge n_1(k)$ by Proposition 5.10.1. Now $n_1(k) = k$ for $202 \le k \le 1500$, and $k \le n_1(k) \le k+17$ for all $k \le 201$. We verify the theorem for $k \le n \le k+16$ with $k \le 201$, case by case. □

A just failed proof of the Sylvester-Schur Theorem. Calculations suggest that $\binom{2k}{k} > (2k)^{\pi(k)}$ for all $k \ge 202$. If so, the Sylvester-Schur Theorem follows for all $k \ge 202$ by Proposition 5.10.1. However we just failed to prove this inequality as a consequence of the upper bound in Theorem 5.3. If one combines the upper bound on $\pi(k/4)$ from Theorem 5.3, together with exercise 5.9.7(b), then we can prove that $\binom{2k}{k} > (2k)^{\pi(k)}$ for all sufficiently large k. However "sufficiently large" here is likely to be extremely large. □

Exercise 5.10.2. Prove that if $\pi(k) < \frac{k \log 4}{\log(2k)} - 1$ for all integers $k \ge 1$, then Theorem 5.7 holds for all $n \ge k \ge 1$.

Proof of the Sylvester-Schur Theorem for all $k > 1500$. If (5.10.1) holds, then the result follows from Proposition 5.10.1. Hence we may assume that (5.10.2) holds. Now, $\pi(k) < k/3$ (which can be proved by accounting for divisibility by 2 and 3), and $\frac{n+k-j}{k-j} > \frac{n+k}{k}$ for $j = 0, \dots, k-1$ so that $\binom{n+k}{k} \ge (\frac{n+k}{k})^k$. Therefore (5.10.2) implies that

$$\left(\frac{n+k}{k}\right)^k \le \binom{n+k}{k} \le (n+k)^{\pi(k)} \le (n+k)^{k/3},$$

which in turn implies that

$$n+k \le k^{3/2}; \text{ that is, } n \le k^{3/2} - k.$$

Next we note that if $p > (n+k)^{1/2}$ and $p^e \| \binom{n+k}{k}$ so that $p^e \le n+k$, then $e = 0$ or 1. Therefore we can refine (5.10.2) to

$$\binom{n+k}{k} \le \prod_{p \le (n+k)^{1/2}} (n+k) \prod_{p \le k} p = k^{\frac{1}{3}k^{3/4}} 4^{k-1}, \tag{5.10.3}$$

by (5.5.4), as $\pi((n+k)^{1/2}) \le \frac{1}{3}(n+k)^{1/2} \le \frac{1}{3}k^{3/4}$.

Now if $n \ge 3k$, then, by exercise 4.14.2 of appendix 4D,

$$\frac{(4^4/3^3)^k}{ek} \le \binom{4k}{k} \le \binom{n+k}{k} \le k^{\frac{1}{2}k^{3/4}} 4^{k-1}$$

which is false for all $k \ge 1$. Therefore $n + k \le 4k$, and so if $n + k > \frac{5}{2}k$, then our inequality becomes

$$\frac{(5^5/3^3 2^2)^{k/2}}{ek} \le \binom{5k/2}{k} \le \binom{n+k}{k} \le (4k)^{k^{1/2}} 4^{k-1}.$$

This is false for all $k \ge 780$.

Finally for the range $k \le n \le 3k/2$ if prime p is in the range $(n+k)/3 < p \le k$, then $2p$ is the only multiple of p that appears in $(n+1)\cdots(n+k)$ and so p does not divide $\binom{n+k}{k}$. Therefore

$$\binom{2k}{k} \le \binom{n+k}{k} \le \prod_{p \le (n+k)^{1/2}} (n+k) \prod_{p \le (n+k)/3} p \le \prod_{p \le (n+k)^{1/2}} (3k)^{\pi(2k^{1/2})} \prod_{p \le 5k/6} p,$$

which implies that

$$\frac{4^k}{ek} \le (4k)^{k^{1/2}} 4^{5k/6-1}$$

which is false for all $k \ge 1471$. □

Exercise 5.10.3. (a) Use Bertrand's postulate and the Sylvester-Schur Theorem to show that if $1 \le r < s$, then there is a prime p that divides exactly one of the integers $r+1, \dots, s$.
(b) Deduce that if $1 \le r < s$, then $\frac{1}{r+1} + \cdots + \frac{1}{s}$ is never an integer.

Bonus read: A review of prime problems

5.11. Prime problems

In this bonus section we will discuss various natural sequences that are expected to contain infinitely many primes, highlighting recent progress.

> *Mathematicians have tried in vain to discover some order in the sequence of the prime numbers and we have every reason to believe that there are some mysteries that the human mind shall never penetrate.*
>
> — Leonhard Euler (1740)

Prime values of polynomials in one variable

In section 5.6 we mentioned the twin prime conjecture, that there are infinitely many pairs of primes that differ by 2. What about other pairs? Obviously there can be no more than one pair of primes that differ by an odd integer k (as one of the two integers must be divisible by 2), but when the difference is an even integer k there is no such obstruction. Calculations then suggest that:

For all even integers $2m > 0$ there are infinitely many pairs of primes that differ by $2m$. That is, there are infinitely many prime pairs $p, p + 2m$.

Here we asked for simultaneous prime values of two *monic* linear polynomials x and $x+2m$. What if we select polynomials with different leading coefficients, like x and $2x+1$? Such *prime pairs* come up naturally in Sophie Germain's Theorem 7.11 (of section 7.27 in appendix 7F) and calculations support the guess that there are many (like 3 and 7; 5 and 11; 11 and 23; 23 and 47; ...). We therefore conjecture:

There are infinitely many pairs of primes $p, 2p + 1$.

One can generalize this to other pairs of linear polynomials but we might again have the problem that at least one is even, as with $p, 3p + 1$.

Exercise 5.11.1. Give conditions on integers a, b, c, d with $a, c > 0$, assuming that $(a, b) = (c, d) = 1$, which guarantee that there are infinitely many integers n for which $an + b$ and $cn + d$ are different and both positive and odd. We conjecture, under these conditions that:

There are infinitely many pairs of primes $am + b, cm + d$.

For triples of linear forms and even k-tuplets of linear forms, there are more exceptional cases. For example, the three polynomials $n, n + 2, n + 4$ can all simultaneously take odd values but, for each integer n, one of them is divisible by 3. We call 3 a *fixed prime divisor*, which plays the same role as 2 in the example $n, n + k$ with k odd. In general we need that a given set of linear forms $a_1x + b_1, a_2x + b_2, \dots, a_kx + b_k$ with integer coefficients is *admissible*; that is, there is no fixed prime divisor p. Specifically, for each prime p, there exists an integer n_p for which none of the $a_jn_p + b_j$ is divisible by p, which implies that p does not divide $a_jn + b_j$ for $1 \le j \le k$ for every integer $n \equiv n_p \pmod p$. This leads us to

The prime k-tuplets conjecture. *Let $a_1x + b_1, \dots, a_kx + b_k$ be an admissible set of k linear polynomials with integer coefficients, such that each a_j is positive. Then there are infinitely many positive integers m for which*

$$a_1m + b_1, \dots, a_km + b_k \text{ are all prime.}$$

Exercise 5.11.2.† Assuming the prime k-tuplets conjecture deduce that there are infinitely many pairs of *consecutive* primes $p, p + 100$.

Exercise 5.11.3.† Assuming the prime k-tuplets conjecture deduce that there are infinitely many triples of *consecutive* primes in an arithmetic progression.

Exercise 5.11.4.† Assuming the prime k-tuplets conjecture deduce that there are infinitely many quadruples of *consecutive* primes formed of two pairs of prime twins.

Exercise 5.11.5.† Let $a_{n+1} = 2a_n + 1$ for all $n \ge 0$. Fix an arbitrarily large integer N. Use the prime k-tuplets conjecture to show that we can choose a_0 so that $a_0, a_1, \dots, a_N$ are all primes.

Exercise 5.11.6. Show that the set of linear polynomials $a_1m + 1, a_2m + 1, \dots, a_km + 1$, with each a_j positive, is admissible.

There is more on prime k-tuplets of linear polynomials in appendix 5E.

What about other polynomials? For example, the polynomial $n^2 + 1$ takes prime values $2, 5, 17, 37, 101, \dots$ seemingly on forever, so we conjecture that:

There are infinitely many primes of the form $n^2 + 1$.

The polynomial $x^2 + 2x$ cannot be prime for many integer values since it is reducible (recall Theorem 5.4 and exercise 5.8.14(c)). This is a different reason (from the fixed prime factors above) for a polynomial not to take more than finitely many prime values. These are the only reasons known for a polynomial not to take infinitely many prime values and, if neither of them holds, then we believe that the polynomial does take on infinitely many prime values. More precisely:

Polynomial prime values conjecture. *Let $f_1(x), \dots, f_k(x) \in \mathbb{Z}[x]$, each irreducible, with positive leading coefficients. If $f_1 \cdots f_k$ has no fixed prime divisor, then:*

There are infinitely many integers m for which $f_1(m), \dots, f_k(m)$ are all prime.

To be precise, if $f_1, \dots, f_k$ have "no fixed prime divisor" then we mean that for every prime p there exists an integer n_p such that $f_1(n_p) \cdots f_k(n_p)$ is not divisible

by p. The polynomial prime values conjecture specialized to linear polynomials is the prime k-tuplets conjecture.[20]

Exercise 5.11.7. Prove that the only prime pair p, p^2+2 is $3, 11$.

Exercise 5.11.8. (a) Prove that if $f_1 \cdots f_k$ has no fixed prime divisor, then, for each prime p, there are infinitely many integers n such that $f_1(n) \cdots f_k(n)$ is not divisible by p.
(b)† Show that if $p > \deg(f_1(x) \cdots f_k(x))$ and p does not divide $f_1(x) \cdots f_k(x)$, then n_p exists.
(c) Prove that if $f_j(x) = x + h_j$ for given integers $h_1, \dots, h_k$, then n_p exists for a given prime p if and only if $\#\{\text{distinct } h_j \pmod p\} < p$.

The only case of the polynomial prime values conjecture that has been proved is when $k = 1$ with $f_1(.)$ is linear. The hypothesis ensures that $f(x) = qx + a$ with $q \geq 1$ and $(a, q) = 1$. This is Dirichlet's Theorem (that there are infinitely many primes $\equiv a \pmod q$ whenever $(a, q) = 1$, which we discuss in sections 8.17 of appendix 8D and 13.7).

Distinguishing primes and P_k's from other integers. The Möbius function was introduced in section 4.5, and in Corollary 4.5.1 we saw that the sum

$$\sum_{d|n} \mu(d)$$

is non-zero only if $n = 1$ and so allows us to distinguish the integer 1 from all other positive integers. In section 4.11 of appendix 4B we saw that if the sum

$$\sum_{d|n} \mu(d) \log(n/d)$$

is non-zero, then n has exactly one prime factor and so allows us to distinguish primes and prime powers from all other positive integers. A positive integer is called a "P_k" if it has no more than k distinct prime factors. In the next exercise we will see how an analogous sum allows us to distinguish P_k's.

Exercise 5.11.9.† (a)‡ Let $x_0, \dots, x_m$ be variables. Prove that if $m > k \geq 0$, then

$$\sum_{S \subset \{1,2,\dots,m\}} (-1)^{|S|} \Big(x_0 + \sum_{j \in S} x_j\Big)^k = 0.$$

(b) Deduce that if n has more than k different prime factors, then

$$\sum_{d|n} \mu(d)(\log(n/d))^k = 0.$$

(c)‡ What value does this take when n has exactly k different prime factors?

Exercise 5.11.10. Show that if each prime factor of n is $> n^{1/3}$, then n is either prime or the product of two primes.

Prime values of polynomials in several variables

One can ask for prime values of polynomials in two or more variables, for example, primes of the form m^2+n^2 or the form a^2+b^2+1 or more complicated polynomials of mixed degree like $4a^3 + 27b^2$. What is known?

[20] This conjecture was first formulated by Andrzej Schinzel in 1958. He called it "*Hypothesis H*" in that paper, and the name has stuck.

The proof of the prime number theorem can be adapted to many situations, for example to primes of the form m^2+n^2 or the form $2u^2+2uv+3v^2$ or indeed the prime values of any irreducible binary quadratic form (which are discussed in chapters 9 and 12) without a fixed prime divisor. The proof for m^2+n^2 uses the fact that $m^2+n^2=(m+in)(m-in)$, the *norm* of $m+in$. One can develop this to prove that any such *norm form* (the appropriate generalization[21] of m^2+n^2 to higher degree) takes on infinitely many prime values as long as it has no fixed prime factor. A norm form is always a degree d polynomial in d variables.

One can then ask for prime values of norm forms in which we fix some of the variables (perhaps to 0). For example, if $m=1$ in m^2+n^2, we are back to the open question about prime values of n^2+1. *However* in 2002 Heath-Brown was able to prove that a^3+2b^3 takes on infinitely prime values and then extended this, with Moroz, to any irreducible cubic form in two variables. In 2018, Maynard proved such a result for a family of norm forms[22] in $3m$ variables of degree $4m$ (or less).

These results on norm forms were all inspired by Friedlander and Iwaniec's 1998 breakthrough in which they took n to be a square in m^2+n^2 (and therefore found prime values of u^2+v^4), following Fouvry and Iwaniec's 1997 paper in which they took n to be prime (and therefore obtained infinitely many prime pairs p, m^2+p^2). This was the first example in which the polynomial in question is *sparse* in that the number of integer values it takes up to x is roughly x^c for some $c<1$. The current record sparsity is $c=\frac{2}{3}$ from the work of Heath-Brown and Moroz. In 2017, Heath-Brown and Xiannan Li went beyond the Fouvry-Iwaniec and Friedlander-Iwaniec results by showing that there are infinitely many prime pairs p, m^2+p^4.

In every case we expect that the proportion of values of the polynomial up to x which are prime is about $c/\log x$, where c is a constant which depends on how often each prime divides values of the polynomial.

Back in 1974, Iwaniec had shown how versatile sieve methods could be by showing that any quadratic polynomial in two variables (which is irreducible and has no fixed prime divisor) takes on infinitely many prime values, for example, m^2+n^2+1. We will see this result put to good use in appendix 12G when tiling a circle with smaller circles.

What about the prime values of more than one polynomial in several variables? We can generalize our conjectures as follows:

Multivariable polynomial prime values conjecture. *Let $f_1(x_1,\dots,x_n),\dots, f_k(x_1,\dots,x_n)\in\mathbb{Z}[x_1,\dots,x_n]$, each of which is irreducible. Suppose that there are infinitely many n-tuplets of integers $m_1,\dots,m_n$ for which each $f_j(m_1,\dots,m_n)$ is positive. If $f_1\cdots f_k$ has no fixed prime divisor, then there are*

Infinitely many n-tuplets of integers $m_1,\dots,m_n$ for which $f_1(m_1,\dots,m_n),\dots,f_k(m_1,\dots,m_n)$ are all prime.

In 1939, van der Corput showed that there are infinitely many three-term arithmetic progressions of primes, which can be written as

$$a, a+d, a+2d,$$

[21] More precisely the norm of $\sum_i x_i\omega_i$ where the ω_i are a basis for the ring of integers of some number field of degree d and the x_i are the variables.

[22] The norm of $\sum_{i=1}^{3m} x_i\omega^i$ where the field, of degree $4m$, is generated by ω over $\mathbb{Q}$.

three degree-one polynomials in two variables. For a long time, methods seemed inadequate to extend this to length four arithmetic progressions, but this was resolved in 2008 by Green and Tao, who proved that for any fixed integer $k \geq 3$ there are infinitely many prime k-tuplets of the form

$$a, a+d, a+2d, \ldots, a+(k-1)d.$$

The methods used were quite new to the search for prime numbers and this has led to widespread interest. In 2012, along with Ziegler, they were able to prove a very general result for linear polynomials, which is as good as one can hope for, given that there has been no progress directly on the prime k-tuplets conjecture:

Until we prove the twin prime conjecture we will be unable to prove the multivariable polynomial prime values conjecture, in full generality, even for linear polynomials, since two of the polynomials might differ by two, for example if $x+3y$ and $x+3y+2$ are in our set. More generally, without progress on the prime k-tuplets conjecture, we must avoid any linear relation between two of our polynomials.

Theorem 5.8 (The Green-Tao-Ziegler Theorem)**.** *Suppose that $f_1(\mathbf{x}), \ldots, f_k(\mathbf{x})$ are linear polynomials which satisfy the hypothesis of the multivariable polynomial prime values conjecture. Moreover assume that if $1 \leq i < j \leq k$, there do not exist integers a, b, c, not all zero, for which $af_i + bf_j = c$. Then there are infinitely many $\mathbf{m} \in \mathbb{Z}^n$ for which $f_1(\mathbf{m}), \ldots, f_k(\mathbf{m})$ are all prime.*

We will discuss applications of the Green-Tao-Ziegler Theorem in appendix 5E.

It is not difficult to show that there are infinitely many primes of the form $b^2 - 4ac$, the discriminant of an arbitrary quadratic polynomial. However we do not know how to prove that there are infinitely many primes of the form $4a^3 + 27b^2$, the discriminant of the cubic polynomial $x^3 + ax + b$. Proving this would have a significant impact on our understanding of various questions about degree 3 Diophantine equations.

Exercise 5.11.11. Let $g(x) = 1 + \prod_{j=1}^{k}(x-j)$. Prove that there exist integers a and b such that the reducible polynomial $f(x) = (ax+b)g(x)$ is prime when $x = n$ for $1 \leq n \leq k$. Compare this to the result in exercise 5.8.14(c) (with $d = k+1$).

Goldbach's conjecture and variants

Goldbach's 1742 conjecture is the statement that every even integer ≥ 4 can be written as the sum of two primes. It is still an open question though it has now been verified for all even numbers $\leq 4 \times 10^{18}$.

Great problems motivate mathematicians to think of new techniques, which can have great influence on the subject, even if they fail to resolve the original question. For example, although there have been few plausible ideas for proving Goldbach's conjecture, it has motivated some of the development of sieve theory, and there are some beautiful results on modifications of the original problem. The most famous are:

In 1975 Montgomery and Vaughan showed that if there are any exceptions to Goldbach's conjecture (that is, even integers n that are not the sum of two primes), then there are very few of them.

In 1973 Jingrun Chen showed that every sufficiently large even integer is the sum of a prime and an integer that is the product of at most two primes. Here "sufficiently large" means enormous.

In 1934 I. M. Vinogradov proved that every sufficiently large odd integer is the sum of three primes. The "sufficiently large" has recently been removed: Harald Helfgott, with computational assistance from David Platt, proved that every odd integer > 1 is the sum of at most three primes.

Exercise 5.11.12. Show that the Goldbach conjecture is equivalent to the statement that every integer > 1 is the sum of at most three primes.[23]

Other questions

Before this chapter we asked if there are infinitely many primes of the form $2^p - 1$ (Mersenne primes) or of the form $2^{2^n} + 1$ (Fermat primes). We can ask other questions in this vein, for example prime values of second-order linear recurrences which start $0, 1$ (like the Fibonacci numbers) or their companion sequences (see exercise 3.9.3) or prime values of high-order linear recurrence sequences.

Mersenne primes written in binary look like $111\ldots111$, and so are palindromic. Some people have been interested in primes of the form $\frac{1}{9}(10^n - 1)$ which equal $111\ldots111$ in base 10 and so are palindromic. We are unable to prove there are infinitely many Mersenne primes, so how about the easier question, are there infinitely many palindromic primes when written in binary or in decimal or indeeed in any other base? Also open.

We saw earlier that it is not difficult to show that there are infinitely many primes with the first few digits given. But how about missing digits? Can one find infinitely many primes which have no 7 in their decimal expansion or no 9 or no consecutive digits 123? These questions are all answered in a remarkable recent paper of Maynard [**4**].

Let M be a given n-by-n matrix. The (i, j)th entry of $M, M^2, \ldots$ can all be described by an nth-order linear recurrence sequence. To see this think of the powers of $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. We have already asked whether the trace can take infinitely many prime values. A recent question of interest is to take two (or more) such matrices M and N say, and then look at the entries of all "words" created by M and N, for example $M^a N^b M^c \cdots N^z$, and ask whether the entries are infinitely often prime (see section 9.15 of appendix 9D and appendix 12G for a beautiful example).

Guides to conjectures and the Green-Tao Theorem

[1] David Conlon, Jacob Fox, and Yufei Zhao, *The Green-Tao theorem: An exposition*, EMS Surv. Math. Sci. **1** (2014), 249–282.

[23] This was in fact the form in which Goldbach made his conjecture. Goldbach was a friend of Euler, arguably the greatest mathematician of the 18th century, and would often send Euler mathematical questions. In one letter Goldbach asked whether every integer > 1 is the sum of at most three primes, and Euler observed that this is equivalent to showing that every even number ≥ 4 is the sum of two primes. Why then does Goldbach get credit for this conjecture that he did not make? Perhaps because "*Euler is rich, and Goldbach is poor.*"

[2] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[3] Bryna Kra, *The Green-Tao theorem on arithmetic progressions in the primes: An ergodic point of view*, Bull. Amer. Math. Soc. **43** (2006), 3–23.

[4] James Maynard, *Small gaps between primes*, Annals Math. **181** (2015), 383–413.

[5] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208; erratum **5** (1958), 259.

Appendices. The extended version of chapter 5 has the following additional appendices:

Appendix 5B. *An important proof of infinitely many primes.* We give Euler's proof that there are infinitely many primes (which yields that the sum of the reciprocals of the primes diverges) and use this to show that the primes make up a vanishing proportion of the integers. We use this to introduce the Riemann zeta-function, as well as Riemann's program for proving the prime number theorem.

Appendix 5C. *What should be true about primes?* Here we explain Cramér's model for the distribution of primes based on Gauss's thoughts and determine what it predicts about the expected longest gaps between primes.

Appendix 5D. *Working with Riemann's zeta-function.* We further develop Riemann's program for proving the prime number theorem, detailing how the zeros of the Riemann zeta-function relate to the count of primes. We are therefore able to state the Riemann Hypothesis and discuss some attractive reformulations.

Appendix 5E. *Prime patterns: Consequences of the Green-Tao Theorem.* We look for all sorts of prime patterns and at fun questions about primes, for example magic squares of primes like

17	89	71
113	59	5
47	29	101

41	71	103	61
97	79	47	53
37	67	83	89
101	59	43	73

Examples of magic squares of primes.

Appendix 5F. *A panoply of prime proofs* presents several further proofs that there are finitely many primes, one by point-set topology, another using irrationality, and yet another via a counting argument.

Appendix 5G. *Searching for primes and prime formulas.* We look for formulas for primes, including Matijasevic's amazing polynomial in 26 variables, discuss their value, explore Conway's prime-producing machine and patterns in Ulam's spiral.

Appendix 5H. *Dynamical systems and infinitely many primes.* Developing a perspective on Euclid's original proof, we show that there are many different polynomials for which there are infinitely many prime divisors of the iterated values of the polynomial, starting from a non-periodic point.

Chapter 6

Diophantine problems

Diophantine equations are polynomial equations in which we study the integer or rational solutions. They are named after Diophantus (who lived in Alexandria in the third century A.D.) who wrote up his understanding of such equations in his thirteen volume *Arithmetica* (though only six part-volumes survive today). This work was largely forgotten until interest was revived by Bachet's 1621 translation of *Arithmetica* into Latin.[1]

6.1. The Pythagorean equation

Right-angled triangles with sides $3, 4, 5$ and $5, 12, 13$, etc, were known to the ancient Babylonians. We wish to determine all right-angled triangles with integer sides, which amounts to finding all solutions in positive integers x, y, z to the Pythagorean equation

$$x^2 + y^2 = z^2.$$

Note that $z > x, y > 0$ as x, y, and z are all positive. We can reduce the problem, without loss of generality, so as to work with some convenient assumptions:

- That x, y, and z are pairwise coprime, by dividing through by their gcd, as in exercise 1.7.8.
- That x is even and y is odd, and therefore that z is odd: First note that x and y cannot both be even, since x, y, and z are pairwise coprime; nor both odd, by exercise 2.5.6(b). Hence one of x and y is even, the other odd, and we interchange them, if necessary, to ensure that x is even and y is odd.

Under these assumptions we reorganize the equation and factor to get

$$(z - y)(z + y) = z^2 - y^2 = x^2.$$

[1] Translations of various ancient Greek texts into Latin helped inspire the Renaissance.

We now prove that $(z-y, z+y) = 2$: We observe that $(z-y, z+y)$ divides $(z+y)-(z-y) = 2y$ and $(z+y)+(z-y) = 2z$, and that $(2y, 2z) = 2(y, z) = 2$. Therefore $(z-y, z+y)$ divides 2, and so equals 2 as $z-y$ and $z+y$ are both even.

Therefore, since $(z-y)(z+y) = x^2$ and $(z-y, z+y) = 2$, there exist integers r, s such that

$$z-y = 2s^2 \text{ and } z+y = 2r^2; \quad \text{or} \quad z-y = -2s^2 \text{ and } z+y = -2r^2,$$

by exercise 3.3.7(c). The second case is impossible since r^2, y, and z are all positive. From the first case we deduce that

$$x = 2rs, \quad y = r^2 - s^2, \quad \text{and} \quad z = r^2 + s^2.$$

To ensure that x, y, and z are pairwise coprime we need $(r, s) = 1$ and $r+s$ odd. If we now multiply back in any common factors, we get the general solution

$$\boxed{x = 2grs, \ \ y = g(r^2 - s^2), \text{ and } z = g(r^2 + s^2).} \tag{6.1.1}$$

If we want an actual triangle, then the side lengths should all be positive so we may assume that $g > 0$ and $r > s > 0$, as well as $(r, s) = 1$ and r and s having different parities.[2] The reader should verify that the integers x, y, and z given by this parametrization always satisfy the Pythagorean equation.

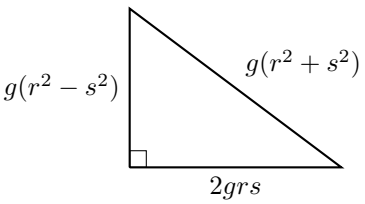


Figure 6.1. Parameterization of all integer-sided right-angled triangles.

One can also give a nice geometric proof of the parametrization in (6.1.1). We start with a reformulation of the question.

Exercise 6.1.1. Prove that the integer solutions to $x^2 + y^2 = z^2$ with $z > 0$ and $(x, y, z) = 1$ are in 1-to-1 correspondence with the rational solutions u, v to $u^2 + v^2 = 1$.

Where else does a line going through $(1, 0)$ intersect the circle $x^2 + y^2 = 1$? Unless the line is vertical it will hit the unit circle in exactly one other point, which we will denote by (u, v). Note that $u < 1$. If the line has slope t, then $t = v/(u-1)$ is rational if u and v are.

[2] That is, one is even, the other is odd.

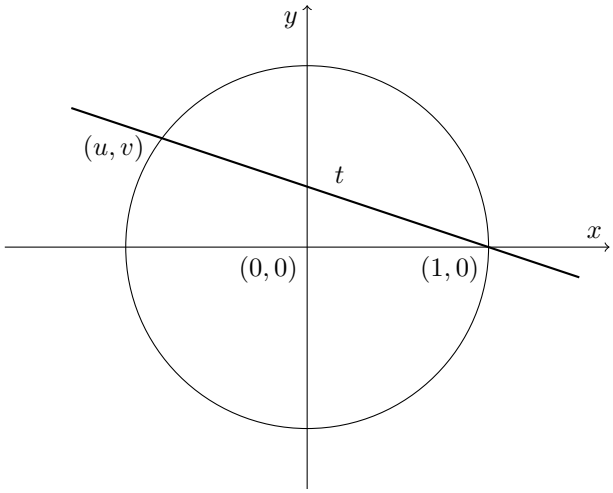


Figure 6.2. A line through $(1,0)$ on the circle $x^2+y^2=1$.

In the other direction, the line through $(1,0)$ of slope t is $y=t(x-1)$ which intersects $x^2+y^2=1$ where $1-x^2=y^2=t^2(x-1)^2$, so that either $x=1$ and $y=0$, or we have $1+x=t^2(1-x)$, which yields the point (u,v) with

$$u \;=\; \frac{t^2-1}{t^2+1} \quad \text{and} \quad v \;=\; \frac{-2t}{t^2+1}\,.$$

These are both rational if t is. We have therefore proved that $u,v\in\mathbb{Q}$ if and only if $t\in\mathbb{Q}$. In other words the line of slope t through $(1,0)$ hits the unit circle again at another rational point if and only if t is rational, and then we can classify those points in terms of t. Therefore, writing $t=-r/s$ where $(r,s)=1$, we have

$$u=\frac{r^2-s^2}{r^2+s^2} \quad \text{and} \quad v=\frac{2rs}{r^2+s^2},$$

the same parametrization to the Pythagorean equation as in (6.1.1) when we clear out denominators.

Exercise 6.1.2.† Find a formula for all the rational points on the curve $x^2-y^2=3$.

Exercise 6.1.3. We call $\{a,b,c\}$ a *primitive Pythagorean triple* if a, b, and c are pairwise coprime integers for which $a^2+b^2=c^2$.

(a) Prove that, in a primitive Pythagorean triple, the difference in length between the hypotenuse and each of the other sides is either a square or twice a square.

(b) Can one find primitive Pythagorean triples in which the hypotenuse is three units longer than one of the other sides? Either give an example or prove that it is impossible.

(c)† One can find primitive Pythagorean triples in which the hypotenuse is one unit longer than one of the other sides, e.g., $\{3,4,5\}$, $\{5,12,13\}$, $\{7,24,25\}$, $\{9,40,41\}$, $\{11,60,61\}$. Parametrize all such solutions.

(d)† One can find primitive Pythagorean triples in which the hypotenuse is two units longer than one of the other sides, e.g., $\{3,4,5\}$, $\{8,15,17\}$, $\{12,35,37\}$, $\{16,63,65\}$, $\{20,99,101\}$. Parametrize all such solutions.

Exercise 6.1.4. (a) Prove that the side lengths of a primitive Pythagorean triple are $\not\equiv 2 \pmod 4$.

(b) Given integer $n > 1$ with $n \not\equiv 2 \pmod 4$, explicitly give a primitive Pythagorean triple which has n as a side length.

Exercise 6.1.5.† Prove that there are infinitely many triples of coprime squares in arithmetic progressions.

Around 1637, Pierre de Fermat was studying the proof of (6.1.1) in his copy of Bachet's translation of Diophantus's *Arithmetica*. In the margin he wrote:

> *I have discovered a truly marvellous proof that it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers. This margin is too narrow to contain it.*
>
> —Pierre de Fermat (1637), in his copy of *Arithmetica*

In other words, Fermat claimed that for every integer $n \geq 3$ there do not exist positive integers x, y, z for which

$$x^n + y^n = z^n.$$

This is known as "Fermat's Last Theorem". Fermat did not subsequently mention this problem or his truly marvellous proof elsewhere, and the proof has not, to date, been rediscovered, despite many efforts.[3] Fermat did show that there are no solutions when $n = 4$ and we will present his proof in section 6.4, as well as some consequences for more general exponents n in Fermat's Last Theorem.

6.2. No solutions to a Diophantine equation through descent

Some Diophantine equations can be shown to have no solutions by starting with a purported smallest solution and finding an even smaller one, thereby establishing a contradiction. Such a *proof by descent* can be achieved in various different ways.

No solutions through prime divisibility

For some equations one can perform descent by considering the divisibility of the variables by various primes. We now give such a proof that $\sqrt{2}$ is irrational.

Proof of Proposition 3.4.1 by 2-divisibility. [$\sqrt{2}$ *is irrational.*] Let us recall that if $\sqrt{2}$ is rational, then we can write it as a/b so that $a^2 = 2b^2$. Let us suppose that (b, a) gives the smallest solution to $y^2 = 2x^2$ in positive integers. Now 2 divides $2b^2 = a^2$ so that $2|a$. Writing $a = 2A$, thus $b^2 = 2A^2$, and so $2|b$. Writing $b = 2B$ we obtain a solution $A^2 = 2B^2$ where A and B are half the size of a and b, contradicting the assumption that (b, a) is minimal. □

Exercise 6.2.1. Show that there are no non-zero integer solutions to $x^3 + 3y^3 + 9z^3 = 0$.

[3] Fermat wrote several important thoughts about number theory on his personal copy of *Arithmetica*, without proof. When he died his son, Samuel, made these available by republishing *Arithmetica* with his father's annotations. This is the *last* of those claims to have been fully understood.

No solutions through geometric descent

Proof of Proposition 3.4.1 by geometric descent. Again assume that $\sqrt{2} = a/b$ with a and b positive integers, where a is minimal. Hence $a^2 = 2b^2$ which gives rise to the smallest isosceles, right-angled triangle, OPQ with integer side lengths $\overline{OP} = \overline{OQ} = b$, $\overline{PQ} = a$ and angles $P\hat{O}Q = 90°$, $P\hat{Q}O = Q\hat{P}O = 45°$. Now mark a point R which is b units along PQ from Q and then drop a perpendicular to meet OP at the point S so that SR is perpendicular to PQ. Then $R\hat{P}S = Q\hat{P}O = 45°$, and so $R\hat{S}P = 180° - 90° - 45° = 45°$ by considering the angles in the triangle RSP. Therefore RSP is a smaller isosceles, right-angled triangle than OPQ. Moreover we have side lengths $\overline{RS} = \overline{PR} = a - b$. To establish our contradiction we need to show that the hypoteneuse, PS, also has integer length.

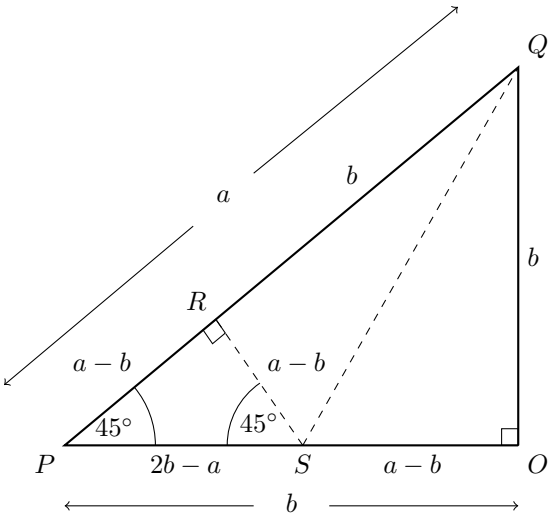


Figure 6.3. No solutions through geometric descent.

The two triangles, OQS and RQS, are congruent, since they both contain a right-angle opposite SQ and adjacent to a side of length b (OQ and RQ, respectively). Therefore $\overline{OS} = \overline{SR} = a - b$ and so $\overline{PS} = \overline{OP} - \overline{OS} = b - (a - b) = 2b - a$. Hence RSP is a smaller isosceles, right-angled triangle than OPQ with integer side lengths, contradicting the assumed minimality of OPQ. □

One can write this proof more algebraically: As $a^2 = 2b^2$, so $a > b > a/2$. Now

$$(2b - a)^2 = a^2 - 4ab + 2b^2 + 2b^2 = a^2 - 4ab + 2b^2 + a^2 = 2(a - b)^2.$$

However $0 < 2b - a < a$, contradicting the minimality of a.

Proof of Proposition 3.4.2 by an analogous descent. [*If d is an integer for which $\sqrt{d}$ is rational, then $\sqrt{d}$ is an integer.*] If $\sqrt{d}$ is rational, then we can write it as a/b so that $a^2 = db^2$. Let us suppose that (b, a) gives the smallest solution

to $y^2 = dx^2$ in positive integers. Let r be the smallest integer $\geq db/a$, so that $\frac{db}{a} + 1 > r \geq \frac{db}{a}$, and therefore $a > ra - db \geq 0$. Then

$$\begin{aligned}(ra - db)^2 &= da^2 - 2rdab + d^2b^2 + (r^2 - d)a^2 \\ &= da^2 - 2rdab + d^2b^2 + (r^2 - d)db^2 = d(rb - a)^2.\end{aligned}$$

However $0 \leq ra - db < a$, contradicting the minimality of a, unless $ra - db = 0$. In this case $r^2 = d \cdot db^2/a^2 = d$. □

6.3. Fermat's "infinite descent"

Fermat proved that there are no right-angled triangles with all integer sides whose area is a square (see exercise 6.3.1 below). In so doing he developed the important technique of "infinite descent", which we now exhibit in two related questions. (The reader can read the proof of only one of the two following similar theorems. They both lead to the same Corollary 6.4.1.)

Theorem 6.1. *There are no solutions in non-zero integers x, y, z to*

$$x^4 + y^4 = z^2.$$

Proof. Assume that there is a solution and let x, y, z be the solution in positive integers with z minimal. We may assume that $\gcd(x, y) = 1$ or else we can divide the equation through by the fourth power of $\gcd(x, y)$ to obtain a smaller solution. Here we have

$$(x^2)^2 + (y^2)^2 = z^2 \quad \text{with} \quad \gcd(x^2, y^2) = 1,$$

and so, by (6.1.1), there exist integers r, s with $(r, s) = 1$ and $r + s$ odd such that

$$x^2 = 2rs, \quad y^2 = r^2 - s^2, \quad \text{and} \quad z = r^2 + s^2$$

(swapping the roles of x and y if necessary to ensure that x is even). Now r and s have the same sign since $rs = x^2/2$, so we may assume they are both > 0 (multiplying each by -1 if necessary). Now $s^2 + y^2 = r^2$ with y odd and $(r, s) = 1$ and so, by (6.1.1), there exist integers a, b with $(a, b) = 1$ and $a + b$ odd such that

$$s = 2ab, \quad y = a^2 - b^2, \quad \text{and} \quad r = a^2 + b^2,$$

and so

$$x^2 = 2rs = 4ab(a^2 + b^2).$$

Now a and b have the same sign since $ab = s/2 > 0$, and therefore we may assume they are both > 0 (multiplying each by -1 if necessary).

Now a, b, and $a^2 + b^2$ are pairwise coprime positive integers whose product is a square so they must each be squares by exercise 3.3.7(b). Write $a = u^2$, $b = v^2$, and $a^2 + b^2 = w^2$ for some positive integers u, v, w. Therefore

$$u^4 + v^4 = a^2 + b^2 = w^2$$

yields another solution to the original equation. We wish to compare this to the

solution (x, y, z) we started with. We find that

$$w \le w^2 = a^2 + b^2 = r < r^2 + s^2 = z,$$

contradicting the minimality of z. □

Theorem 6.2. *There are no solutions in positive integers x, y, z to*

$$x^4 - y^4 = z^2.$$

Proof. If there is a solution, take the one with x minimal. We may assume $(x, y) = 1$ or else we divide through by the fourth power of the common factor.

We begin by noting that

$$(y^2)^2 + z^2 = (x^2)^2 \quad \text{with} \quad \gcd(x^2, y^2) = 1.$$

If z is even, then, by (6.1.1), there exist integers X, Y with $(X, Y) = 1$, of opposite parity, for which

$$x^2 = X^2 + Y^2 \quad \text{and} \quad y^2 = X^2 - Y^2, \quad \text{so that} \quad X^4 - Y^4 = (xy)^2.$$

Now $X^2 < x^2$, contradicting the minimality of x.

Therefore z is odd. By (6.1.1) there exist integers r, s with $(r, s) = 1$, of opposite parity, for which

$$x^2 = r^2 + s^2 \quad \text{and} \quad y^2 = 2rs.$$

Now r and s have the same sign since $rs = y^2/2 > 0$, and therefore we may assume they are both > 0 (multiplying each by -1 if necessary). From the equation $2rs = y^2$ we deduce that $r = 2R^2, s = Z^2$ for some integers R, Z (swapping the roles of r and s, if necessary). From (6.1.1) applied to the equation $r^2 + s^2 = x^2$, there exist integers u, v with $(u, v) = 1$, of opposite parity, for which $r = 2uv$ and $s = u^2 - v^2$. Now $uv = r/2 = R^2$, so we may assume they are both positive (multiplying each by -1 if necessary), and so $u = m^2, v = n^2$ for some integers m, n. Therefore

$$m^4 - n^4 = u^2 - v^2 = s = Z^2.$$

Now $m^2 < (mn)^2 = uv = r/2 < x/2$, contradicting the minimality of x. □

Exercise 6.3.1 (Fermat, 1659)**.**

(a)† Prove that there is no right-angled, integer-sided, triangle whose area is a square.

(b) Deduce that there is no right-angled, rational-sided, triangle whose area is 1.

(c) Deduce that there are no integer solutions to $x^4 + 4y^4 = z^2$.

In appendix 6B we will see an alternative proof of these results using classical Greek geometry.

6.4. Fermat's Last Theorem

Fermat's Last Theorem is the assertion that for every integer $n \ge 3$ there do not exist positive integers x, y, z for which

$$x^n + y^n = z^n.$$

Corollary 6.4.1 (Fermat)**.** *There are no solutions in non-zero integers x, y, z to*

$$x^4 + y^4 = z^4.$$

Exercise 6.4.1. Prove this using Theorem 6.1 or Theorem 6.2.

We deduce that Fermat's Last Theorem holds for all exponents $n \geq 3$ if it holds for all odd prime exponents:

Proposition 6.4.1. *If Fermat's Last Theorem is false, then there exists an odd prime p and pairwise coprime non-zero integers x, y, z such that*

$$x^p + y^p + z^p = 0.$$

Proof. Suppose that $x^n + y^n = z^n$ with $x, y, z > 0$ and $n \geq 3$. If two of x, y, and z have a common factor, then it must divide the third and so we can divide out the common factor. Hence we may assume that x, y, z are pairwise coprime positive integers. Now any integer $n \geq 3$ has a factor m which is either $= 4$ or is an odd prime (see exercise 3.1.3(b)). Hence, if $n = dm$, then $(x^d)^m + (y^d)^m = (z^d)^m$, so we get a solution to Fermat's Last Theorem with exponent m. We can rule out $m = 4$ by Corollary 6.4.1. Therefore $m = p$ is an odd prime and we have the desired solution $(x^d)^p + (y^d)^p + (-z^d)^p = 0$. □

A brief history of equation solving

There have been many attempts to prove Fermat's Last Theorem, inspiring the development of much great mathematics, for example, ideal theory (see appendices 3D and 12B). We will discuss one beautiful advance due to Sophie Germain from the beginning of the 19th century (see section 7.27 of appendix 7F).

In 1994 Andrew Wiles proved Fermat's Last Theorem, developing ideas of Frey, Ribet, and Serre involving modular forms, a subject far removed from the original question. The proof is extraordinarily deep, involving some of the most profound themes in arithmetic geometry.[4] If the whole proof were written in the leisurely style of, say, this book, it would probably take a couple of thousand pages. This could not be the proof that Fermat believed that he had—could Fermat have been correct? Could there be a short, elementary, marvelous proof still waiting to be found? Or will Fermat's claim always remain a mystery?

To some extent one can measure the difficulty of solving Diophantine equations (especially rational solutions to equations with two variables) by their degree.[5] The first three chapters of this book focus on linear (degree-one) equations, culminating in section 3.6. Much of the rest of this book provides tools for studying degree-two (quadratic) equations; see chapters 8 and 9, sections 11.2 and 11.3, and chapter 12. Degree-three (cubic) equations give rise to elliptic curves; many of the key questions about elliptic curves lay shrouded in mystery and so they are intensively researched in number theory today (see chapter 17). In 1983 Gerd Faltings showed that higher-degree Diophantine equations only have finitely many rational solutions (though not how to find those solutions).

For higher-degree equations perhaps the most interesting cases are Diophantine equations with varying degree, like the Fermat equation. Another famous example is *Catalan's conjecture*: The positive integer powers are

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, \ldots$$

[4] See our sequel [**Grab**] for some discussion of the ideas involved in the proof.

[5] A better but more sophisticated invariant is the *genus*, which requires quite a bit of algebraic geometry to define and is beyond the scope of this book.

which seem to get wider spread out as they get larger. Only two of the numbers in our list, 8 and 9, differ by 1, and Catalan conjectured that this is the only example of powers differing by 1. That is, the only integer solution to

$$x^p - y^q = 1 \text{ with } x, y \neq 0 \text{ and } p, q \geq 2,$$

is $3^2 - 2^3 = 1$. This was shown to be true by Preda Mihăilescu in 2002.

Combining these two famous equations leads to the *Fermat-Catalan equation*

$$x^p + y^q = z^r \text{ where } (x, y, z) = 1 \text{ and } \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

We insist that $(x, y, z) = 1$ because one can find "trivial" solutions like $2^k + 2^k = 2^{k+1}$ in many cases (see exercise 6.5.8 for more examples). Obviously there are solutions when one of p, q, r is 1, so we insist they are all ≥ 2. One can find solutions when two of the exponents equal 2, and so the peculiar looking condition $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ turns out to be the correct one. We do know of ten solutions:

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2,$$

$$17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7,$$

$$43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

It is conjectured that there are only finitely many solutions x^p, y^q, z^r to the Fermat-Catalan equation; perhaps these ten are all the solutions. All of our ten solutions have an exponent equal to 2. So one might further conjecture that there are no solutions to the Fermat-Catalan equation with p, q, r all > 2. These are open questions and mathematicians are making headway. Henri Darmon and I proved in 1995 that there are only finitely many solutions for each *fixed* triple p, q, r. Today we know that for various infinite families exponent triples p, q, r, the Fermat-Catalan equation has no solutions: For example when $p = q$ and $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ there are no solutions if r is divisible by 2 or by 3 or by p, or if p is even and r is divisible by 5, etc. (see [**1**] for the state of the art).

Now that Fermat's Last Theorem has been proved, what can take its place as the "holy grail" of Diophantine equations? The *abc*-conjecture is clearly an important problem that would have profound effects on equations and even in other areas of number theory. In appendix 6A we will discuss its analogy for polynomials and then discuss the *abc*-conjecture itself and its influence on other equations, in section 11.5.

References for this chapter

[1] Michael Bennett, Imin Chen, Sander Dahmen, Soroosh Yazdani, *Generalized Fermat equations: A miscellany*, Int. J. Number Theory **11** (2015), 1–28.

[2] John J. Watkins, chapter 5 of *Number theory, a historical approach*, Princeton University Press, 2014.

Additional exercises

Exercise 6.5.1. Find all rational-sided right-angled triangles in which the area equals the perimeter. Prove that $5, 12, 13$ and $6, 8, 10$ are the only such integer-sided triangles.

Exercise 6.5.2.† Let n be an integer > 2 that is $\not\equiv 2 \pmod 4$. Prove that there are $2^{\omega(n)-1}$ distinct primitive Pythagorean triangles in which n is the length of a side which is not the hypotenuse, where $\omega(n)$ counts the number of distinct prime factors of n.

Exercise 6.5.3.† Find a 1-to-1 correspondence between pairs of integers $b, c > 0$ for which $x^2 - bx - c$ and $x^2 - bx + c$ are both factorable over $\mathbb{Z}$, and right-angled triangles in which all three sides are integers.

Exercise 6.5.4. Prove that if $f(x) \in \mathbb{Z}[x]$ is a quadratic polynomial for which $f(x)$ and $f(x) + 1$ both have integer roots, then $f(x) + 1$ is the square of a linear polynomial. (Try substituting the roots of $f(x)$ into $f(x) + 1$ and studying divisibilities of the differences of the roots.)

Exercise 6.5.5.† We wish to show that $\alpha = \frac{\sqrt{5}+1}{2}$ is irrational. Suppose it is rational, so that $\alpha = p/q$ with $(p, q) = 1$. Now α satisfies the equation $x^2 = x + 1$, so dividing through by x we have $x = (1 + x)/x$, and so $\alpha = (p + q)/p$. Prove that p/q cannot equal $(p + q)/p$ and therefore establish a contradiction.

Exercise 6.5.6.† Generalize the proof in the last exercise, to prove that if α is a rational root of $x^2 - ax - b \in \mathbb{Z}[x]$, then α is an integer which divides b.

Exercise 6.5.7.‡ Prove that $2n$ is the length of the perimeter of a right-angled integer-sided triangle if and only if there exist divisors d_1, d_2 of n for which $d_1 < d_2 < 2d_1$.

Exercise 6.5.8. Suppose that integers p, q, r are given. For any integers a and b let $c = a^p + b^q$. If we multiply this through by c^n, where n is divisible by p and q, then $(ac^{n/p})^p + (bc^{n/q})^q = c^{n+1}$. Determine conditions on p, q, and r under which we find an integer n such that c^{n+1} is an rth power (and therefore find an integer solution to $x^p + y^q = z^r$, albeit with $(x, y, z) > 1$).

Exercise 6.5.9. Calculations show that every integer in $[129, 300]$ is the sum of distinct squares. Deduce that every integer > 128 is the sum of distinct squares. (In exercise 2.5.6(f) we showed that there are infinitely many integers that cannot be written as the sum of three squares. In appendix 12E we will show that every integer is the sum of four squares.)

Exercise 6.5.10. Prove that there are infinitely many integers that cannot be written as the sum of three cubes.

Exercise 6.5.11.‡ Calculations show that every integer in $[12759, 30000]$ is the sum of distinct cubes of positive integers. Deduce that every integer > 12758 is the sum of distinct cubes of positive integers. (In 2015 Siksek showed that every integer > 454 is the sum of at most seven positive cubes. It is believed, but not proven, that every sufficiently large integer is the sum of at most four positive cubes.)

Exercise 6.5.12. Verify the identity $6x = (x + 1)^3 + (x - 1)^3 - 2x^3$. Deduce that every prime is the sum of no more than five cubes of integers (which can be positive or negative).

Exercise 6.5.13. (a) Prove that $n^4 \equiv 0$ or $1 \pmod{16}$ for all integers n.
Let N be divisible by 16.
(b) Show that if N is the sum of 15 fourth powers, then each of those fourth powers is even.
(c) Deduce that N is the sum of 15 fourth powers if and only if $N/16$ is the sum of 15 fourth powers.
(d) Prove that 31 is not the sum of 15 fourth powers but is the sum of 16 fourth powers.
(e) Deduce that there are infinitely positive integers N that are not the sum of 15 fourth powers.

(In 2005, Deshouillers, Kawada, and Wooley showed that every integer > 13792 can be written as the sum of 16 fourth powers.)

In 1770 Waring asked whether for all integers k there exists an integer $g(k)$ such that every positive integer is the sum of at most $g(k)$ kth powers of positive integers. This was proved by Hilbert in 1909 but it is still a challenge to evaluate the smallest possible $g(k)$ for each k. We discuss this further in appendix 17D.

Appendix 6A. Polynomial solutions of Diophantine equations

6.6. Fermat's Last Theorem in $\mathbb{C}[t]$

The notation $\mathbb{C}[t]$ denotes polynomials whose coefficients are complex numbers. In section 6.1 we saw that all integer solutions to $x^2+y^2=z^2$ are derived from letting t be a rational number in the polynomial solution

$$(t^2-1)^2+(2t)^2 \;=\; (t^2+1)^2.$$

We now prove that there are no "genuine" polynomial solutions to Fermat's equation

$$x^p+y^p=z^p \tag{6.6.1}$$

with exponent p larger than 2 (where by *genuine* we mean that $(x(t),y(t),z(t))$ is not a polynomial multiple of a solution of (6.6.1) in complex numbers).

Proposition 6.6.1. *There are no genuine polynomial solutions $x(t),y(t),z(t)\in\mathbb{C}[t]$ to $x(t)^p+y(t)^p=z(t)^p$ with $p\geq 3$.*

Proof. Assume that there is a solution with x, y, and z all non-zero to (6.6.1) where $p\geq 3$. We may assume that x, y, and z have no common (polynomial) factor or else we can divide out by that factor (and that they are pairwise coprime by the same argument as in section 6.1). Our first step will be to differentiate (6.6.1) to get

$$px^{p-1}x'+py^{p-1}y'=pz^{p-1}z'$$

and after dividing out the common factor p, this leaves us with

$$x^{p-1}x'+y^{p-1}y'=z^{p-1}z'. \tag{6.6.2}$$

We now have two linear equations (6.6.1) and (6.6.2) (thinking of x^{p-1}, y^{p-1}, and z^{p-1} as our variables), which suggests we use linear algebra to eliminate a variable: Multiply (6.6.1) by y' and (6.6.2) by y, and subtract, to get

$$x^{p-1}(xy' - yx') = x^{p-1}(xy' - yx') + y^{p-1}(yy' - yy') = z^{p-1}(zy' - yz').$$

Therefore x^{p-1} divides $z^{p-1}(zy' - yz')$, but since x and z have no common factors, this implies that

$$x^{p-1} \text{ divides } zy' - yz'. \tag{6.6.3}$$

This is a little surprising, for if $zy' - yz'$ is non-zero, then a high power of x divides $zy' - yz'$, something that does not seem consistent with (6.6.1).

Now, if $zy' - yz' = 0$, then $(y/z)' = 0$ and so y is a constant multiple of z, contradicting our statement that y and z have no common factor. Therefore (6.6.3) implies, taking degrees of both sides, that

$$(p-1)\ \deg(x) \le \deg(zy' - yz') \le \deg(y) + \deg(z) - 1,$$

since $\deg(y') = \deg(y) - 1$ and $\deg(z') = \deg(z) - 1$. Adding $\deg(x)$ to both sides gives

$$p\ \deg(x) < \deg(x) + \deg(y) + \deg(z). \tag{6.6.4}$$

The right side of (6.6.4) is symmetric in x, y, and z. The left side is a function of x simply because of the order in which we chose to do things above. We could just as easily have derived the same statement with y or z in place of x on the left side of (6.6.4), so that

$$p\ \deg(y) < \deg(x) + \deg(y) + \deg(z)$$
$$\text{and} \quad p\ \deg(z) < \deg(x) + \deg(y) + \deg(z).$$

Adding these last three equations together and then dividing out by $\deg(x) + \deg(y) + \deg(z)$ implies

$$p < 3,$$

and so Fermat's Last Theorem is proved, at least for polynomials. □

That Fermat's Last Theorem is not difficult to prove for polynomials is an old result, going back certainly as far as Liouville in 1851.

Exercise 6.6.1. Prove that all solutions to $x(t)^2 + y(t)^2 = z(t)^2$ in polynomials are a scalar multiple of some solution of the form $(r(t)^2 - s(t)^2)^2 + (2r(t)s(t))^2 = (r(t)^2 + s(t)^2)^2$.

6.7. $a + b = c$ in $\mathbb{C}[t]$

We now intend to extend the idea in our proof of Fermat's Last Theorem for polynomials to as wide a range of questions as possible. It takes a certain genius to generalize to something far simpler than the original. But what could possibly be more simply stated, yet more general, than Fermat's Last Theorem? It was Richard C. Mason (1983) who gave us that insight: *Look for solutions to*

$$a + b = c.$$

We will just follow through the above proof of Fermat's Last Theorem for polynomials (Proposition 6.6.1) and see where it leads: Start by assuming, with no loss

of generality, that a, b, and c are all non-zero polynomials without common factors (or else all three share the common factor and we can divide it out). Then we differentiate to get

$$a'+b'=c'.$$

Next we need to do linear algebra. It is not quite so obvious how to proceed analogously, but what we do learn in a linear algebra course is to put our coefficients in a matrix and solutions follow if the determinant is non-zero. This suggests defining

$$\Delta(t):=\begin{vmatrix} a(t) & b(t) \\ a'(t) & b'(t)\end{vmatrix}.$$

Then if we add the first column to the second, we get

$$\Delta(t)=\begin{vmatrix} a(t) & c(t) \\ a'(t) & c'(t)\end{vmatrix},$$

and similarly

$$\Delta(t)=\begin{vmatrix} c(t) & b(t) \\ c'(t) & b'(t)\end{vmatrix}$$

by adding the second column to the first, a beautiful symmetry.

We note that $\Delta(t)\neq 0$, or else $ab'-a'b=0$ so b is a scalar multiple of a (with the same argument as above), contradicting our hypothesis.

To find the appropriate analogy to (6.6.3), we consider the power to which the factors of a (as well as b and c) divide our determinant: Let α be a root of $a(t)$, and suppose that $(t-\alpha)^e$ is the highest power of $(t-\alpha)$ which divides $a(t)$ (we write $(t-\alpha)^e\|a(t)$). Now we can write $a(t)=U(t)(t-\alpha)^e$ where $U(t)$ is a polynomial that is not divisible by $(t-\alpha)$, so that $a'(t)=(t-\alpha)^{e-1}V(t)$ where $V(t):=U'(t)(t-\alpha)+eU(t)$. Now $(t-\alpha,V(t))=(t-\alpha,eU(t))=1$, and so $(t-\alpha)^{e-1}\|a'(t)$. Therefore

$$\Delta(t)=a(t)b'(t)-a'(t)b(t)=(t-\alpha)^{e-1}W(t)$$

where $W(t):=U(t)(t-\alpha)b'(t)-V(t)b(t)$ and $(t-\alpha,W(t))=(t-\alpha,V(t)b(t))=1$ as $t-\alpha$ does not divide $b(t)$ or $V(t)$. Therefore we have proved that

$$(t-\alpha)^{e-1}\|\Delta(t).$$

This implies that $(t-\alpha)^e$ divides $\Delta(t)(t-\alpha)$. Multiplying all such $(t-\alpha)^e$ together we obtain (since they are pairwise coprime) that

$$a(t) \text{ divides } \Delta(t)\prod_{a(\alpha)=0}(t-\alpha).$$

In fact $a(t)$ only appears on the left side of this equation because we studied the linear factors of a; analogous statements for $b(t)$ and $c(t)$ are also true, and since $a(t),b(t),c(t)$ have no common roots, we can combine those statements to read

$$a(t)b(t)c(t) \quad \text{divides} \quad \Delta(t)\prod_{(abc)(\alpha)=0}(t-\alpha). \tag{6.7.1}$$

The next step is to take the degrees of both sides of (6.7.1). The degree of $\prod_{(abc)(\alpha)=0}(t-\alpha)$ is precisely the total number of distinct roots of $a(t)b(t)c(t)$.

Therefore

$$\text{degree}(a) + \text{degree}(b) + \text{degree}(c) \leq \text{degree}(\Delta) + \#\{\alpha \in \mathbb{C} : \ (abc)(\alpha) = 0\}.$$

Now, using the three different representations of Δ above, we have

$$\text{degree}(\Delta) \leq \begin{cases} \text{degree}(a) + \text{degree}(b) - 1, \\ \text{degree}(a) + \text{degree}(c) - 1, \\ \text{degree}(c) + \text{degree}(b) - 1. \end{cases}$$

Inserting all this into the previous inequality we get

$$\text{degree}(a), \text{degree}(b), \text{degree}(c) < \#\{\alpha \in \mathbb{C} : \ (abc)(\alpha) = 0\}.$$

Put another way, this result can be read as:

Theorem 6.3 (The *abc* Theorem for Polynomials)**.** *If $a(t), b(t), c(t) \in \mathbb{C}[t]$ do not have any common roots and provide a genuine polynomial solution to $a(t)+b(t) = c(t)$, then the maximum of the degrees of $a(t), b(t), c(t)$ is less than the number of distinct roots of $a(t)b(t)c(t) = 0$.*

This is a "best possible" result in that we can find infinitely many examples where there is exactly one more zero of $a(t)b(t)c(t) = 0$ than the largest of the degrees, for example the familiar identity

$$(2t)^2 + (t^2 - 1)^2 = (t^2 + 1)^2;$$

or the rather less interesting

$$t^n + 1 = (t^n + 1).$$

Exercise 6.7.1. Let a, b, and c be given non-zero integers, and suppose $n, p, q, r > 1$.

(a) Prove that there are no genuine polynomial solutions $x(t), y(t), z(t)$ to $ax^n + by^n = cz^n$ with $n \geq 3$.

(b) Prove that if there is a genuine polynomial solution $x(t), y(t), z(t)$ to $ax^p + by^q = cz^r$ in which x, y, and z have no common root, then $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$.

(c) Deduce in (b) that this implies that at least one of p, q, and r must equal 2.

(d) One can find solutions in (b) if one allows common factors, for example $x^3 + y^3 = z^4$ where $x = t(t^3 + 1)$ and $y = z = t^3 + 1$. Generalize this construction to as many other sets of exponents p, q, r as you can. (Try to go beyond the construction in exercise 6.5.8.)

Exercise 6.7.2. Let a and b be given non-zero integers, $p, q > 1$, and $x(t), y(t) \in \mathbb{C}[t]$. Let D be the maximum of the degrees of x^p and y^q, and assume that $ax^p + by^q \neq 0$.

(a) Prove that the degree of $ax^p + by^q$ is $> D(1 - \frac{1}{p} - \frac{1}{q})$.

(b)† Prove that if $g = (p, q) > 1$, then the degree of $ax^p + by^q$ is $\geq D/g$.

(c) Deduce that the degree of $ax^p + by^q$ is always $> D/6$.
(This is "best possible" in the case $(t^2 + 2)^3 - (t^3 + 3t)^2 = 3t^2 + 8$.)

Appendices. The extended version of chapter 6 has the following additional appendices:

Appendix 6B. *No Pythagorean triangle of square area via Euclidean geometry* presents another proof (due to a student, Stephanie Chan, in 2017) of this theorem of Fermat, now via clever geometric manipulations.

Appendix 6C. *Can a binomial coefficient be a square?* addresses and resolves the question of whether a binomial coefficient can be a square.

Power residues

We begin by calculating the least residues of the small powers of each given residue mod m, to look for interesting patterns:

a^0	a	a^2
1	0	0
1	1	1

Least power residues (mod 2).

a^0	a	a^2	a^3	a^4	a^5
1	0	0	0	0	0
1	1	1	1	1	1
1	2	1	2	1	2

Least power residues (mod 3).[1]

In these small examples, the columns soon settle into repeating patterns as we go from left to right: For example, in the mod 3 case, the columns alternate between $0, 1, 1$ and $0, 1, 2$. How about for slightly larger moduli?

a^0	a	a^2	a^3	a^4	a^5
1	0	0	0	0	0
1	1	1	1	1	1
1	2	0	0	0	0
1	3	1	3	1	3

Least power residues (mod 4).

a^0	a	a^2	a^3	a^4	a^5
1	0	0	0	0	0
1	1	1	1	1	1
1	2	4	3	1	2
1	3	4	2	1	3
1	4	1	4	1	4

Least power residues (mod 5).

[1] Why did we take 0^0 to be 1 (mod m) for $m = 2$, 3, 4, and 5? In mathematics we create symbols and protocols (like taking powers) to represent numbers and actions on those numbers, and then we need to be able to interpret all combinations of those symbols and protocols. Occasionally some of those combinations do not have an immediate interpretation, for example 0^0. So how do we deal with this? Usually mathematicians develop a convenient interpretation that allows that not-well-defined use of a protocol to nonetheless be consistent with the many appropriate uses of the protocol. Therefore, for example, we let 0^0 be 1, because it is true that $a^0 = 1$ for *every* non-zero number a, so it makes sense (and is often convenient) to define this to also be so for $a = 0$.

Perhaps the best known dilemma of this sort comes in asking whether ∞ is a number. The correct answer is "No, it is a symbol" (representing an upper bound on the set of real numbers) but it is certainly convenient to treat it as a number in many situations.

Again the patterns repeat, every second power mod 4, and every fourth power mod 5. Our goal in this chapter is to understand the power residues, and in particular when we get these repeated patterns.

7.1. Generating the multiplicative group of residues

We begin by verifying that for each coprime pair of integers a and m, the power residues do repeat periodically:

Lemma 7.1.1. *For any integer a, with $(a,m) = 1$, there exists an integer k, $1 \le k \le \phi(m)$, for which $a^k \equiv 1 \pmod m$.*

Proof. Each term of the sequence $1, a, a^2, a^3, \dots$ is coprime with m by exercise 3.3.5. But then each is congruent to some element from any given reduced set of residues mod m (which has size $\phi(m)$). Therefore, by the pigeonhole principle, there exist i and j with $0 \le i < j \le \phi(m)$ for which $a^i \equiv a^j \pmod m$.

Next we divide both sides of this equation by a^i. To justify doing this we observe that $(a^i, m) = 1$ (as $(a,m) = 1$) and so we can use Corollary 3.5.1 to obtain our result with $k = j - i$, so that $1 \le k \le \phi(m)$. □

Exercise 7.1.1. (a) Show that for *any integers* a and $m \ge 2$, there exist integers i and k, with $0 \le i \le m-1$ and $1 \le k \le m - i$ such that $a^{n+k} \equiv a^n \pmod m$ for every $n \ge i$.
(b) For each integer $m \ge 2$ determine an integer a such that $a \not\equiv 1 \pmod m$ but $a^2 \equiv a \pmod m$. (This explains why we need the hypothesis that $(a,m) = 1$ in Lemma 7.1.1.)

Another proof of Corollary 3.5.2. [*If $(a,m) = 1$, then a has an inverse* mod m.] Let $r = a^{k-1}$ so that $ar = a^k \equiv 1 \pmod m$. □

Examples. In the geometric progression $2, 4, 8, \dots$, the first term $\equiv 1 \pmod{13}$ is $2^{12} = 4096$. The first term $\equiv 1 \pmod{23}$ is $2^{11} = 2048$. Similarly $5^6 = 15625 \equiv 1 \pmod 7$ but $5^5 \equiv 1 \pmod{11}$. We see that in some cases the power needed is as big as $\phi(p) = p - 1$, the bound given by Lemma 7.1.1, but not always.

If $a^k \equiv 1 \pmod m$, then $a^{k+j} \equiv a^j \pmod m$ for all $j \ge 0$, and so the geometric progression $a^0, a^1, a^2, \dots$ modulo m has period k. Thus if $u \equiv v \pmod k$, then $a^u \equiv a^v \pmod m$. Therefore one can easily determine the residues of powers $\pmod m$. For example, to compute $3^{1000} \pmod{13}$, first note that $3^3 \equiv 1 \pmod{13}$. Now $1000 \equiv 1 \pmod 3$, and so $3^{1000} \equiv 3^1 = 3 \pmod{13}$.

If $(a,m) = 1$, then let $\mathrm{ord}_m(a)$, the *order* of $a \pmod m$, denote the smallest positive integer k for which $a^k \equiv 1 \pmod m$. We know that there must be such an integer, by Lemma 7.1.1. We have $\mathrm{ord}_3(2) = \mathrm{ord}_4(3) = 2$, $\mathrm{ord}_5(2) = \mathrm{ord}_5(3) = 4$ (from the tables above), and $\mathrm{ord}_{13}(2) = 12$, $\mathrm{ord}_{23}(2) = 11$, $\mathrm{ord}_7(5) = 6$, and $\mathrm{ord}_{11}(5) = 5$ from the examples above. The powers of 3 $\pmod{16}$ are $1, 3, 9, 3^3 \equiv 11, 3^4 \equiv 1, 3, 9, 11, 1, 3, 9, 11, 1, \dots$ so that the residues are periodic with period $\mathrm{ord}_{16}(3) = 4$.

Lemma 7.1.2. *Suppose that a and m are coprime integers with $m \ge 1$. Then n is an integer for which $a^n \equiv 1 \pmod m$ if and only if $\mathrm{ord}_m(a)$ divides n.*

Proof. Let $k := \mathrm{ord}_m(a)$ so that $a^k \equiv 1 \pmod m$. Suppose that n is an integer for which $a^n \equiv 1 \pmod m$. There exist integers q and r such that $n = qk + r$ where $0 \le r \le k-1$. Hence $a^r = a^n/(a^k)^q \equiv 1/1^q \equiv 1 \pmod m$. Therefore $r = 0$ by the minimality of k (from the definition of order), and so k divides n as claimed.

In the other direction, if k divides n, then $a^n = (a^k)^{n/k} \equiv 1 \pmod m$. □

Exercise 7.1.2. Let $k := \mathrm{ord}_m(a)$ where $(a, m) = 1$.
(a) Show that $1, a, a^2, \dots, a^{k-1}$ are distinct (mod m).
(b) Deduce that $a^j \equiv a^i \pmod m$ if and only if $j \equiv i \pmod k$.

We see that $\mathrm{ord}_m(a)$ is the smallest period of the sequence $1, a, a^2, \dots \pmod m$.

We wish to understand the possible values of $\mathrm{ord}_m(a)$, especially for fixed m, as a varies over integers coprime to m. We begin by taking $m = p$ prime. The theory for composite m can be deduced from an understanding of the prime power modulus case, using the Chinese Remainder Theorem as determined in detail in section 7.18 of appendix 7B.

Theorem 7.1. *If p is a prime and p does not divide a, then $\mathrm{ord}_p(a)$ divides $p-1$.*

Proof. Let $k := \mathrm{ord}_p(a)$ and $A = \{1, a, a^2, \dots, a^{k-1} \pmod p\}$. For any non-zero $b \pmod p$ define the set $bA = \{b\alpha \pmod p : \alpha \in A\}$.

Let b and b' be any two reduced residues mod p. We now show that either bA and $b'A$ are disjoint or they are equal: If they have an element, c, in common, then there exists $0 \le i, j \le k-1$ such that $ba^i \equiv c \equiv b'a^j \pmod p$. Therefore $b' \equiv ba^h \pmod p$ where h is the least non-negative residue of $i - j \pmod k$. Hence

$$b'a^\ell \equiv \begin{cases} ba^{h+\ell} \pmod p & \text{if } 0 \le \ell \le k-1-h, \\ ba^{h+\ell-k} \pmod p & \text{if } k-h \le \ell \le k-1, \end{cases}$$

which implies that $b'A \subset bA$. Since the two sets are finite and of the same size they must be identical.

Since any two sets of the form bA are either identical or disjoint, we deduce that they partition the non-zero elements mod p. That is, the reduced residues $1, \dots, p-1 \pmod p$ may be partitioned into disjoint *cosets* bA, of A, each of which has size $|A|$; and therefore $|A| = k$ divides $p-1$. □

To highlight this proof let $a = 5$ and $p = 13$ so that $A = \{1,\ 5,\ 5^2 \equiv 12,\ 5^3 \equiv 8 \pmod{13}\}$. Then the *cosets* $A,\ 2A \equiv \{2,\ 10,\ 11,\ 3 \pmod{13}\}$, and $4A \equiv \{4,\ 7,\ 9,\ 6 \pmod{13}\}$ partition the reduced residues mod 13, and therefore $3|A| = 12$. Also note that $7A \equiv \{7,\ 9,\ 6,\ 4 \pmod{13}\} = 4A$, as claimed, the same residues but in a rotated order.

7.2. Fermat's Little Theorem

Theorem 7.1 limits the possible values of $\mathrm{ord}_p(a)$. The beauty of the proof of Theorem 7.1, which is taken from Gauss's *Disquisitiones Arithmeticae*, is that it works in any finite group, as we will see in Proposition 7.22.1 of appendix 7D.[2] This

[2]What is especially remarkable is that Gauss produced this surprising proof before anyone had thought up the abstract notion of a group!

result leads us directly to one of the great results of elementary number theory, first observed by Fermat in a letter to Frénicle on October 18, 1640:

Theorem 7.2 (Fermat's "Little" Theorem)**.** *If p is a prime and a is an integer that is not divisible by p, then*

$$p \text{ divides } a^{p-1} - 1.$$

Proof. We know that $\mathrm{ord}_p(a)$ divides $p-1$ by Theorem 7.1, and therefore $a^{p-1} \equiv 1 \pmod{p}$ by Lemma 7.1.2. □

Here is a useful reformulation of Fermat's "Little" Theorem:

Fermat's Little Theorem, v2. *If p is a prime and a is a positive integer, then*

$$p \text{ divides } a^p - a.$$

Exercise 7.2.1. Prove that our two versions of Fermat's Little Theorem are *equivalent* to each other (that is, easily imply one another).

We now present several different proofs of Fermat's "Little" Theorem and then a surprising proof in appendix 7A.

"Sets of reduced residues" proof. In exercise 3.5.2 we proved that $\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$ form a reduced set of residues mod p. The residues of these integers mod p are therefore the same as the residues of $\{1, 2, \ldots, p-1\}$ although in a different order. Since the two sets are the same mod p, the products of the elements of each set are equal mod p, and so

$$(a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p};$$

that is,

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

As $(p, (p-1)!) = 1$, we can divide the $(p-1)!$ out from both sides to obtain the desired

$$a^{p-1} \equiv 1 \pmod{p}.$$ □

Euler's 1741 proof. We shall show that $a^p - a$ is divisible by p for every integer $a \geq 1$. We proceed by induction on a: For $a = 1$ we have $1^{p-1} - 1 = 0$, and so the result is trivial. Otherwise, by the binomial theorem,

$$(a+1)^p - a^p - 1 = \sum_{i=1}^{p-1} \binom{p}{i} a^i \equiv 0 \pmod{p},$$

as p divides the numerator but not the denominator of $\binom{p}{i}$ for each $i, 1 \leq i \leq p-1$ (as in exercise 2.5.8). Reorganizing we obtain

$$(a+1)^p - (a+1) \equiv (a^p + 1) - (a+1) \equiv a^p - a \equiv 0 \pmod{p},$$

the last congruence following from the induction hypothesis. □

Combinatorial proof. The numerator, but not the denominator, of the multinomial coefficient $\binom{p}{i,j,k,\dots}$ is divisible by p unless one of $i, j, k, \dots$ equals p and the others equal 0. In this case the multinomial coefficient equals 1. Therefore, by the multinomial theorem,[3]

$$(a+b+c+\cdots)^p \equiv a^p + b^p + c^p + \cdots \pmod{p}.$$

Taking $a = b = c = \cdots = 1$ gives $\ell^p \equiv \ell \pmod{p}$ for all integers $\ell \geq 1$. □

Another proof of Theorem 7.1. Theorem 7.1 follows from Fermat's Little Theorem and Lemma 7.1.2 with $m = p$ and $n = p-1$. (This is not a circular argument as our last three proofs of Fermat's Little Theorem do not use Theorem 7.1.) □

We can use Fermat's Little Theorem to help quickly determine large powers in modular arithmetic. For example for $2^{1000001} \pmod{31}$, we have $2^{30} \equiv 1 \pmod{31}$ by Fermat's Little Theorem, and so, as $1000001 \equiv 11 \pmod{30}$, we obtain $2^{1000001} \equiv 2^{11} \pmod{31}$ and it remains to do the final calculation. However, using the order makes this calculation significantly easier: Since $\mathrm{ord}_{31}(2) = 5$ we have $2^5 \equiv 1 \pmod{31}$ and therefore, as $1000001 \equiv 1 \pmod{5}$, we obtain $2^{1000001} \equiv 2^1 \equiv 2 \pmod{31}$.

It is worth stating the converse to Fermat's Little Theorem:

Corollary 7.2.1. *If $(a, n) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite.*

For example $(2, 15) = 1$ and $2^4 = 16 \equiv 1 \pmod{15}$ so that $2^{14} \equiv 2^2 \equiv 4 \pmod{15}$. Hence 15 is a composite number. The surprise here is that we have proved that 15 is composite without having to factor 15. Indeed whenever Corollary 7.2.1 is applicable we will not have to factor n to show that it is composite. This is important because we do not know a fast way to factor an arbitrarily large integer n, but one can compute rapidly with Corollary 7.2.1 (as discussed in section 7.13 of appendix 7A). We will discuss such compositeness tests in section 7.6.

Exercise 7.2.2. Prove that for any $m > 1$ if $(a, m) = 1$, then $\mathrm{ord}_m(a)$ divides $\phi(m)$ (by an analogous proof to that of Theorem 7.1).

Theorem 7.3 (Euler's Theorem)**.** *For any $m > 1$ if $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Proof. By definition $a^{\mathrm{ord}_m(a)} \equiv 1 \pmod{m}$. By exercise 7.2.2 there exists an integer k for which $\phi(m) = k\ \mathrm{ord}_m(a)$ and so $a^{\phi(m)} = (a^{\mathrm{ord}_m(a)})^k \equiv 1 \pmod{m}$. □

This result and proof generalizes even further, to any finite group, as we will see in Corollary 7.23.1 of appendix 7D.

Exercise 7.2.3. Prove Euler's Theorem using the idea in the "sets of reduced residues" proof of Fermat's Little Theorem, given above.

Exercise 7.2.4. Determine the last decimal digit of 3^{8643}.

[3] For the reader who has seen it before.

7.3. Special primes and orders

We now look at prime divisors of the Mersenne and Fermat numbers using our results on orders.

Exercise 7.3.1. Show that if p is prime and q is a prime dividing $2^p - 1$, then $\mathrm{ord}_q(2) = p$.

Hence, by exercise 7.3.1, if q divides $2^p - 1$, then $p = \mathrm{ord}_2(q)$ divides $q - 1$ by Theorem 7.1; that is, $q \equiv 1 \pmod{p}$.

Another proof that there are infinitely many primes. If p is the largest prime, let q be a prime factor of $2^p - 1$. We have just seen that p divides $q - 1$, so that $p \leq q - 1 < q$. This contradicts the assumption that p is the largest prime. □

Exercise 7.3.2.† Show that if prime p divides $F_n = 2^{2^n} + 1$, then $\mathrm{ord}_p(2) = 2^{n+1}$. Deduce that $p \equiv 1 \pmod{2^{n+1}}$.

Theorem 7.4. *Fix $k \geq 2$. There are infinitely many primes $\equiv 1 \pmod{2^k}$.*

Proof. If p_n is a prime factor of $F_n = 2^{2^n} + 1$, then $p_n \equiv 1 \pmod{2^k}$ for all $n \geq k - 1$, by exercise 7.3.2. We saw that the p_n are all distinct in section 5.1. □

7.4. Further observations

Lemma 5.7.1, a weak form of the Fundamental Theorem of Algebra (Theorem 3.11), states that any polynomial in $\mathbb{C}[x]$ of degree d has at most d roots. An analogous result can be proved for polynomials mod p.

Proposition 7.4.1 (Lagrange)**.** *Suppose that p is a prime and that $f(x)$ is a non-zero polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$ of degree d. Then $f(x)$ has no more than d roots* mod p *(counted with multiplicity).*

Proof. By induction on $d \geq 0$. This is trivial for $d = 0$. For $d \geq 1$ we will suppose that $f(a) \equiv 0 \mod p$. Then write $f(x) = \sum_{i=0}^{d} f_i x^i$ and define

$$g(x) = \frac{f(x) - f(a)}{x - a} = \sum_{i=0}^{d} f_i \frac{x^i - a^i}{x - a} = \sum_{i=0}^{d} f_i (x^{i-1} + ax^{i-2} + \cdots + a^{i-1}),$$

a polynomial of degree $d - 1$ with leading coefficient f_d (so is non-zero). Therefore $g(x)$ has no more than $d - 1$ roots mod p, by the induction hypothesis. Now

$$f(x) = f(x) - f(a) = (x - a)g(x)$$

and so if $f(b) \equiv 0 \pmod{p}$, then $(b - a)g(b) \equiv 0 \pmod{p}$. Either $b \equiv a \pmod{p}$ or $g(b) \equiv 0 \pmod{p}$, and so f has no more than $1 + (d - 1) = d$ roots mod p. □

Fermat's Little Theorem implies that $1, 2, 3, \ldots, p-1$ are $p-1$ distinct roots of $x^{p-1} - 1 \pmod{p}$, and are therefore all the roots, by Proposition 7.4.1. Therefore the polynomials $x^{p-1} - 1$ and $(x - 1)(x - 2) \cdots (x - (p - 1))$ mod p are the same up to a multiplicative constant. Since they are both monic they must be identical; that is,

$$x^{p-1} - 1 \equiv (x - 1)(x - 2) \cdots (x - (p - 1)) \pmod{p}, \tag{7.4.1}$$

which implies that

$$x^p - x \equiv x(x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

Theorem 7.5 (Wilson's Theorem)**.** *For any prime p we have*

$$\boxed{(p-1)! \equiv -1 \pmod{p}.}$$

Proof. Take $x = 0$ in (7.4.1), and note that $(-1)^{p-1} \equiv 1 \pmod{p}$. □

Gauss's proof of Wilson's Theorem. Let S be the set of pairs (a, b) for which $1 \le a < b < p$ and $ab \equiv 1 \pmod{p}$; that is, every residue is paired up with its inverse unless it equals its inverse. Now if $a \equiv a^{-1} \pmod{p}$, then $a^2 \equiv 1 \pmod{p}$, in which case $a \equiv 1$ or $p-1 \pmod{p}$ by Lemma 3.8.1. Therefore

$$1 \cdot 2 \cdots (p-1) = 1 \cdot (p-1) \cdot \prod_{(a,b)\in S} ab \equiv 1 \cdot (-1) \cdot \prod_{(a,b)\in S} 1 \equiv -1 \pmod{p}. \quad \square$$

Example. For $p = 13$ we have

$$12! = 12(2\times 7)(3\times 9)(4\times 10)(5\times 8)(6\times 11) \equiv -1\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1 \equiv -1 \pmod{13}.$$

Exercise 7.4.1. (a) Show that if $n > 4$ is composite, then n divides $(n-1)!$.
(b) Show that $n \ge 2$ is prime if and only if n divides $(n-1)! + 1$.

Combining Wilson's Theorem with the last exercise we have an indirect primality test for integers $n > 2$: Compute $(n-1)! \pmod{n}$. If it is $\equiv -1 \pmod{n}$, then n is prime; if it is $\equiv 0 \pmod{n}$, then n is composite. Note however that in determining $(n-1)!$ we need to do $n-2$ multiplications, so that this primality test takes far more steps than trial division (see section 5.2)!

Exercise 7.4.2. (a) Use the idea in Gauss's proof of Wilson's Theorem to show that

$$\prod_{\substack{1\le a\le n\\(a,n)=1}} a \equiv \prod_{\substack{1\le b\le n\\ b^2\equiv 1 \pmod{n}}} b \pmod{n}.$$

(b) Evaluate this product using exercise 3.8.3 or by pairing b with $n-b$.

Exercise 7.4.3. (a) Show that $\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}$.
(b) Deduce that if $p \equiv 3 \pmod{4}$, then $\left(\frac{p-1}{2}\right)! \equiv 1$ or $-1 \pmod{p}$.
(c) Deduce that if $p \equiv 1 \pmod{4}$, then $\left(\frac{p-1}{2}\right)!$ is a root of $x^2 \equiv -1 \pmod{p}$.[4]

7.5. The number of elements of a given order, and primitive roots

In Theorem 7.1 we saw that the order modulo p of any integer a which is coprime to p must be an integer which divides $p-1$. In this section we show that for each divisor m of $p-1$, there are residue classes mod p of order m.

[4] This explicitly provides a square root of $-1 \pmod{p}$ which is interesting, as there is no easy way in general to determine square roots mod p. However we do not know how to rapidly calculate the least residue of $\left(\frac{p-1}{2}\right)! \pmod{p}$.

Example. For the primes $p = 13$ and $p = 19$ we have

Order	$a \pmod{13}$
1	1
2	12
3	3, 9
4	5, 8
6	4, 10
12	2, 6, 7, 11

Order	$a \pmod{19}$
1	1
2	18
3	7, 11
6	8, 12
9	4, 5, 6, 9, 16, 17
18	2, 3, 10, 13, 14, 15

How many residues are there of each order? From these examples we might guess the following result.

Theorem 7.6. *If m divides $p-1$, then there are exactly $\phi(m)$ elements $a \pmod p$ of order m.*

A *primitive root* $a \bmod p$ is a reduced residue mod p of order $p-1$. The least residues of the powers

$$1, a, a^2,\ a^3,\ \ldots,\ a^{p-2} \pmod p$$

are distinct reduced residues by exercise 7.1.2 and so must equal

$$1, 2, \ldots, p-1$$

in some order. Therefore every reduced residue is congruent to some power $a^j \pmod p$ of a, and the power j can be reduced mod $p-1$. For example, 2, 3, 10, 13, 14, and 15 are the primitive roots mod 19. We can verify that the powers of 3 mod 19 yield a reduced set of residues:

$$1, 3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, 3^{13}, 3^{14}, 3^{15}, 3^{16}, 3^{17}, 3^{18}, \ldots$$
$$\equiv 1, 3,\ 9,\ 8,\ 5, -4,\ 7,\ 2,\ 6, -1, -3, -9, -8, -5,\ \ 4, -7, -2,\ -6,\ 1, \ldots \pmod{19},$$

respectively, so 3 is a primitive root mod p. Taking $m = p-1$ in Theorem 7.6 we obtain the following:

Corollary 7.5.1. *For every prime p there exists a primitive root* mod p. *In fact there are $\phi(p-1)$ distinct primitive roots* mod p.

To prove Theorem 7.6 it helps to first establish the following lemma:

Lemma 7.5.1. *If m divides $p-1$, then there are exactly m elements $a \pmod p$ for which $a^m \equiv 1 \pmod p$.*

Proof. We saw in (7.4.1) that

$$x^{p-1} - 1 = (x^m - 1)(x^{p-1-m} + x^{p-1-2m} + \cdots + x^m + 1)$$

factors into distinct linear factors mod p, and therefore $x^m - 1$ does so also. □

The residue $a \pmod p$ is counted in Lemma 7.5.1 if and only if the order of a divides m. Now we prove Theorem 7.6 which counts the number of residue classes $a \pmod p$ whose order is exactly m.

Proof of Theorem 7.6. Let $\psi(d)$ denote the number of elements $a \pmod p$ of order d. The set of roots of $x^m - 1 \pmod p$ is precisely the union of the sets of residue classes mod p of order d, over each d dividing m, so that

$$\sum_{d|m} \psi(d) = m \tag{7.5.1}$$

for all positive integers m dividing $p-1$, by Lemma 7.5.1. We now prove that $\psi(m) = \phi(m)$ for all m dividing $p-1$, by induction on m. The only element of order 1 is $1 \pmod p$, so that $\psi(1) = 1 = \phi(1)$. For $m > 1$ we have $\psi(d) = \phi(d)$ for all $d < m$ that divide m, by the induction hypothesis. Therefore

$$\psi(m) = m - \sum_{\substack{d|m \\ d<m}} \psi(d) = m - \sum_{\substack{d|m \\ d<m}} \phi(d) = \phi(m),$$

the last equality following from Proposition 4.1.1. The result follows. □

Although there are many primitive roots mod p ($\phi(p-1)$ of them by Theorem 7.6), it is not obvious how to always find one rapidly. In section 7.15 of appendix 7B we will present Gauss's practical algorithm for finding primitive roots (as well as special cases in exercises 8.9.20, 8.9.21, and 8.9.22).

It is believed that 2 is a primitive root mod p for infinitely many primes p though this remains an open question. Artin's *primitive root conjecture* states that every prime q is a primitive root mod p for infinitely many primes p. This is known to be true for all, but at most two, primes.[5] Gauss himself conjectured that 10 is a primitive root mod p for infinitely many primes p and this is also an open question. Any integer m, which is neither a perfect square nor -1, is conjectured to be a primitive root mod p for infinitely many primes p.

Corollary 7.5.2. *For every prime p and every integer k, we have*

$$1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} 0 & \text{if } p-1 \nmid k \\ -1 & \text{if } p-1 | k \end{cases} \pmod p.$$

Proof. Let $S_k := 1^k + 2^k + \cdots + (p-1)^k$. If $p-1$ divides k, then each $j^k \equiv 1 \pmod p$ by Fermat's Little Theorem and so $S_k \equiv 1 + \cdots + 1 = p-1 \pmod p$, as claimed. So, henceforth assume that $p-1$ does not divide k.

Let a be a primitive root mod p, so that $a^k \not\equiv 1 \pmod p$ since $p-1$ does not divide k. The integers $\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$ form a reduced set of residues mod p and so are a rearrangement of the residues of $\{1, 2, \ldots, p-1\}$ mod p. Therefore any symmetric function of these two sets of integers residues are congruent mod p (as we saw in the "Sets of reduced residues" proof of Fermat's Little Theorem); in particular,

$$S_k \equiv \sum_{j=1}^{p-1} (aj)^k = a^k S_k \pmod p.$$

Therefore $(a^k - 1)S_k \equiv 0 \pmod p$ but $a^k \not\equiv 1 \pmod p$ and so $S_k \equiv 0 \pmod p$. □

[5] This result is strangely formulated because of the nature of what was proved (by Heath-Brown [**2**], improving a result of Gupta and Murty, see [**3**])—that in any set of three distinct primes q_1, q_2, q_3, at least one is a primitive root mod p for infinitely many primes p. Therefore there cannot be three exceptions to the conjecture, and we believe that there are none.

Near the beginning of this section we noted that if a is a primitive root (mod p), then every reduced residue is congruent to some power $a^j \pmod p$. This property is extremely useful for it allows us to treat multiplication as addition of exponents in the same way that the introduction of logarithms simplifies usual multiplication. We will discuss this further in section 7.16 of appendix 7B.

Exercise 7.5.1. Write each reduced residue mod p as a power of the primitive root a, and use this to evaluate $1^k + 2^k + \cdots + (p-1)^k \pmod p$ as a function of a and k. Use this to give another proof of Corollary 7.5.2.

Exercise 7.5.2. Let g be a primitive root modulo odd prime p.
(a) Prove that $g^a \equiv 1 \pmod p$ if and only if $p-1$ divides a.
(b) Show that $g^{(p-1)/2} \equiv -1 \pmod p$.

In order to determine the order of an element mod n, one can use the following result:

Proposition 7.5.1. *Suppose that a and n are coprime integers. Then d is the order of $a \pmod n$ if and only if $a^d \equiv 1 \pmod n$ and $a^{d/q} \not\equiv 1 \pmod n$ for every prime q dividing d.*

Proof. If d is the order of $a \pmod n$, then $a^d \equiv 1 \pmod n$ and $a^{d/q} \not\equiv 1 \pmod n$ by the definition of order, since $d/q < d$.

On the other hand let $m := \mathrm{ord}_n(a)$. By Lemma 7.1.2 we know that m divides d but does not divide d/q for any prime q dividing d. Therefore q does not divide d/m for any prime q dividing d, so there cannot be any primes q that divide d/m. This implies that $d/m = 1$ and so $\mathrm{ord}_n(a) = m = d$. □

We deduce an important practical way to recognize primitive roots mod p:

Corollary 7.5.3. *Suppose that p is a prime that does not divide integer a. Then a is a primitive root $\pmod p$ if and only if*

$$a^{(p-1)/q} \not\equiv 1 \pmod p$$

for all primes q dividing $p-1$.

Proof. By definition a is a primitive root (mod p) if and only if $m := \mathrm{ord}_p(a) = p-1$. The result follows from Proposition 7.5.1. □

Exercise 7.5.3. Find all residues of order 5 mod 31, given that $2^5 \equiv 1 \pmod{31}$.

Exercise 7.5.4. (a) Prove that 2 is a primitive root (mod 13).
(b) *Use this* to determine all of the other primitive roots (mod 13).

Exercise 7.5.5. Let g be a primitive root modulo odd prime p.
(a) Prove that if m divides $p-1$, then g^m has order $\frac{p-1}{m}$.
(b)† Prove that $g^k \pmod p$ is a primitive root mod p if and only if $(k, p-1) = 1$.
(c) Deduce that there are $\phi(p-1)$ primitive roots mod p.

7.6. Testing for composites, pseudoprimes, and Carmichael numbers

In the converse to Fermat's Little Theorem, Corollary 7.2.1, we saw that if an integer n *does not divide* $a^{n-1}-1$ for some integer a coprime to n, then n is composite. For example, taking $a=2$ we calculate that

$$2^{1000} \equiv 562 \pmod{1001},$$

so we know that 1001 is composite. We might ask whether this always works. In other words:

Is it true that *if n is composite, then n does not divide 2^n-2*?

For, if so, we have a very nice way to distinguish primes from composites. Unfortunately the answer is "no" since, for example,

$$2^{340} \equiv 1 \pmod{341},$$

but $341 = 11 \times 31$. We call 341 a *base-2 pseudoprime*. Note though that

$$3^{340} \equiv 56 \pmod{341},$$

and so the converse to Fermat's Little Theorem, with $a=3$, implies that 341 is composite.

Are there composites n for which $2^{n-1} \equiv 3^{n-1} \equiv 1 \pmod{n}$? Or $2^{n-1} \equiv 3^{n-1} \equiv 5^{n-1} \equiv 1 \pmod{n}$? Or, even *Carmichael numbers*, composite numbers that "masquerade" as primes in that $a^{n-1} \equiv 1 \pmod{n}$ for all integers a coprime to n? A quick computer search finds the smallest example: $561 = 3 \cdot 11 \cdot 17$. The next few Carmichael numbers are $1105 = 5 \cdot 13 \cdot 17$, then $1729 = 7 \cdot 13 \cdot 19$, etc.

Exercise 7.6.1. Show that squarefree n is a Carmichael number if and only if n is composite and divides $a^n - a$ for all integers a.

Carmichael numbers are a nuisance, masquerading as primes like this (and so preventing a quick and easy, surefire primality test). Calculations reveal that Carmichael numbers are rare, but in 1994 Alford, Pomerance, and I [**1**] proved that there are infinitely many of them. Here is a more elegant way to recognize Carmichael numbers:

Lemma 7.6.1. *A positive integer n is a Carmichael number if and only if n is squarefree and composite and $p-1$ divides $n-1$ for every prime p dividing n.*

Proof. Suppose that n is squarefree and composite and $p-1$ divides $n-1$ for every prime p dividing n. If $(a,n)=1$ and prime p divides n, then $\mathrm{ord}_p(a)$ divides $p-1$ by Theorem 7.1, which divides $n-1$, and so $a^{n-1} \equiv 1 \pmod{p}$ by Lemma 7.1.2. Therefore $a^{n-1} \equiv 1 \pmod{n}$ by the Chinese Remainder Theorem as n is squarefree, and so it is a Carmichael number.

Now suppose that n is a Carmichael number. If prime p divides n, then $a^{n-1} \equiv 1 \pmod{p}$ for all integers a coprime to n. In particular, if a is a primitive root mod p, then $p-1 = \mathrm{ord}_p(a)$ divides $n-1$ by Lemma 7.1.2.

Now assume that $p^e \| n$ with $e \geq 2$. We note that $(1+p)^k \equiv 1 + kp \pmod{p^2}$ for all integers $k \geq 1$, by the binomial theorem, so that $\mathrm{ord}_{p^2}(1+p) = p$. Select $a \equiv 1+p \pmod{p^e}$ with $a \equiv 1 \pmod{n/p^e}$ so that $(a,n)=1$. As $p|n$ we have

$1 \equiv (1+p)^n \equiv a^n \equiv a \equiv 1+p \pmod{p^2}$, a contradiction. Therefore n must be squarefree. □

Lemma 7.6.1 imples that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number as $2, 10$, and 16 divide 560.

Exercise 7.6.2. Show that if n is a Carmichael number, then it is odd.

Exercise 7.6.3.† Show that if n is a Carmichael number, then it has at least three prime factors.

Exercise 7.6.4. Prove that if $6m+1$, $12m+1$, and $18m+1$ are all primes, then their product is a Carmichael number. (It is an open problem whether there exist infinitely many such prime triples, though it is not difficult to find examples, like $7 \times 13 \times 19$ and $37 \times 73 \times 109$.)

7.7. *Divisibility tests, again*

In section 2.4 we found simple tests for the divisibility of integers by 7, 9, 11, and 13, promising to return to this theme later. The key to these earlier tests was that $10 \equiv 1 \pmod 9$ and $10^3 \equiv -1 \pmod{7 \cdot 11 \cdot 13}$; that is, $\mathrm{ord}_9(10) = 1$ and $\mathrm{ord}_7(10)$, $\mathrm{ord}_{11}(10)$, and $\mathrm{ord}_{13}(10)$ divide 6. For all primes $p \neq 2$ or 5 we know that $k := \mathrm{ord}_p(10)$ is an integer dividing $p-1$. Hence if $n = \sum_{j=0}^{d} n_j 10^j$, then

$$n \;=\; \sum_{m\geq 0} \left(\sum_{i=0}^{k-1} n_{km+i} 10^i \right) (10^k)^m \;\equiv\; \sum_{m\geq 0} \left(\sum_{i=0}^{k-1} n_{km+i} 10^i \right) \pmod p,$$

since if $j = km+i$, then $10^j \equiv 10^i \pmod p$. In the displayed equation we have cut up the integer n, written in decimal, into blocks of digits of length k and added these blocks together, which is clearly an efficient way to test for divisibility. The length of these blocks, k, is always $\leq p-1$ no matter what the size of n. Therefore we can, in practice, quickly test whether n is divisible by p, once we know the p-divisibility of every integer $< 10^k$ ($\leq 10^{p-1}$).

If $k = 2\ell$ is even, we can do a little better (as we did with $p = 7$, 11, and 13) since $10^\ell \equiv -1 \pmod p$, namely that

$$n = \sum_{j=0}^{d} n_j 10^j \equiv \sum_{m\geq 0} \left(\sum_{i=0}^{\ell-1} n_{km+i} 10^i - \sum_{i=0}^{\ell-1} n_{km+\ell+i} 10^i \right) \pmod p,$$

thus breaking n up into blocks of length $\ell = k/2$.

7.8. *The decimal expansion of fractions*

The fraction $\frac{1}{3} = .3333\ldots$ is given by a recurring digit 3, so we write it as $.\overline{3}$. More interesting to us are the set of fractions

$$\frac{1}{7} = .\overline{142857}, \quad \frac{2}{7} = .\overline{285714}, \quad \frac{3}{7} = .\overline{428571},$$
$$\frac{4}{7} = .\overline{571428}, \quad \frac{5}{7} = .\overline{714285}, \quad \frac{6}{7} = .\overline{857142}.$$

These decimal expansions of the six fractions $\frac{a}{7}$, $1 \leq a \leq 6$, are each periodic of period length 6, and each contains the same six digits in the same order but starting at a different place. Starting with the period for $1/7$ we find that we go through the fractions $a/7$ with $a = 1, 3, 2, 6, 4, 5$ when we rotate the period one step at a time.

Do you recognize this sequence of numbers? These are the least positive residues of $10^0, 10^1, 10^2, 10^3, 10^4, 10^5 \pmod 7$. To prove this, we begin by noting that since $10^6 \equiv 1 \pmod 7$, we have that

$$\frac{10^6 - 1}{7} \;=\; 142857 \text{ is an integer,}$$

which is ≤ 6 digits long. Putting the $1/7$ on the other side and dividing through by 10^6, we obtain

$$\frac{1}{7} = \frac{142857}{10^6} + \frac{10^{-6}}{7} = .142857 + \frac{1}{10^6} \cdot \frac{1}{7}.$$

Substituting this expression in for the last term, divided by 10^6, we obtain

$$\frac{1}{7} = .142857 + \frac{.142857}{10^6} + \frac{1}{10^{12}} \cdot \frac{1}{7} = \cdots = .\overline{142857},$$

the final equality by repeating this process infinitely often. Now if we multiply this through by 10, we obtain

$$\frac{10}{7} = 1.\overline{428571}, \text{ so that } \frac{3}{7} = \frac{10}{7} - 1 = .\overline{428571},$$

and similarly, as $10^2 \equiv 2 \pmod 7$,

$$\frac{2}{7} = \frac{10^2}{7} - \left[\frac{10^2}{7}\right] = .\overline{28574}.$$

We obtain all the other decimal expansions analogously.

What happens when we multiply $1/7$ through by 10^k? For example, if $k = 4$, then

$$\frac{10^4}{7} \;=\; 1428.\overline{571428} \;=\; 1428 + \frac{4}{7}.$$

The part after the decimal point is always $\{\frac{10^k}{7}\}$ which equals $\frac{\ell}{7}$ where ℓ is the least positive residue of $10^k \pmod 7$ (as in exercise 1.7.4(b)). We can now give two results.

Proposition 7.8.1. *Suppose that m is an integer that is coprime to 10. If $1 \leq a < m$, then the decimal expansion of the period for a/m is periodic with period of length $\operatorname{ord}_m(10)$. This is the minimal period length if $(a, m) = 1$.*

Proof sketch. We proceed analogously to the above. Let $n = \operatorname{ord}_m(10)$ and $r = (10^n - 1)a/m$, so that r is a positive integer $< 10^n$. Let $\mathbf{r}$ be the sequence of digits that give the integer r. The same argument as above gives that

$$\frac{a}{m} = \frac{r}{10^n} + \frac{1}{10^n} \cdot \frac{a}{m} = \frac{r}{10^n} + \frac{r}{10^{2n}} + \frac{1}{10^{2n}} \cdot \frac{a}{m} = \cdots = \overline{\mathbf{r}}.$$

On the other hand, if this equation holds and the decimal expansion has period n, then $(10^n - 1)a/m = (10^n - 1).\overline{\mathbf{r}} = \mathbf{r}.\overline{\mathbf{r}} - .\overline{\mathbf{r}} = \mathbf{r}$. In other words, $(10^n - 1)a/m$ is the integer r, so that $10^n \equiv 1 \pmod m$ if $(a, m) = 1$. □

Exercise 7.8.1.† Suppose that p is an odd prime for which 10 is a primitive root. Let a_k be the least residue of $10^k \pmod p$, and suppose that $a_k/p = .\overline{r_k}$ where $1 \leq r_k < 10^{p-1}$. Prove that r_k is obtained from r_1, by removing the leading k digits and concatenating them on to the end.

Exercise 7.8.2. Prove that the decimal expansion of every rational number is eventually periodic. (One can see why we need "eventually" with the example $\frac{1}{30} = .03333\ldots$.)

7.9. Primes in arithmetic progressions, revisited

We can use the ideas in this chapter to prove that there are infinitely many primes in certain arithmetic progressions $1 \pmod m$.

Theorem 7.7. *There are infinitely many primes* $\equiv 1 \pmod 3$.

Proof. Suppose there are only finitely many primes $\equiv 1 \pmod 3$, say $p_1, p_2, \dots, p_k$. Let $a = 3p_1p_2\cdots p_k$, and let q be a prime dividing $a^2 + a + 1$. Now $q \neq 3$ as $a^2 + a + 1 \equiv 1 \pmod 3$. Moreover q divides $a^3 - 1 = (a-1)(a^2 + a + 1)$, but not $a - 1$ (or else $0 \equiv a^2 + a + 1 \equiv 1 + 1 + 1 \equiv 3 \pmod q$ but $q \neq 3$). Therefore $\operatorname{ord}_q(a) = 3$ and so $q \equiv 1 \pmod 3$ by Theorem 7.1. Hence $q = p_j$ for some j, so that q divides a as well as $a^2 + a + 1$, and thus q divides $(a^2 + a + 1) - a(a + 1) = 1$, which is impossible. □

This, together with Theorem 5.2, proves that there are infinitely many primes in both of the residue classes $1 \pmod 3$ and $2 \pmod 3$, as predicted from the data at the start of section 5.3.

Exercise 7.9.1. Generalize this argument to primes that are $1 \pmod 4$, to primes that are $1 \pmod 5$, and to primes that are $1 \pmod 6$.

In order to generalize this argument to proving the existence of primes $\equiv 1 \pmod m$ for every integer $m \geq 3$, including composite m, we need to replace the polynomial $a^2 + a + 1$ by one that recognizes when a has order m. Evidently this must be a divisor of the polynomial $a^m - 1$; indeed $a^m - 1$ divided through by all of the factors corresponding to orders which are proper divisors of m. This discussion leads us to define the *cyclotomic polynomials* $\phi_n(t) \in \mathbb{Z}[t]$, inductively, by the requirement

$$t^m - 1 = \prod_{d|m} \phi_d(t) \qquad \text{for all } m \geq 1, \tag{7.9.1}$$

with each $\phi_d(t)$ monic (see also appendix 4E). Therefore $\phi_1(t) = t - 1$,

$\phi_2(t) = t + 1,\ \phi_3(t) = t^2 + t + 1,\ \phi_4(t) = t^2 + 1,\ \phi_5(t) = t^4 + t^3 + t^2 + t + 1, \dots$.

Theorem 7.8. *For any integer* $m \geq 2$, *there are infinitely many primes* $\equiv 1 \pmod m$.

Proof. Suppose that $p_1, \dots, p_k$ are all the primes that are $\equiv 1 \pmod m$ and let $a = mp_1\cdots p_k$. Let q be a prime divisor of $\phi_m(a)$, which divides $a^m - 1$, so that $a^m \equiv 1 \pmod q$. This implies that (q, a) divides $(a^m - 1, a) = 1$ and so $(q, a) = 1$. In particular q is not a p_j and does not divide m.

Let $d = \operatorname{ord}_q(a)$ so that $q \equiv 1 \pmod d$ by Theorem 7.1. Moreover d divides m as $a^m \equiv 1 \pmod q$. But q is not a p_j and so $q \not\equiv 1 \pmod m$, which implies that $d \neq m$, and therefore $d < m$.

Now $\phi_m(x)$ divides $\frac{x^m-1}{x^d-1}$ by definition. Substituting in $x = a$ we deduce that q divides both $\frac{a^m-1}{a^d-1}$ and $a^d - 1$, so that

$$0 \equiv \frac{a^m - 1}{a^d - 1} = \sum_{j=0}^{m/d-1} (a^d)^j \equiv \sum_{j=0}^{m/d-1} 1 = m/d \pmod q.$$

This implies that q divides m/d, and therefore divides m, which contradicts what we proved above. □

References for this chapter

[1] W. Red Alford, Andrew Granville, and Carl Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), 703–722.

[2] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. **37** (1986), 27–38.

[3] M. Ram Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), 59–67.

Additional exercises

Exercise 7.10.1. Prove that we can write any polynomial $f(x)$ mod p of degree $\le p-1$ as

$$f(x) \equiv \sum_{a=0}^{p-1} f(a)(1-(x-a)^{p-1}) \pmod p.$$

Exercise 7.10.2.† Prove that if $f(x) \in \mathbb{Z}[x]$ is monic and has degree d and if prime p divides $f(0), f(1), \dots, f(d)$, then $p \le d$ and p divides $f(n)$ for all integers n.

Exercise 7.10.3. We will find all powers of 2 and 3 that differ by 1, a special case of Catalan's conjecture mentioned in section 6.4.

(a) What are the powers of 3 (mod 8)? What are the powers of 2 (mod 8)?
(b) Show that if $2^n - 3^m \equiv 1 \pmod 8$ for some positive integers m, n, then $n = 1$ or 2.
(c) Deduce that the only solutions to $2^n - 3^m = 1$ are $4 - 3 = 2 - 1 = 1$.
(d) Prove that if $3^m - 2^n = 1$ with m odd, then $m = n = 1$.
(e) Prove that if $3^{2k} - 2^n = 1$, then both $3^k - 1$ and $3^k + 1$ are powers of 2, and that this is only possible if $k = 1$. We deduce that the only solutions to $3^m - 2^n = 1$ are $3 - 2 = 9 - 8 = 1$.

(This is the proof of Levi ben Gershon from around 1320.)

Exercise 7.10.4.† Show that if $\binom{n}{3}$ with $n > 3$ has no more than one prime factor which is > 3, then $n = 3$, 4, 5, 6, 8, 9, 10, or 18. (Use exercise 7.10.3.)

Exercise 7.10.5. (a) Prove that if $a > 1$, then the order of a mod $N := a^q - 1$ is exactly q. Now let q be a prime.
(b) Deduce that if prime p divides $a^q - 1$ but not $a - 1$, then p is a prime $\equiv 1 \pmod q$.
(c) Prove that $(\frac{a^q-1}{a-1}, a-1) = (q, a-1)$.
(d)† Prove that there are infinitely many primes $\equiv 1 \pmod q$.

Exercise 7.10.6. Let p be an odd prime, and let x, y, and z be pairwise coprime, positive integers.

(a)† Prove that if p divides $z - y$, then $\frac{z^p - y^p}{z-y} \equiv p \pmod{p^2}$.
(b) Show that if $x^p + y^p = z^p$, then there exists an integer r for which $z - y = r^p$ or $z - y = p^{p-1}r^p$.

(This problem continues on from exercise 3.9.7.)

Exercise 7.10.7. Deduce Theorem 7.6 from (7.5.1) using the Möbius inversion formula (Theorem 4.4).

Exercise 7.10.8. Let p be a prime. Prove that every quadratic non-residue (mod p) is a primitive root if and only if p is a Fermat prime.

Exercise 7.10.9. Suppose that g is a primitive root modulo odd prime p. Prove that $-g$ is also a primitive root mod p if and only if $p \equiv 1 \pmod 4$.

Exercise 7.10.10. (a) Show that the number of primes up to N equals, exactly,

$$\sum_{2\le n\le N} \frac{n}{n-1}\cdot\left\{\frac{(n-1)!}{n}\right\} - \frac{2}{3}.$$

(Here $\{t\}$ is the fractional part of t, defined as in exercise 1.7.4(b).)

(b) Suppose that $n > 1$. Show that n and $n+2$ are both odd primes if and only if $n(n+2)$ divides $4((n-1)!+1)+n$.

Exercise 7.10.11. Prove that if $f(x) \in \mathbb{Z}[x]$ has degree $\le p-2$, then $\sum_{a=0}^{p-1} f(a) \equiv 0 \pmod p$.

Exercise 7.10.12.† Let p be an odd prime and k be an odd integer which is $\not\equiv 1 \pmod{p-1}$. Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p^2}$.

Exercise 7.10.13.† Let $a_{n+1} = 2a_n + 1$ for all $n \ge 0$. Can we choose a_0 so that this sequence consists entirely of primes?

We define n to be a *base-b pseudoprime* if n is composite and $b^{n-1} \equiv 1 \pmod n$.

Exercise 7.10.14. Show that if n is not prime, then it a base-b pseudoprime if and only if $\mathrm{ord}_{p^k}(b)$ divides $n-1$ for every prime power p^k dividing n.

Exercise 7.10.15. Suppose that n is a squarefree, composite integer.

(a) Show that $\#\{a \pmod p : a^{n-1} \equiv 1 \pmod p\} = (p-1, n-1)$.

(b) Show that there are $\prod_{p|n}(p-1, n-1)$ reduced residue classes $b \pmod n$ for which n is a base-b pseudoprime.

Exercise 7.10.16. (a) Prove that if n is composite, then $\{b \pmod n : n \text{ is a base-}b \text{ pseudoprime}\}$ is a subgroup of the reduced residues mod n.

(b)† Prove that if n is not a Carmichael number, then it is not a base-b pseudoprime for at least half of the reduced residues $b \pmod n$.

(c)† Suppose that p and $2p-1$ are both prime and let $n = p(2p-1)$. Prove that $\#\{b \pmod n : n \text{ is a base-}b \text{ pseudoprime}\} = \frac{1}{2}\phi(n)$.

Exercise 7.10.17. (a) Show that if p is prime, then the Mersenne number $2^p - 1$ is either a prime or a base-2 pseudoprime.

(b) Show that every Fermat number $2^{2^n}+1$ is either a prime or a base-2 pseudoprime.

(c) Show that p^2 divides $2^{p-1}-1$ if and only if p^2 is a base-2 pseudoprime.

None of these criteria guarantee that there are infinitely many base-2 pseudoprimes. However this is provable:

Exercise 7.10.18.† Prove that there are infinitely many base-2 pseudoprimes by proving and developing one of the following two observations:

- Start with 341, and show that if n is a base-2 pseudoprime, then so is $N := 2^n - 1$.
- Prove that if $p > 3$ is prime, then $(4^p-1)/3$ is a base-2 pseudoprime.

Can you generalize either of these proofs to other bases?

Exercise 7.10.19. Let a, b, c be pairwise coprime positive integers. Prove that there exists a (unique) residue class $m_0 \pmod{abc}$ such that if $m \equiv m_0 \pmod{abc}$ and if $am+1$, $bm+1$, and $cm+1$ are all primes, then their product is a Carmichael number (for example, $a=1, b=2, c=3$ in exercise 7.6.4 with $m_0 = 0$).

Exercise 7.10.20. Let D be a finite set of at least two distinct positive integers, the elements of which sum to n. Suppose that d divides n for every $d \in D$. Prove that if there exists an integer m for which $p_d := dnm+1$ is prime for every $d \in D$, then $\prod_{d\in D} p_d$ is a Carmichael number. (In particular note the case in which n is perfect and D is the set of proper divisors of n. The perfect number 6, for example, gives rise to the triple $6m+1, 12m+1, 18m+1$, which we explored in exercise 7.6.4.)

Exercise 7.10.21. (a) Prove that .010010000100... is irrational. (Here we put a "1" two digits after the decimal point, then 3 digits later, then 5 digits later, etc., with all the other digits being 0, the spacings between the "1"'s being $p-1$ for each consecutive prime p.)
(b)† Develop this idea to find a large class of irrationals.

Appendix 7A. Card shuffling and Fermat's Little Theorem

In this appendix we will define order in terms of card shuffling, give a combinatorial proof of Fermat's Little Theorem, and discuss quick calculations of powers mod n.

7.11. Card shuffling and orders modulo n

The cards in a 52-card deck can be arranged in $52! \approx 8 \times 10^{67}$ different orders. Between card games we shuffle the cards to make the order of the cards unpredictable. But what if someone can shuffle "perfectly"? How unpredictable will the order of the cards then be? Let's analyze this by carefully figuring out what happens in a "perfect shuffle". There are several ways of shuffling cards, the most common being the *riffle shuffle*. In a riffle shuffle one splits the deck in two, places the two halves in either hand, and then drops the cards, using one's thumbs, in order to more or less interlace the cards from the two decks.

One begins with a deck of 52 cards and, to facilitate our discussion, we will call the top card, card 1, the next card down, card 2, etc. If one performs a *perfect riffle shuffle*, one cuts the cards into two 26 card halves, one half with the cards 1 through 26, the other half with the cards 27 through 52. An "out-shuffle" then interlaces the two halves so that the new order of the cards becomes (from the top) cards

$$1, 27, 2, 28, 3, 29, 4, 30, \ldots.$$

That is, cards $1, 2, 3, \ldots, 26$ go to positions $1, 3, 5, \ldots, 51$, and cards $27, 28, \ldots, 52$ go to positions $2, 4, \ldots, 52$, respectively. We can give formulas for each half:

$$k \to \begin{cases} 2k-1 & \text{for } 1 \le k \le 26, \\ 2k-52 & \text{for } 27 \le k \le 52. \end{cases}$$

These coalesce into one formula $k \to 2k - 1 \pmod{51}$ for all $k, 1 \le k \le 52$. The top and bottom cards do not move, that is, $1 \to 1$ and $52 \to 52$, so we focus on understanding the permutation of the other fifty cards:

Any shuffle induces a *permutation* σ on $\{1, \ldots, 52\}$.[6] For the out-shuffle, $\sigma(1) = 1, \sigma(52) = 52$, and

$$\sigma(1 + m) \text{ is the least positive residue of } 1 + 2m \pmod{51} \text{ for } 1 \le m \le 50.$$

To determine what happens after two or more out-shuffles, we simply compute the function $\sigma^k(.)$ $(= \underbrace{\sigma(\sigma(\ldots\sigma}_{k \text{ times}}(.))))$. Evidently $\sigma^k(1) = 1, \sigma^k(52) = 52$, and then

$$\sigma^k(1 + m) \text{ is the least positive residue of } 1 + 2^k m \pmod{51} \text{ for } 1 \le m \le 50.$$

Now $2^8 \equiv 1 \pmod{51}$, and so $\sigma^8(1 + m) \equiv 1 + m \pmod{51}$ for all m. Therefore eight perfect out-shuffles return the deck to its original state—so much for the 52! possible orderings!

Eight more perfect out-shuffles will also return the deck to its original state, a total of 16 perfect out-shuffles, and also 24 or 32 or 40, etc. Indeed any multiple of 8. So we see that the order of 2 (mod 51) is 8 and that $2^r \equiv 1 \pmod{51}$ if and only if r is divisible by 8. This shows, we hope, why the notion of order is interesting and exhibits one of the key results (Lemma 7.1.2) about orders.

Exercise 7.11.1.† An "in-shuffle" is the riffle shuffle that interlaces the cards the other way; that is, after one shuffle, the order becomes cards $27, 1, 28, 2, 29, \ldots, 52, 26$. Analyze this in an analogous way to the above, and determine how many "in-shuffles" it takes to get the cards back into their original order.

Exercise 7.11.2.† What happens when one performs riffle shuffles on n-card decks, with n even?

Exercise 7.11.3.‡ Suppose that the dealer alternates between in-shuffles and out-shuffles. How many such pairs of shuffles does it take to get the deck of cards back into their original order?

Persi Diaconis is a Stanford mathematics professor who left home at the age of fourteen to learn from sleight-of-hand legend Dai Vernon.[7] It is said that Diaconis can shuffle to obtain any permutation of a deck of playing cards. We are interested in the highest possible order of a shuffle. To analyze this question, remember that a shuffle can be reinterpreted as a permutation σ on $\{1, \ldots, n\}$ (where $n = 52$ for a usual deck). One way to explicitly write down a permutation is to track the orbit of each number. For example, for the permutation σ on 5 elements given by

$$\sigma(1) = 4,\ \sigma(2) = 5,\ \sigma(3) = 1,\ \sigma(4) = 3,\ \sigma(5) = 2,$$

1 gets mapped to 4, which gets mapped to 3, and 3 gets mapped back to 1, whereas 2 gets mapped to 5 and 5 gets mapped back to 2, so we can write

$$\sigma = (1, 4, 3)(2, 5).$$

Each of $(1, 4, 3)$ and $(2, 5)$ is a *cycle*, and cycles cannot be decomposed any further. Any permutation can be decomposed into cycles in a unique way, the analogy of the Fundamental Theorem of Arithmetic, for permutations. What is the order of σ? Now $\sigma^n = (1, 4, 3)^n (2, 5)^n$, so that $\sigma^n(1) = 1,\ \sigma^n(4) = 4$, and $\sigma^n(3) = 3$ if

[6] That is, $\sigma : \{1, \ldots, 52\} \to \{1, \ldots, 52\}$ such that the $\sigma(i)$ are all distinct (and so σ has an inverse).
[7] Check out this story, and these larger-than-life characters, on Wikipedia.

and only if 3 divides n, while $\sigma^n(2) = 2$ and $\sigma^n(5) = 5$ if and only if 2 divides n. Therefore σ^n is the identity if and only if 6 divides n, and so σ has order 6.

Exercise 7.11.4. Suppose that σ is a permutation on $\{1, \dots, n\}$ and that $\sigma = C_1 \cdots C_k$ where $C_1, \dots, C_k$ are disjoint cycles.

(a) Show that the order of σ equals the least common multiple of the lengths of the cycles C_j, $1 \le j \le k$.

(b) Use this to find the order of the permutation corresponding to an out-shuffle.

(c) Prove that if $n_1, \dots, n_k$ are any set of positive integers for which $n_1 + \cdots + n_k = n$, then there exists a permutation $\sigma = C_1 \cdots C_k$ on $\{1, \dots, n\}$, where each C_j has length n_j.

(d) Deduce that the maximum order, $m(n)$, of a permutation σ on $\{1, \dots, n\}$ is given by

$$\max \operatorname{lcm}[n_1, \dots, n_k] \text{ over all integers } n_1, \dots, n_k \ge 1 \text{ for which } n_1 + \cdots + n_k = n.$$

Our goal is to determine $m(52)$, the highest order of any shuffle that Diaconis can perform on a regular deck of 52 playing cards. However it is unclear how to determine $m(n)$ systematically. Working through the possibilities for small n, using exercise 7.11.4, we find that

$$\begin{aligned}
m(5) &= 6 \text{ obtained from } 6 = 3\cdot 2 \text{ and } 5 = 3+2,\\
m(6) &= 6 \text{ obtained from } 6 = 3\cdot 2\cdot 1 \text{ and } 6 = 3+2+1,\\
m(7) &= 12 \text{ obtained from } 12 = 4\cdot 3 \text{ and } 7 = 4+3,\\
m(8) &= 12 \text{ obtained from } 12 = 4\cdot 3\cdot 1 \text{ and } 8 = 4+3+1,\\
m(9) &= 20 \text{ obtained from } 20 = 5\cdot 4 \text{ and } 9 = 5+4,\\
m(10) &= 30 \text{ obtained from } 30 = 5\cdot 3\cdot 2 \text{ and } 10 = 5+3+2,\\
m(11) &= 30 \text{ obtained from } 30 = 6\cdot 5 \text{ and } 11 = 6+5,\\
m(12) &= 60 \text{ obtained from } 60 = 5\cdot 4\cdot 3 \text{ and } 12 = 5+4+3.
\end{aligned}$$

No obvious pattern jumps out (at least to the author) from this data, though one observes one technical issue:

Exercise 7.11.5.† Show that there is a permutation $\sigma = C_1 \cdots C_k$ on $\{1, \dots, n\}$ of order $m(n)$ in which the length of each cycle is either 1 or a power of a distinct prime.

Exercise 7.11.6.† Use the previous exercise to determine $m(52)$.

Exercise 7.11.7.‡ Use exercise 5.4.3 to prove that $\log m(n) \sim \sqrt{n \log n}$.

7.12. The "necklace proof" of Fermat's Little Theorem

Little Sophie has a necklace-making kit, which comes with wires that each accommodate p beads, and unlimited supplies of beads of a different colors. How many genuinely *different* necklaces can be Sophie make? Two necklaces are *equivalent* if they can be obtained from each other by a rotation; otherwise they are different; and so Sophie is asking for the number of equivalence classes of sequences of length p where each entry is selected from a possible colors.

Suppose we have a necklace with the jth bead having color $c(j)$ for $1 \le j \le p$. One can rotate the necklace in p different ways: If we rotate the necklace k places for some k in the range $0 \le k \le p-1$, then the jth bead will have color $c(j+k)$ for $1 \le j \le p$, where $c(.)$ is taken to be a function of period p. If two of these equivalent necklaces are identical, then $c(j+k) = c(j+\ell)$ for all j, for some $0 \le k < \ell \le p-1$. Then $c(n+d) = c(n)$ for all n, where $d = \ell - k \in [1, p-1]$, and so $c(md) = c(0)$ for all m; that is, all of the beads in the necklace have the same color.

Therefore we have proved that, other than the a necklaces made of beads of the same color which each belong to an equivalence class of size 1, all other necklaces belong to equivalence classes of size p. Since there are a^p possible sequences of length p with a possible colors for each entry, and a sequences that all have the same color, the total number of equivalence classes (different necklaces) is

$$a + \frac{a^p - a}{p}.$$

In particular, we have established that p divides $a^p - a$ for all a, as desired.[8]

Exercise 7.12.1. Let p be prime. Let X denote a finite set and $f : X \to X$ where $f^p = i$, the identity map. (Here f^p means composing f with itself p times.) Let $X_{\text{fixed}} := \{x \in X : f(x) = x\}$.

(a) Prove that $|X| \equiv |X_{\text{fixed}}| \pmod p$.

Let G be a finite multiplicative group and $X = \{(x_1, \dots, x_p) \in G^p : \ x_1 \cdots x_p = 1\}$.

(b)† Deduce that $\#\{g \in G : g \text{ has order } p\} \equiv |G|^{p-1} - 1 \pmod p$.

(c) Deduce that if p divides the order of finite group G, then G contains an element of order p. Combined with Lagrange's Theorem, Corollary 7.23.1 of appendix 7D, this is an "if and only if" criterion.

Exercise 7.12.2. Let p be a given prime.

(a) Use (4.12.3) of appendix 4C to determine the number of irreducible polynomials mod p of prime degree q.

(b) Deduce that $q^p \equiv q \pmod p$ for every prime q.

(c) Deduce Fermat's Little Theorem.

More combinatorics and number theory

[1] Melvin Hausner, *Applications of a simple counting technique*, Amer. Math. Monthly **90** (1983), 127–129.

7.13. Taking powers efficiently

How can one raise a residue class mod m to the nth power "quickly", when n is very large? In 1785 Legendre computed high powers mod p by *fast exponentiation*: To determine $5^{65} \pmod{161}$, we write 65 in base 2, that is, $65 = 2^6 + 2^1$, so that $5^{65} = 5^{2^6} \cdot 5^{2^1}$. Let $f_0 = 5$ and $f_1 \equiv f_0^2 \equiv 5^2 \equiv 25 \pmod{161}$. Next let $f_2 \equiv f_0^4 \equiv f_1^2 \equiv 25^2 \equiv 142 \pmod{161}$, and then $f_3 \equiv f_0^8 \equiv f_2^2 \equiv 142^2 \equiv 39 \pmod{161}$. We continue computing $f_k \equiv f_0^{2^k} \equiv f_{k-1}^2 \pmod{161}$ by successive squaring: $f_4 \equiv 72$, $f_5 \equiv 32$, $f_6 \equiv 58 \pmod{161}$ and so $5^{65} = 5^{64+1} \equiv f_6 \cdot f_0 \equiv 58 \cdot 5 \equiv 129 \pmod{161}$. We have determined the value of $5^{65} \pmod{161}$ in seven multiplications mod 161, as opposed to 64 multiplications by the more obvious algorithm.

In general to compute $a^n \pmod m$ quickly: Define

$$f_0 = a \text{ and then } f_j \equiv f_{j-1}^2 \pmod m \text{ for } j = 1, 2, \dots, j_1,$$

where j_1 is the largest integer for which $2^{j_1} \le n$. Writing n in binary, say as $n = 2^{j_1} + 2^{j_2} + \cdots + 2^{j_\ell}$ with $j_1 > j_2 > \cdots > j_\ell \ge 0$, let $g_1 = f_{j_1}$ and then

[8] We've seen that Fermat's Little Theorem arises in many different contexts. Even its earliest discoverers got there for different reasons: Fermat, Euler, and Lagrange were led to Fermat's Little Theorem by the search for perfect numbers, whereas Gauss was led to it by studying the periods in the decimal expansion of fractions (as in section 7.8). It seems to be a universal truth, rather than simply an ad hoc discovery.

$g_i \equiv g_{i-1} f_{j_i} \pmod m$ for $i = 2, 3, \dots, \ell$. Therefore

$$g_\ell \equiv f_{j_1} \cdot f_{j_2} \cdots f_{j_\ell} \equiv a^{2^{j_1}+2^{j_2}+\cdots+2^{j_\ell}} = a^n \pmod m.$$

This involves $j_\ell + \ell - 1 \le 2j_\ell \le \frac{2 \log n}{\log 2}$ multiplications mod m as opposed to n multiplications mod m by the more obvious algorithm.

One can often use fewer multiplications. For example, for $31 = 1+2+4+8+16$ the above uses 8 multiplications, but we can use just 7 multiplications if, instead, we determine $a^{31} \pmod m$ by computing $a^2 \equiv a \cdot a$; $a^3 \equiv a^2 \cdot a$; $a^6 \equiv a^3 \cdot a^3$; $a^{12} \equiv a^6 \cdot a^6$; $a^{24} \equiv a^{12} \cdot a^{12}$; $a^{30} \equiv a^{24} \cdot a^6 \pmod m$; and finally $a^{31} \equiv a^{30} \cdot a \pmod m$.

These exponents form an *addition chain*, a sequence of integers $e_1 = 1 < e_2 < \cdots < e_k$ where, for all $k > 1$, we have $e_k = e_i + e_j$ for some $i, j \in \{1, \dots, k-1\}$. In the example above, the binary digits of 31 led to the addition chain $1, 2, 3, 4, 7, 8, 15, 16, 31$, but the addition chain $1, 2, 3, 6, 12, 24, 30, 31$ is shorter.

For most exponents n, there is an addition chain which is substantially shorter than $j_\ell + \ell - 1$, though never less than half that size. There are many open questions about addition chains. The best known is Scholz's conjecture that the shortest addition chain for $2^n - 1$ has length $\le n - 1$ plus the length of the shortest addition chain for n. For much more on addition chains, see Knuth's classic book [**Knu98**].

7.14. Running time: The desirability of polynomial time algorithms

In this section we discuss how to measure how fast an algorithm is. The inputs into the algorithm in the previous section for calculating $a^n \pmod m$ are the integers a and m, with $1 \le a \le m$, and the exponent n. We will suppose that m has d digits (so that d is proportional to $\log m$). The usual algorithms for adding and subtracting integers with d digits take about $2d$ steps, whereas the usual algorithm for multiplication takes about d^2 steps.[9]

Exercise 7.14.1. Justify that multiplying two residues mod m together and reducing mod m takes no more than $2d^2$ steps.

The algorithm described in the previous section involves about $c \log n$ multiplications of two residues mod m, for some constant $c > 0$, and so the total number of steps is proportional to

$$(\log m)^2 \log n.$$

Is this good? Given any mathematical problem, the cost (measured by the number of steps) of an algorithm to resolve the question must include the time taken to read the input data, which can be measured by the number of digits, D, in the input. In this case the input is the numbers a, m, and n, so that D is proportional to $\log m + \log n$. Now if a and m are fixed and we allow n to grow, then the algorithm takes CD steps for some constant $C > 0$, which is C times as long as it takes to read the input. You cannot hope to do much better than that. On the other hand, if m and n are roughly the same size, then the algorithm takes time proportional

[9] Since we have to multiply each pair of digits together, one from each of the given numbers.

to D^3. We still regard this as fast—any algorithm whose speed is bounded by a polynomial in D is a *polynomial time algorithm* and is considered to be pretty fast.

It is important to distinguish between a mathematical problem and an algorithm used for resolving it. There can be many choices of algorithm and one wants a fast one. However, we might only know a slowish algorithm which, even though it may seem clever, does not necessarily mean that there is no fast algorithm.

Let `P` be the class of problems that can be resolved by an algorithm that runs in polynomial time. Few mathematical problems belong to `P` and the key question is whether we can identify which problems. We'll discuss `P` in section 10.4.

Exercise 7.14.2. Prove that the Euclidean algorithm works in polynomial time.

Appendices. The extended version of chapter 7 has the following additional appendices:

Appendix 7B. *Orders and primitive roots* discusses how the order mod p^k of an integer prime to p varies as k increases. As a consequence we determine the structure of $(\mathbb{Z}/p^k\mathbb{Z})^*$ and calculate orders modulo composite m. We go on to discuss Gauss's extraordinary algorithm to construct primitive roots mod p, which works even better in the computer age than it did in his time.

Appendix 7C. *Finding nth roots modulo prime powers* introduces the question of explicitly determining all of the nth roots mod p, of a given nth power. Using the ideas in appendix 7B we can efficiently find all nth roots of 1 mod p, so our question boils down to finding one mth root, where $m = (n, p-1)$. We use this to find the nth roots of $a \pmod{p^k}$ for increasing k. We finish by looking at special cases in which one can find nth roots mod p through a formula (this is not always the case), which works if n divides $p-1$ and $(n, \frac{p-1}{n}) = 1$.

Appendix 7D. *Orders for finite groups.* Here we generalize the concept of order and Fermat's Little Theorem to arbitrary finite groups, and Wilson's Theorem if the group is also commutative. Finally we look at normal subgroups and develop the analogy of the Fundamental Theorem of Arithmetic, for finite groups.

Appendix 7E. *Constructing finite fields.* We show that all finite fields have order p^r for some prime p and integer $r \geq 1$ and show how to construct them. Moreover we find two different generalizations of (7.4.1).

Appendix 7F. *Sophie Germain andFermat's Last Theorem* proves Sophie Germain's famous result, which substantially restricts possible solutions to Fermat's Last Theorem with exponent p, when p and $2p+1$ are both primes.

Appendix 7G. *Primes of the form* $2^n + k$ shows how to construct integers k such that $2^n + k$ is never prime, using a surprisingly simple idea of Paul Erdős. We then go on to extend this idea to show there are integers k for which there are no primes of the form $F_n + k$ as F_n ranges through the Fibonacci numbers.

Appendix 7H. *Further congruences.* Here we study Fermat quotients and in particular whether p^2 ever divides $2^p - 2$. We also look at binomial coefficients mod p^2, Bernoulli numbers mod p, the Wilson quotient, sums of powers of integers mod p^2, and go beyond Fermat's Little Theorem.

Appendix 7I. *Primitive prime factors of recurrence sequences* are prime factors of a particular term of the recurrence sequence that divide no earlier term. For certain recurrence sequences, we show that every term, except perhaps the first few, has a primitive prime factor, and we discuss what is known on this subject.

Quadratic residues

In this chapter we will develop an understanding of the squares mod n, in particular how many there are and how to quickly identify whether a given residue is a square mod n. We mostly discuss the squares modulo primes and from there understand the squares mod prime powers via "lifting", and modulo composites through the Chinese Remainder Theorem.

8.1. Squares modulo prime p

There are two types of squares mod p. We always have $0^2 \equiv 0 \pmod{p}$. Then there are the "*quadratic residues* (mod p)", which are the non-zero residues a (mod p) which are congruent to a square modulo p. All other residue classes are "*quadratic non-residues*". If there is no ambiguity, we simply say "residues" and "non-residues". In the next table we list the quadratic residues modulo each of the primes between 5 and 17.

Modulus	Quadratic residues
5	1, 4
7	1, 2, 4
11	1, 3, 4, 5, 9
13	1, 3, 4, 9, 10, 12
17	1, 2, 4, 8, 9, 13, 15, 16

Exercise 8.1.1. (a) Prove that 337 is not a square (that is, the square of an integer) by reducing it mod 5.
(b) Prove that 391 is not a square by reducing it mod 7.
(c) Prove that there do not exist integers x and y for which $x^2 - 3y^2 = -1$, by reducing any solution mod 3.

In each row of our table there seem to be $\frac{p-1}{2}$ quadratic residues mod p:

Lemma 8.1.1. *The distinct quadratic residues* mod p *are given by* $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod{p}$.

Proof. If $r^2 \equiv s^2 \pmod{p}$ with $1 \le s < r \le p-1$, then $p \mid r^2 - s^2 = (r-s)(r+s)$ and so p divides either $r - s$ or $r + s$. Now $0 < r - s < p$ and so p does not divide

$r-s$. Therefore p divides $r+s$, and $0 < r+s < 2p$, so we must have $r+s=p$. Hence the residues of $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod p$ are distinct, and if $s = p-r$, then $s^2 \equiv (-r)^2 \equiv r^2 \pmod p$. This implies our result. □

Define the *Legendre symbol* as follows: For each odd prime p let

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod p, \\ 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

Exercise 8.1.2. (a) Prove that if $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) Prove that $\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = 0$.

Corollary 8.1.1. *There are exactly* $1 + \left(\frac{a}{p}\right)$ *residues classes* $b \pmod p$ *for which* $b^2 \equiv a \pmod p$.

Proof. If a is a quadratic non-residue, there are no solutions. For $a = 0$ if $b^2 \equiv 0 \pmod p$, then $b \equiv 0 \pmod p$ so there is just one solution. If a is a quadratic residue, then, by definition, there exists b such that $b^2 \equiv a \pmod p$, and then there are the two solutions $(p-b)^2 \equiv b^2 \equiv a \pmod p$ and no others, by the proof in Lemma 8.1.1 (or by Proposition 7.4.1). We have therefore proved

$$\#\{b \pmod p : b^2 \equiv a \pmod p\} = \begin{cases} 1 & \text{if } a \equiv 0 \pmod p, \\ 2 & \text{if } a \text{ is a quadratic residue mod } p, \\ 0 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

This equals $1 + \left(\frac{a}{p}\right)$, looking above at the definition of the Legendre symbol. □

Theorem 8.1. *We have* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *for any integers* a, b. *That is:*

(i) *The product of two quadratic residues* (mod p) *is a quadratic residue.*

(ii) *The product of a quadratic residue and a non-residue is itself a non-residue.*

(iii) *The product of two quadratic non-residues* (mod p) *is a quadratic residue.*

Proof (Gauss). (i) If $a \equiv A^2$ and $b \equiv B^2$, then $ab \equiv (AB)^2 \pmod p$.

Let $R := \{r \pmod p : (r/p) = 1\}$ be the set of quadratic residues mod p. We saw that if $(a/p) = 1$, then $(ar/p) = 1$ for all $r \in R$. In other words, $ar \in R$; that is, $aR \subset R$. The elements of aR are distinct, so that $|aR| = |R|$, and therefore $aR = R$.

(ii) Let $N = \{n \pmod p : (n/p) = -1\}$ be the set of quadratic non-residues mod p, so that $N \cup R$ partitions the reduced residues mod p. By exercise 3.5.2, we deduce that $aR \cup aN$ also partitions the reduced residues mod p, and therefore $aN = N$ since $aR = R$. That is, the elements of the set $\{an : (n/p) = -1\}$ are all quadratic non-residues mod p.

By Lemma 8.1.1, we know that $|R| = \frac{p-1}{2}$, and hence $|N| = \frac{p-1}{2}$ since $N \cup R$ partitions the $p-1$ reduced residues mod p.

(iii) In (ii) we saw that if $(n/p) = -1$ and $(a/p) = 1$, then $(na/p) = -1$. Hence $nR \subset N$ and, as $|nR| = |R| = \frac{p-1}{2} = |N|$, we deduce that $nR = N$. But $nR \cup nN$ partitions the reduced residues mod p, and so $nN = R$. That is, the elements of the set $\{nb : (b/p) = -1\}$ are all quadratic residues mod p. □

Exercise 8.1.3. Suppose that prime p does not divide ab.
(a) Prove that $\left(\frac{a/b}{p}\right) = \left(\frac{ab}{p}\right)$.
(b) Prove that there are non-zero residues x and $y \pmod p$ for which $ax^2 + by^2 \equiv 0 \pmod p$ if and only if $\left(\frac{-ab}{p}\right) = 1$.

Exercise 8.1.4. Prove that if odd prime p divides $b^2 - 4ac$ but neither a nor c, then $\left(\frac{a}{p}\right) = \left(\frac{c}{p}\right)$.

Exercise 8.1.5. Let p be a prime > 3. Prove that if there is no residue $x \pmod p$ for which $x^2 \equiv 2 \pmod p$, and no residue $y \pmod p$ for which $y^2 \equiv 3 \pmod p$, then *there is* a residue $z \pmod p$ for which $z^2 \equiv 6 \pmod p$.

We deduce from Theorem 8.1 that $\left(\frac{\cdot}{p}\right)$ is a multiplicative function. Therefore if we have a factorization of a into prime factors as $a = \pm q_1^{e_1} q_2^{e_2} \dots q_k^{e_k}$, and $(a, p) = 1$, then[1]

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \prod_{i=1}^{k} \left(\frac{q_i}{p}\right)^{e_i} = \left(\frac{\pm 1}{p}\right) \prod_{\substack{i=1 \\ e_i \text{ odd}}}^{k} \left(\frac{q_i}{p}\right),$$

since $(q/p)^2 = 1$ whenever $p \nmid q$ as this implies that $\left(\frac{q_i}{p}\right)^{e_i} = 1$ if e_i is even, and $\left(\frac{q_i}{p}\right)^{e_i} = \left(\frac{q_i}{p}\right)$ if e_i is odd. Therefore, in order to determine $\left(\frac{a}{p}\right)$ for all integers a, it is only necessary to know the values of $\left(\frac{-1}{p}\right)$, and of $\left(\frac{q}{p}\right)$ for all primes q.

Exercise 8.1.6. One can write each non-zero residue mod p as a power of a primitive root g.
(a) Prove that the quadratic residues are precisely those residues that are an even power of g, and the quadratic non-residues are those that are an odd power.
(b) Deduce that $\left(\frac{g}{p}\right) = -1$.

Exercise 8.1.7. (a) Show that if n is odd and p divides $a^n - 1$, then $\left(\frac{a}{p}\right) = 1$.
(b) Show that if n is prime and p divides $a^n - 1$, but $a \not\equiv 1 \pmod p$, then $p \equiv 1 \pmod n$.
(c) Give an example to show that (b) can be false if we only assume that n is odd.

Exercise 8.1.8. (a) Prove that, for every prime $p \neq 2, 5$, at least one of 2, 5, and 10 is a quadratic residue mod p.
(b)† Prove that, for every prime $p > 5$, there are two consecutive positive integers that are both quadratic residues mod p and are both ≤ 10.

8.2. The quadratic character of a residue

Fermat's Little Theorem (Theorem 7.2) states that the $(p-1)$st power of any reduced residue mod p is congruent to 1 $\pmod p$. Are there other patterns to be found among the lower powers?

[1] Each of "$\pm$" and "± 1" is to be read as "either '+' or '−' ". We deal with these two cases together since the proofs are entirely analogous, taking care throughout to be consistent with the choice of sign.

a	a^2	a^3	a^4
1	**1**	1	1
2	**-1**	-2	1
-2	**-1**	2	1
-1	**1**	-1	1

The powers of a mod 5

a	a^2	a^3	a^4	a^5	a^6
1	1	**1**	1	1	1
2	-3	**1**	2	-3	1
3	2	**-1**	-3	-2	1
-3	2	**1**	-3	2	1
-2	-3	**-1**	2	3	1
-1	1	**-1**	1	-1	1

The powers of a mod 7

As expected the $(p-1)$st column is all 1's, but there is another pattern that emerges: The entries in the "middle" column, that is, the a^2 column mod 5 and the a^3 column mod 7, are all -1's and 1's. This column represents the least residues of numbers of the form $a^{\frac{p-1}{2}} \pmod p$, and it appears that these are all -1's and 1's. Can we decide which are $+1$ and which are -1? For $p=5$ we see that $1^2 \equiv 4^2 \equiv 1 \pmod 5$ and $2^2 \equiv 3^2 \equiv -1 \pmod 5$; recall that 1 and 4 are the quadratic residues mod 5. For $p=7$ we see that $1^3 \equiv 2^3 \equiv 4^3 \equiv 1 \pmod 7$ and $3^3 \equiv 5^3 \equiv 6^3 \equiv -1 \pmod 7$; recall that 1, 2, and 4 are the quadratic residues mod 7. So we have observed a pattern: The ath entry in the middle column is $+1$ if a is a quadratic residues mod p, and it is -1 if a is a quadratic residues mod p; in either case it equals the value of the Legendre symbol, $\left(\frac{a}{p}\right)$. This observation was proved by Euler in 1732.

Theorem 8.2 (Euler's criterion)**.** *We have $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ for all primes p and integers a.*

Proof #1. If $\left(\frac{a}{p}\right) = 1$, then there exists b such that $b^2 \equiv a \pmod p$ so that $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p$, by Fermat's Little Theorem.

If $\left(\frac{a}{p}\right) = -1$, then we proceed as in Gauss's proof of Wilson's Theorem though pairing up the residues slightly differently. Let

$$S = \{(r,s) : \ 1 \le r < s \le p-1, \ rs \equiv a \pmod p\}.$$

Note that if $rs \equiv a \pmod p$, then $r \not\equiv s \pmod p$, or else $a \equiv r^2 \pmod p$, contradicting that $\left(\frac{a}{p}\right) = -1$. Therefore each integer m, $1 \le m \le p-1$, appears exactly once, in exactly one pair in S. We deduce that

$$(p-1)! = \prod_{(r,s)\in S} rs \equiv a^{|S|} = a^{\frac{p-1}{2}} \pmod p,$$

and the result follows from Wilson's Theorem. □

For example, for $p=13, a=2$ we have

$$-1 \equiv 12! = (1\cdot 2)(3\cdot 5)(4\cdot 7)(6\cdot 9)(8\cdot 10)(11\cdot 12) \equiv 2^6 \pmod{13}.$$

Exercise 8.2.1.† Prove Euler's criterion for $(a/p) = 1$, by evaluating $(p-1)! \pmod p$ as in the second part of proof #1, but now taking account of the solutions $r \pmod p$ to $r^2 \equiv a \pmod p$.

Proof #2 of Euler's criterion. We began Proof #1 by showing that if $\left(\frac{a}{p}\right) = 1$, then $a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$. This implies that a is a root of $x^{\frac{p-1}{2}} - 1 \pmod p$. By Lemma 8.1.1 there are exactly $\frac{p-1}{2}$ quadratic residues mod p, and we now know that these are all roots of $x^{\frac{p-1}{2}} - 1 \pmod p$ and are therefore *all* of the roots of $x^{\frac{p-1}{2}} - 1 \pmod p$. That is,

$$x^{\frac{p-1}{2}} - 1 \equiv \prod_{\substack{1\le a\le p\\(a/p)=1}} (x-a) \pmod p. \tag{8.2.1}$$

In (7.4.1) we noted that

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod p;$$

that is, the $p-1$ roots of $x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1) \pmod p$ are precisely the reduced residues mod p, each occurring exactly once. Since the set of reduced residues mod p is the union of the set of quadratic residues and the set of quadratic non-residues, we can divide this last equation through by (8.2.1), to obtain

$$x^{\frac{p-1}{2}} + 1 \equiv \prod_{\substack{1\le b\le p\\(b/p)=-1}} (x-b) \pmod p. \tag{8.2.2}$$

This implies that if b is a quadratic non-residue mod p, then $b^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$; that is, $b^{\frac{p-1}{2}} \equiv -1 = \left(\frac{b}{p}\right) \pmod p$. □

We can use Euler's criterion to determine the value of Legendre symbols as follows: $\left(\frac{3}{13}\right) = 1$ since $3^6 = 27^2 \equiv 1^2 \equiv 1 \pmod{13}$, and $\left(\frac{2}{13}\right) = -1$ since $2^6 = 64 = -1 \pmod{13}$.

Exercise 8.2.2. Let p be an odd prime. Explain how one can determine the integer $\left(\frac{a}{p}\right)$ by knowing $a^{\frac{p-1}{2}} \pmod p$. (Euler's criterion gives a congruence, but here we are asking for the value of the integer $\left(\frac{a}{p}\right)$.)

Exercise 8.2.3. Use Euler's criterion to reprove Theorem 8.1.

Proof #3 of Euler's criterion. Let g be a primitive root mod p. We have $g^{\frac{p-1}{2}} \equiv -1 \pmod p$ by exercise 7.5.2. Suppose that $a \equiv g^r \pmod p$ for some integer r, so that $a^{\frac{p-1}{2}} \equiv (g^r)^{\frac{p-1}{2}} = (g^{\frac{p-1}{2}})^r \equiv (-1)^r \pmod p$. If a is a quadratic residue mod p, then r is even by exercise 8.1.6, and so $a^{\frac{p-1}{2}} \equiv (-1)^r \equiv 1 \pmod p$. If a is a quadratic non-residue mod p, then r is odd, and so $a^{\frac{p-1}{2}} \equiv (-1)^r \equiv -1 \pmod p$. □

Square roots and non-squares modulo p. How can we tell whether a reduced residue $a \pmod p$ is a square mod p? One idea is to try to find the square root, but it is not clear how to go about this efficiently (for example, try to find the square root of 77 (mod 101)). One consequence of Euler's criterion is that one does not have to try to find the square root to determine whether a given residue class is a square mod p. Indeed one can determine whether a is a square mod p by calculating

$a^{\frac{p-1}{2}} \pmod p$. This might look like it will be equally difficult, but we have shown in section 7.13 of appendix 7A that one can calculate a high power of a mod p quite efficiently.

There are some special cases in which *one can determine* a square root of $a \pmod p$ quite easily. For example, when $p \equiv 3 \pmod 4$:

Exercise 8.2.4. Let p be a prime $\equiv 3 \pmod 4$. Show that if $\left(\frac{a}{p}\right) = 1$ and $b \equiv a^{\frac{p+1}{4}} \pmod p$, then $b^2 \equiv a \pmod p$. (This idea is explored further in section 7.21 of appendix 7C.)

However if $p \equiv 1 \pmod 4$, then it is not so easy to determine a square root. For example, -1 is a square mod p (as we will prove in the next section) but we do not know a simple practical way to quickly determine a square root of $-1 \pmod p$.

How can one quickly find a quadratic non-residue mod p? One would think it would be easy, as half of the residues mod p are quadratic non-residues, but there is no simple way to guarantee finding one quickly. In practice it is most efficient to select numbers in $[1, p-1]$ at random, independently. The probability that any given selection is a quadratic residue is $\frac{1}{2}$; so the probability that every one of the first k choices is a quadratic residue is $1/2^k$. Therefore, the probability that none of the first 20 selections is a quadratic non-residue mod p is less than one in a million. Moreover it is easy to verify whether each selection is a quadratic residue mod p, using Euler's criterion. This algorithm will almost always rapidly determine a quadratic non-residue mod p, but one might just be terribly unlucky and the algorithm might fail.

It is useful to determine for which primes p a given small integer a is a quadratic residue $\pmod p$. We study this for $a = -1$, 2, and -2 in the next few sections.

8.3. The residue -1

Theorem 8.3. *If p is an odd prime, then -1 is a quadratic residue* (mod p) *if and only if $p \equiv 1 \pmod 4$.*

We will give five proofs of this result (even though we don't need more than one!) to highlight how the various ideas in the book dovetail in this key result. It is worth recalling that in exercise 7.4.3(c) we showed that if $p \equiv 1 \pmod 4$, then $\left(\frac{p-1}{2}\right)!$ is a square root of $-1 \pmod p$. We developed more efficient ways of finding a square root of $-1 \pmod p$ in section 7.21 of appendix 7C.

Proof #1. Euler's criterion implies that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Since each side of the congruence is -1 or 1, and p, which is > 2, divides their difference, they must be equal and so $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, and the result follows. □

Proof #2. In exercise 7.5.2 we saw that $-1 \equiv g^{(p-1)/2} \pmod p$ for any primitive root g modulo p. Now if $-1 \equiv (g^k)^2 \pmod p$ for some integer k, then $\frac{p-1}{2} \equiv 2k \pmod{p-1}$, and there exists such an integer k if and only if $\frac{p-1}{2}$ is even. □

Proof #3. The number of quadratic non-residues (mod p) is $\frac{p-1}{2}$, and so, by Wilson's Theorem, we have

$$\left(\frac{-1}{p}\right) = \left(\frac{(p-1)!}{p}\right) = \prod_{a \pmod p} \left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}. \qquad \square$$

Proof #4. If a is a quadratic residue, then so is $1/a \pmod p$. Therefore we may "pair up" the quadratic residues (mod p), except those for which $a \equiv 1/a \pmod p$. The only solutions to $a \equiv 1/a \pmod p$ (that is, $a^2 \equiv 1 \pmod p$) are $a \equiv 1$ and $-1 \pmod p$. Therefore the product of the quadratic residues mod p is congruent to $-(-1/p)$. On the other hand the roots of $x^{\frac{p-1}{2}} - 1 \pmod p$ are precisely the quadratic residues mod p, and so, taking $x = 0$ in (8.2.1), the product of the quadratic residues mod p is congruent to $(-1)(-1)^{\frac{p-1}{2}} \pmod p$. Comparing these yields that $(-1/p) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, and the result follows. $\square$

Proof #5. (Euler) The first part of Proof #4 implies that

$$\frac{p-1}{2} = \#\{\text{a (mod } p) : \text{a is a quadratic residue (mod } p)\}$$

has the same parity as

$$\#\{a \in \{1,-1\} : \ a \text{ is a quadratic residue (mod } p)\} = \frac{1}{2}\left(3 + \left(\frac{-1}{p}\right)\right).$$

Multiplying through by 2 yields $p \equiv \left(\frac{-1}{p}\right) \pmod 4$, and the result follows. $\square$

Theorem 8.3 implies that if $p \equiv 1 \pmod 4$, then $\left(\frac{-r}{p}\right) = \left(\frac{r}{p}\right)$; and if $p \equiv -1 \pmod 4$, then $\left(\frac{-r}{p}\right) = -\left(\frac{r}{p}\right)$.

Exercise 8.3.1. Let p be a prime $\equiv 3 \pmod 4$, which does not divide integer a. Prove that either there exists $x \pmod p$ for which $x^2 \equiv a \pmod p$ or there exists $y \pmod p$ for which $y^2 \equiv -a \pmod p$, but not both.

Exercise 8.3.2. (a) Prove that every prime factor p of $4n^2 + 1$ satisfies $p \equiv 1 \pmod 4$.
(b) Deduce that there are infinitely many primes $\equiv 1 \pmod 4$.

8.4. The residue 2

Calculations reveal that the odd primes $p < 100$ for which $\left(\frac{2}{p}\right) = 1$ are

$$p = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, \text{ and } 97.$$

These are exactly the primes < 100 that are $\equiv \pm 1 \pmod 8$. This observation is established as fact as follows:

Theorem 8.4. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } -1 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } -3 \pmod 8. \end{cases}$$

Proof. We will evaluate the product

$$S := \prod_{\substack{1\le m\le p-1\\ m \text{ even}}} m \pmod p$$

in two different ways. First note that each m in the product can be written as $2k$ with $1 \le k \le \frac{p-1}{2}$, and so

$$S = \prod_{k=1}^{\frac{p-1}{2}} (2k) = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!.$$

One can also rewrite each m in the product as $p-n$ where n is odd; and if m is in the range $\frac{p+1}{2} \le m \le p-1$, then $1 \le n \le \frac{p-1}{2}$. Therefore

$$S = \prod_{\substack{1\le m\le \frac{p-1}{2}\\ m \text{ even}}} m \cdot \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n \text{ odd}}} (p-n).$$

Let's suppose there are r such values of n, and note that each $p-n \equiv -n \pmod p$. Therefore

$$S \equiv \prod_{\substack{1\le m\le \frac{p-1}{2}\\ m \text{ even}}} m \cdot \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n \text{ odd}}} (-n) = (-1)^r \left(\frac{p-1}{2}\right)! \pmod p.$$

Comparing the two ways that we have evaluated S, and dividing through by $\left(\frac{p-1}{2}\right)!$, we find that

$$2^{\frac{p-1}{2}} \equiv (-1)^r \pmod p.$$

The result follows from Euler's criterion and verifying that r is even if $p \equiv \pm 1 \pmod 8$, while r is odd if $p \equiv \pm 3 \pmod 8$ (see exercise 8.4.1). □

Exercise 8.4.1. For any odd integer q, let r denote the number of positive odd integers $\le \frac{q-1}{2}$. Prove that r is even if $q \equiv \pm 1 \pmod 8$, while r is odd if $q \equiv \pm 3 \pmod 8$.

Gauss's Lemma (Theorem 8.6 in appendix 8A) cleverly generalizes this proof of Theorem 8.4 to classify the values of $\left(\frac{a}{p}\right)$ for any fixed integer a.

Calculations reveal that the odd primes $p < 100$ for which $\left(\frac{-2}{p}\right) = 1$ are

$$p = 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, \text{ and } 97.$$

These are exactly the primes < 100 that are $\equiv 1$ or $3 \pmod 8$. This observation is established as fact by combining Theorems 8.3 and 8.4, which allow us to evaluate $\left(\frac{-2}{p}\right)$ by taking $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ for every odd prime p.

Exercise 8.4.2. Prove that if p is an odd prime, then

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 3 \pmod 8,\\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod 8.\end{cases}$$

Exercise 8.4.3. Prove that if 2 is a primitive root mod p, then $p \equiv 3$ or $5 \pmod 8$.

Exercise 8.4.4.† (a) Prove that if prime $p | M_n := 2^n - 1$ where $n > 2$ is prime, then $p \equiv 1 \pmod n$ and $p \equiv \pm 1 \pmod 8$.

(b) Prove that if $p = 2n+1$ is prime, then $p | 2^n - 1$ if and only if $p \equiv \pm 1 \pmod 8$.

(c) Prove that if $p = 2n+1$ is prime, then $p | 2^n + 1$ if and only if $p \equiv \pm 3 \pmod 8$.

(d) Prove that if q and $p = 2q + 1$ are both prime, then p divides $2^q - 1$ if and only if $q \equiv 3 \pmod 4$.
(e) Factor $2^{11} - 1 = 2047$.

Exercise 8.4.5.† In exercise 7.3.2 we proved that if prime p divides $2^{2^k} + 1$, then $p \equiv 1 \pmod{2^{k+1}}$. Now show that $p \equiv 1 \pmod{2^{k+2}}$ if $k \geq 2$.[2]

8.5. The law of quadratic reciprocity

We have already seen that if p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv -1 \pmod 4 \end{cases}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } -1 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } -3 \pmod 8. \end{cases}$$

To be able to evaluate arbitrary Legendre symbols we will also need the *law of quadratic reciprocity*.

Theorem 8.5 (The law of quadratic reciprocity)**.** *If p and q are given distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv q \equiv -1 \pmod 4. \end{cases}$$

These rules, taken together, allow us to rapidly evaluate any Legendre symbol. For example, to evaluate (m/p), we first reduce m mod p, so that $(m/p) = (n/p)$ where $n \equiv m \pmod p$ and $|n| < p$. Next we factor n and, by the multiplicativity of the Legendre symbol, we can evaluate (n/p) in terms of $(-1/p), (2/p)$ and the (q/p) for those primes q dividing n. We can easily determine the values of $(-1/p)$ and $(2/p)$ from determining $p \pmod 8$, and then we need to evaluate each (q/p) where $q \leq |n| < p$. We do this by the law of quadratic reciprocity since $(q/p) = \pm(p/q)$ depending only on the values of p and q mod 4.[3] We repeat the procedure on each (p/q). Clearly this process will quickly finish as the numbers involved are always getting smaller. Let us work through some examples.

$$\begin{aligned} \left(\frac{111}{71}\right) = \left(\frac{40}{71}\right) &= \left(\frac{2}{71}\right)^3 \left(\frac{5}{71}\right) && \text{as } 111 \equiv 40 \pmod{71} \text{ and } 40 = 2^3 \cdot 5, \\ &= 1^3 \cdot 1 \cdot \left(\frac{71}{5}\right) && \text{as } 71 \equiv -1 \pmod 8 \text{ and } 5 \equiv 1 \pmod 4, \\ &= \left(\frac{1}{5}\right) = 1 && \text{as } 71 \equiv 1 \pmod 5. \end{aligned}$$

[2] We can use this to "demystify" Euler's factorization of F_5: Exercise 8.4.5 implies that any prime factor p of F_5 must be of the form $128m + 1$. This is divisible by 3, 5, and 3 for $m = 1$, 3, and 4, respectively, so is not prime. If $m = 2$, then $p = F_4$ which we proved is coprime with F_5 in section 5.1. Finally, if $m = 5$, then $p = 541$ is a prime factor of F_5.

[3] Note that if $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \eta\ (= \pm 1)$ by the law of quadratic reciprocity, then $\left(\frac{q}{p}\right) = \eta\left(\frac{p}{q}\right)$.

There is more than one way to proceed with these rules:

$$\begin{aligned}\left(\frac{111}{71}\right) &= \left(\frac{-1}{71}\right)\left(\frac{31}{71}\right) && \text{as } 111 \equiv -31 \pmod{71},\\ &= (-1)\cdot(-1)\cdot\left(\frac{71}{31}\right) && \text{as } 71 \equiv 31 \equiv -1 \pmod{4},\\ &= \left(\frac{9}{31}\right) = \left(\frac{3}{31}\right)^2 = 1 && \text{as } 71 \equiv 9 \equiv 3^2 \pmod{31}.\end{aligned}$$

A slightly larger example is

$$\begin{aligned}\left(\frac{869}{311}\right) &= \left(\frac{247}{311}\right) = \left(\frac{13}{311}\right)\left(\frac{19}{311}\right) = 1\cdot\left(\frac{311}{13}\right)\cdot(-1)\cdot\left(\frac{311}{19}\right)\\ &= -\left(\frac{-1}{13}\right)\left(\frac{7}{19}\right) = -1\cdot 1\cdot(-1)\left(\frac{19}{7}\right) = \left(\frac{-2}{7}\right) = -1.\end{aligned}$$

Although longer, each step is straightforward except when we factored $247 = 13\times 19$ (a factorization which is not obvious for most of us, and imagine how difficult factoring might be when we are dealing with much larger numbers). Indeed, this is an efficient procedure provided that one is capable of factoring the numbers n that arise. Although this may be the case for small examples, it is not practical for large examples. We can bypass this potential difficulty by using the Jacobi symbol, a generalization of the Legendre symbol, which we will discuss in section 8.7.

In the next subsection we will prove the law of quadratic reciprocity, justifying the algorithm used above to determine the value of any given Legendre symbol.

The law of quadratic reciprocity is easily used to determine various other rules. For example, when is 3 a square mod p? This is the same as asking when $(3/p) = 1$. Now by quadratic reciprocity we have two cases:

- If $p \equiv 1 \pmod 4$, then $(3/p) = (p/3)$, and $(p/3) = 1$ when $p \equiv 1 \pmod 3$, so we have $(3/p) = 1$ when $p \equiv 1 \pmod{12}$ (using the Chinese Remainder Theorem).
- If $p \equiv -1 \pmod 4$, then $(3/p) = -(p/3)$, and $(p/3) = -1$ when $p \equiv -1 \pmod 3$, so we have $(3/p) = 1$ when $p \equiv -1 \pmod{12}$ (using the Chinese Remainder Theorem).

We have therefore proved that $(3/p) = 1$ if and only if $p \equiv 1$ or $-1 \pmod{12}$.

Exercise 8.5.1. Determine (a) $\left(\frac{13}{31}\right)$; (b) $\left(\frac{323}{31}\right)$; (c) $\left(\frac{377}{233}\right)$; (d) $\left(\frac{13}{71}\right)$; (e) $\left(\frac{-104}{131}\right)$.

Exercise 8.5.2. (a) Show that if prime $p \equiv 1 \pmod 5$, then 5 is a quadratic residue mod p.
(b) Show that if prime $p \equiv 3 \pmod 5$, then 5 is a quadratic non-residue mod p.
(c) Determine all odd primes p for which $(5/p) = -1$.

Exercise 8.5.3. Prove that if $p := 2^n - 1$ is prime with $n > 2$, then $(3/p) = -1$.

Exercise 8.5.4.† Suppose that $F_m = 2^{2^m} + 1$ with $m \geq 2$ is prime. Prove that $3^{\frac{F_m-1}{2}} \equiv 5^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}$.

Exercise 8.5.5.† (a) Determine all odd primes p for which $(7/p) = 1$.
(b) Find all primes p such that there exists $x \pmod p$ for which $2x^2 - 2x - 3 \equiv 0 \pmod p$.

Exercise 8.5.6. Show that if p and $q = p + 2$ are "twin primes", then p is a quadratic residue mod q if and only if q is a quadratic residue mod p.

Exercise 8.5.7. Prove that $(-3/p) = (p/3)$ for all primes p.

8.6. Proof of the law of quadratic reciprocity

Suppose that $p < q$ are odd primes, and let $n = pq$. Given residue classes $a \pmod p$ and $b \pmod q$ there exists a unique residue class $r \pmod n$ for which $r \equiv a \pmod p$ and $\equiv b \pmod q$, by the Chinese Remainder Theorem. Let $r(a,b)$ be the least residue of r mod n in absolute value and let $m(a,b) = |r(a,b)|$, so that $1 \le m(a,b) \le n/2$, and $m(a,b) = r(a,b)$ or $-r(a,b)$. We claim that

$$\left\{ m(a,b) : 1 \le a \le p-1 \text{ and } 1 \le b \le \frac{q-1}{2} \right\} = \left\{ m : 1 \le m \le \frac{n}{2} \text{ with } (m,n) = 1 \right\},$$

since the two sets both have $\phi(n)/2$ elements, each such $m(a,b) \in [1, \frac{n}{2})$ with $(m,n) = 1$, and the $m(a,b)$ are distinct. This last assertion holds or else if $m(a,b) = m(a',b')$, then $r(a,b) \equiv \pm r(a',b') \pmod n$, so that $b \equiv \pm b' \pmod q$. As $1 \le b, b' \le \frac{q-1}{2}$ this implies that $b = b'$ so that the sign is "+", and therefore $a \equiv a' \pmod p$ implying that $a = a'$.

Since each $m(a,b) = \pm r(a,b)$, we deduce that there exists $\sigma = -1$ or 1 such that

$$\sigma \prod_{\substack{1 \le a < p-1 \\ 1 \le b \le \frac{q-1}{2}}} r(a,b) = \prod_{\substack{1 \le a < p-1 \\ 1 \le b \le \frac{q-1}{2}}} m(a,b) = \prod_{\substack{1 \le m < n/2 \\ (m,n)=1}} m. \tag{8.6.1}$$

We will calculate the two sides in this identity, mod p and mod q, and compare.

As $r(a,b) \equiv a \pmod p$ the product on the left-hand side of (8.6.1) is

$$\prod_{\substack{1 \le a < p-1 \\ 1 \le b \le \frac{q-1}{2}}} r(a,b) \equiv \prod_{1 \le b \le \frac{q-1}{2}} \prod_{1 \le a < p-1} a = (p-1)!^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \pmod p,$$

using Wilson's Theorem. We rewrite the right-hand side of (8.6.1), multiplying top and bottom by the integers $m \in [1, \frac{n}{2})$ that are divisible by q, to obtain

$$\prod_{\substack{1 \le m < n/2 \\ (m,p)=1}} m \Big/ \prod_{\substack{1 \le m < n/2 \\ q \mid m}} m.$$

We partition the m's in the numerator into intervals of length p, because

$$\prod_{\substack{ip \le m < (i+1)p \\ (m,p)=1}} m = \prod_{j=1}^{p-1} (ip + j) \equiv \prod_{j=1}^{p-1} j \equiv (p-1)! \equiv -1 \pmod p,$$

by Wilson's Theorem. Applying this for $0 \le i \le \frac{q-3}{2}$ we get a contribution of $(-1)^{\frac{q-1}{2}}$ to the numerator. The remaining integers in the numerator contribute

$$\prod_{\substack{\frac{q-1}{2} \cdot p \le m < \frac{n}{2} \\ (m,p)=1}} m = \prod_{j=1}^{(p-1)/2} \left(\frac{q-1}{2} p + j \right) \equiv \prod_{j=1}^{(p-1)/2} j \equiv \left(\frac{p-1}{2} \right)! \pmod p.$$

On the other hand the m's in the denominator can be written as qk with $1 \le k \le \frac{p-1}{2}$, and so

$$\prod_{\substack{1\le m<n/2\\ q|m}} m \;=\; \prod_{1\le k\le \frac{p-1}{2}} qk \;=\; q^{(p-1)/2}\left(\frac{p-1}{2}\right)! \;\equiv\; \left(\frac{q}{p}\right)\left(\frac{p-1}{2}\right)! \pmod p,$$

by Euler's criterion. Cancelling the $\left(\frac{p-1}{2}\right)!$ from the numerator and denominator, we deduce that the right-hand side of (8.6.1) is $\equiv (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p$. Comparing our calculation of the left- and right-hand sides of (8.6.1) mod p, we obtain

$$\sigma(-1)^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p. \tag{8.6.2}$$

Since both sides are 1 or -1 and are congruent mod p, they must be equal and so we deduce that

$$\sigma = \left(\frac{q}{p}\right).$$

Next we reduce (8.6.1) mod q. For the right-hand side we proceed entirely analogously to how we did mod p, with the roles of p and q reversed and so obtain $(-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod q$.

For the left-hand side of (8.6.1) mod q , we note that each $r(a,b) \equiv b \pmod q$, so that

$$\prod_{\substack{1\le a<p-1\\ 1\le b\le \frac{q-1}{2}}} r(a,b) \equiv \prod_{1\le a<p-1}\ \prod_{1\le b\le \frac{q-1}{2}} b = \left(\left(\frac{q-1}{2}\right)!\right)^{p-1} \pmod q.$$

In exercise 7.4.3 we saw $\binom{q-1}{(q-1)/2} \equiv (-1)^{\frac{q-1}{2}} \pmod q$,[4] and therefore

$$\left(\left(\frac{q-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{q-1}{2}}(q-1)! \equiv -(-1)^{\frac{q-1}{2}} \pmod q,$$

by Wilson's Theorem. Therefore

$$\prod_{\substack{1\le a<p-1\\ 1\le b\le \frac{q-1}{2}}} r(a,b) \equiv \left(\left(\left(\frac{q-1}{2}\right)!\right)^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod q.$$

Substituting this and the above into (8.6.1) we obtain

$$\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod q. \tag{8.6.3}$$

Again both sides are 1 or -1 and are congruent mod q, so must be equal. Multiplying both sides through by $(-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right)$ implies that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

[4] See the solution to exercise 7.4.3 at the end of the book for a proof.

From here we work through the four cases for p and q mod 4 and deduce the law of quadratic reciprocity (Theorem 8.5). □

There are many proofs of the law of quadratic reciprocity, 246 at the last count (see the list at `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`). In this chapter's appendices we present two of the best: the original proof due to Gauss and an elegant proof due to Eisenstein. We also discuss two other proofs in the exercises and then two sophisticated but shorter proofs in chapter 14.

8.7. *The Jacobi symbol*

The *Jacobi symbol* is defined as follows: If m is a positive odd integer, we write $m = \prod_p p^{e_p}$, where the p are distinct odd primes, and then

$$\left(\frac{a}{m}\right) = \prod_p \left(\frac{a}{p}\right)^{e_p}.$$

This is defined only for odd m, not for even m.

If a is a square modulo m, then, by the Chinese Remainder Theorem, a is a square modulo every prime p dividing m; that is, $(a/p) = 0$ or 1 for all $p|m$ and so $(a/m) = 0$ or 1. However the converse is not always true; for example, 2 is not a square mod 15 as

$$\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = -1, \text{ even though this implies that } \left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = 1.$$

Exercise 8.7.1. Suppose that m is an odd positive integer.
(a) Prove that $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$ whenever $a \equiv b \pmod m$.
(b) Prove that $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.
(c) Prove that if $\left(\frac{a}{m}\right) = -1$, then a is not a square mod m.
(d) Prove that $\left(\frac{a}{m}\right) = 0$ if and only if $(a, m) > 1$.

Exercise 8.7.2. (a) Prove that $\sum_{a=0}^{m-1} \left(\frac{a}{m}\right) = 0$ for every non-square odd integer $m \geq 2$.
(b) For how many residues a mod m do we have $(a/m) = 1$?
(c) For how many residues a mod m do we have $(a/m) = -1$?

Exercise 8.7.3. Show that if $n \geq 1$, then $\left(\frac{n}{4n-1}\right) = 1$.

Theorems 8.3, 8.4, and 8.5 can all be extended to the Jacobi symbol (as we will prove at the end of this section): If m and n are odd, coprime integers > 1, then

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4, \\ -1 & \text{if } n \equiv -1 \pmod 4, \end{cases} \tag{8.7.1}$$

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \text{ or } -1 \pmod 8, \\ -1 & \text{if } n \equiv 3 \text{ or } -3 \pmod 8, \end{cases} \tag{8.7.2}$$

and the law of quadratic reciprocity

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}. \tag{8.7.3}$$

We can use these three rules to easily evaluate (m/n) for any odd coprime integers m and n. One begins by selecting $M \equiv m \pmod n$ as conveniently as possible, usually with $|M| < n$. Then we factor $M = \pm 2^k \ell$ where ℓ is an odd positive integer $< n$, so that $\left(\frac{m}{n}\right) = \left(\frac{M}{n}\right) = \left(\frac{\pm 1}{n}\right)\left(\frac{2}{n}\right)^k \left(\frac{\ell}{n}\right)$. We can evaluate the first two Jacobi symbols using the first two rules above (which depend only on the value of $n \pmod 8$), and then we know that $\left(\frac{\ell}{n}\right) = \pm\left(\frac{n}{\ell}\right)$ by the third rule. To evaluate $\left(\frac{n}{\ell}\right)$ we repeat this process, but now with a smaller pair of numbers, so that the algorithm will terminate after finitely many steps.

This algorithm only involves dividing out powers of 2 and a possible minus sign, so it goes fast and avoids serious factoring; in fact it is guaranteed to go at least as fast as the Euclidean algorithm since it involves very similar steps.[5] Here is a first straightforward example using the Jacobi symbol, instead of the Legendre symbol:

$$\left(\frac{106}{71}\right) = \left(\frac{35}{71}\right) = -\left(\frac{71}{35}\right) = -\left(\frac{1}{35}\right) = -1.$$

(Note that (71/35) is not the Legendre symbol as 35 is not prime, but it is a Jacobi symbol.) Now let's revisit the example $\left(\frac{869}{311}\right)$ from section 8.5 and avoid factoring 247:

$$\left(\frac{869}{311}\right) = \left(\frac{247}{311}\right) = (-1)\left(\frac{311}{247}\right) = -\left(\frac{64}{247}\right) = -1.$$

We did not need to factor 247, and each step of the algorithm was straightforward.

Exercise 8.7.4. Determine (a) $\left(\frac{13}{27}\right)$; (b) $\left(\frac{323}{225}\right)$; (c) $\left(\frac{233}{377}\right)$; (d) $\left(\frac{-104}{135}\right)$.

Proof of (8.7.1)**,** (8.7.2)**, and** (8.7.3)**.** We proceed by induction on the number of prime factors of m and n. The results follows when m and n have one prime factor by Theorems 8.3, 8.4, and 8.5, respectively. Otherwise we write $n = ap$ for some prime p dividing n (swapping the roles of m and n if necessary).

Exercise 8.7.5. Prove that $\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2$ for any odd integers a, b.

Equation (8.7.1) can be rephrased as $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$. By induction, using the multiplicativity of the denominator of the Jacobi symbol,

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{ap}\right) = \left(\frac{-1}{a}\right)\left(\frac{-1}{p}\right) = (-1)^{\frac{a-1}{2}+\frac{p-1}{2}} = (-1)^{\frac{ap-1}{2}} = (-1)^{\frac{n-1}{2}}$$

by exercise 8.7.5.

Similarly by induction and multiplicativity of the numerator and denominator,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \left(\frac{m}{ap}\right)\left(\frac{ap}{m}\right) = \left(\frac{m}{a}\right)\left(\frac{m}{p}\right)\cdot\left(\frac{a}{m}\right)\left(\frac{p}{m}\right) = \left(\frac{m}{a}\right)\left(\frac{a}{m}\right)\cdot\left(\frac{m}{p}\right)\left(\frac{p}{m}\right)$$
$$= (-1)^{\frac{m-1}{2}\cdot\frac{a-1}{2}+\frac{m-1}{2}\cdot\frac{p-1}{2}} = (-1)^{\frac{m-1}{2}\cdot\frac{ap-1}{2}} = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$$

by exercise 8.7.5.

[5] As in the "speeded up" version of the Euclidean algorithm, given in section 1.11 of appendix 1B.

If $(\frac{2}{a}) = (\frac{2}{p})$, then $a \equiv \pm p \pmod 8$, so that $n = ap \equiv \pm 1 \pmod 8$, and therefore $(\frac{2}{n}) = (\frac{2}{a})(\frac{2}{p}) = (\pm 1)^2 = 1$. If $(\frac{2}{a}) = -(\frac{2}{p})$, then $a \equiv \pm 3p \pmod 8$, so that $n = ap \equiv \pm 3 \pmod 8$, and therefore $(\frac{2}{n}) = (\frac{2}{a})(\frac{2}{p}) = (1)(-1) = -1$. □

Gauss gave a different proof of (8.7.2), tying the question directly into finding solutions to quadratic equations. This foreshadows Gauss's proof of the full law of quadratic reciprocity, which we will give in appendix 8C.

Gauss's induction step for integers $n \equiv \pm 3 \pmod 8$. We suppose that (8.7.2) is true for all odd integers $m < n$ and that $n \equiv \pm 3 \pmod 8$. If $n = ab$ is composite with $1 < a, b < n$, then $\left(\frac{2}{n}\right) = \left(\frac{2}{a}\right)\left(\frac{2}{b}\right)$ and the result for n follows by applying the induction hypothesis with $m = a$ and with $m = b$.

Therefore we may suppose that $n = p$ is prime and assume that $(\frac{2}{p}) = 1$. Let a be the smallest odd positive integer for which $a^2 \equiv 2 \pmod p$ so that $1 \le a \le p-1$ (for if b is the smallest positive integer for which $b^2 \equiv 2 \pmod p$, then let $a = b$ if b is odd, and $a = p - b$ if b is even), and write $a^2 - 2 = pr$. Evidently $pr \equiv a^2 - 2 \equiv -1 \pmod 8$ and so $r \equiv p^2 r \equiv p(pr) \equiv -p \equiv \pm 3 \pmod 8$. Now $a^2 \equiv 2 \pmod r$ and so $\left(\frac{2}{r}\right) = 1$ with $r = \frac{a^2-2}{p} < p$ and $r \equiv \pm 3 \pmod 8$. This contradicts the induction hypothesis, and so our assumption is wrong. Therefore $(\frac{2}{p}) = -1$. □

Exercise 8.7.6. Prove an analogous induction step for integers $n \equiv 5$ or $7 \pmod 8$ when establishing the value of $\left(\frac{-2}{n}\right)$.

Exercise 8.7.7 (A useful reformulation of the law of quadratic reciprocity)**.** For a given odd, squarefree integer $n > 1$ let $n^* = \left(\frac{-1}{n}\right) n$. Prove that $n^* \equiv 1 \pmod 4$ and that we have $\left(\frac{m}{n}\right) = \left(\frac{n^*}{m}\right)$ for all odd integers $m > 1$.

8.8. *The squares modulo* m

To determine the squares mod m, that is, the residues $a \pmod m$ for which there exists $b \pmod m$ with $b^2 \equiv a \pmod m$, we may use the Chinese Remainder Theorem: We know that a is a square mod m if and only if a is a square modulo every prime power factor of m. So it is sufficient to understand the squares modulo every prime power.

Above we have understood the squares modulo every prime p. We now "lift" these squares to determine the squares modulo every prime power, p^k. Let's begin by studying the squares mod p^2:

The squares mod 9 are 0, 1, 4, and 7 mod 9 (these are the least residues of $0^2, 1^2, \dots, 8^2 \pmod 9$, excluding repetitions). The non-zero residues, 1, 4, and 7 are all $\equiv 1 \pmod 3$; in fact they are all of the residue classes $a \pmod 9$ for which $a \equiv 1 \pmod 3$. We have seen that $1 \pmod 3$ is the only quadratic residue mod 3.

Similarly mod 25 we have the squares

$$0, 1, 4, 9, 16, 11, 24, 14, 6, 21, \text{and } 19 \pmod{25}.$$

The non-zero squares here are 1, 6, 11, 16, and 21 (mod 25), the residue classes a (mod 25) for which $a \equiv 1 \pmod 5$, and 4, 9, 14, 19, and 24 (mod 25), the residue classes $a \pmod{25}$ for which $a \equiv 4 \pmod 5$. Moreover 1 and 4 (mod 5) are the quadratic residues mod 5.

A pattern begins to emerge. Define a to be a *quadratic residue* (mod m) if $(a, m) = 1$ and there exists $b \pmod m$ for which $b^2 \equiv a \pmod m$.

Proposition 8.8.1. *Let p be a prime. If r is a quadratic residue* mod p^k*, then r is a quadratic residue* mod p^{k+1} *whenever $k \geq 1$, except perhaps when $p^k = 2$ or 4.*

Proof. There exists an integer x for which $x^2 \equiv r \pmod{p^k}$, and $(x, p) = 1$ as $(r, p) = 1$. We let n be that integer for which $x^2 = r + np^k$.

Now if p is odd, then, for any integer j, we have

$$(x - jp^k)^2 \ = \ x^2 - 2jxp^k + j^2p^{2k} \ \equiv r + (n - 2jx)p^k \pmod{p^{k+1}}.$$

This is $\equiv r \pmod{p^{k+1}}$ if and only if $2jx \equiv n \pmod p$, which holds if and only if $j \equiv n/2x \pmod p$ (as $(2x, p) = 1$). Therefore r is a square mod p^{k+1}, and our proof yields that there is a unique $X \pmod{p^{k+1}}$ for which $X \equiv x \pmod{p^k}$ and $X^2 \equiv r \pmod{p^{k+1}}$, namely $X \equiv x - jp^k \pmod{p^{k+1}}$ where $j \equiv n/2x \pmod p$.

If $p = 2$, then $x^2 = r + n \cdot 2^k$ and x is odd so that $x^2 - nx2^k \equiv r \pmod{2^{k+1}}$. Therefore

$$(x - n2^{k-1})^2 \ = \ x^2 - nx2^k + n^2 2^{2k-2} \ \equiv r \pmod{2^{k+1}},$$

provided the exponent $2k - 2 \geq k + 1$; that is, $k \geq 3$. □

Exercise 8.8.1. Deduce that an integer r is a quadratic residue mod p^k if and only if r is a quadratic residue mod p, when p is odd, and if and only if $r \equiv 1 \pmod{\gcd(2^k, 8)}$ when $p = 2$.

This implies that exactly half of the reduced residue classes mod p^k are quadratic residues, when p is odd, and exactly one quarter when $p = 2$ and $k \geq 3$.

Using the Chinese Remainder Theorem we therefore deduce from exercise 8.8.1 the following:

Corollary 8.8.1. *Suppose that $(a, m) = 1$. Then a is a square* mod m *if and only if $\left(\frac{a}{p}\right) = 1$ for every odd prime p dividing m, and $a \equiv 1 \pmod{\gcd(m, 8)}$.*

Exercise 8.8.2. Suppose that $(a, n) = 1$ and that $b^2 \equiv a \pmod n$. Prove that the set of solutions $x \pmod n$ to $x^2 \equiv a \pmod n$ is given by the values $br \pmod n$ as r runs through the solutions to $r^2 \equiv 1 \pmod n$. (Determining the square roots of 1 (mod n) is discussed in section 3.8.)

Additional exercises

Exercise 8.9.1. Let p be an odd prime where $p \nmid a$. Show that the congruence $ax^2 + bx + c \equiv 0 \pmod p$ has a solution $x \pmod p$ if and only if $b^2 - 4ac$ is a square mod p.

Exercise 8.9.2.† Prove that m^2 and $m^2 + 1$ are both squares mod p, for m equal to at least one of a, $a + 1$, or $a^2 + a + 1$, for any integer a. (This generalizes exercise 8.1.8(a).)

Exercise 8.9.3. The polynomial $x^4 - 4x^2 + 1$ is irreducible over $\mathbb{Q}[x]$ by Theorem 3.4.

(a) Prove that $x^4 - 4x^2 + 1$ can be factored mod p as $(x^2 - \alpha)(x^2 - \beta)$ or $(x^2 - ax + 1)(x^2 + ax + 1)$ or $(x^2 - ax + 1)(x^2 + ax + 1)$ if 3 or 6 or 2 is a square mod p, respectively.

(b) Deduce that $x^4 - 4x^2 + 1 \pmod p$ is reducible for every prime p.
(c)† Prove that every quadratic polynomial of the form $x^4 + ax^2 + b^2$ factors into two quadratics mod p, for every prime p.

Exercise 8.9.4. Prove that if $p \equiv 1 \pmod 4$, then $x^4 + 4$ factors into four linear factors mod p.

Exercise 8.9.5. Let $f(.)$ be the totally multiplicative function for which $f(3) = 1$ and $f(p) = \left(\frac{p}{3}\right)$ if $p \neq 3$.
(a) Give a formula for $f(n)$ for an arbitrary integer n.
(b)† For any given large constant B, suppose that p is a prime for which $(q/p) = f(q)$ for every prime $q \leq B$. Show that there are no three consecutive squares mod p that are all $\leq B$.

This shows that the result in exercise 8.1.8(b) cannot be extended to three consecutive integers provided the hypothesis in (b) holds. This hypothesis will be justified in exercise 8.17.2 of appendix 8D.

Exercise 8.9.6. Show that if $\left(\frac{n}{p}\right) = -1$, then $\sum_{d|n} \left(\frac{d}{p}\right) = 0$.

Exercise 8.9.7. Suppose that a and b are integers and $\{x_n : n \geq 0\}$ is the second-order linear recurrence sequence given by (0.1.2) with $x_0 = 0$ and $x_1 = 1$. Using exercise 0.4.10(b) prove that if odd prime p divides some x_n with n odd, then $(-b/p) = 1$. Deduce that if $(-b/p) = -1$ and p divides x_n, then n is even.

Exercise 8.9.8. (a) Suppose that p^k is an odd prime power. Prove that there are $1 + \left(\frac{a}{p}\right)$ residue classes $b \pmod{p^k}$ for which $b^2 \equiv a \pmod{p^k}$.
(b) Suppose that n is an odd positive integer. Prove that there are $\prod_{p \text{ prime: } p|n} \left(1 + \left(\frac{a}{p}\right)\right)$ residue classes $b \pmod n$ for which $b^2 \equiv a \pmod n$.
(c) Show that this equals $\sum_{d|n} \left(\frac{a}{d}\right)$ where the sum is restricted to squarefree integers d.

Exercise 8.9.9.† Let p be a given odd prime.
(a) Prove that for every $m \pmod p$ there exist a and b mod p such that $a^2 + b^2 \equiv m \pmod p$.
(b) Deduce that there are three squares, not all divisible by p, whose sum is divisible by p.
(c) Generalize this argument to show that if a, b, and c are not divisible by p, then there are at least p solutions $x, y, z \pmod p$ to $ax^2 + by^2 + cz^2 \equiv 0 \pmod p$.

Exercise 8.9.10.† Let m be a squarefree integer $\neq 1$, and let a be an odd positive integer.
(a) Prove that the Jacobi symbol $\left(\frac{4m}{a}\right)$ is a periodic function of a of period dividing $4m$.
(b) Show that the Jacobi symbol $\left(\frac{12}{a}\right)$ has minimal period 12.
(c) Prove that if m is odd and $(a, 2m) = 1$, then $\left(\frac{4m}{a+2m}\right) = \left(\frac{-1}{m}\right)\left(\frac{4m}{a}\right)$.
Now suppose that $m \equiv 3 \pmod 4$.
(d) Prove that there exists an integer r for which $\left(\frac{4m}{r}\right) = -1$.
(e) Prove that $\sum_{a=1}^{4m} \left(\frac{4m}{a}\right) = 0$.

Exercise 8.9.11. (This extends exercise 8.2.4.)
(a) Let $n = pq$ where p and q are distinct primes $\equiv 3 \pmod 4$, and $m = \frac{1}{2}(\frac{p-1}{2} \cdot \frac{q-1}{2} + 1)$. Show that if $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$ and $b \equiv a^m \pmod n$, then $b^2 \equiv a \pmod n$.
(b) Any odd prime p can be written uniquely in the form $p = 1 + 2^k m$ where m is odd and $k \geq 1$. Prove that if a is a 2^kth power mod p and $b \equiv a^{\frac{m+1}{2}} \pmod p$, then $b^2 \equiv a \pmod p$.

If prime $p \equiv 1 \pmod 4$ and $(a/p) = 1$ but a is not a fourth power mod p, then we do not know how to use this idea to find a square root of $a \pmod p$. Known methods in this case are considerably more complicated (see, e.g., [**CP05**]).

Exercise 8.9.12. Suppose that p is a prime $\equiv 3 \pmod 4$ and $\left(\frac{b}{p}\right) = 1$. Prove that there are exactly two solutions $x \pmod p$ to $x^4 \equiv b \pmod p$.

Exercise 8.9.13.† Show that if p is a prime which divides $m^2 - 15$ for some integer m, then either $p = 2$, 3, or 5, or $p \equiv \pm 1, \pm 7, \pm 11$, or $\pm 17 \pmod{60}$.

Exercise 8.9.14.† Show that if p is a prime $\equiv 1 \pmod 4$, then -1 is a fourth power (mod p) if and only if 2 is a square mod p.

Exercise 8.9.15.† If $(a, n) = 1$, then multiplication by $a \pmod n$ generates a permutation of the reduced residues mod n. For example for 3 (mod 7) we get the permutation $\sigma_{3,7} := (1, 3, 2, -1, -3, -2)$, whereas for 2 (mod 7) we get the permutation $\sigma_{2,7} := (1, 2, 4)(3, 6, 5)$. Prove that if p is prime and $(a, p) = 1$, then the signature[6] of the permutation

$$\epsilon(\sigma_{a,p}) = \left(\frac{a}{p}\right).$$

Exercise 8.9.16. (a) Prove that $\left(\frac{2^n-1}{2^m-1}\right) = 0$ if $(m, n) > 1$.

(b) Suppose that $n = mq + r$ where $n \geq m \geq r \geq 2$. Prove that $\left(\frac{2^n-1}{2^m-1}\right) = -\left(\frac{2^m-1}{2^r-1}\right)$.

(c)‡ Prove that if $n/m = [a_0, a_1, \dots, a_k]$ with $(n, m) = 1$ and $a_k \geq 2$, then $\left(\frac{2^n-1}{2^m-1}\right) = (-1)^{k+1}$.

Infinitely many primes.

Exercise 8.9.17.† Fix odd, squarefree integer $n > 1$. Prove that there are infinitely many primes p for which $(p/n) = -1$.

Exercise 8.9.18.† Let n be a squarefree integer.

(a) By considering the prime divisors of $m^2 - n$, for well-chosen values of m, prove that there are infinitely many primes p for which $(n/p) = 1$.
(b) Deduce that there are infinitely many primes $\equiv 1 \pmod 3$.
(c) Refine this to deduce that there are infinitely many primes $\equiv 7 \pmod{12}$.
(d) Prove that there are infinitely many primes $\equiv 11 \pmod{12}$.
(e) Prove that there are infinitely many primes $\equiv 5 \pmod 8$.
(f) Prove that there are infinitely many primes $\equiv 7 \pmod 8$.
(g) Prove that there are infinitely many primes $\equiv 3 \pmod 8$.
(h) Prove that there are infinitely many primes $\equiv 5 \pmod{12}$.

Exercise 8.9.19.† Fix odd, squarefree integer $n > 1$. Using exercises 8.9.18(a) and 8.7.7 prove that there are infinitely many primes p for which $(p/n) = 1$.

In Ram Murty's undergraduate thesis (1976, Carleton University, Ottawa) he defined a *Euclidean proof* that there are infinitely many primes $\equiv a \pmod q$ to be one in which we use a polynomial all of whose prime divisors either divide q or are $\equiv 1$ or $a \pmod q$. Several of the proofs for the different arithmetic progressions in the last three questions can be formulated in this way. We gave such a proof for $a = 1$ in Theorem 7.8. Murty went on to show that there is a Euclidean proof that there are infinitely many primes $\equiv a \pmod q$ if and only if $a^2 \equiv 1 \pmod q$ (as in all our examples here). To prove that there are infinitely many primes $\equiv 2$ or $\equiv 3 \pmod 5$, or $5 \pmod 7$, etc., we will have to develop other techniques.

[6] Any permutation can be described by a sequence of transpositions (swaps) of pairs of elements. Although the sequence, and even the number of swaps in such a sequence is not unique, the parity of the number of swaps is. This is called the *signature* of the permutation and is given by -1 or 1 (for an odd or even number of transpositions, respectively).

Further reading on Euclidean proofs

[1] M. Ram Murty and N. Thain, *Primes in certain arithmetic progressions*, Funct. Approx. Comment. Math. **35** (2006), 249–259.

Primitive roots for specially chosen primes.

Exercise 8.9.20.† Suppose that q and $p = 2q + 1$ are odd (Sophie Germain twin) primes.
(a) Show that if $p \equiv 3 \pmod 8$, then 2 is a primitive root mod p (e.g., 11, 59, 83, 107, ...).
(b) Show that if $p \equiv 7 \pmod 8$, then -2 is a primitive root mod p.
(c) Prove that -3 is a primitive root mod p, but 3 is not.

Exercise 8.9.21.† Suppose that q and $p = 4q + 1$ are odd primes. Prove that 2, -2, 3, and -3 are all primitive roots mod p.

Exercise 8.9.22.† Suppose that the Fermat number $F_m = 2^{2^m} + 1$ is prime with $m \geq 1$. Prove that if $(q/F_m) = -1$, then q is a primitive root mod F_m. (We deduce that 3 and 5 (for $m > 1$) are primitive roots mod F_m by exercise 8.5.4.)

Alternate proofs of the value of $(2/n)$.

Exercise 8.9.23. Let p be a prime $\equiv 1 \pmod 4$ so that there exists a reduced residue $r \pmod p$ such that $r^2 \equiv -1 \pmod p$.
(a) By expanding $(r + 1)^2 \pmod p$ prove that 2 is a square mod p if and only if r is a square mod p.
(b) Prove that r is a square mod p if and only if there is an element of order 8 mod p.
(c) Use Theorem 7.6 to deduce that 2 is a square mod p if and only if $p \equiv 1 \pmod 8$.

Exercise 8.9.24 (Proof of (8.7.2))**.** By induction on odd $n \geq 1$. By the law of quadratic reciprocity, as stated in (8.7.3), we have

$$\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{n-2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{n}{n-2}\right) = \left(\frac{-1}{n}\right)\left(\frac{2}{n-2}\right),$$

as one of n and $n - 2$ is $\equiv 1 \pmod 4$. Complete the proof.

Exercise 8.9.25. Every odd prime p may be written in the form $p = 4k + \sigma$ with $\sigma = \left(\frac{-1}{p}\right)$. We will show that $\left(\frac{2}{p}\right) = (-1)^k$ which implies Theorem 8.4. Let $m = 2k + \sigma$ so that $2m = p + \sigma$. Verify that

$$\left(\frac{2\sigma}{p}\right) = \left(\frac{2p+2\sigma}{p}\right) = \left(\frac{4m}{p}\right) = \left(\frac{m}{p}\right) = \left(\frac{\sigma p}{m}\right) = \left(\frac{2\sigma m - 1}{m}\right) = \left(\frac{-1}{m}\right)$$

and deduce the result from here.

Further proofs of the law of quadratic reciprocity.

Exercise 8.9.26.† (a) In the mid-18th century, Euler conjectured that if $m > n$ are coprime, odd, positive integers, then $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$ where $m - n = 4a$ if $m \equiv n \pmod 4$, and $m + n = 4a$ otherwise. Use the law of quadratic reciprocity to prove Euler's conjecture.
(b) Use Euler's conjecture to prove (8.7.3), the law of quadratic reciprocity.

Scholze (1938) proved Euler's conjecture using Gauss's Lemma (Theorem 8.6) and so gave a different proof of the law of quadratic reciprocity.

Exercise 8.9.27.‡ Finally we present my own variation of Rousseau's proof of quadratic recipocity, as a series of (challenging) exercises. Let $p < q$ be odd primes, and let $n = pq$. Let $A = \prod_{1 \leq m < n/2,\ (m,n)=1} m$. In the proof given of Theorem 8.5 in section 8.6, we showed that $A \equiv \left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) \pmod p$ and, analogously, $A \equiv \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right) \pmod q$. We now evaluate $A \pmod n$ much as in Gauss's proof of Wilson's Theorem, where we paired up each residue with its inverse: Let S be the set of (unordered) pairs $\{a, b\} \in [1, \frac{n}{2})$ for which $ab \equiv 1$ or $-1 \pmod n$.

(a) Prove that the residues a and b are distinct unless $a^2 \equiv 1$ or $-1 \pmod{n}$.
(b) Prove that if $a^2 \equiv 1 \pmod{n}$, then $a \equiv 1, -1, r$, and $-r \pmod{n}$ for some $r \not\equiv \pm 1 \pmod{n}$.
(c) Prove that the product of the integers $a \in [1, \frac{n}{2})$ with $a^2 \equiv 1 \pmod{n}$ is $\equiv \pm r \pmod{n}$.
(d) Prove that if $b^2 \equiv -1 \pmod{n}$, then $p \equiv q \equiv 1 \pmod{4}$. In this case:
- Deduce that the product of the integers $b \in [1, \frac{n}{2})$ for which $b^2 \equiv -1 \pmod{n}$ is $\equiv \pm r \pmod{n}$.
- Deduce that $A \equiv \pm 1 \pmod{n}$.
- Combine the above to show that $\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right)$.

(e) If at least one of p and q is $\equiv 3 \pmod{4}$:
- Deduce that $A \equiv \pm r \pmod{n}$.
- Combine the above to show that $\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) = -\left(\frac{-1}{p}\right)\left(\frac{p}{q}\right)$.

(f) Deduce Theorem 8.5.

Appendix 8A. Eisenstein's proof of quadratic reciprocity

8.10. Eisenstein's elegant proof, 1844

A lemma of Gauss gives a complicated but useful formula to determine (a/p):

Theorem 8.6 (Gauss's Lemma)**.** *Given an integer a which is not divisible by odd prime p, define r_n to be the absolutely least residue of $an \pmod p$, and then define the set $\mathcal{N} := \{1 \le n \le \frac{p-1}{2} : \ r_n < 0\}$. Then $\left(\frac{a}{p}\right) = (-1)^{|\mathcal{N}|}$.*

For example, if $a = 3$ and $p = 7$, then $r_1 = 3, r_2 = -1, r_3 = 2$ so that $\mathcal{N} = \{2\}$ and therefore $\left(\frac{3}{7}\right) = (-1)^1 = -1$.

Proof. For each $m, 1 \le m \le \frac{p-1}{2}$, there is exactly one integer n, $1 \le n \le \frac{p-1}{2}$, such that $r_n = m$ or $-m \pmod p$ (for if $an \equiv \pm an' \pmod p$, then $p|a(n \mp n')$, and so $p|n \mp n'$, which is possible in this range only if $n = n'$). Therefore

$$\left(\frac{p-1}{2}\right)! = \prod_{1\le m\le \frac{p-1}{2}} m = \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n\notin\mathcal{N}}} r_n \cdot \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n\in\mathcal{N}}} (-r_n)$$

$$\equiv \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n\notin\mathcal{N}}} (an) \cdot \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n\in\mathcal{N}}} (-an) = a^{\frac{p-1}{2}}(-1)^{|\mathcal{N}|} \cdot \left(\frac{p-1}{2}\right)! \pmod p.$$

Cancelling out the $\left(\frac{p-1}{2}\right)!$ from both sides, the result follows from Euler's criterion. □

This proof is a clever generalization of the proof of Theorem 8.4.

Exercise 8.10.1.† Use Gauss's Lemma to determine the values of (a) $(-1/p)$ and of (b) $(3/p)$, for all primes $p > 3$.

Exercise 8.10.2.† Let r be the absolutely least residue of $N \pmod p$. Prove that the least non-negative residue of $N \pmod p$ is given by

$$N - p\left[\frac{N}{p}\right] = \begin{cases} r & \text{if } r \geq 0, \\ p + r & \text{if } r < 0. \end{cases}$$

Corollary 8.10.1. *If p is a prime > 2 and a is an odd integer not divisible by p, then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left[\frac{an}{p}\right]}. \tag{8.10.1}$$

Proof. (Gauss) By exercise 8.10.2 we have

$$\sum_{n=1}^{\frac{p-1}{2}} \left(an - p\left[\frac{an}{p}\right]\right) = \sum_{\substack{n=1 \\ n \notin \mathcal{N}}}^{\frac{p-1}{2}} r_n + \sum_{\substack{n=1 \\ n \in \mathcal{N}}}^{\frac{p-1}{2}} (p + r_n) = \sum_{n=1}^{\frac{p-1}{2}} r_n + p|\mathcal{N}|. \tag{8.10.2}$$

In the proof of Gauss's Lemma we saw that for each $m, 1 \leq m \leq \frac{p-1}{2}$, there is exactly one integer n, $1 \leq n \leq \frac{p-1}{2}$, such that $r_n = m$ or $-m$, and so $r_n \equiv m \pmod 2$. Therefore, as a and p are odd, (8.10.2) implies that

$$|\mathcal{N}| \equiv \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{an}{p}\right] \pmod 2 \quad \text{as} \quad \sum_{n=1}^{\frac{p-1}{2}} r_n \equiv \sum_{m=1}^{\frac{p-1}{2}} m \equiv a \sum_{n=1}^{\frac{p-1}{2}} n \pmod 2.$$

We now deduce (8.10.1) from Gauss's Lemma. □

The exponent $\sum_{n=1}^{\frac{p-1}{2}} \left[\frac{an}{p}\right]$ on the right-hand side of (8.10.1) looks excessively complicated. However it arises in a different context that is easier to work with:

Lemma 8.10.1. *Suppose that a and b are odd, coprime positive integers. There are*

$$\sum_{n=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right]$$

lattice points $(n, m) \in \mathbb{Z}^2$ for which $bm < an$ with $0 < n < b/2$.

Proof. We seek the number of lattice points (n, m) inside the triangle bounded by the lines $y = 0$, $x = \frac{b}{2}$, and $by = ax$. For such a lattice point, n can be any

integer in the range $1 \le n \le \frac{b-1}{2}$. For a given value of n, the triangle contains the lattice points (n, m) where m is any integer in the range $0 < m < \frac{an}{b}$. These are the lattice points in the shaded rectangle in Figure 8.1.

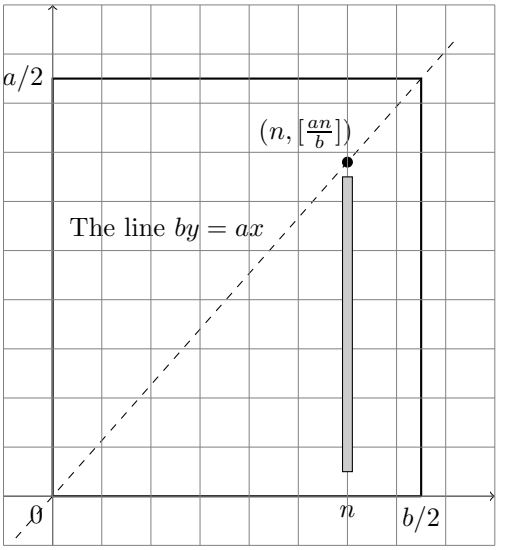


Figure 8.1. The shaded rectangle covers the lattice points (n, m) with $1 \le m \le [\frac{an}{b}]$.

Evidently m ranges from 1 to $[\frac{an}{b}]$, and so there are $[\frac{an}{b}]$ such lattice points. Summing this up over the possible values of n gives the lemma. □

Corollary 8.10.2. *If a and b are odd coprime positive integers, then*

$$\sum_{n=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right] + \sum_{m=1}^{\frac{a-1}{2}} \left[\frac{bm}{a}\right] = \frac{(a-1)(b-1)}{2}.$$

Proof. The idea is to split the triangle

$$R := \left\{(x, y) : \ 0 < x < \frac{b}{2} \text{ and } 0 < y < \frac{a}{2}\right\}$$

into two parts: the points in R on or below the line $by = ax$, that is, in the region

$$A := \{(x, y) : \ 0 < x < b/2 \text{ and } 0 < y \le ax/b\};$$

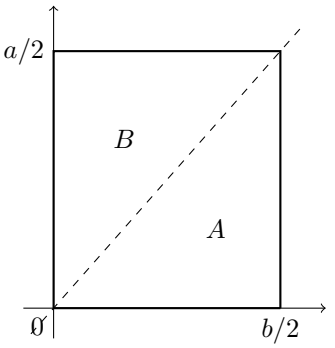


Figure 8.2. Splitting the rectangle R into two parts.

and the points in R above the line $by = ax$, that is, in the region

$$B := \{(x, y) : \ 0 < x < by/a \text{ and } 0 < y < a/2\}.$$

We count the lattice points (that is, the points with integer coordinates) in R and then in A and B together. To begin with

$$R \cap \mathbb{Z}^2 = \left\{(n, m) \in \mathbb{Z}^2 : \ 1 \le n \le \frac{b-1}{2} \text{ and } 1 \le m \le \frac{a-1}{2}\right\},$$

so that $|R \cap \mathbb{Z}^2| = \frac{a-1}{2} \cdot \frac{b-1}{2}$.

Since there are no lattice points in R on the line $by = ax$, as $(a, b) = 1$, therefore

$$A \cap \mathbb{Z}^2 = \left\{(n, m) \in \mathbb{Z}^2 : \ 0 < n < b/2 \text{ and } bm < an\right\},$$

and so $|A \cap \mathbb{Z}^2| = \sum_{n=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right]$ by Lemma 8.10.1. Similarly

$$B \cap \mathbb{Z}^2 = \left\{(n, m) \in \mathbb{Z}^2 : \ 0 < m < a/2 \text{ and } an < bm\right\},$$

and so $|B \cap \mathbb{Z}^2| = \sum_{m=1}^{\frac{a-1}{2}} \left[\frac{bm}{a}\right]$ by Lemma 8.10.1 (with the roles of a and b interchanged). The result then follows from the observation that $A \cap \mathbb{Z}^2$ and $B \cap \mathbb{Z}^2$ partition $R \cap \mathbb{Z}^2$. □

Eisenstein's proof of the law of quadratic reciprocity. By Corollary 8.10.1 with $a = q$, and then with the roles of p and q reversed, and then by Corollary 8.10.2, we deduce the desired law of quadratic reciprocity:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}}\left[\frac{qn}{p}\right]} \cdot (-1)^{\sum_{m=1}^{\frac{q-1}{2}}\left[\frac{pm}{q}\right]} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \qquad \square$$

Appendices. The extended version of chapter 8 has the following additional appendices:

Appendix 8B. *Small quadratic non-residues.* For a given prime p we show that there are small integers m and n for which $\left(\frac{m}{p}\right) = 1$ and $\left(\frac{n}{p}\right) = -1$, and we discuss some of the latest developments in bounding m and n.

Appendix 8C. *The first proof of quadratic reciprocity* presents Gauss's original proof of quadratic reciprocity. It is a wonderfully ingenious use of solutions to quadratic equations, though a little more complicated than the proofs already presented.

Appendix 8D. *Dirichlet characters and primes in arithmetic progressions.* Here we present the vitally important generalization of the Legendre and Jacobi symbols to Dirichlet characters. To determine all of the characters themselves requires a neat theory. We then indicate how these were applied by Dirichlet to prove that there are infinitely many primes in any arithmetic progression $a \pmod q$ with $(a, q) = 1$.

Appendix 8E. *Quadratic reciprocity and recurrence sequences.* We study the p divisbility of second-order linear recurrence sequences, which depends on the values of certain Legendre symbols.

Chapter 9

Quadratic equations

Can we tell whether a given large integer is the sum of two squares of integers (other than by summing every possible pair of smaller squares)? How about the values of other quadratics? We will show, in this chapter, how we can understand a lot about solutions to quadratic equations in integers, by understanding the solutions to those quadratic equations modulo p, for every prime p. We begin by studying the values taken by $x^2 + y^2$ when we substitute integers in for x and y, then $ax^2 + by^2$ for arbitrary integer coefficients a, b, and then finally the general *binary quadratic form*, $ax^2 + bxy + cy^2$.

9.1. Sums of two squares

The list of integers that are the sum of two squares of integers begins:

$$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, \ldots.$$

Is there a pattern? Can we easily determine whether a given integer is the sum of two squares by any means other than trying to find two squares that sum to it? No pattern emerges easily from the list above so we begin focusing on the primes that appear in this list, namely

$$2 = 1^2+1^2,\ 5 = 1^2+2^2,\ 13 = 2^2+3^2,\ 17 = 1^2+4^2,\ 29 = 5^2+2^2,\ 37 = 1^2+6^2, \ldots.$$

What do the odd primes in the list, $5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, \ldots$ have in common? The only easy-to-spot pattern is that the differences between consecutive odd primes in our list, $13-5, 17-13, 29-17, \ldots$ are all multiples of 4, which implies that they are *all* $\equiv 1 \pmod 4$.

Proposition 9.1.1. *If p is an odd prime that is the sum of two squares, then $p \equiv 1 \pmod 4$.*

Proof. If $p = a^2+b^2$, then $p \nmid a$, or else $p|p-a^2 = b^2$ so that $p|b$ and $p^2|a^2+b^2 = p$, which is impossible. Similarly $p \nmid b$. Now $a^2 \equiv -b^2 \pmod p$ so that

$$1 = \left(\frac{a}{p}\right)^2 = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right)^2 = \left(\frac{-1}{p}\right),$$

and therefore $p \equiv 1 \pmod 4$ by Theorem 8.3. □

Exercise 9.1.1. Prove that any odd integer n that can be written as the sum of two squares must be $\equiv 1 \pmod 4$. Deduce Proposition 9.1.1.

Exercise 9.1.2. Prove that if prime p divides $a^2 + b^2$, then either $p = 2$ or p divides (a, b) or $p \equiv 1 \pmod 4$.

Remarkably this is an "if and only if " condition:

Theorem 9.1. *Every prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares (of integers).*

Proof. Since $p \equiv 1 \pmod 4$ we know that there exists an integer b such that $b^2 \equiv -1 \pmod p$. Consider now the set of integers

$$\{j + kb : \ 0 \le j, k \le [\sqrt{p}]\}.$$

The number of pairs of integers j, k used in the construction of this set is $([\sqrt{p}] + 1)^2 > p$, and so by the pigeonhole principle, two of the numbers in the set must be congruent mod p; say that

$$j + kb \equiv J + Kb \pmod p$$

where $0 \le j, k, J, K \le [\sqrt{p}]$ and $\{j, k\} \ne \{J, K\}$. Let $r = j - J$ and $s = K - k$ so that

$$r \equiv bs \pmod p$$

where $|r|, |s| \le [\sqrt{p}] < \sqrt{p}$ and r and s are not both 0. Now

$$r^2 + s^2 \equiv (bs)^2 + s^2 = s^2(b^2 + 1) \equiv 0 \pmod p,$$

and $0 < r^2 + s^2 < \sqrt{p}^2 + \sqrt{p}^2 = 2p$. The only multiple of p between 0 and $2p$ is p, and therefore $r^2 + s^2 = p$. □

We will use the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{9.1.1}$$

to determine which composite integers can be written as the sum of two squares. Theorem 9.1 tells us that any prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares; for example $5 = 1^2 + 2^2$ and $13 = 2^2 + 3^2$. Then (9.1.1) yields that $65 = 4^2 + 7^2$; if we write instead $13 = 3^2 + 2^2$, then we obtain $65 = 1^2 + 8^2$. Indeed any integer that is the product of two distinct primes $\equiv 1 \pmod 4$ can be written as the sum of two squares like this, and even in two different ways. We will discuss the number of representations further in appendix 9C.

Exercise 9.1.3. Find four distinct representations of $1105 = 5 \times 13 \times 17$ as a sum of two squares.

Exercise 9.1.4. Prove that if $n = n_1 \cdots n_k$ where $n_1, \dots, n_k$ are each the sum of two squares, then n is the sum of two squares.

Theorem 9.2. *Positive integer n can be written as the sum of two squares of integers if and only if for every prime $p \equiv 3 \pmod 4$ which divides n, the exact power of p dividing n is even.*

Proof. Suppose that $n = a^2+b^2$ where $g = (a,b)$, so we can write $a = gA$, $b = gB$, and $n = g^2N$ for some coprime integers A and B, with $N = A^2 + B^2$. Therefore if p is a prime $\equiv 3 \pmod 4$, then p cannot divide N, by exercise 9.1.2; and so if $p|n$, then $p|g$. Moreover if $p^k \| g$, then $p^{2k} \| n$, as claimed.

On the other hand, if $n = g^2m$ where m is squarefree, then m has no prime factors $\equiv 3 \pmod 4$ by the hypothesis. Therefore all the prime factors of m can be written as the sum of two squares by Theorem 9.1, and so their product, m, is the sum of two squares by exercise 9.1.4, say $m = u^2+v^2$. Then $n = (gu)^2+(gv)^2$. □

Exercise 9.1.5. Prove that if n is squarefree and is the sum of two squares, then every positive divisor of n is also the sum of two squares.

We saw that (9.1.1) is a useful identity. To find such an identity let i be a complex number for which $i^2 = -1$. Then $x^2+y^2 = (x+iy)(x-iy)$, a factorization into numbers of the form $a + bi$ where a and b are integers. Therefore

$$\begin{aligned}(a^2+b^2)\cdot(c^2+d^2) &= (a+bi)(a-bi) \cdot (c+di)(c-di)\\ &= (a+bi)(c+di) \cdot (a-bi)(c-di)\\ &= ((ac-bd)+(ad+bc)i)\cdot((ac-bd)-(ad+bc)i)\\ &= (ac-bd)^2+(ad+bc)^2,\end{aligned}$$

and so we get (9.1.1). A different rearrangement leads to a different identity:

$$(9.1.2)\quad (a^2+b^2)(c^2+d^2) = (a+bi)(c-di)\cdot(a-bi)(c+di) = (ac+bd)^2+(ad-bc)^2.$$

Theorem 9.2 has the following surprising corollary:

Exercise 9.1.6. Deduce that positive integer n can be written as the sum of two squares of *rationals* if and only if n can be written as the sum of two squares of integers.

This suggests that we can focus, in this question, on rational solutions. In section 6.1 we saw how to find all solutions to $x^2 + y^2 = 1$ in rationals x, y. How about all rational solutions to $x^2 + y^2 = n$?

Proposition 9.1.2. *Suppose that $n = a^2 + b^2$. Then all solutions in rationals x, y to $x^2 + y^2 = n$ are given by the parametrization*

$$(9.1.3)\qquad x = \frac{2brs + a(r^2-s^2)}{r^2+s^2},\quad y = \frac{2ars + b(s^2-r^2)}{r^2+s^2},$$

where r and s are coprime integers.

Proof. Let x, y be any rationals for which $x^2 + y^2 = n$. Just as in our geometric proof of (6.1.1) we will parametrize these rational points (x, y) by noting that if t is the slope of the line between (a, b) and (x, y), then t is rational, and vice versa. In particular we let $u = x - a$ and $t = (y - b)/u$ when $u \neq 0$, which must both be rational numbers. Then

$$0 = n - n = (a+u)^2 + (b+tu)^2 - (a^2+b^2) = 2u(a+bt) + u^2(1+t^2),$$

so that, as $u \neq 0$, we have

$$u = \frac{-2(a+bt)}{1+t^2} = \frac{2brs - 2as^2}{r^2+s^2}$$

writing the rational number t as $t = -r/s$ where r and s are coprime integers. Substituting this value of u into $x = a + u$ and $y = b + ut$ gives the claimed parametrization.

If $u = 0$, then $x = a$ so that either $y = b$ or $y = -b$. The line between (a, b) and $(a, -b)$ is the vertical line $x = a$ (corresponding to $r = 1, s = 0$ so that $t = \infty$).

Finally we obtain the initial point (a, b) in this parametrization by taking $r = a, s = b$. This is obtained by taking the slope to be $t = -a/b$, the slope of the tangent line to the curve $x^2 + y^2 = n$ at the point (a, b). □

In Theorem 9.1 we saw that every prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares. Examples suggest that there is a unique such representation, up to signs and changing the order of the squares, as the reader will now prove:

Exercise 9.1.7.† Suppose that prime $p = a^2 + b^2$.

(a) Prove that $|a|, |b| < \sqrt{p}$.
(b) Prove that if $r^2 \equiv -1 \pmod p$, then either $r \equiv a/b \pmod p$ or $r \equiv b/a \pmod p$.
(c) If prime p divides $c^2 + d^2$ but $p \nmid cd$, show that p divides either $ac - bd$ or $ad - bc$, and deduce that p divides both terms on the right-hand side of either (9.1.1) or (9.1.2), respectively.
(d) Suppose that $p = a^2 + b^2 = c^2 + d^2$ where $a, b, c, d > 0$. Show that $\{a, b\} = \{c, d\}$.

In other words, we have proved that each prime $\equiv 1 \pmod 4$ has a unique representation as the sum of two squares, unique up to changing the order of the squares, or their signs.

Exercise 9.1.8.† Prove, using the method of Theorem 9.1, that a squarefree integer n can be written as the sum of two squares if and only if -1 is a square mod n.

9.2. The values of $x^2 + dy^2$

What values does $x^2 + 2y^2$ take? Let's start again with the prime values:

$$2, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, \ldots.$$

There is no obvious pattern; *but* this list contains exactly the same odd primes that we found in section 8.4 when exploring when $\left(\frac{-2}{p}\right) = 1$. This link is no coincldence for if we suppose that odd prime $p = x^2 + 2y^2$, then p does not divide x or y and so

$$1 = \left(\frac{x}{p}\right)^2 = \left(\frac{x^2}{p}\right) = \left(\frac{-2y^2}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{y}{p}\right)^2 = \left(\frac{-2}{p}\right).$$

From (8.7.1) and (8.7.2), we know that $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1$ or $3 \pmod 8$.

On the other hand if $(-2/p) = 1$, then select $b \pmod p$ such that $b^2 \equiv -2 \pmod p$. We take $R = 2^{1/4}\sqrt{p}$, $S = 2^{-1/4}\sqrt{p}$ in exercise 9.7.3, so that there exist integers r and s, not both 0, with $|r| \leq R$ and $|s| \leq S$, for which p divides $r^2 + 2s^2$. Therefore $0 < r^2 + 2s^2 \leq 2^{3/2}p < 3p$, and so $r^2 + 2s^2 = p$ or $2p$. In the latter case, 2 divides $2p - 2s^2 = r^2$ so that $2|r$. Writing $r = 2R$ we have $s^2 + 2R^2 = p$. Hence, either way, p can be written in the form $m^2 + 2n^2$. Therefore we have proved:

Theorem 9.3. *Odd prime p can be written in the form $m^2 + 2n^2$ if and only if $p \equiv 1$ or $3 \pmod 8$.*

The identity

$$(a^2 + 2b^2)(c^2 + 2d^2) = (ac + 2bd)^2 + 2(ad - bc)^2$$

is analogous to (9.1.1). Using this, one can prove, analogous to the proof for u^2+v^2 in the first half of section 9.1, that positive integer n can be written as $r^2 + 2s^2$ if and only if for every prime $p \equiv 5$ or $7 \pmod 8$ which divides n, the exact power of p dividing n is even.

Can we also modify this proof for values of x^2+3y^2? Or x^2+5y^2? We explore this in the following exercises.

Exercise 9.2.1. Fix integer $d \geq 1$. Give an identity showing that the product of two integers of the form $a^2 + db^2$ is also of this form.

Exercise 9.2.2. Which primes are of the form $a^2 + 3b^2$? Which integers?

Exercise 9.2.3. Which primes are of the form $a^2 + 5b^2$? Try listing what primes are represented and compare the list with the set of primes p for which $(-5/p) = 1$.

9.3. Is there a solution to a given quadratic equation?

It is easy to see that there do not exist non-zero integers a, b, c such that $a^2 + 5b^2 = 3c^2$, for, if we take the smallest non-zero solution, then we have

$$a^2 \equiv 3c^2 \pmod 5$$

which implies that $a \equiv c \equiv 0 \pmod 5$ since $(3/5) = -1$, and so $b \equiv 0 \pmod 5$. Therefore $a/5, b/5, c/5$ gives a smaller solution to $x^2 + 5y^2 = 3z^2$, contradicting minimality.

Another proof stems from looking at the equation mod 4 since then $a^2+b^2+c^2 \equiv 0 \pmod 4$, and 0 and 1 are the only squares mod 4. Therefore if three squares sum to an integer that is $0 \pmod 4$, then they must all be even. But then $a/2, b/2, c/2$ gives a smaller solution, contradicting minimality.

So we have now presented two different proofs that there are no non-zero solutions in integers to $a^2 + 5b^2 = 3c^2$, by working with two different moduli.

For all quadratic equations in three or more variables with real solutions, there is never just one prime or prime power modulo which there are no solutions to the given equation—when there is one, there is always a second. And indeed when there is a third proof, then there is always a fourth. A remarkable consequence of the theory (see appendix 9B) is that if a given quadratic equation in three or more variables has non-zero real solutions but no non-zero integer solutions, then there are always exactly *an even number of different primes* p such that the given equation has no non-trivial solutions mod p^k for some $k \geq 1$. Moreover the odd primes involved must divide the coefficients of the equation. On the other hand, if there are no such "mod p^k obstructions", then there must be at least one non-zero integer solution (implying that there must be a real solution!).

In exercise 3.6.4 we proved that there are integer solutions (m, n) to $am+bn = c$ if and only if there are solutions $u, v \pmod b$ to $au + bv \equiv c \pmod b$. Similarly we will show that if a, b, and c are pairwise coprime, positive integers, then there are rational solutions (x, y) to $ax^2 + by^2 = c$ if and only if there are coprime solutions $u, v \pmod{4abc}$ to $au^2 + bv^2 \equiv c \pmod{4abc}$. This is an amazing theorem since

to determine whether a quadratic equation has solutions in rationals we need only verify whether it has solutions modulo a finite modulus.

To work on rational solutions (x, y) to $ax^2 + by^2 = c$ it is convenient to develop this into a question about integer solutions and to manipulate the equation to a more convenient form:

(i) We may assume that each of a, b, c is a squarefree integer or else, if, say, $a = p^2A$, the rational solutions to $ax^2 + by^2 = c$ are in 1-to-1 correspondence with those of $AX^2 + by^2 = c$, taking $X = px$. If b is divisible by a square, we proceed analogously. If $c = q^2C$, then the rational solutions to $ax^2 + by^2 = c$ are in 1-to-1 correspondence with those of $aX^2 + bY^2 = C$, taking $X = x/q$ and $Y = y/q$.

(ii) We may assume that a, b, c are pairwise coprime or else if, say, $a = pA$ and $b = pB$, then $AX^2 + BY^2 = C$ with $X = px$, $Y = py$, and $C = pc$; and if $a = qA$ and $c = qC$, then $Ax^2 + BY^2 = C$ with $B = bq$ and $Y = y/q$.

(iii) Letting n be the lowest common denominator of the rationals x and y, we write $x = \ell/n$ with $y = m/n$ so that ℓ, m, n are integers with $(\ell, m, n) = 1$ and $a\ell^2 + bm^2 = cn^2$.

(iv) We may assume that $a\ell^2, bm^2, cn^2$ are pairwise coprime. If not, suppose that prime p divides $a\ell^2$ and bm^2, so that p divides $a\ell^2 + bm^2 = cn^2$. Now p can only divide one of a, b, c (since they are pairwise coprime), say, c, and so must divide ℓ^2 and m^2. But then p divides ℓ and m, and so p^2 divides $a\ell^2 + bm^2 = cn^2$. Hence p divides n, as $p^2 \nmid c$, contradicting that $(\ell, m, n) = 1$.

Therefore the correct formulation of our result is as follows:

Theorem 9.4 (The local-global principle for quadratic equations)**.** *Let a, b, and c be given pairwise coprime, squarefree integers. There are solutions in*

Non-zero integers ℓ, m, n to $a\ell^2 + bm^2 + cn^2 = 0$ with $(a\ell^2, bm^2) = 1$

if and only if *there are solutions in*

Non-zero real numbers λ, μ, ν to $a\lambda^2 + b\mu^2 + c\nu^2 = 0$,

and*, for all positive integers r, there exist*

Residue classes $u, v, w \pmod r$ for which $au^2 + bv^2 + cw^2 \equiv 0 \pmod r$,

with $(au^2, bv^2, cw^2, r) = 1$.

Proof $\Longrightarrow$: We may take $\lambda = u = \ell,\ \mu = v = m,\ \nu = w = n$ throughout. □

The proof in the other direction is the difficult part; it follows along the lines of the proof of Theorem 9.1 but is more complicated. In appendix 9a we rephrase that proof in the language of lattices, before completing the proof of the local-global principle.

We can reduce the set of moduli to be considered using the following lemma.

Lemma 9.3.1. *Let a, b, c be given pairwise coprime, squarefree integers. There are residue classes $u, v, w \pmod r$ with $(au^2, bv^2, cw^2, r) = 1$ for which*

$$au^2 + bv^2 + cw^2 \equiv 0 \pmod r$$

for every positive integer r, if and only if there are such solutions for $r = 8$, and for $r = p$ for every odd prime p dividing abc.

This result implies that, as in exercise 3.6.4, we can restrict our attention in Theorem 9.4 to just one modulus, namely $r = 8|abc|$.

Proof. We can restrict our attention to prime power moduli p^k by the Chinese Reminder Theorem. We will prove that there are such appropriate solutions mod p^k by induction on k: for $k \geq 1$ when p is odd and for $k \geq 3$ when $p = 2$. There are appropriate solutions modulo every odd prime p and modulo 2^3, by the hypothesis for primes p dividing $2abc$, and by exercise 8.9.9 for all odd primes p that do not divide abc.

So now assume we have an appropriate solution mod p^k, so that p does not divide at least one of au^2, bv^2, cw^2, say, au^2 (and an analogous argument works if p does not divide one of the others). Let $R = -a^{-1}(bv^2 + cw^2)$, so that $u^2 \equiv R \pmod{p^k}$ by the induction hypothesis. By Proposition 8.8.1 there exists $U \pmod{p^{k+1}}$ for which $U^2 \equiv R \pmod{p^{k+1}}$ so that $aU^2 + bv^2 + cw^2 \equiv 0 \pmod{p^{k+1}}$ and $(U, p) = 1$. □

Now if $au^2 + bv^2 + cw^2 \equiv 0 \pmod{a}$ with $(a, bv^2, cw^2) = 1$, then $-bc \equiv (cw/v)^2 \pmod{a}$; that is, $-bc$ is a square (mod p) for every prime dividing a. Making similar remarks modulo b and c, we find Legendre's formulation of the local-global principle.[1]

Theorem 9.5 (Legendre's local-global principle, 1785)**.** *Let a, b, c be given pairwise coprime, squarefree integers which do not all have the same sign. There are solutions in non-zero integers ℓ, m, n to $a\ell^2 + bm^2 + cn^2 = 0$* if and only if *$-ab$ is a square* mod $|c|$, *$-ac$ is a square* mod $|b|$, *and $-bc$ is a square* mod $|a|$.

Note that $a\ell^2 + bm^2 + cn^2 = 0$ has solutions in non-zero reals if and only if a, b, c do not all have the same sign.

This principle may be extended to the rational solutions of more or less any quadratic equation: Any quadratic polynomial in n variables can be *diagonalized*; that is, a linear change of variables can change the polynomial into a diagonal quadratic polynomial. We know that in the example $g = ax^2 + bxy + cy^2$ we can let $X = x + by/2a$ and then $g = aX^2 + Dy^2$ where $D = -(b^2 - 4ac)/4a$. In a three-variable example we take the polynomial

$$f = x^2 + 2xy + 3xz + 4y^2 + 5yz + 6z^2 + 7x + 8y + 9z + 10;$$

we let $X = x + y + \frac{3}{2}z + \frac{7}{2}$ replace x to obtain $f = X^2 + 3y^2 + 2yz + \frac{15}{4}z^2 + y - \frac{3}{2}z - \frac{9}{4}$. Then letting $Y = y + \frac{z}{3} + \frac{1}{6}$ we obtain $f = X^2 + 3Y^2 + \frac{41}{12}z^2 - \frac{11}{6}z - \frac{7}{3}$, and if $z = 6Z + \frac{11}{41}$, this becomes

$$F = X^2 + 3Y^2 + 123Z^2 - \frac{423}{164},$$

[1] The careful reader will note that we do not seem to have made adequate remarks about the solution modulo powers of 2. However, we noted earlier in this section that if there are solutions in the reals and modulo all but one prime, then there is a solution modulo all powers of this last prime. For more details see appendix 9B.

a diagonal quadratic with no "cross terms" (like XY). Notice that the rational solutions to $F(X,Y,Z)=0$ are in 1-to-1 correspondence with the rational solutions to $f(x,y,z)=0$.

Whether or not a given diagonal quadratic with three or more terms has rational solutions can then be resolved by the local-global principle.[2]

Exercise 9.3.1. Given one integer solution to $ax_0^2+by_0^2+cz_0^2=0$, show that all other integer solutions to $ax^2+by^2+cz^2=0$ are given by the parametrization

$$x:y:z \;=\; (ar^2-bs^2)x_0+2brsy_0 \;:\; 2arsx_0-(ar^2-bs^2)y_0 \;:\; (ar^2+bs^2)z_0\ .$$

9.4. Representation of integers by ax^2+by^2 with x,y rational, and beyond

Coprime integer solutions to $au^2+bv^2=cw^2$ with $w>0$ are in 1-to-1 correspondence with the rational solutions to $ax^2+by^2=c$, by taking $x=u/w$ and $y=v/w$. Therefore the local-global principle can be restated to give an "if and only if" criterion to determine whether c can be written as ax^2+by^2 with x and y rational. This is most usefully modified as follows:

Corollary 9.4.1. *Suppose that a,b,c are given integers with $(a,b,c)=1$, and suppose $d=b^2-4ac$ is not divisible by the square of any odd prime. For any given squarefree integer N with $(N,d)=1$, there exist rationals u and v for which $N=au^2+buv+cv^2$ if and only if the following criteria hold:*

- *N has the same sign as a or c, or $d>0$;*
- *d is a square* mod N*;*
- *$\left(\frac{N}{p}\right)=\left(\frac{a}{p}\right)$ for all odd primes p dividing d that do not divide a;*
- *$\left(\frac{N}{p}\right)=\left(\frac{c}{p}\right)$ for all odd primes p dividing both d and a.*

Proof. If $N=au^2+buv+cv^2$, then we multiply through by $4a$ to obtain $4aN=(2au+bv)^2-dv^2$; in other words, $aN=U^2-dV^2$ for some rationals U,V. We may reverse this argument, and so there exist rationals u and v for which $N=au^2+buv+cv^2$ if and only if there exist rationals U,V for which $aN=U^2-dV^2$. We now apply Legendre's version of the local-global principle to rational solutions to the equation $aN=u^2-dv^2$.

We have real solutions if and only if $aN>0$ or $d>0$.

Now $U^2\equiv dV^2 \pmod{aN}$ and so d must be a square mod aN. But $d=b^2-4ac\equiv b^2 \pmod a$, so we need only verify that d is a square mod N.

If odd prime p divides d, then $aN\equiv u^2 \pmod p$, and so $\left(\frac{N}{p}\right)=\left(\frac{a}{p}\right)$ if p does not divide a.

If odd prime p divides both d and a, then it divides b, as it divides $b^2=d+4ac$. Therefore p does not divide c as $(a,b,c)=1$. We then run through the analogous argument with a replaced by c. (For the primes p dividing d, but not $4ac$, our results that $\left(\frac{N}{p}\right)=\left(\frac{a}{p}\right)$ and $\left(\frac{N}{p}\right)=\left(\frac{c}{p}\right)$ are consistent; see exercise 8.1.4.) □

[2]Which we have only proved in three variables but is true in three or more variables.

9.5. *The failure of the local-global principle for quadratic equations in integers*

We have seen how the local-global principle allows us to determine whether there are *rational solutions* x, y to a given equation of the form $ax^2 + by^2 = c$. However we will now show that it does not help when we ask for *integer solutions*. The example

$$x^2 + 23y^2 = 52$$

has rational solutions, like $(\frac{1}{2}, \frac{3}{2}), (\frac{25}{4}, \frac{3}{4}), (\frac{29}{12}, \frac{17}{12}), \ldots$. There are obviously no integer solutions or else $23y^2 \le x^2 + 23y^2 = 52$ and so $y^2 = 0$ or 1, but then $x^2 = 52 - 23y^2 = 52$ or 29, which are not squares. Since there are rational solutions we know that there are non-trivial solutions to $a^2 + 23b^2 \equiv 52c^2 \pmod{p^k}$ for all prime powers p^k by the local-global principle, but not necessarily to $a^2 + 23b^2 \equiv 52 \pmod{p^k}$. To prove that there are such solutions, we show that solutions exist modulo 8 and all odd prime moduli p, and then we lift these solutions to all prime power moduli p^k, using Proposition 8.8.1.

We have the solutions $2^2 + 23 \cdot 4^2 = 372 \equiv 52 \pmod 8$, $4^2 + 23 \cdot 1^2 = 39 \equiv 52 \pmod{13}$, and $11^2 + 23 \cdot 0^2 = 121 \equiv 52 \pmod{23}$. For any odd prime p other than 13 or 23, there are $\frac{p+1}{2}$ residues mod p of the form $23y^2$, and $\frac{p+1}{2}$ residues mod p of the form $52 - x^2$, so two of these residues must be equal. Therefore there is a solution to $x^2 + 23y^2 \equiv 52 \pmod p$, and evidently one of x and y must be non-zero (mod p) (or else p would divide 52).

Therefore we have shown that the local-global principle holds for integer and rational solutions of linear equations, and for rational but not integer solutions of quadratic equations. However it does not even hold for rational solutions of cubic equations: In 1957, Selmer showed that $3x^3 + 4y^3 = 5$ has solutions in the reals, and mod r for all $r \ge 1$, yet has no rational solutions. Further discussion of the failure of the local-global principle for cubic equations can be found in [**Grab**], with a motivating discussion in chapter 7.

9.6. Primes represented by $x^2 + 5y^2$

Calculations reveal that the primes > 5 that are represented by $x^2 + 5y^2$ are

$$29, 41, 61, 89, 101, 109, 149, 181, \ldots.$$

From our explorations of the binary quadratic forms $x^2 + y^2$, $x^2 + 2y^2$, and $x^2 + 3y^2$ we might guess that this should be the set of primes for which $(-5/p) = 1$. However the list of primes for which $(-5/p) = 1$ also includes the primes

$$3, 7, 23, 43, 47, 67, 83, 103, 107, 127, 163, 167, \ldots.$$

What is going on? We quickly see that the primes in the first list end in a 1 or a 9, whereas the primes in the second list end in a 3 or a 7, so there seems to be a further congruence condition that partitions the list. Further examination of the equation $p = x^2 + 5y^2$ makes this evident: Besides $(-5/p) = 1$, we can also deduce that $p \equiv x^2 \pmod 5$ so that $(p/5) = 1$. Combined with $(-5/p) = 1$, this also yields that $p \equiv 1 \pmod 4$. These two conditions together give that $p \equiv 1$ or $9 \pmod{20}$,

the primes that we see in the first list, and if $(p/5) = -1$, then we obtain $p \equiv 3$ or 7 (mod 20), the primes that we see in the second list.

Where do the primes in the second list come from? It turns out there is a second, fundamentally different binary quadratic form, $2x^2 + 2xy + 3y^2$, which has the same discriminant -20 as $x^2 + 5y^2$. We first observe that these quadratic forms definitely do not represent the same integers because $2x^2 + 2xy + 3y^2$ represents 3, whereas $x^2 + 5y^2$ evidently does not. A quick calculation reveals that the second list is precisely the set of odd primes represented by $2x^2 + 2xy + 3y^2$. This dichotomy will be explored further in chapter 12, though we observe here that if prime $p = 2x^2 + 2xy + 3y^2$, then $2p = 4x^2 + 4xy + 6y^2 = (2x + y)^2 + 5y^2$; that is, $2p$ can be represented by $a^2 + 5b^2$

In general if we wish to represent the odd prime p by $x^2 + dy^2$, then $-d$ must be a square mod p. On the other hand, suppose that $-d$ is a square mod p, say $u^2 \equiv -d \pmod p$ with $|u| < p/2$.

If $p < 2\sqrt{d}$, then we can write $u^2 + d = ap$, so the binary quadratic form, $pm^2 + 2umn + an^2$, has discriminant $-4d$, the same as $x^2 + dy^2$, and takes the value p when $m = 1, n = 0$.

Now assume that $p > 2\sqrt{d}$. By exercise 9.7.3(a) with $R = d^{1/4}\sqrt{p}, S = d^{-1/4}\sqrt{p}$, there exist integers r and s, not both 0, for which $r \equiv us \pmod p$ and so, squaring, $r^2 \equiv -ds^2 \pmod p$; that is, $r^2 + ds^2$ is a multiple of p. Moreover we have $0 < r^2 + ds^2 \le R^2 + dS^2 = 2\sqrt{d}p$. Therefore there exists an integer a in the range $1 \le a \le 2\sqrt{d}$ for which

$$r^2 + ds^2 = ap.$$

We may assume that $(r, s) = 1$ for if $g = (r, s)$, then we claim that g^2 divides a, so we can divide r and s through by g. To justify our claim, note that g^2 divides $r^2 + ds^2 = ap$ so if g^2 does not divide a, then p divides g. But then $p^2 \le g^2 \le r^2 + ds^2 = ap$ and so $p \le a \le 2\sqrt{d}$, a contradiction.

Now $(s, a) = 1$ or else if prime q divides a and s, then it divides $ap = -ds^2 = r^2$, and so it divides r, contradicting that $(r, s) = 1$. Let b be an integer for which $b \equiv r/s \pmod a$ so that $b^2 \equiv -d \pmod a$. We define integers $n = s$, $m = (r - bs)/a$, and $c = (b^2 + d)/a$. This implies that $am + bn = r$ and so

$$am^2 + 2bmn + cn^2 = \frac{(am + bn)^2 - (b^2 - ac)n^2}{a} = \frac{r^2 + ds^2}{a} = p.$$

Therefore, whenever $-d$ is a square mod p, there is a quadratic equation in two variables, with positive leading coefficient $\le 2\sqrt{d}$, and of discriminant $-4d$, which takes the value p. This is the first hint of a general theory: We will study the solutions to quadratic equations in two variables, like this, in detail, in chapter 12.

Additional exercises

Exercise 9.7.1. Let $f(n)$ be the arithmetic function for which $f(n) = 1$ if n can be written as the sum of two squares, and $f(n) = 0$ otherwise. Prove that $f(n)$ is a multiplicative function.

Exercise 9.7.2. Let p be a prime $\equiv 1 \pmod 4$. This exercise yields another proof that p is the sum of two squares.

(a) Use Theorem 8.3 to prove that there exist integers a and b such that $a^2 + b^2$ is a positive multiple of p.

(b) Let rp be the smallest such multiple of p. Prove that $r \le p/2$.

(c)† Prove that if $r > 1$, then there exists a positive integer $s \le r/2$ such that $rs = c^2 + d^2$ for some integers c and d, selected so that $ad - bc$ is divisible by r.

(d) Use (9.1.2) to deduce that if $r > 1$, then sp is a sum of two squares.

This contradicts the minimality of r unless $r = 1$; that is, p is the sum of two squares.

Exercise 9.7.3. Let p be an odd prime.

(a)† Suppose that $b \pmod p$ is given and that $R, S \ge 1$ such that $RS = p$. Prove that there exist integers r, s with $|r| \le R, 0 < s \le S$ such that $b \equiv r/s \pmod p$.

(b) Prove that there exists an integer m with $|m| < \sqrt{p}$ for which $\left(\frac{m}{p}\right) = -1$.

(c) Deduce that if $p \equiv 1 \pmod 4$, then there exists an integer n in the range $1 < n < \sqrt{p}$ for which $\left(\frac{n}{p}\right) = -1$.

Exercise 9.7.4. Show that x and y are integers in (9.1.3) if and only if $r^2 + s^2$ divides $2(ar + bs)$, and show that this can only happen if $r^2 + s^2$ divides $2n$.

Exercise 9.7.5. What values of r and s yield the point $(-a, -b)$ in Proposition 9.1.2?

Exercise 9.7.6. Reprove exercise 9.1.8 using Theorem 9.1 and (9.1.1).

Exercise 9.7.7.† $33^2 + 56^2 = 65^2$ and $16^2 + 63^2 = 65^2$ are examples of the side lengths of different primitive Pythagorean triangles with the same hypotenuse. Classify those integers that appear as the hypotenuse of at least two different primitive Pythagorean triangles.

Exercise 9.7.8. Prove that for every integer m there exists an integer n which is the length of the hypoteneuse of at least m different primitive Pythagorean triples. (You may use Theorem 7.4 which implies that there are infinitely many primes $\equiv 1 \pmod 4$.)

Exercise 9.7.9.† Prove that an integer of the form $a^2 + 4b^2$ with $(a, 2b) = 1$ cannot be divisible by any integer of the form $m^2 - 2$ with $m > 1$, or $m^2 + 2$. Conversely prove that an integer of the form $m^2 - 2n^2$ or $m^2 + 2n^2$ with $(m, 2n) = 1$ cannot be divisible by any integer of the form $a^2 + 4$.

Exercise 9.7.10.‡ (Zagier's proof that every prime $\equiv 1 \pmod 4$ is the sum of two squares) Let

$$S := \{(x, y, z) \in \mathbb{N}^3 : \ p = x^2 + 4yz\}.$$

Define the map $\phi : S \to S$ by

$$\phi : (x, y, z) \to \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z, \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y, \\ (x - 2y, x - y + z, y) & \text{if } x > 2y. \end{cases}$$

(a) Show that ϕ is an *involution*, that is, $\phi^2 = 1$, and verify that each $\phi(S)$ belongs to S.

(b) Prove that if $\phi(v) = v$, then $v = (1, 1, \frac{p-1}{4})$.

(c) Deduce that there are an odd number of elements of S (in particular, S is non-empty). Let $\psi : S \to S$ be the involution $\psi(x, y, z) = (x, z, y)$.

(d) Prove that ψ has a fixed point (x, y, y) so that $z = y$.

(e) Deduce that $p = x^2 + (2y)^2$ for some integers x, y.

Appendix 9A. Proof of the local-global principle for quadratic equations

In this appendix we will give the difficult part of the proof of the local-global principle for quadratic equations, Theorem 9.4, as discussed at length in section 9.3.

The local-global principle for quadratic equations. *Let a, b, c be given pairwise coprime, squarefree integers. There are solutions in*

$$\text{non-zero integers } \ell, m, n \text{ to } a\ell^2 + bm^2 + cn^2 = 0 \text{ with } (a\ell^2, bm^2) = 1$$

$$\text{if and only if } \textit{there are solutions in}$$

$$\text{non-zero real numbers } \lambda, \mu, \nu \text{ to } a\lambda^2 + b\mu^2 + c\nu^2 = 0,$$

and*, for all positive integers r, there exist*

$$\text{residue classes } u, v, w \pmod r \text{ for which } au^2 + bv^2 + cw^2 \equiv 0 \pmod r,$$

with $(au^2, bv^2, cw^2, r) = 1$.

Our proof depends on an understanding of lattices.

9.8. Lattices and quotients

A *lattice* Λ in $\mathbb{R}^n$ is the set of points obtained by integer linear combinations of n given linearly independent vectors. If the *basis* is $x_1, x_2, \dots, x_n \in \mathbb{R}^n$, then

$$\Lambda := \{m_1x_1 + m_2x_2 + \cdots + m_nx_n : \ m_1, m_2, \dots, m_n \in \mathbb{Z}\}.$$

One can see that Λ is an additive group, but it also has some geometry connected to it. The *fundamental domain* of Λ with respect to $x_1, x_2, \dots, x_n$ is the set

$$P = P(\Lambda) := \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : 0 \le a_i < 1\},$$

the interior (and part of the boundary) of one of the diamond-shaped cells in Figure 9.1. If $\lambda \in \Lambda$, then $\lambda + P$ gives us another of the diamond shapes, shifted from the original by λ. Therefore the sets $\lambda + P$, $\lambda \in \Lambda$ are disjoint and their union is $\mathbb{R}^n$. Therefore $P(\Lambda)$ is a set of representatives of

$$\mathbb{R}^n/\Lambda,$$

which is often called "$\mathbb{R}^n$ mod Λ".

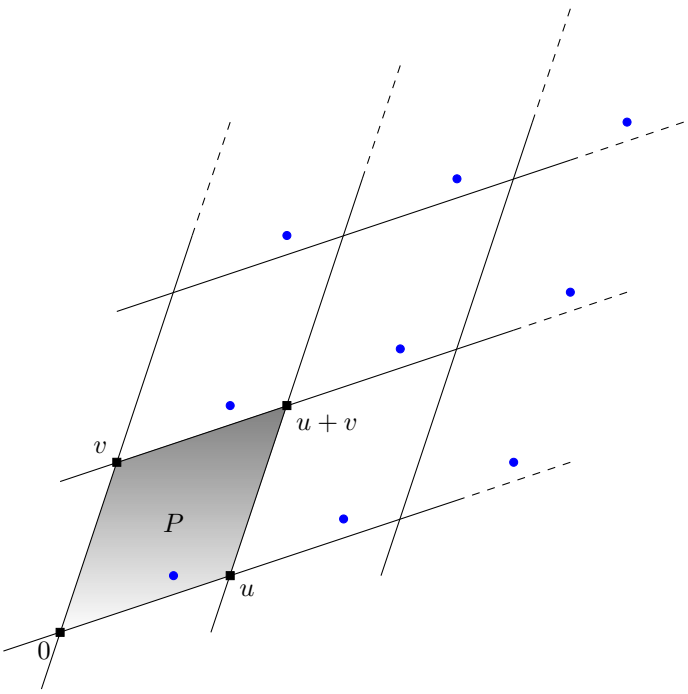


Figure 9.1. Constructing a lattice in $\mathbb{R}^2$, generated by vectors u and v. The shaded grey parallelogram is the fundamental domain $P(\Lambda)$. The dots represent the same point in $\mathbb{R}^2/\Lambda$ repeated in each copy of $P(\Lambda)$; that is, they are the points $P + \lambda$ for each vector $\lambda \in \Lambda$.

In the non-trivial example with $n = 1$, for which $\Lambda = \mathbb{Z}$, we can write every real number z as $m + a$ where $m \in \mathbb{Z}$ and $a \in [0, 1)$, letting $m = [z]$ and $a = \{z\}$. We prefer to think of this as $z = a$ in the ring $\mathbb{R}/\mathbb{Z}$ since their difference, m, is an integer. This generalizes to n dimensions, in which case we can identify $\mathbb{R}^n/\Lambda$ with $(\mathbb{R}/\mathbb{Z})^n$.

The *determinant* $\det(\Lambda)$ of Λ is the volume of P; in fact $\det(\Lambda) = |\det(A)|$, where A is the matrix with column vectors $x_1, x_2, \ldots, x_n$ (written as vectors in $\mathbb{R}^n$). A *convex body* K is a bounded convex open subset[3] of $\mathbb{R}^n$.

[3]These are all common terms in geometry. A set $S \subset \mathbb{R}^n$ is *bounded* if it can be contained inside a ball of some finite radius. The set S is *convex* if all the points on the straight line between any two points of S also belong to S. The set S is open if there is a ball around any given point of S, perhaps of very small radius, that also is contained within S.

If $\Lambda \subset \mathbb{Z}^n$, then there are $\det(\Lambda)$ cosets of Λ in $\mathbb{Z}^n$; that is,

$$|\mathbb{Z}^n/\Lambda| = \det(\Lambda).$$

In the proof of Theorem 9.1 we work with the lattice

$$\Lambda := \{(r,s) \in \mathbb{Z}^2 : \quad r - ks \equiv 0 \pmod{p}\}$$

(where $k^2 \equiv -1 \pmod{p}$). This lattice is presented there somewhat differently from the definition here, but it can easily be seen that Λ is generated by $(k,1)$ and $(p,0)$, and that $(0,p) = p(k,1) - k(p,0)$. Hence $\det(\Lambda) = p$; in particular we deduce that there are p distinct cosets of Λ within $\mathbb{Z}^2$.

Let S be the set constructed in the proof of Theorem 9.1: S is a convex set of $> p$ elements of $\mathbb{Z}^2$ so that the difference, d, of two of them lies on the lattice Λ. The set S was constructed so that the difference, d, must lie close to the origin. Moreover Λ was constructed so that if $(r,s) \in \Lambda$, then $r^2 + s^2 \equiv 0 \pmod{p}$ (since if $r \equiv ks \pmod{p}$, then $r^2 + s^2 \equiv (ks)^2 + s^2 \equiv (k^2+1)s^2 \equiv 0 \pmod{p}$.)

We will now develop these ideas to give a proof of the local-global principle. In the next section we will modify the last step to make it more elegant.

Proof of the local-global principle. Assume that a, b, and c are squarefree, pairwise coprime integers, with $a, b > 0 > c$ (so that there are non-zero real solutions to $ax^2 + by^2 + cz^2 = 0$), and that there exists a solution to

$$au^2 + bv^2 + cw^2 \equiv 0 \pmod{|abc|},$$

with $(au^2, bv^2, cw^2, abc) = 1$.[4] We may assume that at least two of $a, b, |c|$ are > 1, for the case $a = b = 1$ can be proved directly from Theorem 9.2, while the case $a = 1, c = -1$ is easy as we always have the solution $x = b - 1, y = 2, z = b + 1$.

Define the lattice

$$\Lambda := \{(x,y,z) \subset \mathbb{Z}^3 : \ aux + bvy + cwz \equiv 0 \pmod{|abc|}\}.$$

We claim that if $(x,y,z) \in \Lambda$, then

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{|abc|}.$$

We now prove that this holds mod a (and the cases mod b and mod $|c|$ proceed analogously, so that the claim follows using the Chinese Remainder Theorem). Now if $(x,y,z) \in \Lambda$, then $bvy \equiv -cwz \pmod{a}$, and so

$$bv^2 \cdot by^2 = (bvy)^2 \equiv (-cwz)^2 = cw^2 \cdot cz^2 \pmod{a}.$$

Dividing through by $bv^2 \equiv -cw^2 \pmod{a}$, we deduce that $by^2 \equiv -cz^2 \pmod{a}$. Therefore $ax^2 + by^2 + cz^2 \equiv 0 \pmod{a}$, as desired.

In the next exercise we will show that $|\det(\Lambda)| = |abc|$. Let

$$S := \{(i,j,k) : \quad 0 \le i \le [\sqrt{|bc|}], \quad 0 \le j \le [\sqrt{|ac|}], \quad 0 \le k \le [\sqrt{|ab|}]\}.$$

The number of integer points in S is $> \sqrt{|bc|} \cdot \sqrt{|ac|} \cdot \sqrt{|ab|} = |abc| = |\mathbb{Z}^3/\Lambda|$, and so, by the pigeonhole principle, there must be two lattice points in S that differ by

[4] Lemma 9.3.1 implies that we should work modulo $8|abc|$ in proving the local-global principle. However, in this first version of our proof, we prefer to not worry about the equation modulo powers of 2. We will revisit this issue in the next section.

non-zero element $(x, y, z) \in \Lambda$. If the two lattice points are (i, j, k) and (I, J, K), then

$$|x| = |i - I| \le [\sqrt{|bc|}], \quad |y| = |j - J| \le [\sqrt{|ac|}], \quad |z| = |k - K| \le [\sqrt{|ab|}].$$

These are all "$<$" as none of $|bc|, |ac|, |ab|$ are squares, since at least two of $a, b, |c|$ are > 1 and they are pairwise coprime. Therefore $ax^2 + by^2 < 2|abc|$ and $|cz^2| < |abc|$, so that

$$-|abc| < ax^2 + by^2 + cz^2 < 2|abc|.$$

This implies that either $ax^2 + by^2 + cz^2 = 0$ or $ax^2 + by^2 + cz^2 = |abc| = -abc$. We need to eliminate the second case. I know of two ways to do this. The first is inelegant and comes from simply noting that if $ax^2 + by^2 + cz^2 + abc = 0$, then

$$a(xz - by)^2 + b(ax + yz)^2 + c(ab + z^2)^2 = (ab + z^2)(ax^2 + by^2 + cz^2 + abc) = 0.$$

The second involves slightly modifying the definition of Λ, by taking the prime 2 into account more carefully, which we discuss in the next section. □

Exercise 9.8.1. (a) Show that there exist integers U, V, W, coprime with abc, for which $U \equiv u \pmod{bc}$, $V \equiv v \pmod{ac}$, $W \equiv w \pmod{ab}$, so that $aU^2 + bV^2 + cW^2 \equiv 0 \pmod{|abc|}$.
(b) Let U^{-1} be an integer $\equiv 1/U \pmod{abc}$ and W^{-1} be an integer $\equiv 1/W \pmod{abc}$. Show that Λ is generated by the vectors $(1, VU^{-1}, WU^{-1})$, $(0, c, -bVW^{-1})$, and $(0, 0, ab)$.)
(c) Deduce that $\det(\Lambda) = |abc|$.

9.9. A better proof of the local-global principle

The idea is to construct a lattice, based on that in the previous section, but now of determinant $4|abc|$. We begin by defining

$$\Lambda_0 := \{(x, y, z) \subset \mathbb{Z}^3 : \ aux + bvy + cwz \equiv 0 \pmod{|abc|}\}.$$

If c is even, then let

$$\Lambda := \{(x, y, z) \in \Lambda_0 : \ y \equiv x \pmod 4 \text{ and } z \equiv wx \pmod 2\}$$

based on the given solution (u, v, w). We construct Λ analogously if a or b is even.

If abc is odd, then one of u, v, w must be even (as $au^2 + bv^2 + cw^2 = 0$), say w. If so, then let

$$\Lambda := \{(x, y, z) \in \Lambda_0 : \ y \equiv x \pmod 2 \text{ and } z \equiv 0 \pmod 2\},$$

using the given solution (u, v, w). We construct Λ analogously if u or v is even.

Exercise 9.9.1. (a) Prove that if $(x, y, z) \in \Lambda$, then $ax^2 + by^2 + cz^2 \equiv 0 \pmod{4|abc|}$.
(b) Prove that $\det(\Lambda) = 4|abc|$.

Consider the set of integer points

$$S := \{(i, j, k) : \ 0 \le i \le [\sqrt{2|bc|}], \ 0 \le j \le [\sqrt{2|ac|}], \ 0 \le k \le [2\sqrt{|ab|}]\}.$$

The number of lattice points in S is $> \sqrt{2|bc|} \cdot \sqrt{2|ac|} \cdot 2\sqrt{|ab|} = 4|abc| = |\mathbb{Z}^3/\Lambda|$ by exercise 9.9.1(b), and so, by the pigeonhole principle, there must be two lattice points in S that differ by a non-zero element $(x, y, z) \in \Lambda$. If the two lattice points are (i, j, k) and (I, J, K), then

$$|x| = |i - I| \le [\sqrt{2|bc|}], \quad |y| = |j - J| \le [\sqrt{2|ac|}], \quad |z| = |k - K| \le [2\sqrt{|ab|}].$$

Therefore $ax^2 + by^2 < 4|abc|$ and $|cz^2| < 4|abc|$ (as equality would only be possible if $a = b = 1$), and so

$$|ax^2 + by^2 + cz^2| < 4|abc|.$$

Now, since $(x, y, z) \in \Lambda$, we know that

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{4|abc|},$$

by exercise 9.9.1(a), and so we must have $ax^2 + by^2 + cz^2 = 0$ as desired. □

A by-product of this proof is that the smallest non-trivial solution satisfies

$$|a\ell^2|,\ |bm^2|,\ |cn^2| \leq 4|abc|.$$

In 1950, Holzer showed that one may replace $4|abc|$ by $|abc|$.

Exercise 9.9.2. Give infinitely many examples in which $\max\{|a\ell^2|,\ |bm^2|,\ |cn^2|\} = |abc|$ in the smallest non-trivial solution of $a\ell^2 + bm^2 + cn^2 = 0$.

Appendices. The extended version of chapter 9 has the following additional appendices:

Appendix 9B. *Reformulation of the local-global principle*. We introduce the Hilbert symbol and go on to formulate and prove the Hasse-Minkowski principle, the local-global principle for quadratics in n variables with $n \geq 3$.

Appendix 9C. *The number of representations* studies how often an integer is the sum of two squares and uses this to introduce some important formulas.

Appendix 9D. *Descent and the quadratics* introduces several famous questions which require descent and can be analyzed through matrix actions and orbits, including the beautiful question of tiling a circle with smaller circles.

Chapter 10

Square roots and factoring

In this chapter we will study the computational side of number theory, which plays an important role in several uses of computers in today's society, particularly when it comes to keeping secrets. We will investigate how to *rapidly* determine whether a given large integer is prime and, if not, how to factor it. The issue of factoring an integer n is closely related to determining square roots mod n:

10.1. Square roots modulo n

How difficult is it to find square roots mod n? The first question to ask is how many square roots does a square have mod n?

Lemma 10.1.1. *If n is an odd integer with k prime factors and A is a square* mod n *with $(A, n) = 1$, then there are exactly 2^k residues* mod n *whose square is $\equiv A$* (mod n).

In particular, all squares mod m, that are coprime to m, have the same number of square roots mod m. We resolved how many square roots $1 \pmod n$ has in Lemma 3.8.1, and here we modify that proof to better suit the discussion in this chapter. We could have immediately deduced Lemma 10.1.1 for if A is a square mod n, then there exists $b \pmod n$ such that $b^2 \equiv A \pmod n$, and then the solutions to $x^2 \equiv A \pmod n$ are in 1-to-1 correspondence with the solutions to $y^2 \equiv 1 \pmod n$ through the invertible transformation $x \equiv by \pmod n$.

Proof. Suppose that $b^2 \equiv A \pmod n$ where $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, and each p_i is odd and distinct. If $x^2 \equiv A \pmod n$, then $n | (x^2 - b^2) = (x-b)(x+b)$ so that p divides $x - b$ or $x + b$ for each prime p dividing n. Now p cannot divide both or else p divides $(x + b) - (x - b) = 2b$ and so $4A \equiv (2b)^2 \equiv 0 \pmod p$, which contradicts the fact that $(p, 2A) | (n, 2A) = 1$. So let

$$d = (n, x - b), \quad \text{and therefore} \quad n/d = (n, x + b),$$

which must be coprime. Then $x \equiv b_d \pmod n$ where b_d is that unique residue class mod n for which

$$b_d \equiv \begin{cases} b \pmod d, \\ -b \pmod{n/d}. \end{cases} \tag{10.1.1}$$

Note that the b_d are well-defined by the Chinese Remainder Theorem, are distinct, and that $x^2 \equiv b_d^2 \equiv b^2 \equiv A \pmod n$ for each d.

The possible values of d are $\prod_{i\in I} p_i^{e_i}$ for each subset I of $\{1, \dots, k\}$, and therefore there are 2^k possibilities. □

To see how the proof works let's obtain the four square roots of $4 \pmod{15}$ from knowing one square root, 2, and the factorization of 15. These four square roots are given by four pairs of congruences which we solve using the Chinese Remainder Theorem:

$2 \pmod 1$	and	$-2 \pmod{15}$	which yield	$13 \pmod{15}$;		
$2 \pmod 3$	and	$-2 \pmod 5$	which yield	$8 \pmod{15}$;		
$2 \pmod 5$	and	$-2 \pmod 3$	which yield	$7 \pmod{15}$;	and	
$2 \pmod{15}$	and	$-2 \pmod 1$	which yield	$2 \pmod{15}$.		

Consequence. *Let n be an odd integer with at least two different prime factors, and suppose that $b^2 \equiv A \pmod n$ with $(A, n) = 1$. Finding square roots of A mod n, other than b and $-b$, is "as difficult as" factoring n into two parts both > 1.*

Sketch of "proof". If we have a factorization $n = d \cdot n/d$, then we select b_d as in (10.1.1) so that $b_d^2 \equiv A \pmod n$ but $b_d \not\equiv \pm b \pmod n$, as $d, n/d > 1$.

In the other direction, suppose that one has a fast algorithm for rapidly finding arbitrary square roots mod n for odd integers n. In particular given $A \pmod n$, the algorithm randomly determines some $x \pmod n$ for which $x^2 \equiv A \pmod n$; by "random" we mean that each time the "square root finding" algorithm is run it is equally likely to produce any one of the 2^k solutions (as in Lemma 10.1.1). Now define $d = (n, x - b)$ (as in the proof of Lemma 10.1.1) and so we factor n as $d \cdot n/d$. This works provided $d \neq 1$ or n, that is, provided that $x \not\equiv b$ or $-b \pmod n$.

Now, the probability that $x \equiv b$ or $-b \pmod n$ is $2/2^k$ which is $\leq \frac{1}{2}$ as $k \geq 2$. Therefore the probability of finding a non-trivial factor of n each time the "square root finding" algorithm is run is $\geq \frac{1}{2}$. This does not seem persuasive, but if we run the "square root finding" algorithm 20 times, then the probability that the algorithm gives 1 or n on every run is $\leq \left(\frac{1}{2}\right)^{20}$, which is less than one in a million. So, in practice, we will quickly find a non-trivial factor of n. □

We have shown that finding square roots mod n and factoring n are more or less equally difficult problems.

Exercise 10.1.1. Find all of the square roots of 49 mod $3^2 \cdot 5 \cdot 11$.

10.2. Cryptosystems

Cryptography has been around for as long as the need to communicate secrets at a distance. Julius Caesar, on campaign, communicated military messages by creating

ciphertext from *plaintext* (the unencrypted message), replacing each letter of the plaintext with that letter which is three letters further on in the alphabet. Thus A becomes D, B becomes E, etc. For example,

```
t h i s i s v e r y i n t e r e s t i n g
                becomes
w k l v l v y h u b l q w h u h v w l q j
```

(Y became B, since we wrap around to the beginning of the alphabet. It is essentially the map $x \to x + 3 \pmod{26}$.) At first sight an enemy might regard $WKLV \ldots WLQJ$ as gibberish even if the message was intercepted. It is easy enough to decrypt the ciphertext, simply by going back three places in the alphabet for each letter, to reconstruct the original message. The enemy could easily do this if (s)he guessed that the *key* is to rotate the letters by three places in the alphabet, or even if they only guessed that one rotates by a fixed number of letters, as there would only be 25 possibilities to try. So in classical cryptography it is essential to keep the key secret, as well as the technique by which the key was created.[1]

One can generalize to arbitrary *substitution ciphers* where one replaces the alphabet by some permutation of the alphabet. There are 26! permutations of our alphabet, which is around 4×10^{26} possibilities, enough one might think to be safe. And it would be if the enemy went through each possibility, one at a time. However the clever *cryptographer* will look for patterns in the ciphertext. In the above short ciphertext we see that L appears four times among the 21 letters, and H, V, W three times each, so it is likely that these letters each represent one of A, E, I, S, T. By looking for multiword combinations (like the ciphertext for THE) one can quickly break any ciphertext of around one hundred letters.

To combat this, armies in the First World War used longer cryptographic keys, rather than of length 1. That is, they would take a word like $ABILITY$ and since A is letter 1 in the alphabet, B is letter 2, and $ILITY$ are letters 9,12,9,20,25, respectively, they would rotate on through the alphabet by $1, 2, 9, 12, 9, -6, -1$ letters to *encrypt* the first seven letters, and then repeat this process on the next seven. For example, we begin with the message, adding the word "ability" as often as is needed:

```
w e n e e d t o m a k e a n e x a m p l e
                    plus
a b i l i t y a b i l i t y a b i l i t y
                  becomes
x g w q n x s p o j w n u m f z j y y f d
```

This can again be "broken" by statistical analysis, though the longer the key length, the harder it is to do. Of course using a long key on a battlefield would be difficult, so one needed to compromise between security and practicality. A *one-time pad*,

[1] *Steganography*, hiding secrets in plain view, is another method for communicating secrets at a distance. In 499 B.C., Histiaeus shaved the head of his most trusted slave, tattooed a message on his bald head, and then sent the slave to Aristagoras, once the slave's hair had grown back. Aristagoras then shaved the slave's head again to recover the secret message telling him to revolt against the Persians. In more recent times, cold war spies reportedly used "microdots" to transmit information, and Al-Qaeda supposedly notified its terrorist cells via messages hidden in images on certain webpages.

where one uses such a long key that one never repeats a pattern, is unbreakable by statistical analysis. This might have been used by spies during the cold war and was perhaps based on the letters in an easily obtained book, so that the spy would not have to possess any obviously incriminating evidence.

During the Second World War the Germans came up with an extraordinary substitution cypher that involved changing several settings on a specially built typewriter (an *Enigma machine*). The number of possibilities was so large that the Germans remained confident that it could not be broken, and they even changed the settings every day so as to ensure that it would be extremely difficult. The Poles managed to obtain an early Enigma machine and their mathematicians determined how it worked. They shared their findings with the Allies so that after a great amount of effort the Allies were able to break German codes quickly enough to be useful, even vital, to their planning and strategy.[2] Early successes led to the Germans becoming more cautious, and thence to horrific decisions having to be made by the Allied leaders to safeguard this most precious secret.[3]

The Allied cryptographers would cut down the number of possibilities (for the settings on the Enigma machine) to a few million, and then their challenge became to build a machine to try out many possibilities very rapidly. Up until then one would have to change, by hand, external settings on the machine to try each possibility; it became a goal to create a machine in which one could change what it was doing, *internally*, by what became known as a *program*, and this stimulated, in part, the creation of the first modern computers.

Exercise 10.2.1. One can also create a cryptosystem using binary addition. For example, our key could be the 20-letter word $k = 10111011101111011001$. Then we could encrypt by using bit-by-bit addition; that is, $0 \bigoplus 0 = 1 \bigoplus 1 = 0$ and $0 \bigoplus 1 = 1 \bigoplus 0 = 1$. Therefore if the plaintext is $p = 11100010101101000011$, then $c = p \bigoplus k$, namely

$$\begin{array}{rl} & \texttt{10111 01110 11110 11001} \\ \bigoplus & \texttt{11100 01010 11010 00011} \\ = & \texttt{01011 00100 00100 11010.} \end{array}$$

It is easy to recover the plaintext since $p = c \bigoplus k$. Prove that one can recover the key if one knows the ciphertext and the plaintext.

10.3. RSA

In the theory of cryptography we always have two (imaginary) people, Alice and Bob, attempting to share a secret over an open communication channel, and the evil Oscar listening in, attempting to figure out what the message says. We will begin by describing a *private key* scheme for exchanging secrets based on the ideas in our number theory course:

Suppose that prime p is given and integers d and e such that $de \equiv 1 \pmod{p-1}$. Alice knows p and e but not d, whereas Bob knows p and d but not e. The numbers

[2] As portrayed, rather inaccurately, in the film *The Imitation Game*.

[3] The ability to crack the Enigma code allowed the Allied leaders to save lives. However if they used it so often that every possible life was saved, the Germans would have realized that the Allies had broken the code, and then the Germans were liable to have moved on to a different cryptographic method, which perhaps the Allied codebreakers might have been unable to decipher. Hence the Allied leadership was forced to use its knowledge sparingly so that it would be available in the militarily most advantageous situations. As a consequence, they knowingly sent many sailors to their doom, knowing where the U-boats were waiting in ambush, but being forced not to disclose that information.

d and e are kept secret by whoever knows them. Thus if Alice's secret message is M,[4] she *encrypts* M by computing $x \equiv M^e \pmod{p}$. She sends the *ciphertext* x over the open channel. Then Bob *decrypts* by raising x to the dth power mod p, since

$$x^d \equiv (M^e)^d \equiv M^{de} \equiv M \pmod{p}$$

as $de \equiv 1 \pmod{p-1}$. As far as we know, Oscar will discover little by intercepting the encrypted messages x, even if he intercepts many different x, and even if he can occasionally make an astute guess at M. However, if Oscar is able to steal the values of p and e from Alice, he will be able to determine d, since d is the inverse of $e \bmod p-1$, and this can be determined by the Euclidean algorithm, as discussed in exercise 3.5.5 (see the second proof of Corollary 3.5.2). He is then able to decipher Alice's future secret messages, in the same way as Bob does.

This is the problem with most classical cryptosystems; once one knows the encryption method it is not difficult to determine the decoding method. In 1975 Diffie and Hellman proposed a sensational idea: Can one find a cryptographic scheme in which the encryption method gives no help in determining a decryption method? If one could, one would then have a *public key* cryptographic scheme, which is exactly what is needed in our age of electronic information, in particular allowing people to use passwords in public places (for instance when using an ATM) without fear any lurking Oscar will be able to figure out how to impersonate them.[5]

In 1977 Rivest, Shamir, and Adleman (RSA) realized this ambition, via a minor variation of the above private key cryptosystem:[6] Now let $p \neq q$ be two large primes[7] and $n = pq$. Select integers d and e such that $de \equiv 1 \pmod{\phi(pq)}$. Alice knows pq and e but not d, while Bob knows pq and d. Thus if Alice's secret message is M, the ciphertext is $x \equiv M^e \pmod{pq}$, and Bob decrypts this by taking $x^d \equiv (M^e)^d \equiv M^{de} \equiv M \pmod{pq}$ as $de \equiv 1 \pmod{\phi(pq)}$ using Euler's Theorem.

Now, if Oscar steals the values of pq and e from Alice, will he be able to determine d, the inverse of $e \bmod \phi(pq) = (p-1)(q-1)$? When the modulus was the prime p, Oscar had no difficulty in determining $\phi(p) = p - 1$. Now that the modulus is pq, can Oscar easily determine $(p-1)(q-1)$? If so, then, since he already knows pq, he would be able to determine $pq+1-(p-1)(q-1) = p+q$ and hence p and q, since they are the roots of $x^2-(p+q)x+pq = 0$. In practice, Oscar needs to only know d to factor n (see exercise 5.27 in [**CP05**][8]). In other words, if Oscar can "break" the RSA algorithm, then he can factor $n = pq$, and vice versa.

We have just shown that breaking RSA is more or less as difficult as factoring. Therefore RSA is a secure cryptographic protocol (when correctly implemented) if and only if n is a difficult integer to factor. But nobody truly knows whether

[4] Of course a message is usually in words, but one converts the letters to numbers using some simple substitutions, like "01" for "A", "02" for "B", ... , "26" for "Z", etc., and concatenates these numbers. Thus "cabbie" becomes "030102020905". It is this number that is our message that we denote by M.

[5] When Alice uses a password, a cryptographic protocol might append a *timestamp* to ensure that the encrypted password (plus timestamp) is different with each use, and so Bob will get suspicious if the same timestamp is used again later.

[6] It is now known that (Sir) Clifford Cocks, working for the British secret cryptography agency, GCHQ, had discovered this *RSA algorithm* in 1974, and it had been classified "Top Secret". See https://www.wired.com/1999/04/crypto/ for the story.

[7] We will develop fast methods to find large primes in appendix 10C.

[8] This uses Pollard's $p-1$ method, which will not be discussed in this book, and is an algorithm that runs in *probabilistic polynomial time*.

factoring is a difficult problem, nor how to select integers that are provably hard to factor. In our current state of knowledge, we do not know any very efficient ways to factor arbitrary large numbers, but that does not necessarily mean that there is no quick way to do so.[9] So why do we put our faith (and secrets and fortunes) in the difficulty of factoring? The security of a cryptographic protocol must evidently be based on the difficulty of resolving *some* mathematical problem,[10] but we do not know how to *prove* that any particular mathematical problem is necessarily difficult to solve.[11] However the problem of factoring efficiently has been studied by many of the greatest minds in history, from Gauss onwards, who have looked for an efficient factoring algorithm and failed. Is this a good basis to have faith in RSA? Probably not, but we have no better. (More on this at the end of section 10.15 of appendix 10F.)

Exercise 10.3.1. Let $n = 11\times53$ be an RSA modulus with encryption exponent $e = 7$. Determine d, the decryption exponent, by hand, using the Euclidean algorithm and the Chinese Remainder Theorem.

Exercise 10.3.2. Let $n = 5891$ be an RSA modulus with encryption exponent $e = 29$ and decryption exponent $d = 197$. Use this information to factor n.

10.4. Certificates and the complexity classes P and NP

Algorithms are typically designed to work on any of an arbitrarily large class of examples, and one wishes them to work as fast as possible. If the example is input in ℓ characters, and the function calculated is genuinely a function of all the characters of the input, then one cannot hope to compute the answer any quicker than the length, ℓ, of the input. A *polynomial time algorithm* is one in which the answer is computed in no more than $c\ell^A$ steps, for some constants $c, A > 0$, no matter what the input. These are considered to be quick algorithms. There are many simple problems that can be answered in polynomial time (the set of such problems is denoted by P and was already discussed in section 7.14 of appendix 7A); see section 10.15 of appendix 10F for more details. In modern number theory, because of the intrinsic interest as well as because of the applications to cryptography, we are particularly interested in the running times of factoring and primality testing algorithms.

At the 1903 meeting of the American Mathematical Society, F. N. Cole came to the blackboard and, without saying a word, wrote down

$$2^{67} - 1 = 147573952589676412927 = 193707721 \times 761838257287,$$

long-multiplying the numbers out on the right side of the equation to prove that he was indeed correct. Afterwards he said that figuring this out had taken him "three years of Sundays". The moral of this tale is that although it took Cole a great deal

[9] There are some families of numbers that we know are easy to factor (for example, see exercise 10.7.2 for a fast factoring method if p and q are close together) so we need to avoid those when selecting a modulus for RSA.

[10] Here we are talking about cryptographic protocols on computers as we know them today. There is a highly active quest to create *quantum computers*, on which cryptographic protocols are based on a very different set of ideas.

[11] We can *prove* that almost all mathematical problems are "difficult to solve" (see section 10.16 of appendix 10F), but we do not know how to identify *one specific problem* that is provably difficult to solve. This is a notoriously challenging and important open problem.

of work and perseverance to find these factors, it did not take him long to justify his result to a room full of mathematicians (and, indeed, to give a proof that he was correct). Thus we see that one can provide a short proof, even if finding that proof takes a long time.

In general one can exhibit factors of a given integer n to give a short proof that n is composite. Such proofs, which can be checked in polynomial time, are called *certificates*. (The set of problems for which the answer can be checked in polynomial time is denoted by NP.) Note that it is not necessary to exhibit factors to give a short proof that a number is composite. Indeed, we already saw in the converse to Fermat's Little Theorem, Corollary 7.2.1, that one can exhibit an integer a coprime to n for which n does not divide $a^{n-1}-1$ to provide a certificate that n is composite.

What about primality testing? If someone gives you an integer and asserts that it is prime, can you quickly check that this is so? Can they give you better evidence than their say-so that it is a prime number? Can they provide some sort of certificate that gives you all the information you need to quickly verify that the number is indeed a prime? We had hoped (see section 7.6) that we could use the converse of Fermat's Little Theorem to establish a quick primality test, but we saw that Carmichael numbers seem to stop that idea from reaching fruition. Here we are asking for less, for a short certificate for a proof of primality. It is not obvious how to construct such a certificate, certainly not so obvious as with the factoring problem. It turns out that some old remarks of Lucas from the 1870s can be modified for this purpose. We begin with a sure-fire primality test, obtained as a consequence of Proposition 7.5.1.

Corollary 10.4.1. *Suppose that $n > 1$ is a positive integer for which there exists an integer g with $(g, n) = 1$ such that $g^{n-1} \equiv 1 \pmod{n}$ and $g^{(n-1)/q} \not\equiv 1 \pmod{n}$ for every prime q dividing $n-1$. Then n is a prime.*

Proof. Proposition 7.5.1 implies that g has order $n-1 \pmod{n}$, so that the $n-1$ reduced residues $1, g, \dots, g^{n-1}$ are all distinct mod n. Therefore every integer a in the range $1 \le a \le n-1$ is coprime to n, implying that n is prime. □

We are not suggesting that Corollary 10.4.1 provides a fast primality test. One can probably find g rapidly, if it exists, using Gauss's algorithm which is discussed in section 7.15 of appendix 7B. However the algorithm requires one to completely factor $n-1$, and we have no particularly fast factoring algorithms. On the other hand, if $n-1$ has already been factored, then one can proceed rapidly. Indeed we can provide a "certificate" to allow a checker to quickly verify that n is prime, which would consist of

$$g \text{ and } \{q \text{ prime} : q \text{ divides } n-1\}.$$

The checker would need to verify that $g^{n-1} \equiv 1 \pmod{n}$ whereas $g^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all primes q dividing $n-1$, something that can be quickly accomplished using fast exponentiation (as explained in section 7.13 of appendix 7A).

There is a problem though: One needs (the additional) certification that each such q is prime. The solution is to iterate the above algorithm; and one can show that no more than $\log n$ odd primes need to be certified prime in the process of proving that n is prime. Thus we have a "short" certificate that n is prime.

At first one might hope that this also provides a quick way to test whether a given integer n is prime. However there are several obstacles. The most important is that we need to factor $n-1$ in creating the certificate. When one is handed the certificate, $n-1$ is already factored, so that is not an obstacle to the use of the certificate; however it is a fundamental impediment to the rapid creation of the certificate (and therefore to using this as a primality test).

Exercise 10.4.1. Assuming only that 2 is prime, provide a certificate that proves that 107 is prime.

Exercise 10.4.2. Let $F_m = 2^{2^m}+1$ with $m \geq 2$ be a Fermat number.

(a) Prove that if there exists an integer q for which $q^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}$, then F_m is prime.
(b) Deduce an "if and only if" condition for the primality of F_m using exercise 8.5.4.

10.5. Polynomial time primality testing

Although the converse to Fermat's Little Theorem does not provide a polynomial time primality test, one can further develop this idea. For example, we know that $a^{\frac{p-1}{2}} \equiv -1$ or $1 \pmod{p}$ by Euler's criterion, and hence if $a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$, then n is composite. This identifies even more composite n than Corollary 7.2.1 alone, but not necessarily all n. We develop this idea further in section 10.8 of appendix 10A to find a criterion of this type that is satisfied by all primes but not by any composites. However we are unable to prove that this is indeed a polynomial time primality test without making certain assumptions that are, as yet, unproved.

There have indeed been many ideas for establishing a primality test which is provably polynomial time, but this was not achieved until 2002. This was of particular interest since the proof was given by a professor, Manindra Agrawal, and two undergraduate students, Kayal and Saxena, working together with Agrawal on a summer research project. Their algorithm is based on the following elegant characterization of prime numbers.

Theorem 10.1 (Agrawal, Kayal, and Saxena (AKS))**.** *For given integer $n \geq 2$, let r be a positive integer $< n$, for which n has order $> 9(\log n)^2$ modulo r. Then n is prime if and only if*

- *n is not a perfect power,*
- *n does not have any prime factor $\leq r$,*
- *$(x+a)^n \equiv x^n + a \mod (n, x^r-1)$ for each integer $a, 1 \leq a \leq 3\sqrt{r}\ \log n$.*

The last equation uses "modular arithmetic" in a way that is new to us, but analogous to what we have seen: $(x+a)^n \equiv x^n + a \mod (n, x^r-1)$ means that there exist $f(x), g(x) \in \mathbb{Z}[x]$ such that $(x+a)^n - (x^n+a) = nf(x) + (x^r-1)g(x)$.

At first sight this might seem to be a rather complicated characterization of the prime numbers. However this fits naturally into the historical progression of ideas in this subject (indeed, see appendix 10G for a discussion and a proof), is not so complicated (compared to some other ideas in use), and has the great advantage that it is straightforward to develop into a fast algorithm for proving the primality of large primes. *However*, although the AKS algorithm satisfies the desire to have a rigorously proved polynomial time primality testing algorithm, it is not in practice

the fastest algorithm for establishing primality of the largest integers currently being considered.[12]

Exercise 10.5.1. Let p^k be the highest power of prime p that divides n, with $k \geq 1$.
(a) Prove that p^k does not divide $\binom{n}{p}$.
(b) Deduce that n does not divide $\binom{n}{p}$.
(c) Show that if n is composite, then n does not divide all the coefficients of the polynomial $(1+x)^n - x^n - 1$.

Exercise 10.5.2. Use the previous exercise to show:
(a) n is prime if and only if $(x+1)^n \equiv x^n + 1 \pmod{n}$.
(b) If $(n, a) = 1$, then n is prime if and only if $(x+a)^n \equiv x^n + a \pmod{n}$.
(c) Prove that if n is prime, then $(x+a)^n \equiv x^n + a \pmod{(n, x^r - 1)}$ for any integer a with $(a, n) = 1$ and any $r > 1$.

10.6. Factoring methods

> *The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and difficult that even for numbers that do not exceed the limits of tables constructed by estimable workers, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers .... It frequently happens that the trained calculator will be sufficiently rewarded by reducing large numbers to their factors so that it will compensate for the time spent. Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated .... It is in the nature of the problem that any method will become more complicated as the numbers get larger. Nevertheless, in the following methods the difficulties increase rather slowly .... The techniques that were previously known would require intolerable labor even for the most indefatigable calculator.*
>
> — from article 329 of *Disquisitiones Arithmeticae* (1801) by C. F. Gauss

The first factoring method, other than trial division, was given by Fermat: His goal was to write a given odd integer n as $x^2 - y^2$, so that $n = (x-y)(x+y)$. He started with m, the smallest integer $\geq \sqrt{n}$, and then looked to see if $m^2 - n$ is a square. If so, say $m^2 - n = r^2$, then $n = (m-r)(m+r)$.

It is not easy to determine (at least by hand) whether a large integer is a square, though most are not. Fermat simplified his algorithm by quickly eliminating non-squares, by testing whether $m^2 - n$ is a square modulo various small primes. If $m^2 - n$ is not a square, then he tested whether $(m+1)^2 - n$ is a square; if that failed, whether $(m+2)^2 - n$ is a square, or $(m+3)^2 - n, \ldots$, etc. Since Fermat computed by hand he also noted the trick that

$$\begin{aligned} (m+1)^2 - n &= \quad m^2 - n + (2m+1), \\ (m+2)^2 - n &= (m+1)^2 - n + (2m+3), \text{ etc.}, \end{aligned}$$

[12] Because other algorithms that we believe, but cannot prove, are polynomial time, run faster.

so that, at each step he only needed to add a relatively small number to the integer he had just tested, and the next add-on is just two larger than the previous one.

For example, Fermat factored $n = 2027651281$ so that $m = 45030$. Then

$$\begin{aligned}
45030^2 - n &= 49619 \text{ which is not a square mod 100;}\\
45031^2 - n = 49619 + 90061 &= 139680 \text{ which is divisible by } 2^5, \text{ not } 2^6;\\
45032^2 - n = 139680 + 90063 &= 229743 \text{ which is divisible by } 3^3, \text{ not } 3^4;\\
45033^2 - n = 229743 + 90065 &= 319808 \text{ which is not a square mod 3; etc.}
\end{aligned}$$

$$\vdots$$

up until $45041^2 - n = 1020^2$, so that

$$n = 2027651281 = 45041^2 - 1020^2 = (45041-1020)\times(45041+1020) = 44021\times 46061.$$

Exercise 10.6.1. Factor 1649 using Fermat's method.

Gauss and other authors further developed Fermat's ideas, most importantly realizing that if $x^2 \equiv y^2 \pmod n$ with $x \not\equiv \pm y \pmod n$ and $(x, n) = 1$, then

$$\gcd(n, x - y) \cdot \gcd(n, x + y)$$

gives a non-trivial factorization of n.

The issue now becomes to rapidly determine two residues x and $y \pmod n$ with $x \not\equiv y$ or $-y \pmod n$, such that $x^2 \equiv y^2 \pmod n$. Several factoring algorithms work by generating a sequence of integers $a_1, a_2, \dots$, with each

$$a_i \equiv b_i^2 \pmod n \text{ but } a_i \neq b_i^2$$

for some known integer b_i, until some subsequence of the a_i's has product equal to a square, say

$$y^2 = a_{i_1} \cdots a_{i_r}.$$

Then one sets $x^2 = (b_{i_1} \cdots b_{i_r})^2$ to obtain $x^2 \equiv y^2 \pmod n$, and there is a good chance that $\gcd(n, x - y)$ is a non-trivial factor of n.

We want to generate the a_i's so that it is not so difficult to find a subsequence whose product is a square; to do so, we need to be able to factor the a_i. This is most easily done by only keeping those a_i that have all of their prime factors $\le B$, for some appropriately chosen bound B. Suppose that the primes up to B are $p_1, p_2, \dots, p_k$. If $a_i = p_1^{a_{i,1}} p_2^{a_{i,2}} \cdots p_k^{a_{i,k}}$, then let $v_i = (a_{i,1}, a_{i,2}, \dots, a_{i,k})$, which is a vector with entries in $\mathbb{Z}$.

Exercise 10.6.2. Show that $\prod_{i\in I} a_i$ is a square if and only if $\sum_{i\in I} v_i \equiv (0, 0, \dots, 0) \pmod 2$.

Hence to find a non-trivial subset of the a_i whose product is a square, we simply need to find a non-trivial linear dependency mod 2 amongst the vectors v_i. This is easily achieved through the methods of linear algebra and guaranteed to exist once we have generated more than k such integers a_i.

The quadratic sieve factoring algorithm selects the b_i so that it is easy to find the small prime factors of the a_i, using Corollary 2.3.1. There are other algorithms that attempt to select the b_i so that the a_i are small and therefore more likely to have small prime factors. We discuss some of these in appendix 10B. The best

algorithm, the number field sieve, is an analogy to the quadratic sieve algorithm over number fields.

There are many other cryptographic protocols based on ideas from number theory. Some of these will be discussed in the appendices to this chapter.

References: See [CP05] and [Knu98], as well as:

[1] Carl Pomerance, *A tale of two sieves*, Notices Amer. Math. Soc. **43** (1996), 1473–1485.

[2] John D. Dixon *Factorization and primality tests*, Amer. Math. Monthly **91** (1984), 333–352.

Additional exercises

Exercise 10.7.1. Suppose that n is an odd composite integer. Prove that for at least half the pairs x, y with $0 \le x, y < n$ and $x^2 \equiv y^2 \pmod{n}$, we have $1 < \gcd(x - y, n) < n$.

Exercise 10.7.2. Factor $n = 62749$. Let $m = [\sqrt{n}] + 1 = 251$. Compute $(m + i)^2 \pmod{n}$ for $i = 0, 1, 2, \ldots$ and retain those residues whose prime factors are all ≤ 11. Therefore we have $251^2 \equiv 2^2 \cdot 3^2 \cdot 7$; $253^2 \equiv 2^2 \cdot 3^2 \cdot 5 \cdot 7$; $257^2 \equiv 2^2 \cdot 3 \cdot 5^2 \cdot 11$; $260^2 \equiv 3^2 7^2 \cdot 11$; $268^2 \equiv 3 \cdot 5^2 \cdot 11^2$; $271^2 \equiv 2^2 \cdot 3^5 \cdot 11 \pmod{n}$. Use this information to factor n.

Exercise 10.7.3. Alice is sending Bob messages using RSA with public key modulus $n = 2027651281$ and encryption exponent $e = 66308903$. Oscar recalls that n is the number Fermat factored in section 10.6. Find the decryption exponent for Oscar.

We wish to determine how many different odd primes are involved in the Lucas certificate of section 10.4.

Exercise 10.7.4. Let n be prime and suppose $q_1, \ldots, q_k$ are the odd prime factors of $n - 1$.

(a) Prove that the product of these primes, $N_1 := q_1 \cdots q_k$, is $\le n/2$.

(b)† To certify that $q_1, \ldots, q_k$ are prime we need the set of odd prime factors of $q_1 - 1, \ldots, q_k - 1$. Let's call those primes $p_1, \ldots, p_\ell$. Prove that the product of these primes, $N_2 := p_1 \cdots p_\ell$, is $\le N_1/2^k$.

(c) Generalize this argument to show that if there are r primes to be certified at the jth stage, then $N_{j+1} \le N_j/2^r$.

(d)† Prove that if there are m primes that were certified to be prime during all the steps of this argument, then $2^m \le n$. Explain why this implies that primality testing is in NP.

Exercise 10.7.5.† Suppose n is an odd composite, and $a^{(n-1)/2} \equiv 1$ or $-1 \pmod{n}$ for every a with $(a, n) = 1$. Deduce that $a^{(n-1)/2} \equiv 1 \pmod{n}$ for every a with $(a, n) = 1$ and that n is a Carmichael number.

Appendix 10A. Pseudoprime tests using square roots of 1

In section 7.6 we noted that the converse to Fermat's Little Theorem may be used to give a quick proof that a given integer n is composite: One simply finds an integer a, not divisible by n, for which $a^{n-1} \not\equiv 1 \pmod{n}$ (if this fails, that is, if $a^{n-1} \equiv 1 \pmod{n}$ and n is composite, then n is called a *base-a pseudoprime*). Such a search often works quickly, especially for randomly chosen values of n, but can fail if the tested n have some special structure. For example, it always fails for Carmichael numbers, which have the property that n is a base-a pseudoprime for every a with $(a, n) = 1$. What can we do in these cases? Can we construct a test, based on similar ideas, that is guaranteed to recognize even these composite numbers?

10.8. The difficulty of finding all square roots of 1

Lemma 10.1.1 implies that there are *at least* four distinct square roots of $1 \pmod{n}$, for any odd n which is divisible by at least two distinct primes. This suggests that we might try to prove that a given base-a pseudoprime n is composite by finding a square root of $1 \pmod{n}$ which is neither 1 nor -1. (If we can find such a square root of $1 \pmod{n}$, then we can partially factor n, as discussed in section 10.1.) The issue then becomes: How do we efficiently search for a square root of 1?

This is not difficult: Since n is a base-a pseudoprime, we have

$$\left(a^{\frac{n-1}{2}}\right)^2 = a^{n-1} \equiv 1 \pmod{n},$$

and so $a^{\frac{n-1}{2}} \pmod{n}$ is a square root of $1 \pmod{n}$. By Euler's criterion we know that if p is prime, then $a^{\frac{p-1}{2}} \equiv (a/p) \pmod{p}$, so that $a^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod{p}$. If n is a base-a pseudoprime (and therefore composite), it is feasible that $a^{\frac{n-1}{2}} \not\equiv (a/n) \pmod{n}$, which would imply that n is composite. If $a^{\frac{n-1}{2}} \pmod{n}$ is neither 1 nor

-1, this allows us to factor n into two parts, since

$$n \;=\; \gcd(a^{\frac{n-1}{2}} - 1, n) \;\cdot\; \gcd(a^{\frac{n-1}{2}} + 1, n).$$

If n is composite and $a^{\frac{n-1}{2}} \equiv (a/n) \pmod n$, then we call n a base-a *Euler pseudoprime*.

For example, 1105 is a Carmichael number, and so $2^{1104} \equiv 1 \pmod{1105}$. We take the square root, and determine that $2^{552} \equiv 1 \pmod{1105}$. So this method fails to prove that 1105 is composite, since 1105 is a base-2 Euler pseudoprime. But, wait a minute, 552 is even, so we can take the square root again, and a calculation reveals that $2^{276} \equiv 781 \pmod{1105}$. That is, 781 is a square root of 1 mod 1105, which proves that 1105 is composite. Moreover, since $\gcd(781-1, 1105) = 65$ and $\gcd(781+1, 1105) = 17$, we can even factor 1105 as 65×17.[13]

This property is even more striking mod 1729. In this case $1728 = 2^6 \cdot 27$ so we can take square roots many times. Indeed, taking successive square roots of 2^{1728} we determine that

$$1 \equiv 2^{1728} \equiv 2^{864} \equiv 2^{432} \equiv 2^{216} \pmod{1729}, \text{ but then } 2^{108} \equiv 1065 \pmod{1729}.$$

This proves that 1729 is composite, and even that

$$1729 = \gcd(1064, 1729) \times \gcd(1066, 1729) = 133 \times 13.$$

This protocol of taking successive square roots can fail to identify that our given pseudoprime is indeed composite; for example, we cannot use 103 to prove that either 561 or 1729 is composite, since

$$103^{35} \equiv 1 \pmod{561}, \text{ and so } 103^{70} \equiv \cdots \equiv 103^{560} \equiv 1 \pmod{561},$$
$$103^{27} \equiv -1 \pmod{1729}, \text{ and so } 103^{54} \equiv \cdots \equiv 103^{1728} \equiv 1 \pmod{1729},$$

but such failures are rare (see exercise 10.8.7).

Suppose that n is a composite integer with $n-1 = 2^k m$ for some integer $k \ge 1$ with m odd. We call n a base-a *strong pseudoprime* if the sequence of residues

$$a^{n-1} \pmod n,\ a^{(n-1)/2} \pmod n, \ldots,\ a^{(n-1)/2^k} \pmod n \tag{10.8.1}$$

is equal to either

$$1, 1, \ldots, 1 \quad \text{or} \quad 1, 1, \ldots, 1, -1, *, \ldots, *$$

where the $*$'s stand for any residue mod n. These are the only two possibilities if n is prime, and so if the sequence of residues in (10.8.1) looks like one of these two possibilities, then this information does not allow us to deduce that n is composite.

On the other hand, if n is a not a base-a strong pseudoprime, then we say that a is a *witness* (to n being composite). To be more precise:

Definition. *Suppose that n is a composite odd integer and $n-1 = 2^k m$ for some integer $k \ge 1$ with m odd. Assume that n is a base-a pseudoprime; that is, $a^{n-1} \equiv 1 \pmod n$. If $a^m \equiv 1 \pmod n$ or $a^{m \cdot 2^j} \equiv -1 \pmod n$ for some integer $j \ge 0$, then n is a* base-a strong pseudoprime. *Otherwise a is a* witness *(to the compositeness of n) and if ℓ is the largest integer for which $a^{m \cdot 2^\ell} \not\equiv -1$ or $1 \pmod n$, then $\gcd(a^{m \cdot 2^\ell} - 1, n)$ is a non-trivial factor of n.*

[13] We have not factored 1105 into prime factors (since 65 factors further as $65 = 5 \times 13$), but rather into two non-trivial factors.

One can compute high powers modulo n very rapidly using "fast exponentiation" (a technique we discussed in section 7.13 of appendix 7A), so this strong pseudoprime test can be done quickly and easily.

In exercise 10.8.7 we will show that at least three-quarters of the integers a, $1 \le a \le n$, with $(a, n) = 1$ are witnesses for n, for each odd composite $n > 9$. So can we find a witness quickly if n is composite?

• The most obvious idea is to try $a = 2, 3, 4, \ldots$ consecutively until we find a witness. It is believed that there is a witness $\le 2(\log n)^2$, but we cannot prove this (though we can deduce this from a famous conjecture, the Generalized Riemann Hypothesis[14]).

• Pick integers $a_1, a_2, \ldots, a_\ell, \ldots$ from $\{1, 2, 3, \ldots, n-1\}$ at random until we find a witness. By what we wrote above, if n is composite, then the probability that none of $a_1, a_2, \ldots, a_\ell$ are witnesses for n is $\le 1/4^\ell$. Thus with a hundred or so such tests we get a probability that is so small that it is inconceivable that it could occur in practice; so we believe that any integer n for which none of a hundred randomly chosen a's is a witness is prime. We call such n "*industrial strength primes*" since they have not been proven to be prime, but there is an enormous weight of evidence that they are not composite.

This test is a *random polynomial time* test for compositeness (like our test for finding a quadratic non-residue given at the end of appendix 8B). If n is composite, then the randomized witness test is almost certain to provide a short proof of n's compositeness in 100 runs of the test. On the other hand, if 100 runs of the test do not produce a witness, then we can be almost certain that n is prime, but we cannot be *absolutely* certain since no proof is provided, and therefore we have an industrial strength prime.

In practice the witness test accomplishes Gauss's dream of quickly distinguishing between primes and composites, for either we will quickly get a witness to n being composite or, if not, we can be almost certain that our industrial strength prime is indeed prime. Although this solves the problem in practice, we cannot be absolutely certain that we have distinguished correctly when we claim that n is prime since we have no proof, and mathematicians like proof. Indeed if you claim that industrial strength primes are prime, without proof, then a cynic might not believe that your randomly chosen a are so random or that you are unlucky or .... No, what we need is a proof that a number is prime when we think that it is.

Exercise 10.8.1. Find all bases b for which 15 is a base-b Euler pseudoprime.

Exercise 10.8.2.† We wish to show that every odd composite n is not a base-b Euler pseudoprime for some integer b, coprime to n. Suppose not, i.e., that n is a base-b Euler pseudoprime for every integer b with $(b, n) = 1$.

(a) Show that n is a Carmichael number.
(b) Show that if prime p divides n, then $p - 1$ cannot divide $\frac{n-1}{2}$.
(c) Deduce that $(b/n) \equiv (b/p) \pmod p$ for each prime p dividing n.
(d) Explain why (c) cannot hold for every integer b coprime to n.

[14] We discussed the Riemann Hypothesis, and its generalizations, in sections 5.16 and 5.17 of appendix 5D. Suffice to say that this is one of the most famous and difficult open problems of mathematics, so much so that the Clay Mathematics Institute has now offered one million dollars for its resolution (see `http://www.claymath.org/millennium-problems/`).

Exercise 10.8.3. Prove that $F_n = 2^{2^n} + 1$ is either a prime or a base-2 strong pseudoprime.

Exercise 10.8.4. Prove that if n is a base-2 pseudoprime, then $2^n - 1$ is a base-2 strong pseudoprime and a base-2 Euler pseudoprime. Deduce that there are infinitely many base-2 strong pseudoprimes.

Exercise 10.8.5. Pépin showed that one can test Fermat numbers F_m for primality by using just one strong pseudoprime test; i.e., F_m is prime if and only if $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$.

(a) Use exercise 8.5.4 to show if F_m is prime, then $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$.
(b) In the other direction show that if $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$, then $\mathrm{ord}_p(3) = 2^{2^m}$ whenever prime $p|F_m$.
(c) Deduce that $F_m - 1 \le p - 1$ in (b) and so F_m is prime.

Exercise 10.8.6.† (a) Prove that $A := (4^p + 1)/5$ is composite for all primes $p > 3$.
(b) Deduce that A is a base-2 strong pseudoprime.

Exercise 10.8.7.‡ How many witnesses are there mod n? Suppose that $n - 1 = 2^k m$ with m odd and $k \ge 1$, and that n has ω distinct prime factors. Let g_p be the largest odd integer dividing $(p-1, n-1)$, and let 2^{R+1} be the largest power of 2 dividing $\gcd(p-1 : p|n)$.

(a) Prove that $R \le k - 1$.
(b) Show that (10.8.1) is $1, 1, \dots, 1$ if and only if $a^{g_p} \equiv 1 \pmod{p^e}$ for every prime power $p^e \| n$.
(c) Show that there are $\prod_{p|n} g_p$ such integers $a \pmod n$.
(d) Show that if (10.8.1) is $1, 1, \dots, 1, -1, *, \dots, *$, with r *'s at the end, then $0 \le r \le R$, and that this holds if and only if $a^{2^r g_p} \equiv -1 \pmod{p^e}$ for every prime power $p^e \| n$.
(e) Show that there are $\le \prod_{p|n} 2^r g_p$ such integers $a \pmod n$.
(f) Show the number of strong pseudoprimes mod n is

$$\prod_{p|n} (2^R g_p) \cdot \left(1 + \frac{1}{2^\omega} + \frac{1}{2^{2\omega}} + \cdots + \frac{1}{2^{(R-1)\omega}} + \frac{2}{2^{R\omega}}\right).$$

(g) Prove that $2^R g_p \le \frac{p-1}{2}$ and so deduce that the quantity in (f) is $\le \frac{\phi(n)}{2^{\omega-1}}$, and so is $< \frac{1}{4}\phi(n)$ if $\omega \ge 3$.
(h) Show that there are $\le \frac{1}{4}\phi(n)$ reduced residues mod n which are not witnesses, whenever $n \ge 10$ with equality holding if and only if either
- $n = pq$ where $p = 2m + 1, q = 4m + 1$ are primes with m odd, or
- $n = pqr$ is a Carmichael number with p, q, r primes each $\equiv 3 \pmod 4$ (e.g., $7 \cdot 19 \cdot 67$).

Appendices. The extended version of chapter 10 has the following additional appendices:

Appendix 10B. *Factoring with squares.* We explain various factoring algorithms such as random squares, the continued fraction method, and the quadratic sieve and its variations, which all construct a multiple of n as the difference of two squares.

Appendix 10C. *Identifying primes of a given size.* We establish primality tests that work when $n - 1$ or $n + 1$ is partially factored. This is useful in practice for quickly finding large primes and was used in the recent proof of the ternary Goldbach conjecture.

Appendix 10D. *Carmichael numbers.* We discuss a construction to find families of Carmichael numbers with many prime factors.

Appendix 10E. *Cryptosystems based on discrete logarithms.* We describe how the discrete log problem lies behind some strong cryptographic protocols, for example the Diffie-Hellman key exchange and the El Gamal cryptosystem.

Appendix 10F. *Running times of algorithms.* No one knows whether there is a truly safe cryptographic protocol. We prove here that if there is one (appropriately defined), then the complexity class NP must be strictly larger than the complexity

class P; that is, P≠NP, the most famous and tantalizing open question of theoretical computer science. We also discuss how, although the overwhelming majority of mathematical problems are not in P, we have yet to identfy one specific example that is not in P.

Appendix 10G. *The AKS test.* We prove that the AKS test, as given in Theorem 10.1, is a valid primality test, though we do not establish its running time.

Appendix 10H. *Factoring algorithms for polynomials* play an important role in number theory. Here we present the very useful Eisenstein irreducibility criterion to test whether a given polynomial can be factored into smaller parts.

Chapter 11

Rational approximations to real numbers

How well can we approximate a real number by rational numbers? Obviously we can approximate π by $3, 3.1, 3.14$, etc., but there are even better approximations like $3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \ldots$ (see section 11.9 of appendix 11B for details). Are these the "best" approximations? And how do we measure how good an approximation is? We study these questions in detail in this chapter.

To start with we could ask how well we could approximate a rational number $\alpha = p/q$ with $(p, q) = 1$ and $q \geq 1$, by other, unequal, rational numbers. For any rational m/n with $n \geq 1$, which is $\neq p/q$, the difference is

$$\left| \frac{p}{q} - \frac{m}{n} \right| = \frac{|pn - qm|}{qn} \geq \frac{1}{qn} \tag{11.0.1}$$

since $|pn - qm|$ is a non-negative integer that cannot be 0 as $p/q \neq m/n$, and so must be ≥ 1. We have therefore shown that the difference between rational α and an approximation m/n is at least some constant (in this case $1/q$) times $1/n$. We will see in the next section that one obtains much better approximations when α is real and irrational.

11.1. The pigeonhole principle

If real irrational α is very close to m/n, then $n\alpha$ must be close to m, so we are interested in how close the integer multiples of a given real number α can be to an integer. Dirichlet noted that one can get a surprisingly good answer to this question using the pigeonhole principle.

Theorem 11.1 (Dirichlet's Theorem)**.** *Suppose that α is a given real number. For every integer $N \geq 1$ there exists a positive integer $n \leq N$ such that*

$$|n\alpha - m| < \frac{1}{N},$$

for some integer m. In other words,

$$\left|\alpha - \frac{m}{n}\right| \ < \ \frac{1}{nN}.$$

Proof. The $N+1$ numbers $\{0\cdot\alpha\}$, $\{1\cdot\alpha\}$, $\{2\cdot\alpha\}, \dots,$ $\{N\cdot\alpha\}$ (where $\{t\}$ denotes the fractional part of t) all lie in the interval $[0,1)$. The intervals

$$\left[0, \frac{1}{N}\right), \ \left[\frac{1}{N}, \frac{2}{N}\right), \dots, \ \left[\frac{N-1}{N}, 1\right)$$

partition $[0,1)$,[1] and so each of our $N+1$ numbers lies in exactly one of the N intervals. Therefore some interval must contain at least two of our numbers by the pigeonhole principle, say $\{i\alpha\}$ and $\{j\alpha\}$ with $0 \leq i < j \leq N$, so that $|\{i\alpha\} - \{j\alpha\}| < \frac{1}{N}$. Therefore, if $n = j - i$, then $1 \leq n \leq N$, and if $m := [j\alpha] - [i\alpha] \in \mathbb{Z}$, then

$$n\alpha - m = (j\alpha - i\alpha) - ([j\alpha] - [i\alpha]) = \{j\alpha\} - \{i\alpha\},$$

and the first result follows by taking absolute values. The second result follows by dividing through by n. □

Exercise 11.1.1. Prove that for any irrational real number α there are arbitrarily small real numbers of the form $a + b\alpha$ with $a, b \in \mathbb{Z}$.

Corollary 11.1.1. *If α is a real irrational number, then there are infinitely many pairs m, n of coprime integers for which*

$$\left|\alpha - \frac{m}{n}\right| \ < \ \frac{1}{n^2}.$$

For large n this is a far better approximation of α than one can obtain for rational numbers, as we saw in (11.0.1).

Proof. Suppose that we are given a finite list, (m_j, n_j), $1 \leq j \leq k$, of solutions to this inequality. Since this is a finite list there is some solution with $|n_j\alpha - m_j|$ minimal, and $|n_j\alpha - m_j|$ must be > 0 as α is irrational. Therefore we can let N be the smallest integer $\geq 1/\min_{1\leq j\leq k}\{|n_j\alpha - m_j|\}$. By Dirichlet's Theorem there exists $n \leq N$ such that

$$\left|\alpha - \frac{m}{n}\right| \ < \ \frac{1}{nN} \ \leq \ \frac{1}{n^2}.$$

Now

$$|n\alpha - m| < \frac{1}{N} \ \leq \ |n_j\alpha - m_j| \ \text{ for all } j,$$

and so (n, m) is another solution to the inequality, not included in the list. This implies that any finite list of solutions can be extended, and so there are infinitely many solutions. □

[1] That is, each point of $[0,1)$ lies in exactly one of these intervals, and the union of these intervals exactly equals $[0,1)$.

Dirichlet's Theorem is a very useful result as we will now exhibit by reproving two big results from earlier in the book:

Another proof of Corollary 3.5.2. [*If* $(a,m)=1$*, then* a *has an inverse* mod m.] Take $m\ge 2$. Let $\alpha=\frac{a}{m}$ and $N=m-1$ in Dirichlet's Theorem so that there exist integers r and s with $r\le m-1$ such that $|ra/m-s|<1/(m-1)$; that is, $|ra-sm|<m/(m-1)\le 2$. Hence $ra-sm=-1,0$, or 1. It cannot equal 0 or else $m|sm=ar$ and $(m,a)=1$ so that $m|r$ which is impossible as $r<m$. Hence $ra\equiv\pm 1 \pmod m$ and so $\pm r$ is the inverse of $a \pmod m$. □

We saw an important use of the pigeonhole principle in number theory in the proof of Theorem 9.1, and this idea was generalized significantly by Minkowski and others. Now we reprove Theorem 9.1 using Dirichlet's Theorem:

Another proof of Theorem 9.1. [*If* -1 *is a square* mod n*, then* n *is the sum of two squares.*] Suppose that $r^2\equiv -1 \pmod n$. By Dirichlet's Theorem there exists a positive integer $b<\sqrt{n}$ such that $|-\frac{r}{n}-\frac{c}{b}|<\frac{1}{b\sqrt{n}}$ for some integer c. Multiplying through by bn we deduce that $|a|<\sqrt{n}$ where $a=rb+cn$. Now $a\equiv rb \pmod n$ and so $a^2+b^2\equiv r^2b^2+b^2=(r^2+1)b^2\equiv 0 \pmod n$, and $0<a^2+b^2<n+n=2n$, and so we must have $a^2+b^2=n$. □

For irrational α one might ask how the numbers $\{\alpha\}$, $\{2\alpha\},\dots,$ $\{N\alpha\}$ are distributed in $[0,1)$ as $N\to\infty$, for α irrational. In section 11.7 of appendix 11A we will show that the values are dense and even (roughly) equally distributed in $[0,1)$. This ties in with the geometry of the torus and with exponential sum theory.

The next two exercises are multidimensional generalizations of Dirichlet's Theorem with not dissimilar proofs.

Exercise 11.1.2 (Simultaneous approximation)**.** Suppose that $\alpha_1,\dots,\alpha_k$ are given real numbers. Prove that for any positive integer N there exists a positive integer $n\le N^k$ such that, for each j in the range $1\le j\le k$, there exists an integer m_j for which

$$|n\alpha_j-m_j| \ < \ \frac{1}{N}.$$

Deduce that given $\alpha_1,\dots,\alpha_k\in\mathbb{R}$ there exist integers q, $1\le q\le Q$, and $p_1,\dots,p_k$ such that

$$\left|\alpha_1-\frac{p_1}{q}\right|\le\frac{1}{q^{1+1/k}},\quad \left|\alpha_2-\frac{p_2}{q}\right|\le\frac{1}{q^{1+1/k}},\ \dots,\ \left|\alpha_k-\frac{p_k}{q}\right|\le\frac{1}{q^{1+1/k}}.$$

Exercise 11.1.3. Suppose that $\alpha_1,\dots,\alpha_k$ are given real numbers. Prove that for any positive integer N there exist integers $n_1,n_2,\dots,n_k$, not all zero, with each $|n_j|\le N$, and an integer m for which

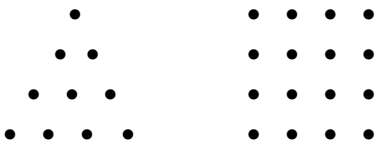
$$|n_1\alpha_1+n_2\alpha_2+\cdots+n_k\alpha_k-m| \ < \ \frac{1}{N^k}.$$

11.2. Pell's equation

Perhaps the most researched equation in the early history of number theory is the so-called *Pell equation*:[2] Are there non-trivial integer solutions x, y to

$$x^2 - dy^2 = 1?$$

(The "trivial solutions" are $x = \pm 1$ and $y = 0$.) The best-known ancient example comes from comparing the number of points in triangles of points, with the number of points in squares of points:



This triangle has $1 + 2 + 3 + 4 = 10$ points, whereas this square has $4 \times 4 = 16$. In general a triangle with m rows has $\frac{m(m+1)}{2}$ points, and a square with n rows has n^2 points. The numbers appearing in these two lists are mostly different, but there are exceptions, for example, 1, and then $36 = \frac{8 \cdot 9}{2} = 6^2$, and then $1225 = \frac{49 \cdot 50}{2} = 35^2$. So are there arbitrarily many "triangular numbers" that are also squares? More precisely, we are asking whether there are infinitely many pairs of integers m, n such that

$$\frac{m(m+1)}{2} = n^2.$$

It makes sense to clear denominators and to "complete the square" on the left side. Then we get

$$(2m+1)^2 = 4m^2 + 4m + 1 = 8 \cdot \frac{m(m+1)}{2} + 1 = 8n^2 + 1.$$

Taking $x = 2m + 1$ and $y = 2n$ gives a solution to the Pell equation

$$x^2 - 2y^2 = 1.$$

On the other hand note that any solution to the Pell equation must have x odd, so is of the form $2m+1$, which implies that $2y^2 = x^2 - 1 \equiv 1 - 1 \equiv 0 \pmod 8$ and so y is even and therefore must be of the form $2n$. (Our examples of triangular numbers above therefore correspond to the solutions $3^2 - 2 \cdot 2^2 = 1$, $17^2 - 2 \cdot 12^2 = 1$, and $99^2 - 2 \cdot 70^2 = 1$ to Pell's equation.) So we have proved that the set of triangular numbers that are also squares are in 1-to-1 correspondence with the positive integer solutions to this Pell equation.

We will show in Theorem 11.2 that there is a non-trivial solution to Pell's equation $x^2 - dy^2 = 1$ for every non-square integer $d > 1$. This was evidently known to Brahmagupta in India in 628 A.D., and one can guess that it was well

[2] In 1657 Fermat challenged Frénicle, Brouncker, Wallis, and "all mathematicians" to create a method for finding solutions to Pell's equation. Brouncker showed that he had done so by determining the smallest solution for $d = 313$, namely $x = 32188120829134849$, $y = 1819380158564160$. It seems that Euler attributed the equation to Pell because Rahn published an algebra book with Pell's help in 1658, which contained an example of this type of equation. The name stuck.

understood by Archimedes far earlier, judging by his "Cattle Problem":

The Sun god's cattle, friend, apply thy care
to count their number, hast thou wisdom's share.
They grazed of old on the Thrinacian floor
of Sic'ly's island, herded into four,
colour by colour: one herd white as cream,
the next in coats glowing with ebon gleam,
brown-skinned the third, and stained with spots the last.
Each herd saw bulls in power unsurpassed,
in ratios these: count half the ebon-hued,
add one third more, then all the brown include;
thus, friend, canst thou the white bulls' number tell.
The ebon did the brown exceed as well,
now by a fourth and fifth part of the stained.
To know the spotted — all bulls that remained —
reckon again the brown bulls, and unite
these with a sixth and seventh of the white.
Among the cows, the tale of silver-haired
was, when with bulls and cows of black compared,
exactly one in three plus one in four.
The black cows counted one in four once more,
plus now a fifth, of the bespeckled breed
when, bulls withal, they wandered out to feed.
The speckled cows tallied a fifth and sixth
of all the brown-haired, males and females mixed.
Lastly, the brown cows numbered half a third
and one in seven of the silver herd.
Tell'st thou unfailingly how many head
the Sun possessed, o friend, both bulls well-fed
and cows of ev'ry colour – no-one will
deny that thou hast numbers' art and skill,
though not yet dost thou rank among the wise.
But come! also the foll'wing recognise.

Whene'er the Sun god's white bulls joined the black,
their multitude would gather in a pack
of equal length and breadth, and squarely throng
Thrinacia's territory broad and long.
But when the brown bulls mingled with the flecked,
in rows growing from one would they collect,
forming a perfect triangle, with ne'er
a diff'rent-coloured bull, and none to spare.
Friend, canst thou analyse this in thy mind,
and of these masses all the measures find,
go forth in glory! be assured all deem
thy wisdom in this discipline supreme!

— from an epigram written to Eratosthenes of Cyrene
by Archimedes (of Alexandria), 250 B.C.[3]

The first paragraph involves only linear equations. To resolve the second, one needs to find a non-trivial solution in integers u, v to

$$u^2 - 609 \cdot 7766v^2 = 1.$$

The smallest solution is enormous, the smallest herd having about 7.76×10^{206544} cattle: It wasn't until 1965 that anyone was able to write down all 206545 decimal digits! How did Archimedes *know* that the solution would be ridiculously large? We don't know, though presumably he did not ask this question by chance.

The next result, the main result of this section, presumably known to many ancient mathematicians, is that there is always a solution to Pell's equation.

Theorem 11.2. *Let $d \geq 2$ be a given non-square integer. There exist integers x, y for which*

$$x^2 - dy^2 = 1,$$

with $y \neq 0$. If x_1, y_1 yields the smallest solution in positive integers,[4] *then all other solutions are given by the recursion*

$$x_{n+1} = x_1 x_n + d y_1 y_n \quad \textit{and} \quad y_{n+1} = x_1 y_n + y_1 x_n \quad \textit{for } n \geq 1.$$

We call the pair (x_1, y_1) the fundamental solution *to Pell's equation. Another way*

[3] *Archimedes, The Cattle Problem*, in English verse by S. J. P. Hillion & H. W. Lenstra Jr., Mercator, Santpoort, 1999.

[4] We measure the size of the solutions in positive integers x, y by the number $x + \sqrt{d}y$, though we would have the same ordering if we used either x or y.

to write the recursion is that

$$x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n \text{ for every integer } n \geq 1,$$

where we match the coefficients of $\sqrt{d}$ *on each side to determine* y_n*, and what remains, the coefficients of* 1 *on each side, to determine* x_n*.*

Proof. We begin by showing that there always exists a solution to $x^2 - dy^2 = 1$ in integers with $y \neq 0$. By Corollary 11.1.1, there exist infinitely many pairs of integers (m, n) such that $|\sqrt{d} - \frac{m}{n}| < \frac{1}{n^2}$. For these pairs (m, n) we have

$$|m^2 - dn^2| = n^2 \left|\sqrt{d} - \frac{m}{n}\right| \cdot \left|\sqrt{d} + \frac{m}{n}\right| < \left|\sqrt{d} + \frac{m}{n}\right| \leq 2\sqrt{d} + \left|\sqrt{d} - \frac{m}{n}\right| < 2\sqrt{d} + 1.$$

This implies that $|m^2 - dn^2|$ must be an integer $< 2\sqrt{d} + 1$, so there must be some non-zero integer r, with $|r| < 2\sqrt{d} + 1$, for which there are infinitely many pairs of positive integers m, n such that $m^2 - dn^2 = r$. Pick the smallest such r. We can assume that each $(m, n) = 1$ or else if $(m, n) = g$ occurs infinitely often, then we have infinitely many solutions $(m/g)^2 - d(n/g)^2 = r/g^2$, contradicting the minimality of r.

Since there are only r^2 pairs of residue classes $(m \mod r,\ n \mod r)$ there must be some pair of residue classes a, b such that there are infinitely many pairs of integers m, n for which $m^2 - dn^2 = r$ with $m \equiv a \pmod r$ and $n \equiv b \pmod r$. Let m_1, n_1 be the smallest such pair, and m, n any other such pair, so that $m_1^2 - dn_1^2 = m^2 - dn^2 = r$ with $m_1 \equiv m \pmod r$ and $n_1 \equiv n \pmod r$. This implies that $r|(m_1 n - n_1 m)$ and

$$(m_1 m - dn_1 n)^2 - d(m_1 n - n_1 m)^2 = (m_1^2 - dn_1^2)(m^2 - dn^2) = r^2,$$

so that r^2 divides $r^2 + d(m_1 n - n_1 m)^2 = (m_1 m - dn_1 n)^2$, and thus $r|(m_1 m - dn_1 n)$. Therefore $x = |m_1 m - dn_1 n|/r$ and $y = |m_1 n - n_1 m|/r$ are integers for which $x^2 - dy^2 = 1$.

Exercise 11.2.1. Show that $y \neq 0$ using the fact that $(m, n) = 1$ for each such pair m, n.

We measure the size of solutions to Pell's equation, using the number $x + \sqrt{d}y$. If $x, y > 0$, then this is > 1. There are four solutions associated with each solution in positive integers u, v, and for these we have

$$u + \sqrt{d}v > 1 > u - \sqrt{d}v > 0 > -u + \sqrt{d}v > -1 > -u - \sqrt{d}v.$$

Therefore $x, y > 0$ if and only if $x + \sqrt{d}y > 1$.

Let x_1, y_1 be the solution to $x^2 - dy^2 = 1$ in positive integers with $x_1 + \sqrt{d}y_1$ minimal. We claim that all other solutions with $x, y > 0$ take the form $x + \sqrt{d}y = (x_1 + \sqrt{d}y_1)^n$. If not, let x, y be the counterexample with $x, y > 0$ for which $x + \sqrt{d}y$ is smallest. Now $x + \sqrt{d}y > x_1 + \sqrt{d}y_1$ since $x_1 + \sqrt{d}y_1$ is minimal.

If $X = x_1 x - dy_1 y$ and $Y = x_1 y - y_1 x$, then $X^2 - dY^2 = (x_1^2 - dy_1^2)(x^2 - dy^2) = 1$, and

$$X + \sqrt{d}Y = (x_1 - \sqrt{d}y_1)(x + \sqrt{d}y) = \frac{x + \sqrt{d}y}{x_1 + \sqrt{d}y_1},$$

which implies that

$$1 < X + \sqrt{d}Y < x + \sqrt{d}y.$$

Hence $X, Y > 0$, and since x, y was the smallest counterexample, we deduce that

$$X + \sqrt{d}Y = (x_1 + \sqrt{d}y_1)^m \text{ for some integer } m \geq 1,$$

and therefore $x+\sqrt{d}y = (x_1+\sqrt{d}y_1)(X+\sqrt{d}Y) = (x_1+\sqrt{d}y_1)^{m+1}$, a contradiction.

If we define $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$, then we obtain the recursion given in the theorem by an easy induction argument. We also deduce that the $x_n, y_n > 0$ and so $x_1 < x_2 < \cdots$ and $y_1 < y_2 < \cdots$ from the recursion formulas. □

Exercise 11.2.2. Prove that if $a + \sqrt{d}b = x + \sqrt{d}y$ where a, b, x, y, d are integers and d is not a square, then $a = x$ and $b = y$.

Exercise 11.2.3. Prove, by induction, that $x_{n+2} = 2x_1x_{n+1} - x_n$ and $y_{n+2} = 2x_1y_{n+1} - y_n$ for all $n \geq 0$.

Exercise 11.2.4. Show that all solutions to Pell's equation (not just the positive integer solutions) are given by the values $\pm(x_1 + \sqrt{d}y_1)^n$ (not just "+"), with $n \in \mathbb{Z}$ (not just $n \in \mathbb{N}$).

For technical reasons it is actually best to develop the analogous theory for the solutions to $x^2 - dy^2 = \pm 4$, as in appendix 11B, when we revisit Pell equations.

In the second half of the proof we saw how all of the solutions in positive integers can be generated from a fundamental solution. The proof is interesting in that it works by "descent": Given a solution we find a smaller one. This is a technique that we saw several times in chapter 6. We will see it play a central role in section 11.3, and later when we study elliptic curves in chapter 17.

The proof of Theorem 11.2 is not constructive, in that the proof does not indicate how to find a solution. In Lemma 11.11.2 of appendix 11B we will show how to find solutions using the continued fraction for $\sqrt{d}$ (as was known to all of the ancient mathematicians discussed here). How large is the smallest solution to Pell's equation? We saw that it can be surprisingly large, as in Archimedes's cattle problem. One can prove that the smallest solution is $\leq (8d)^{\sqrt{d}}$ (see section 13.7 of appendix 13B). However what is surprising is that the smallest solution seems to usually be this large. This is not something that has been proved; indeed understanding the distribution of sizes of the smallest solutions to Pell's equation is an outstanding open question in number theory.

In Theorem 11.2 we saw that if $d > 1$ is a non-square integer, then there are always solutions in integers $x, y > 0$ to Pell's equation $x^2 - dy^2 = 1$. This implies that

$$\sqrt{d}y(x - \sqrt{d}y) < (x + \sqrt{d}y)(x - \sqrt{d}y) = 1,$$

and so, dividing through by $\sqrt{d}y^2$, we exhibit rational approximations x/y to $\sqrt{d}$ that satisfy

$$\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{\sqrt{d}y^2},$$

which are better approximations than those that are given by Corollary 11.1.1.

Another issue is whether there is a solution to $u^2 - dv^2 = -1$, the *negative Pell equation*. Notice, for example, that $2^2 - 5 \cdot 1^2 = -1$. Evidently if there is a solution, then -1 is a square mod d, so that d has no prime factors $\equiv -1 \pmod 4$. Moreover d cannot be divisible by 4 or else $u^2 \equiv -1 \pmod 4$ which is impossible. We saw that $x^2 - dy^2 = 1$ has solutions for every non-square $d > 1$, and one might

have guessed that there would be some simple criterion to decide whether there are solutions to $u^2 - dv^2 = -1$, but there does not appear to be. For example there are no solutions for $d = 34$, 205, or 221, yet in each case there is no congruence that easily explains why not. This is a subject of ongoing research. We will discuss the negative Pell equation in the next paragraph as well as in section 11.13 of appendix 11B .

The case $d = 5$ has many fascinating properties. For example

$$1^2 - 5 \cdot 1^2 = -4,\ 3^2 - 5 \cdot 1^2 = 4,\ 4^2 - 5 \cdot 2^2 = -4,\ 7^2 - 5 \cdot 3^2 = 4, \dots .$$

All these solutions to $x^2 - 5y^2 = -4$ or 4 are given by $\frac{x+\sqrt{5}y}{2} = (\frac{1+\sqrt{5}}{2})^n$. If there are solutions to $x^2 - dy^2 = \pm 4$ with x, y both odd (as in this example), then $1 - d \equiv x^2 - dy^2 \equiv 0 \pmod 4$; that is, $d \equiv 1 \pmod 4$. If $d \equiv 1 \pmod 4$, then the proof of Theorem 11.2 can be used to prove there exist integers $u, v > 0$ such that:

All solutions to $x^2 - dy^2 = \pm 4$ with $x, y > 0$ are given by

$$\frac{x + \sqrt{d}y}{2} = \left(\frac{u + \sqrt{d}v}{2}\right)^n \text{ for some integer } n \geq 1.$$

To establish that there is at least one solution take $x = 2r, y = 2s$ from a solution to $r^2 - ds^2 = 1$ given by Theorem 11.2. Now select the solution to our equation with $\frac{u+\sqrt{d}v}{2} > 1$ but minimal. The proof of Theorem 11.2, suitably modified, then gives that all other solutions are given by a power of this first one.

We call $\frac{u+\sqrt{d}v}{2}$ the *fundamental solution* to Pell's equation and denote it by ϵ_d.

Exercise 11.2.5. The smallest solution to $x^2 - 2y^2 = 1$ is given by $(x, y) = (3, 2)$, which implies that 2^3 and 3^2 are consecutive *powerful numbers* (integer n is powerful if p^2 divides n whenever a prime p divides n). Use the theory of the solutions to $x^2 - 2y^2 = 1$ to prove that there are infinitely many pairs of consecutive powerful numbers.

11.3. *Descent on solutions of* $x^2 - dy^2 = n,\ d > 0$

Let x_1, y_1 be the fundamental solution to Pell's equation, and let $\epsilon_d = x_1 + y_1\sqrt{d}$ as in Theorem 11.2, so that $\epsilon_d > 1$.

Proposition 11.3.1. *Given integers d, $n > 0$, the integer solutions x, y to $x^2 - dy^2 = n$ are all given by $\pm\epsilon_d^k\beta$ for some integer k, where*

$$\beta \in B := \{u + \sqrt{d}v \in [\sqrt{n}, \sqrt{n}\epsilon_d) :\ u, v \geq 1 \text{ and } u^2 - dv^2 = n\}.$$

Proof. Given a solution to $x^2 - dy^2 = n$, let $\alpha = |x + y\sqrt{d}|$. As $\epsilon_d > 1$ the sequence of numbers $1, \epsilon_d, \epsilon_d^2, \dots$ increases to infinity, and the sequence of numbers $1, \epsilon_d^{-1}, \epsilon_d^{-2}, \dots$ decreases to 0. Therefore there exists a unique integer k such that

$$\epsilon_d^k \leq |\alpha|/\sqrt{n} < \epsilon_d^{k+1}.$$

Let $\beta := |\alpha|\epsilon_d^{-k}$, so that $\sqrt{n} \leq \beta < \sqrt{n}\epsilon_d$. Therefore α is of the form $\pm\beta\epsilon_d^k$, where $\beta \in [\sqrt{n}, \sqrt{n}\epsilon_d)$. Writing $\beta = u + \sqrt{d}v$ we obtain

$$\begin{aligned} u^2 - dv^2 &= |(x + y\sqrt{d})(x - y\sqrt{d})| \cdot ((x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d}))^{-k} \\ &= (x^2 - dy^2)(x_1^2 - dy_1^2)^{-k} = n \cdot 1^{-k} = n. \end{aligned}$$

Moreover for a solution of $r^2 - ds^2 = n$ where $n > 0$, with $r, s \geq 0$, we have

$$\gamma := r + s\sqrt{d} > \sqrt{n} > n/\gamma = r - s\sqrt{d} > 0 > -r + s\sqrt{d} > -r - s\sqrt{d},$$

so of these four closely related solutions the unique one $> \sqrt{n}$ has both coordinates positive. In particular this implies that $u, v > 0$, so that $\beta \in B$. □

For $n = 1$ we have $B = \{1\}$. In some questions B can be empty; in others it can be large. For example, there are no solutions to $x^2 - dy^2 = n$ in integers if n is not a square mod d.

In the example $x^2 - 5y^2 = 209$, we have $\epsilon_5 = \left(\frac{1+\sqrt{5}}{2}\right)^6 = 9 + 4\sqrt{5}$ and, after a brief search we discover that $B = \{17 + 4\sqrt{5},\ 47 + 20\sqrt{5}\}$.

Exercise 11.3.1. Find all integer solutions x, y to (a) $x^2 - 5y^2 = -4$; (b) $x^2 - 5y^2 = 4$; (c) $x^2 - 5y^2 = -1$; (d) $x^2 - 5y^2 = 1$; (e) $x^2 - 5y^2 = -20$; (f) $x^2 - 5y^2 = -11$.

Exercise 11.3.2. Prove that for any non-square positive integer d and integer n there is either no solution or infinitely many solutions to $x^2 - dy^2 = n$.

11.4. Transcendental numbers

In section 3.4 we proved that $\sqrt{d}$ is irrational if d is an integer that is not the square of an integer. We can also prove that certain numbers are irrational simply by establishing how well they can be approximated by rationals:

Proposition 11.4.1. *Suppose that α is a given real number. Then α is irrational if and only if for every integer $q \geq 1$ there exist integers m, n such that*

$$0 < |n\alpha - m| < \frac{1}{q}.$$

Proof. If α is rational, then $\alpha = p/q$ for some coprime integers p, q with $q \geq 1$. For any integers m, n we then have $n\alpha - m = (np - mq)/q$. Now, the value of $np - mq$ is an integer $\equiv np \pmod{q}$. Hence $|np - mq| = 0$ or is an integer ≥ 1, and therefore $|n\alpha - m| = 0$ or is $\geq 1/q$.

If α is irrational, then Corollary 11.1.1 tells us that there are arbitrarily large coprime integers m, n for which $0 < |n\alpha - m| < \frac{1}{n}$. We select $n > q$ to prove the result claimed here. □

There are several other methods to prove that numbers are irrational, but it is more challenging to prove that a number is *transcendental*, that is, that the number is *not* the root of a polynomial with integer coefficients.[5] Next we show that algebraic numbers cannot be too well approximated by rationals. This suggests a method to identify a number as transcendental, generalizing how we identified irrationality in Proposition 11.4.1.

Theorem 11.3 (Liouville's Theorem)**.** *Suppose that α is a root of an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree $d \geq 2$. There exists a constant $c_\alpha > 0$ (which*

[5] The root of a polynomial with integer coefficients is called *an algebraic number*.

depends only on α)[6] *such that for any rational p/q with $(p,q)=1$ and $q\geq 1$ we have*

$$\left|\alpha-\frac{p}{q}\right| \;\geq\; \frac{c_\alpha}{q^d}.$$

Proof. Since $I:=[\alpha-1,\alpha+1]$ is a closed interval, there exists a bound $B\geq 1$ for which $|f'(t)|\leq B$ for all $t\in I$. We will prove the result with $c_\alpha=1/B$. If $p/q\notin I$, then $|\alpha-p/q|\geq 1\geq c_\alpha\geq c_\alpha/q^d$ as desired. Henceforth we may assume that $p/q\in I$.

If $f(x)=\sum_{i=0}^d f_i x^i$ with each $f_i\in\mathbb{Z}$, then $q^d f(p/q)=\sum_{i=0}^d f_i p^i q^{d-i}\in\mathbb{Z}$. Now $f(p/q)\neq 0$ since f is irreducible of degree ≥ 2 and so $|q^d f(p/q)|\geq 1$.

The mean value theorem tells us that there exists t lying between α and p/q, and hence in I, such that

$$f'(t)=\frac{f(\alpha)-f(p/q)}{\alpha-p/q}.$$

Therefore, as $f(\alpha)=0$,

$$\left|\alpha-\frac{p}{q}\right| \;=\; \frac{|q^d f(p/q)|}{q^d|f'(t)|} \;\geq\; \frac{1}{Bq^d} = \;\frac{c_\alpha}{q^d}. \qquad \square$$

Often students first learn to prove that there are transcendental numbers by showing that the set of real numbers is uncountable; in contrast, the set of algebraic numbers is countable, so the vast majority of real numbers are transcendental. This argument yields that most real numbers are transcendental, without actually constructing any! (See section 11.16 in appendix 11D.) The great advantage of Liouville's Theorem is that it can be used to actually construct transcendental numbers.

Corollary 11.4.1. *A* Liouville number *is an irrational real number α such that for every integer $n\geq 1$ there is a rational number p/q with $(p,q)=1$ and $q>1$ for which*

$$\left|\alpha-\frac{p}{q}\right| \;<\; \frac{1}{q^n}.$$

Every Liouville number is transcendental.

Proof. Let α be a Liouville number. Suppose that α is algebraic so that there exist d and c_α as in Liouville's Theorem. Select $n>d$ sufficiently large so that $2^{n-d}>1/c_\alpha$. Then, selecting the approximation p/q with $q>1$ as in the hypothesis we have

$$\frac{1}{q^n}>\left|\alpha-\frac{p}{q}\right|\geq\frac{c_\alpha}{q^d},$$

by Liouville's Theorem. Therefore $2^{n-d}>1/c_\alpha>q^{n-d}$, contradicting that $q\geq 2$. Therefore α is not algebraic and so must be transcendental. $\square$

[6] In this chapter there are several constants like c_α which depend only on the variable given in the subscript. We do not attempt to be more precise about the constant because calculating a value for the constant will make things much more complicated, yet one will gain little from knowing its precise value.

For example

$$\alpha = \frac{1}{10} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots$$

is a Liouville number, since if p/q with $q = 10^{n!}$ is the sum of the first n terms, then $0 < \alpha - p/q < 2/q^{n+1} < 1/q^n$.

Liouville numbers are easily identifiable transcendental numbers, but there are many transcendental numbers which are not Liouville numbers, like π and e.

Liouville's Theorem has been improved to its, more or less, final form by Roth. To explain his result we have to introduce an ϵ and that sort of thing: For any *fixed* $\epsilon > 0$ (which should be thought of as being small), there exists a constant $\kappa_\epsilon > 0$, which depends on ϵ, and is chosen so it works in the proof.[7] In the notation in Roth's Theorem we have to go a little further than this since the constant also depends on the value of α we need to approximate, so our constant is $c_{\alpha,\epsilon}$, which depends on both α and ϵ, but nothing else. These dependencies do restrict our use of the inexplicit constants $c_{\alpha,\epsilon}$; for example, one cannot compare the constants that arise from different values of α.

Theorem 11.4 (Roth's Theorem, 1955)**.** *Suppose that α is an irrational real algebraic number. For any fixed $\epsilon > 0$ there exists a constant $c_{\alpha,\epsilon} > 0$ such that for any rational p/q with $(p, q) = 1$ and $q \geq 1$ we have*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c_{\alpha,\epsilon}}{q^{2+\epsilon}}.$$

The exponent "$2 + \epsilon$" in Roth's Theorem cannot be improved much since if α is irrational, then there are infinitely many p/q with $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$, by Corollary 11.1.1. We will prove that approximations which are a little better than this must be convergents of the continued fraction of α (see Corollary 11.10.1 in section 11.10 of appendix 11B). The "worst approximable" irrational number is therefore $\frac{1+\sqrt{5}}{2}$, for which the best approximations are given by F_{n+1}/F_n where F_n is the nth Fibonacci number. One can show that the difference, $|\frac{1+\sqrt{5}}{2} - \frac{F_{n+1}}{F_n}|$, is roughly $1/(\sqrt{5}F_n^2)$ with an error $< 1/F_n^4$.

Exercise 11.4.1. Prove that if $\alpha \in \mathbb{C}\backslash\mathbb{R}$, then there exists a constant $\beta_\alpha > 0$ such that $|\alpha - p/q| \geq \beta_\alpha$ for all rational approximations p/q.

Exercise 11.4.2. Prove that if $f(t) = a_d \prod_{i=1}^{d}(t - \alpha_i)$, then $f'(\alpha_i) = a_d \prod_{j=1,\ j\neq i}^{d}(\alpha_i - \alpha_j)$.

There are many beautiful applications of Roth's Theorem to Diophantine equations. We highlight one:

Corollary 11.4.2 (Thue-Siegel Theorem)**.** *Suppose that $f(t) = a_0 + a_1 t + \cdots + a_d t^d \in \mathbb{Z}[t]$ is an irreducible polynomial of degree $d \geq 3$. Then for any integer A there are only finitely many pairs of integers m, n for which*

$$n^d f(m/n) = a_0 n^d + a_1 n^{d-1} m + \cdots + a_d m^d = A.$$

[7] A proof that is far too involved for inclusion in this book.

Proof. If $A = 0$, the only solution is $m = n = 0$, as f is irreducible. So we may assume that $|A| \geq 1$ and write $f(t) = a_d \prod_{i=1}^{d}(t - \alpha_i)$; the α_i are distinct as $f(t)$ is irreducible. For any given pair of integers m, n select j so that $|\alpha_j - \frac{m}{n}|$ is minimized. If $i \neq j$, then

$$2\left|\alpha_i - \frac{m}{n}\right| \geq \left|\alpha_i - \frac{m}{n}\right| + \left|\alpha_j - \frac{m}{n}\right| \geq |\alpha_i - \alpha_j|,$$

so that, since $f'(\alpha_j) = a_d \prod_{1\leq i\leq d,\ i\neq j}(\alpha_j - \alpha_i)$ (as in exercise 11.4.2),

$$\left|\alpha_j - \frac{m}{n}\right| \frac{|f'(\alpha_j)|}{2^{d-1}} = \left|\alpha_j - \frac{m}{n}\right| a_d \prod_{\substack{1\leq i\leq d\\ i\neq j}} \frac{|\alpha_i - \alpha_j|}{2} \leq a_d \prod_{1\leq i\leq d} \left|\alpha_i - \frac{m}{n}\right|$$

$$= |f(m/n)| = \frac{|a_0 n^d + a_1 n^{d-1} m + \cdots + a_d m^d|}{|n|^d} = \frac{|A|}{|n|^d}.$$

We now apply Roth's Theorem with $\alpha = \alpha_j$ and $\epsilon = \frac{1}{2}$, so that

$$\left|\alpha_j - \frac{m}{n}\right| \geq \frac{c_{\alpha_j,1/2}}{|n|^{5/2}}.$$

Substituting this into the previous equation, then squaring both sides and multiplying through by denominators, we obtain either $|n| \leq 1$ or

$$|n|/2 \leq (|n|/2)^{2d-5} \leq B$$

where $B = 8\max_j(A/c_{\alpha_j,1/2}|f'(\alpha_j)|)^2$. Either way there are only finitely many possibilities for integer n, and for each such n there are at most d integers m which can be roots of the polynomial

$$a_d x^d + \cdots + a_1 n^{d-1} x + (a_0 n^d - A) = 0.$$

This proves the claimed result. □

11.5. *The abc-conjecture*

In chapter 6 we discussed various Diophantine equations with three monomials like $x^2 + y^2 = z^2$, even $x^n + y^n = z^n$ for any integer $n \geq 2$, and there are others of interest like $x^p - y^q = 1$. So how do we determine which of these have infinitely many solutions in integers? This is not an easy question, and indeed the focus of a lot of research. One modern approach (motivated by deep considerations) is to study the prime powers dividing each term.

We begin by proving the following consequence of Roth's Theorem:

Corollary 11.5.1. *Let $F(x, y) \in \mathbb{Z}[x, y]$ be a homogenous polynomial of degree d, with no repeated linear factors. For each $\epsilon > 0$ there exists a constant $\kappa_{F,\epsilon} > 0$ such that for any coprime positive integers m, n:*

$$\textit{Either } F(m, n) = 0 \textit{ or } |F(m, n)| \geq \kappa_{F,\epsilon}|n|^{d-2-\epsilon}.$$

In other words, either $F(m, n) = 0$ or $|F(m, n)|$ is large.

Proof. A *homogenous polynomial* in two variables takes the form

$$F(x, y) = \sum_{j=0}^{d} a_j x^j y^{d-j}.$$

As there are no repeated factors, $F(x,y)$ can be divisible by y but not y^2. Then $f(t) = F(t,1)$ as a polynomial of degree $d-1$ or d (depending on whether $F(x,y)$ is divisible by y or not) and has no repeated roots (as F has no repeated linear factors).

Now if m and n are coprime integers, then either $F(m,n) = 0$ or, from the inequality in the proof of the Thue-Siegel Theorem,

$$\frac{|F(m,n)|}{|n|^d} = |F(m/n,1)| = |f(m/n)| \geq \frac{|f'(\alpha_j)|}{2^{d-1}} \cdot \left|\alpha_j - \frac{m}{n}\right| \geq \frac{\kappa_{F,\epsilon}}{|n|^{2+\epsilon}},$$

with $\kappa_{F,\epsilon} := \min_j c_{\alpha_j,\epsilon}|f'(\alpha_j)|/2^{d-1}$, where the last inequality follows from Roth's Theorem.[8] The result follows by multiplying each side through by $|n|^d$. □

Exercise 11.5.1. Let α be an algebraic number which is a root of $f(t) \in \mathbb{Z}[t]$, a polynomial of degree d. Let $F(x,y) = y^d f(x/y)$, and suppose that there exists a constant $\kappa > 0$ such that $|F(m,n)| \geq \kappa |n|^{d-2-\epsilon}$ for all integers m, n. Deduce that there exists a constant $c > 0$ such that $|\alpha - m/n| > c/n^{2+\epsilon}$ for all integers $m, n \neq 0$. (Thus Corollary 11.5.1 is "equivalent" to Roth's Theorem.)

We are going to move to what seems to be a rather different question but will eventually tie in closely with Corollary 11.5.1. We study pairwise coprime, positive integer solutions to the equation

$$a + b = c,$$

bounding the size of a, b, and c in terms of the product of the distinct primes that divide a, b, and c:

Conjecture 11.1 (The *abc*-conjecture)**.** *Fix $\epsilon > 0$. There exists a constant $\kappa_\epsilon > 0$ such that if a and b are coprime positive integers with $c = a + b$, then*

$$\prod_{\substack{p \text{ prime} \\ p \text{ divides } abc}} p \geq \kappa_\epsilon c^{1-\epsilon}.$$

This is the *abc-conjecture*, one of the great open questions of modern mathematics.

For example, if we have a putative solution to Fermat's Last Theorem, like $x^n + y^n = z^n$ with $x, y, z > 0$, then we take $a = x^n$, $b = y^n$, and $c = z^n$. Now the product of the primes dividing $abc = (xyz)^n$ is the same as the product of the primes dividing xyz. Therefore the *abc*-conjecture with $\epsilon = 1/5$ implies for $n \geq 5$ that

$$\kappa(z^n)^{4/5} \leq \prod_{\substack{p \text{ prime} \\ p \text{ divides } x^n y^n z^n}} p = \prod_{\substack{p \text{ prime} \\ p \text{ divides } xyz}} p \leq xyz \leq z^3 \leq z^{3n/5},$$

where $\kappa = \kappa_{1/5}$, from which we deduce $z^n \leq 1/\kappa^5$. Since $x^n, y^n < z^n$ we deduce, from the *abc*-conjecture, that in every solution to $x^n + y^n = z^n$ with $n \geq 5$, the numbers x^n, y^n, and z^n are all bounded by some absolute constant, and therefore

[8] Yet again this seems like a lot of notation for a constant, especially an inexplicit constant, but the notation reflects what the constant depends on, and given the complicated derivation of this constant, it is certainly simpler not to try to be explicit about it.

there are only finitely many solutions. Therefore we have proved that the *abc*-conjecture implies that there are only finitely many solutions to $x^n + y^n = z^n$ with $(x, y) = 1$ and $n > 4$.

One can compare the *abc*-conjecture with the *abc*-theorem for polynomials (as in section 6.7 of appendix 6A). The size of the integers replaces the degrees of the polynomials; the prime divisors replace the irreducible polynomial factors. One cannot prove the *abc*-conjecture in the same way, since we relied heavily in our proof of the *abc*-theorem for polynomials on calculus, for which there is no analogy for numbers.

We now state a conjecture which implies both the *abc*-conjecture and Corollary 11.5.1 of Roth's Theorem:

Conjecture 11.2 (The *abc*-Roth conjecture)**.** *Let $F(x, y) \in \mathbb{Z}[x, y]$ be a homogenous polynomial of degree d, with no repeated linear factors. For each $\epsilon > 0$ there exists a constant $\kappa_{F,\epsilon} > 0$ such that for any coprime positive integers m, n, either $F(m, n) = 0$ or*

$$\prod_{\substack{p \text{ prime} \\ p \text{ divides } F(m,n)}} p \geq \kappa_{F,\epsilon} |n|^{d-2-\epsilon}.$$

The *abc*-Roth conjecture implies both Corollary 11.5.1, since the product of the primes dividing non-zero $F(m, n)$ is $\leq |F(m, n)|$, and the *abc*-conjecture, taking $F(x, y) = xy(x+y)$ (since then $F(a, b) = abc$ when $a+b = c$). Quite remarkably Conjecture 11.2 follows from the *abc*-conjecture using some clever algebraic geometry. (See [**2**].)

Further reading for this chapter

[1] Edward B. Burger, *Diophantine olympics and world champions: Polynomials and primes down under*, Amer. Math. Monthly **107** (2000), 822–829.

[2] Andrew Granville and Thomas J. Tucker, *It's as easy as abc*, Notices Amer. Math. Soc **49** (2002), 1224–1231.

[3] Serge Lang, *Old and new conjectured Diophantine inequalities*, Bull. Amer. Math. Soc. **23** (1990), 37–75.

[4] H. W., Lenstra, Jr., *Solving the Pell equation*, Notices Amer. Math. Soc. **49** (2002), 182–192.

[5] Barry Mazur, *Questions about powers of numbers*, Notices Amer. Math. Soc. 47 (2000), no. 2, 195–202.

Additional exercises

Exercise 11.6.1. Suppose $(p, q) = 1$ and $q \geq 1$. Determine *all* rationals m/n for which $\left|\frac{p}{q} - \frac{m}{n}\right| = \frac{1}{qn}$.

Exercise 11.6.2. Reprove exercise 7.10.21(a) using (11.0.1).

Exercise 11.6.3.† Prove that there are infinitely many solutions to the Pell equation $u^2 - dv^2 = 1$ with $u \equiv 1 \pmod{d}$.

Exercise 11.6.4. Prove that if α is transcendental, then so is α^k for every non-zero integer k.

Exercise 11.6.5 (The "three gaps" theorem).‡ Given $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, we put the fractional parts $\{\alpha\}, \{2\alpha\}, \dots, \{N\alpha\} \in [0,1)$ in ascending order as $0 < \{a_1\alpha\} < \{a_2\alpha\} < \cdots < \{a_N\alpha\} < 1$ (so that $\{a_1, \dots, a_N\}$ is a reordering of $\{1, \dots, N\}$). We will prove that there are at most three distinct values in the set of consecutive differences, $D(A) := \{\{a_{j+1}\alpha\} - \{a_j\alpha\} : j = 1, \dots, N-1\}$.

(a) Show that if $\{(a_{j+1}-1)\alpha\} - \{(a_j-1)\alpha\} \notin D(A)$, then either $a_j = 1$ or $a_{j+1} = 1$, or there exists k such that $\{(a_j-1)\alpha\} < \{a_k\alpha\} < \{(a_{j+1}-1)\alpha\}$.

(b) Show that if $\{(a_j-1)\alpha\} < \{a_k\alpha\} < \{(a_{j+1}-1)\alpha\}$, then $a_k = N$.

(c) Deduce from (a) and (b) that every element of $D(A)$ equals one of $\{a_1\alpha\}$, $1 - \{a_N\alpha\}$, or $\{a_1\alpha\} + 1 - \{a_N\alpha\}$.

Exercise 11.6.6. Suppose that a and b are given integers, with $3 \nmid a$.

(a) Show that we can select a congruence class $r \pmod 3$ such that if integer $m \equiv r \pmod 3$, then $x + y\sqrt{3} = (2+\sqrt{3})^m(a + b\sqrt{3})$, then 3 divides y.

(b) Deduce that if integer N can be written in the form $a^2 - 3b^2$ where $3 \nmid N$, then there are infinitely many pairs of powerful numbers that differ by exactly N.

Exercise 11.6.7. Find an explicit value that can be used for c_α in Liouville's Theorem when $\alpha = \sqrt{D}$ where $D > 1$ is a squarefree positive integer.

Exercise 11.6.8. Fix $\epsilon > 0$, and integers $a_0, \dots, a_d$. Deduce from Roth's Theorem that there are only finitely many pairs of coprime integers m, n for which $|a_0n^d + a_1n^{d-1}m + \cdots + a_dm^d| \le \max\{|m|, |n|\}^{d-2-\epsilon}$.

Exercise 11.6.9. Assume the *abc*-conjecture to show that there are only finitely many sets of integers $x, y > 0$ and $p, q > 1$ for which $x^p - y^q = 1$.

Exercise 11.6.10. Suppose that $x^p + y^q = z^r$ with x, y, z pairwise coprime and $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$.

(a) Prove that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \le \frac{41}{42}$.

(b) Assume the *abc*-conjecture. Prove that there exists a constant B for which $|x^p|, |y^q|, |z^r| < B$.

Exercise 11.6.11. The *abc*-conjecture is "best possible" in that one cannot take $\epsilon = 0$. To establish this, we need to find examples of solutions to $a + b = c$ in which $(1/c)\prod_{p|abc} p$ gets arbitrarily small.

(a) Prove that if $m^2|b$, then $\prod_{p|b} p \le b/m$.

(b) Prove that for any odd integer m there exists an integer n for which $2^n \equiv 1 \pmod{m^2}$.

(c)† Combine these two observations to show that for any $\epsilon > 0$ there exist coprime integers $a + b = c$ for which $\prod_{p|abc} p < \epsilon c$.

Appendix 11A. Uniform distribution

11.7. $n\alpha$ mod 1

Dirichlet's Theorem, in section 11.1, implies that $n\alpha$ mod 1 gets arbitrarily close to 0 as n runs through a sequence of integers n. One might also ask whether $n\alpha$ mod 1 gets arbitrarily close to any given $\theta \in (0,1)$.

Theorem 11.5 (Kronecker's Theorem)**.** *If α is a real irrational number, then the numbers $\{n\alpha\}$ are dense on $[0,1)$.*

Proof. Fix $\epsilon > 0$. By Dirichlet's Theorem there exists an integer n with $\|n\alpha\| < \epsilon$, where $\|t\|$ is the distance from t to the nearest integer. As α is irrational we also have that $\|n\alpha\| \neq 0$, and so $\{n\alpha\} \in (0,\epsilon)$ *or* $\{n\alpha\} \in (1-\epsilon, 1)$. We will assume that $\{n\alpha\} \in (0,\epsilon)$ (the case with $\{n\alpha\} \in (1-\epsilon,1)$ being proved analogously).

Let $\delta = \{n\alpha\} \in (0,\epsilon)$. Select D to be the largest integer $< 1/\delta$ and so

$$\{n\alpha\},\ \{2n\alpha\}, \ldots, \{Dn\alpha\} = \delta, 2\delta, \ldots, D\delta$$

is a set of points in $[0,1)$, consecutive points being spaced $\delta < \epsilon$ apart. Therefore if $\theta \in [0,1)$, then we let $k = [\theta/\delta]$ and so $\theta - k\delta \in [0,\delta)$, which implies that

$$\theta - \{kn\alpha\} = \theta - k\{n\alpha\} = \theta - k\delta \in [0,\delta) \subset [0,\epsilon).$$

That is, there are integer multiples of α in $\mathbb{R}/\mathbb{Z}$ that are arbitrarily close to θ. □

Exercise 11.7.1. Show that the conclusion of the theorem is not true if α is rational.

Exercise 11.7.2. Prove Kronecker's Theorem when $n\alpha \pmod 1 \in (1-\epsilon, 1)$.

Now we know that if α is irrational, then $n\alpha$ mod 1 gets arbitrarily close to any given $\theta \in [0,1)$, we might ask how often $n\alpha$ mod 1 gets close to each $\theta \in [0,1)$. Are the values of $n\alpha$ mod 1 roughly equidistributed? To answer this question we must

determine how often $\{n\alpha\} \in [\theta - \epsilon, \theta + \epsilon]$ for $\theta \in (0,1)$ and sufficiently small $\epsilon > 0$. If the numbers $\{n\alpha\}$ are equidistributed, then we might expect the frequency to be roughly proportional to the length of the interval. The analogous question can be asked for any sequence of numbers $x_1, x_2, \ldots \in [0,1)$. We say that $\{x_n\}_{n\geq 1}$ is *uniformly distributed* mod 1 (or *equidistributed* mod 1) if for any $a < b \in [0,1)$,

$$\lim_{N\to\infty} \frac{1}{N}\#\{n \leq N : a \leq x_n \leq b\} \text{ exists and equals } b-a.$$

The values of $x \pmod 1$ are in 1-to-1 correspondence with the values of $e(x)$ (where $e(t) := e^{2i\pi t}$) as its value depends on $x \pmod 1$ and not on x. Moreover the values $e(kx)$ for any given integer $k \neq 0$ remain consistent for x with any given value mod 1. That is, if $x = m + \delta$ with $0 \leq \delta < 1$, then $kx = km + k\delta$ so that $\{kx\} = \{k\delta\}$. This suggests that to study a sequence of values $x_n \bmod 1$, we might use Fourier analysis. This thinking leads to the famous theorem of Hermann Weyl (for more on this, including the proof, see [**GG**]):

Theorem 11.6 (Weyl's uniform distribution theorem)**.** *The sequence* $\{x_n\}_{n\geq 1}$ *is uniformly distributed* mod 1 *if and only if for all non-zero integers* k *we have*

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e(kx_n) \text{ exists and equals } 0.$$

Exercise 11.7.3. (a) Show that $\sum_{n=1}^{N} e(\{n\alpha\}) = \frac{e(N\alpha)-1}{1-e(-\alpha)}$ if $\alpha \notin \mathbb{Z}$, and then deduce that $|\sum_{n=1}^{N} e(\{n\alpha\})| \leq \frac{1}{|\sin \pi\alpha|}$.

(b) Use Weyl's uniform distribution theorem to deduce that if α is a real, irrational number, then $\{n\alpha\}_{n\geq 1}$ is uniformly distributed mod 1.

One can prove that $\{n\alpha\}$ is uniformly distributed mod 1 using fairly elementary ideas though it is not easy:

Exercise 11.7.4. Let $x_1, x_2, \ldots \in [0,1)$ be a sequence of numbers. Suppose that there are arbitrarily large integers M for which

$$\lim_{N\to\infty} \frac{1}{N}\#\left\{n \leq N : \frac{m}{M} \leq x_n \leq \frac{m+1}{M}\right\} \text{ exists and equals } \frac{1}{M},$$

for $0 \leq m \leq M-1$. Deduce that $\{x_n\}_{n\geq 1}$ is uniformly distributed mod 1.

Exercise 11.7.5.‡ Let α be a real, irrational number. In this exercise we sketch a proof that $\{n\alpha\}_{n\geq 1}$ is uniformly distributed mod 1. Fix $\epsilon > 0$ arbitrarily small.

(a) Use Kronecker's Theorem to show that there exists an integer $N \geq 1$ such that $\{N\alpha\} = \delta \in (0, \epsilon)$.

(b) Prove that if $\{n\alpha\} < 1 - \delta$, then $\{(n+N)\alpha\} = \{n\alpha\} + \delta$. What if $\{n\alpha\} \geq 1 - \delta$?

(c) Suppose that $0 < t < 1 - 2\delta$. Show that $\{n\alpha\} \in [t, t+\delta]$ if and only if $\{(n+N)\alpha\} \in [t+\delta, t+2\delta]$, and so deduce that

$$|\#\{1 \leq n \leq x : t \leq \{n\alpha\} < t+\delta\} - \#\{1 \leq n \leq x : t+\delta \leq \{n\alpha\} < t+2\delta\}| \leq N.$$

Now let $\delta = 1/M$ for some large integer M.

(d)† Use (c) to show that if $0 \leq m \leq M-1$, then

$$\left|\#\left\{1 \leq n \leq x : \frac{m}{M} \leq \{n\alpha\} < \frac{m+1}{M}\right\} - \frac{x}{M}\right| \leq MN.$$

(e) Deduce that $\{n\alpha\}_{n\geq 1}$ is uniformly distributed mod 1 using exercise 11.7.4.

Kronecker's Theorem in n dimensions. In exercise 11.1.2 we saw that Dirichlet's Theorem may be generalized to k dimensions; that is, given $\alpha_1, \dots, \alpha_k \in \mathbb{R}$, for any $\epsilon > 0$ there exist infinitely many integers n such that each $\|n\alpha_j\| < \epsilon$. To generalize Kronecker's Theorem we would like that for $\theta_1, \dots, \theta_k \in \mathbb{R}$ there are infinitely many n for which each $\|n\alpha_j - \theta_j\| < \epsilon$. However this is not true in all cases, even when $k = 1$: In the hypothesis of Theorem 11.5 we needed that α is irrational, and we showed that this is necessary in exercise 11.7.1. Another way to state that α is irrational is to insist that 1 and α are linearly independent over $\mathbb{Z}$.

In two dimensions we find another obstruction: Suppose that $\alpha_1 = \alpha$ and $\alpha_2 = 1 - \alpha$. If $\|n\alpha_j - \theta_j\| < \epsilon$ for each j, then

$$\|\theta_1 + \theta_2\| = \|n - \theta_1 - \theta_2\| \le \|n\alpha_1 - \theta_1\| + \|n\alpha_2 - \theta_2\| < 2\epsilon.$$

But this should hold for any $\epsilon > 0$ which implies that $\theta_1 + \theta_2$ is an integer. Notice that in this example $1, \alpha_1, \alpha_2$ are not linearly independent over $\mathbb{Z}$.

Exercise 11.7.6. Let $\alpha_1, \dots, \alpha_k, \theta_1, \dots, \theta_k \in \mathbb{R}$ be given, and assume that there are integers $c_0, \dots, c_k$ for which $c_0 + c_1\alpha_1 + \cdots + c_k\alpha_k = 0$. Suppose that for all $\epsilon > 0$ there are infinitely many n for which $\|n\alpha_j - \theta_j\| < \epsilon$ for $j = 1, 2, \dots, k$. Prove that $c_1\theta_1 + \cdots + c_k\theta_k \in \mathbb{Z}$.

These are the only obstructions to the generalization:

Theorem 11.7 (Kronecker's Theorem in n dimensions)**.** *Assume that the real numbers $1, \alpha_1, \dots, \alpha_k$ are linearly independent over $\mathbb{Z}$. Then the points*

$$(n\alpha_1, \dots, n\alpha_k)_{n \ge 1} \text{ are dense in } (\mathbb{R}/\mathbb{Z})^k.$$

In other words, for any given $\theta_1, \dots, \theta_k \in \mathbb{R}$ and any $\epsilon > 0$ there are infinitely many integers n for which $\|n\alpha_j - \theta_j\| < \epsilon$ for all $j = 1, \dots, k$.

This can be proved in several different ways that are accessible though tough. We refer the reader to sections 23.5–23.8 of [**HW08**].

11.8. Bouncing billiard balls

Billiards, snooker, and pool are all played on a rectangular table, hitting the ball along the surface. The sides of the table are cushioned so that the ball bounces off the side at the opposite angle to which it hits. That is, if it hits at angle α°, then it bounces off at angle $(180 - \alpha)^\circ$. Sometimes one miscues and the ball carries on around the table, coming to a stop without hitting another ball. Have you ever wondered what would happen if there were no friction, so that the ball never stops? Would your ball eventually hit the ball it is supposed to hit, no matter where that other ball is placed? Or could it go on bouncing forever without ever getting to the other ball? We could rephrase this question more mathematically by supposing that we play on a table in the complex plane, with two sides along the x- and y-axes. Say the table length is ℓ and width is w so that it is the rectangle with corners at $(0,0), (0,\ell), (w,0), (w,\ell)$. Let us suppose that the ball is hit from the point (u, v) along a line with slope α (that is, at an angle α from the horizontal).

As the line continues on indefinitely inside the box, does it get arbitrarily close to every point inside the box?

Exercise 11.8.1. Show that by rescaling with the map $x \to x/\ell,\ y \to y/w$ we can assume, without any loss of generality, that the billiards table is the unit square.

As a consequence of exercise 11.8.1, we may henceforth assume that $w = \ell = 1$.

The ball would run along the line $\mathcal{L} := \{(u + t, v + \alpha t),\ t \geq 0\}$ if it did not hit the sides of the table. Notice though that if after each time it hit a side, we reflected the true trajectory through the line that represents that side, then indeed the ball's trajectory would be $\mathcal{L}$.

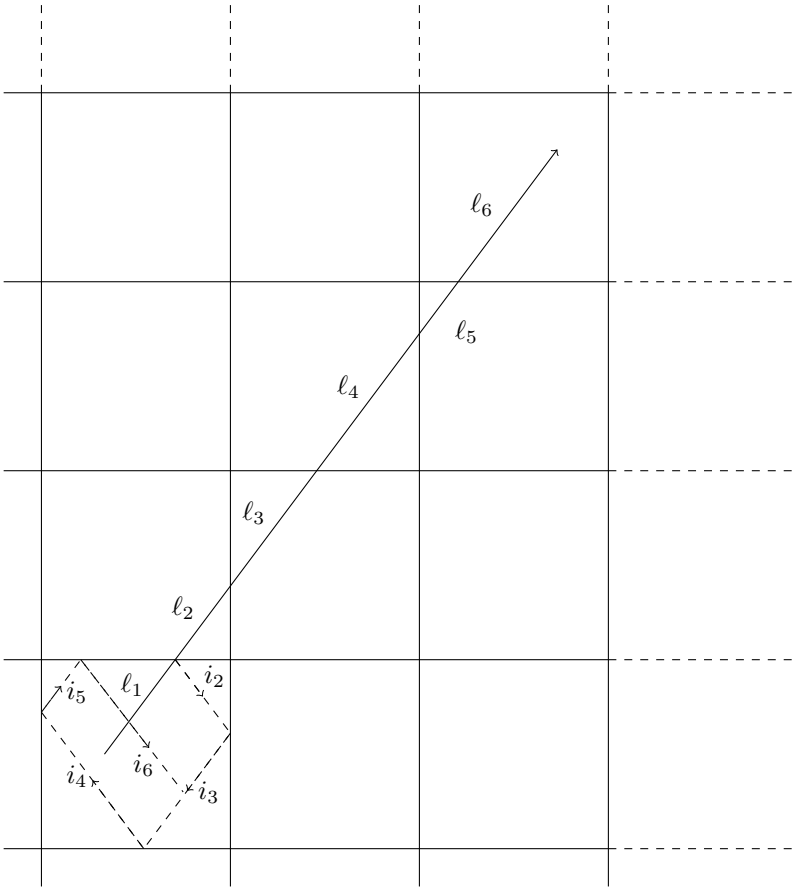


Figure 11.1. Billiards on the complex plane and on the unit square. Following a path inside the fundamental domain of a lattice: The path segment ℓ_j gets mapped to i_j for $j = 2, \ldots, 6$.

Develop this to prove:

Exercise 11.8.2. Show that the billiard ball is at (x, y) after time t, where x and y are given as follows:
Let $m = [u + t]$. If m is even, let $x = \{u + t\}$; if m is odd, let $x = 1 - \{u + t\}$.
Let $n = [v + \alpha t]$. If n is even, let $y = \{v + \alpha t\}$; if n is odd, let $y = 1 - \{v + \alpha t\}$.

Exercise 11.8.3. Show that if α is rational, then the ball eventually ends up exactly where it started from, and so it does not get arbitrarily close to every point on the table.

So how close does the trajectory get to the point (r, s), where $r, s \in [0, 1)$? Let us consider all of those values of t for which $x = r$, with m and n even to simplify matters (with m and n as in exercise 11.8.2), and see if we can determine whether y is ever close to s.

Exercise 11.8.4. Show that $[z]$ is even if and only if $\{z/2\} \in [0, 1/2)$. Deduce that $[z]$ is even and $\{z\} = r$ if and only if $\{z/2\} = r/2$.

Hence we want $(u+t)/2 = k+r/2$ for some integer k; that is, $t = 2k+(r-u)$, $k \in \mathbb{Z}$. In that case $v + \alpha t = 2\alpha k + \alpha(r - u) + v$ so we want $\{\alpha k + (\alpha(r - u) + v)/2\}$ close to $s/2$. That is, $k\alpha \bmod 1$ should be close to $\theta := \{\frac{(s-v)+\alpha(u-r)}{2}\}$. Now, in Kronecker's Theorem (Theorem 11.5) we showed that the values $k\alpha \bmod 1$ are dense in $[0, 1)$ when α is irrational, and so in particular there are values of k that allow $k\alpha \bmod 1$ to be arbitrarily close to θ. Hence we have proved the difficult part of the following corollary:

Corollary 11.8.1. *If α is a real irrational number, then any ball moving at angle α (to the coordinate axes) will eventually get arbitrarily close to any point on a* 1*-by-*1 *billiards table.*

We finish with a challenge question to develop a similar theory of billiards played on a circular table!

Exercise 11.8.5. Imagine a trajectory inside the unit circle. A ball is hit and continues indefinitely. When it hits a side at angle θ (compared to the normal line at that point), it bounces off at angle $-\theta$.

(a) Suppose that the first two points at which the ball hits the edge are at $e(\beta)$ and then at $e(\beta + \alpha)$. Show that the ball hits the edge at $e(\beta + n\alpha)$ for $n = 0, 1, 2, \ldots$.
(b) Prove that the ball falls into a repeated trajectory if and only if α is rational.
(c) Show that if α is irrational, then the points at which the ball hits the circle edge are dense (i.e., eventually the ball comes arbitrarily close to any point on the edge) but that it never hits the same edge point twice.
(d) Prove that the ball's trajectory never comes inside the circle of radius $|\cos(\alpha/2)|$. Deduce that the trajectory of the ball is *never* dense inside the unit circle.
(e) Prove that if α is irrational, then the trajectory of the ball is dense inside the ring between the circle of radius $|\cos(\alpha/2)|$ and the circle of radius 1. (The technical word for a ring is an *annulus*.)

Appendices. The extended version of chapter 11 has the following additional appendices:

Appendix 11B. *Continued fractions* introduces and analyzes continued fractions for all real numbers, focusing on continued fractions for quadratic irrationals. We find and justify a particularly efficient algorithm for finding all the solutions to Pell's equation using continued fractions.

Appendix 11C. *Two-variable quadratic equations* establishes that, other than in certain special cases, if there is one solution to a given two-variable quadratic equation, then there are infinitely many.

Appendix 11D. *Transcendental numbers* discusses how many transcendental numbers there are, via Cantor's diagonalization argument. We show that e and π are irrational and then discuss "normal numbers".

Chapter 12

Binary quadratic forms

Let a, b, and c be given integers. We saw in Corollary 1.3.1 that the integers that can be represented by the binary linear form $ax + by$ are those integers divisible by $\gcd(a, b)$. We are now interested in what integers can be represented by the *binary quadratic form*,[1]

$$f(x, y) := ax^2 + bxy + cy^2.$$

As in the linear case, we can immediately reduce our considerations to the case that $\gcd(a, b, c) = 1$.

The first important result of this type was given by Fermat for the particular example $f(x, y) = x^2 + y^2$, as discussed in section 9.1. The two main results were that an odd prime p can be represented by $f(x, y)$ if and only if $p \equiv 1 \pmod 4$, and that the product of two integers that can be written as the sum of two squares can also be written as the sum of two squares, a consequence of the identity (9.1.1). One can combine these two facts to classify exactly which integers are represented by the binary quadratic form $x^2 + y^2$.

At first sight it looks like it might be difficult to work with the example $f(x, y) = x^2+20xy+101y^2$. However, this can be rewritten as $(x+10y)^2+y^2$ and so represents exactly the same integers as $g(x, y) = x^2 + y^2$. In other words

$$n = f(u, v) \text{ if and only if } n = g(r, s), \text{ where } \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} 1 & 10 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

This 2-by-2 matrix is invertible over the integers, so we can express u and v as integer linear combinations of r and s. Thus every representation of n by f corresponds to one by g, and vice versa, a 1-*to*-1 *correspondence*, obtained using the invertible *linear transformation* $u, v \to u + 10v, v$. Such a pair of quadratic forms, f and g, are said to be *equivalent*; and we have just seen how equivalent binary quadratic forms represent exactly the same integers. The *discriminant* of

[1] "Binary" as in the **two** variables x and y, and "quadratic" as in degree **two**. The monomials ax^2, bxy, cy^2 each have degree two, since the degree of a term is given by the degree in x plus the degree in y.

$ax^2+bxy+cy^2$ is b^2-4ac. We will show that equivalent binary quadratic forms have the same discriminant, so that it is an *invariant* of the equivalence class of binary quadratic forms. All of this will be discussed in this chapter and, in appendix 12A, we will study generalizations of the identity (9.1.1).

12.1. Representation of integers by binary quadratic forms

An integer N is *represented* by f if there exist integers m, n for which $N = f(m, n)$, and N is *properly represented* if $(m, n) = 1$ (see exercise 3.9.13 for the same question for linear forms).

Exercise 12.1.1. Prove that if N is squarefree, then all representations of N are proper.

What integers can be properly represented by $ax^2 + bxy + cy^2$? That is, for what integers N do there exist coprime integers m, n such that

$$N = am^2 + bmn + cn^2? \tag{12.1.1}$$

We may reduce to the case that $\gcd(a, b, c) = 1$ by dividing though by $\gcd(a, b, c)$. (If $\gcd(a, b, c) = 1$, then f is a *primitive* binary quadratic form.) One idea is to complete the square to obtain

$$4aN = (2am + bn)^2 - dn^2 \tag{12.1.2}$$

where the *discriminant* $d := b^2 - 4ac$. This implies that the discriminant always satisfies

$$d \equiv 0 \text{ or } 1 \pmod 4.$$

There is always at least one binary quadratic form of discriminant d, for such d, which we call the *principal form*:

$$\begin{cases} x^2 - (d/4)y^2 & \text{when } d \equiv 0 \pmod 4, \\ x^2 + xy + \frac{(1-d)}{4}y^2 & \text{when } d \equiv 1 \pmod 4. \end{cases}$$

We call d a *fundamental discriminant* if $d = D \equiv 1 \pmod 4$, or $d = 4D$ with $D \equiv 2$ or $3 \pmod 4$, and if $D = d/(d, 4)$ is squarefree. These are precisely the discriminants for which every binary quadratic form is primitive (see exercise 12.1.3). We met this notion already in exercise 8.16.4 of appendix 8D, when classifying the genuinely different Jacobi symbols.

When $d < 0$ the right side of (12.1.2) can only take positive values, which makes our discussion easier than when $d > 0$. For this reason we will restrict ourselves to the case $d < 0$ here and revisit the case $d > 0$ in appendix 12C. If $d < 0$ and $a < 0$, we replace a, b, c by $-a, -b, -c$, so as to ensure that $am^2 + bmn + cn^2$ is always ≥ 0; in this case, we call $ax^2 + bxy + cy^2$ a *positive definite* binary quadratic form.

At the start of this chapter we worked through one example of equivalence of binary quadratic forms, and here is another: The binary quadratic form $x^2 + y^2$ represents the same integers as $X^2 + 2XY + 2Y^2$, for if $N = m^2 + n^2$, then $N = (m-n)^2+2(m-n)n+2n^2$, and similarly if $N = u^2+2uv+2v^2$, then $N = (u+v)^2+v^2$. The reason is that the substitution

$$\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} X \\ Y \end{pmatrix} \text{ where } M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

transforms x^2+y^2 into $X^2+2XY+2Y^2$, and the transformation is invertible, since $\det M = 1$. We therefore say that x^2+y^2 and $X^2+2XY+2Y^2$ are *equivalent* which we denote by

$$x^2+y^2 \sim X^2+2XY+2Y^2.$$

Much more generally define

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \ \alpha,\beta,\gamma,\delta \in \mathbb{Z} \text{ and } \alpha\delta-\beta\gamma = 1 \right\}.$$

We can represent the binary quadratic form as

$$ax^2+bxy+cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Its discriminant is -4 times the determinant of $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. We deduce that if

$$\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} X \\ Y \end{pmatrix} \text{ where } M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}),$$

then

$$AX^2+BXY+CY^2 = \begin{pmatrix} X & Y \end{pmatrix} M^{\mathrm{T}} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M \begin{pmatrix} X \\ Y \end{pmatrix},$$

so that

$$\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} = M^{\mathrm{T}} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M, \tag{12.1.3}$$

which yields the somewhat painful looking explicit formulas

$$\begin{cases} A &= f(\alpha,\gamma) = a\alpha^2+b\alpha\gamma+c\gamma^2, \\ B &= 2\alpha\beta a + (\alpha\delta+\beta\gamma)b + 2\gamma\delta c, \\ C &= f(\beta,\delta) = a\beta^2+b\beta\delta+c\delta^2. \end{cases} \tag{12.1.4}$$

When working with binary quadratic forms it is convenient to represent $ax^2+bxy+cy^2$ by the notation $[a,b,c]$. We have just proven the following.

Proposition 12.1.1. *If $f=[a,b,c] \sim F=[A,B,C]$, then there exist integers $\alpha,\beta,\gamma,\delta$ with $\alpha\delta-\beta\gamma=1$ for which $A=f(\alpha,\gamma)$ and $C=f(\beta,\delta)$. Moreover f and F represent the same integers, and there is a 1-to-1 correspondence between their representations and proper representations of a given integer.*

Exercise 12.1.2. (a) Suppose that d is a fundamental discriminant. Prove that the character $(d/\cdot)$ has conductor dividing d.

(b) Prove that for any non-zero integer d, the character $(d/\cdot)$ has conductor that divides $4d$.

The *conductor* of $f(\cdot)$ is the minimum $p>0$ such that $f(n+p)=f(n)$ for all integers n.

Exercise 12.1.3. Suppose that $d \equiv 0$ or $1 \pmod 4$. Show that every binary quadratic form of discriminant d is primitive if and only if d is a fundamental discriminant.

Exercise 12.1.4. (a) Show that if $d<0$, then $am^2+bmn+cn^2$ has the same sign as a, no matter what the choices of integers m and n.

(b) Show that if $ax^2+bxy+cy^2$ is positive definite, then $a,c>0$.

(c) Show that if $d>0$, then $am^2+bmn+cn^2$ can take both positive and negative values, by making explicit choices of integers m,n.

Exercise 12.1.5. Use (12.1.3) to show that two equivalent binary quadratic forms have the same discriminant.

Exercise 12.1.6. Show that the principal form is equivalent to every binary quadratic form $x^2 + bxy + cy^2$ with leading coefficient 1, up to equivalence.

Exercise 12.1.7. In each part, determine whether the two binary quadratic forms are equivalent. If so, make the equivalence explicit; if not, explain why not.
(a) $y^2 + xy + 4x^2$ and $x^2 - 5xy + 10y^2$.
(b) $x^2 + 3xy + 5y^2$ and $3x^2 - 4xy + 11y^2$.

12.2. Equivalence classes of binary quadratic forms

In this section we will develop an algorithm that will allow us to show, for example, that $29X^2 + 82XY + 58Y^2$ is equivalent to $x^2 + y^2$. We do this as it is surely more intuitive to work with the latter form rather than the former. Gauss observed that every equivalence class of binary quadratic forms (with $d < 0$) contains a unique smallest representative, called the *reduced* representative, which we now prove: The quadratic form $ax^2 + bxy + cy^2$ with discriminant $d < 0$ is *reduced* if

$$-a < b \le a \le c \text{ and } b \ge 0 \text{ whenever } a = c.$$

Theorem 12.1. *Every positive definite binary quadratic form is equivalent to a reduced form.*

Proof. We will define a sequence of properly equivalent forms; the algorithm terminates when we reach one that is reduced. Given a form $[a, b, c]$, we use one of three transformations, described in terms of matrices from $\mathrm{SL}(2, \mathbb{Z})$:

(i) If $c < a$, the transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

yields the form $[c, -b, a]$ which is properly equivalent to $[a, b, c]$ (as $ax^2 + bxy + cy^2 = a(-Y)^2 + b(-Y)(X) + c(X)^2 = cX^2 - bXY + aY^2$). Hence $A = c < a = C$.

(ii) If $b > a$ or $b \le -a$, then select B to be the absolutely least residue of $b \pmod{2a}$, so that $-a < B \le a$, say $B = b - 2ka$. The transformation matrix will be

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

The resulting form $[A, B, C]$ with $A = a$ is properly equivalent to $[a, b, c]$, where $-A < B \le A$.

(iii) If $c = a$ and $-a < b < 0$, then the transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

yields the form $[A, B, A]$ with $A = a$ and $B = -b$, so that $0 < B < A$.

If the resulting form is not reduced, then repeat the algorithm. If none of these hypotheses holds, then one can easily verify that the form is reduced. To prove that the algorithm terminates in finitely many steps we follow the leading coefficient

a: a starts as a positive integer. Each transformation of type (i) reduces the size of a. It stays the same after transformations of type (ii) or (iii), but after a type (iii) transformation the algorithm terminates, and after a type (ii) transformation we either have another type (i) transformation or else the algorithm stops after at most one more transformation. Hence the algorithm finishes in no more than $2a+1$ steps. □

Examples. Applying the reduction algorithm to the form $[76, 217, 155]$ of discriminant -31, one finds the sequence of forms

$$[76, 65, 14], [14, -65, 76], [14, -9, 2], [2, 9, 14], [2, 1, 4],$$

the sought-after reduced form. Similarly the form $[11, 49, 55]$ of discriminant -19 gives the sequence of forms $[11, 5, 1], [1, -5, 11], [1, 1, 5]$.

This proof of Theorem 12.1 can be rephrased to prove Theorem 1.2 of section 1.10 (of appendix 1A), that every matrix in $\mathrm{SL}(2, \mathbb{Z})$ can be represented as the product of powers of the matrices $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. The matrices used in the transformations in the proof of Theorem 12.1 are $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = T^{-1}$ and $\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} = S^{-k}$.

The very precise conditions in the definition of "reduced" were chosen so that every positive definite binary quadratic form is properly equivalent to a *unique* reduced form. The key to proving uniqueness is exercise 12.6.1; the (messy) details are completed in exercise 12.6.2.

12.3. Congruence restrictions on the values of a binary quadratic form

What restrictions are there on the values that can be taken by a binary quadratic form (in analogy to Theorem 9.2)?

Proposition 12.3.1. *Let $d = b^2 - 4ac$ where $(a, b, c) = 1$.*

(i) *If integer N is properly represented by $ax^2+bxy+cy^2$, then d is a square* mod $4N$.

(ii) *If d is a square* mod $4N$, *then there exists a binary quadratic form of discriminant d that properly represents N.*

Proof. (ii) If $d \equiv b^2 \pmod{4N}$, then $d = b^2 - 4Nc$ for some integer c, and so $Nx^2 + bxy + cy^2$ is a quadratic form of discriminant d which represents $N = N \cdot 1^2 + b \cdot 1 \cdot 0 + c \cdot 0^2$.

(i) Suppose that $N = am^2 + bmn + cn^2$ with $(m, n) = 1$. Then $(2am + bn)^2 - dn^2 = 4aN$ so that $dn^2 \equiv (2am + bn)^2 \pmod{4N}$; that is, dn^2 is a square mod $4N$ and, analogously, dm^2 is a square mod $4N$. Now if p is a prime such that $p^k \| 4N$, then p does not divide at least one of m and n, as $(m, n) = 1$. We deduce that d is a square mod p^k from the fact that dn^2 is a square mod p^k if p does not divide n, and from the fact that dm^2 is a square mod p^k if p does not divide m. The result, that d is a square mod $4N$ now follows from the Chinese Remainder Theorem. □

For a given odd prime p, Proposition 12.3.1 tells us that p is represented by some binary quadratic form of discriminant d if and only if $(d/p) = 1$ or 0. However it does not tell us which binary quadratic form. In section 9.6 we could not immediately determine which of the two reduced binary quadratic forms of discriminant -20, namely $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$, represents which primes p with $(-20/p) = 1$. There we found we could distinguish which prime was represented by which form by also studying the values of (p/d). We now see how this works out in general.

We can appeal to Corollary 9.4.1 to restrict the possibilities for the binary quadratic forms of discriminant d that represent N. Given a primitive binary quadratic form f of discriminant d we define, for each odd prime p dividing d,

$$\sigma_f(p) = \left(\frac{a}{p}\right) \text{ if } p \text{ does not divide } a, \text{ and } \sigma_f(p) = \left(\frac{c}{p}\right) \text{ if } p \text{ does divide } a.$$

If p divides a, then p divides $d + 4ac = b^2$ and so divides b, and therefore cannot divide c as f is primitive. Therefore $\sigma_f(p)$ equals 1 or -1 for each such p.

Exercise 12.3.1.† Prove that if $f \sim g$, then $\sigma_f(p) = \sigma_g(p)$ for all odd primes p dividing d.

Corollary 12.3.1. *Suppose that d is a fundamental discriminant and that N is a squarefree integer for which $(N, d) = 1$. If d is a square* mod $4N$*, then there exists a binary quadratic form f of discriminant d that properly represents N such that $\sigma_f(p) = \left(\frac{N}{p}\right)$ for every odd prime p dividing d.*

Proof. There exists a binary quadratic form f of discriminant d that properly represents N, by Proposition 12.3.1(ii). Therefore N is represented by inserting rationals into f and this happens, by Corollary 9.4.1, if and only if $\left(\frac{N}{p}\right) = \sigma_f(p)$ for every odd prime p dividing d. □

When $d = -20$ we have $\sigma_f(5) = 1$ for $f = x^2 + 5y^2$ and $\sigma_f(5) = (2/5) = -1$ for $f = 2x^2 + 2xy + 3y^2$. This can certainly settle such issues in several cases.

There are three reduced quadratic forms $[1, 1, 6], [2, \pm 1, 3]$ with $d = -23$. However $\sigma_f(23) = 1$ for each of these, so this does not help us to distinguish between the integers represented by these quadratic forms. This case is **much** more complicated and beyond the scope of this book.

We develop these ideas further in section 12.11 of appendix 12B.

Exercise 12.3.2. Prove that if $p_1, \dots, p_k$ are distinct primes that are each represented by some form of discriminant d, then $p_1 \cdots p_k$ is also represented by some form of discriminant d.

12.4. Class numbers

Theorem 12.2. *If $d < 0$, then there are only finitely many reduced binary quadratic forms of discriminant d.*

Proof. For a reduced binary quadratic form, $|d| = 4ac - (|b|)^2 \geq 4a \cdot a - a^2 = 3a^2$ and so a is a positive integer for which

$$a \leq \sqrt{|d|/3}.$$

Therefore for a given $d < 0$ there are only finitely many a, and so b (as $|b| \le a$), but then $c = (b^2 - d)/4a$ is determined, and so there are only finitely many reduced binary quadratic forms of discriminant d. □

Let $h(d)$ denote the *class number*, the number of equivalence classes of binary quadratic forms of discriminant d. We have just shown $h(d)$ is finite, and the proof of Theorem 12.2 even describes an algorithm to easily find all the reduced binary quadratic forms of a given discriminant $d < 0$. In fact $h(d) \ge 1$ since we always have the principal form. If $h(d) = 1$, then all binary quadratic forms are equivalent to the principal form.

Example. If $d = -163$, then $|b| \le a \le \sqrt{163/3} < 8$. But b is odd, since $b \equiv b^2 = d + 4ac \equiv d \pmod 2$, so $|b| = 1, 3, 5$, or 7. Therefore $ac = (b^2 + 163)/4 = 41, 43, 47$, or 53, a prime, with $0 < a < c$ and hence $a = 1$. Since b is odd and $-a < b \le a$, we deduce that $b = 1$ and so $c = 41$. Hence $x^2 + xy + 41y^2$ is the only reduced binary quadratic form of discriminant -163, and therefore $h(-163) = 1$.

Exercise 12.4.1. Determine all of the reduced binary quadratic forms of discriminant d for $-20 \le d \le -1$ as well as for $d = -28, -43, -67, -167$, and -171.

Exercise 12.4.2. Determine all of the reduced binary quadratic forms of discriminant d for $d = -3, -15, -23, -39, -47, -87, -71$, and -95.

Exercise 12.4.3. Determine all of the reduced binary quadratic forms of discriminant d for $d = -4, -20, -56$, and -104.

Exercise 12.4.4. Prove that if $ax^2 + bxy + cy^2$ is a reduced binary quadratic of discriminant $d < 0$, then $|c| \ge \sqrt{|d|}/2$.

12.5. Class number one

Corollary 12.5.1. *Suppose that $h(d) = 1$. Then N is properly represented by the form of discriminant d if and only if d is a square* mod $4N$.

Proof. This follows immediately from Proposition 12.3.1, since there is just one equivalence class of quadratic forms of discriminant d, and forms in the same equivalence class represent the same integers by Proposition 12.1.1. □

We have $h(-4) = 1$ and so Corollary 12.5.1 implies that integer N is properly represented by $x^2 + y^2$ if and only if -4 is a square mod $4N$. This is more or less Theorem 9.2 (and can be deduced from its proof).

In the example in section 12.4 we showed that $x^2 + xy + 41y^2$ is the only binary quadratic form of discriminant -163. This implies, by Corollary 12.5.1, that if prime $p \ne 2$ or 163, then it can be represented by the binary quadratic form $x^2 + xy + 41y^2$ if and only if $(-163/p) = 1$.

In exercise 12.4.1 we exhibited nine fundamental discriminants $d < 0$ with $h(d) = 1$, namely $d = -3, -4, -7, -8, -11, -19, -43, -67$, as well as -163. It

turns out these are the only ones with class number one.[2] Therefore, as in the example above, if $p \nmid 2d$, then

$$\begin{gathered}
p \text{ is represented by } x^2+y^2 \text{ if and only if } (-1/p)=1;\\
p \text{ is represented by } x^2+2y^2 \text{ if and only if } (-2/p)=1;\\
p \text{ is represented by } x^2+xy+y^2 \text{ if and only if } (-3/p)=1;\\
p \text{ is represented by } x^2+xy+2y^2 \text{ if and only if } (-7/p)=1;\\
p \text{ is represented by } x^2+xy+3y^2 \text{ if and only if } (-11/p)=1;\\
p \text{ is represented by } x^2+xy+5y^2 \text{ if and only if } (-19/p)=1;\\
p \text{ is represented by } x^2+xy+11y^2 \text{ if and only if } (-43/p)=1;\\
p \text{ is represented by } x^2+xy+17y^2 \text{ if and only if } (-67/p)=1;\\
p \text{ is represented by } x^2+xy+41y^2 \text{ if and only if } (-163/p)=1.
\end{gathered}$$

Euler noticed that the polynomial x^2+x+41 is prime for $x=0,1,2,\dots,39$, and similarly the other polynomials above. Rabinowiscz proved that this is an "if and only if" condition:

Theorem 12.3 (Rabinowiscz's criterion)**.** *We have $h(1-4A)=1$ for $A\geq 2$ if and only if x^2+x+A is prime for $n=0,1,2,\dots,A-2$.*

At $n=A-1$ the polynomial takes value $(A-1)^2+(A-1)+A=A^2$ which is composite. We will prove Rabinowiscz's criterion below.

What about when the class number is not one? In the example with $d=-20$ we have $h(-20)=2$; the two reduced forms are x^2+5y^2 and $2x^2+2xy+3y^2$. By Proposition 12.3.1, p is represented by at least one of these two forms if and only if $(-5/p)=0$ or 1, that is, if $p\equiv 1,3,7$, or 9 (mod 20) or $p=2$ or 5. Can we decide which of these primes are represented by which of the two forms? Note that if $p=x^2+5y^2$, then $(p/5)=0$ or 1 and so $p=5$ or $p\equiv\pm 1 \pmod 5$, and thus $p\equiv 1$ or 9 (mod 20). If $p=2x^2+2xy+3y^2$, then $2p=(2x+y)^2+5y^2$ and so $p=2$ or $(2p/5)=1$; that is, $(p/5)=-1$, and hence $p\equiv 3$ or 7 (mod 20). Hence we have proved

p is represented by x^2+5y^2 if and only if $p=5$, or $p\equiv 1$ or 9 (mod 20);

p is represented by $2x^2+2xy+3y^2$ if and only if $p=2$, or $p\equiv 3$ or 7 (mod 20).

That is, we can distinguish which primes can be represented by which binary quadratic form of discriminant -20, through congruence conditions, despite the fact that the class number is not one. However we cannot always do this; that is, we cannot always distinguish which primes are represented by which binary quadratic form of discriminant d. It is understood how to recognize those discriminants d for which we can determine which binary quadratic forms of discriminant d represent

[2]The proof that the above list gives all of the $d<0$, for which $h(d)=1$, has an interesting history. By 1934 it was known that there is no more than one further such d, but that putative d could not be ruled out by the method. In 1952, Kurt Heegner, a German school teacher proposed an extraordinary proof that there are no further d. At the time his paper was ignored since it was based on a result from an old book (of Weber) whose proof was known to be incomplete. In 1966 Alan Baker gave a very different (and more obviously correct) proof that this was the complete list of discriminants with class number one, and this was widely acknowledged to be correct. However, soon afterwards Stark realized that the proofs in Weber are easily corrected, so that Heegner's work had been fundamentally correct. Heegner was subsequently given credit for solving this famous problem, but sadly only after he had died. Heegner's paper contains a most extraordinary construction, widely regarded to be one of the most creative and influential in modern number theory.

which integers simply through congruence conditions (see section 12.11 of appendix 12B). These *idoneal numbers* were recognized by Euler. He found 65 of them, and no more are known—it is an open conjecture as to whether Euler's list is complete. It is known that there can be at most one further undiscovered idoneal number, but it seems unlikely whether the techniques used can rule out this putative example.[3]

Exercise 12.5.1. (a) Determine the two reduced binary quadratic forms of discriminant -15.
(b) Determine which reduced residue classes can be represented by some form of discriminant -15?
(c) Distinguish which primes are represented by which form (with proof).

Proof of Rabinowiscz's criterion. We begin by showing that $f(n) := n^2+n+A$ is composite for some integer n in the range $0 \le n \le A-2$, if and only if $d = 1-4A$ is a square mod $4p$ for some prime $p < A$. For if n^2+n+A is composite, let p be its smallest prime factor so that $p \le f(n)^{1/2} < f(A-1)^{1/2} = A$. Then $(2n+1)^2 - d = 4(n^2+n+A) \equiv 0 \pmod{4p}$ so that d is a square mod $4p$. On the other hand if d is a square mod $4p$ where p is a prime $\le A-1$, select m to be the smallest positive integer such that $d \equiv m^2 \pmod{4p}$. Then $m < 2p$ (or else replace m by $4p-m$) and m is odd (as d is odd), so write $m = 2n+1$ and then $0 \le n \le p-1 \le A-2$ with $d \equiv (2n+1)^2 \bmod 4p$. Therefore p divides n^2+n+A with $p < A = f(0) < f(n)$ so that n^2+n+A is composite.

Now we show that $h(d) > 1$ if and only if $d = 1-4A$ is a square mod $4p$ for some prime $p < A$. If $h(d) > 1$, then there exists a reduced binary quadratic $ax^2+bxy+cy^2$ of discriminant d with $1 < a \le \sqrt{|d|/3} < A$ by the proof of Theorem 12.2. If p is a prime factor of a, then $p \le a < A$ and $d = b^2-4ac$ is a square mod $4p$. On the other hand if d is a square mod $4p$ for some prime $p < A$, and $h(d) = 1$, then p is represented by $x^2+xy+Ay^2$ by Proposition 12.3.1(ii). Now $y \ne 0$ as p is not a square. Therefore $4p = (2x+y)^2 + |d|y^2 \ge 0^2 + |d| \cdot 1^2 = |d|$; that is, $p \ge A$, a contradiction. (We will extend this proof to obtain more on the small values taken by any binary quadratic form of negative discriminant, in exercise 12.6.1(a).) Hence $h(d) > 1$.

Putting these two results together, we deduce that $h(d) > 1$ if and only if $f(n) := n^2+n+A$ is composite for some integer n in the range $0 \le n \le A-2$, which implies Rabinowiscz's criterion. □

Exercise 12.5.2.† Prove that if n^2+n+A is prime for all integers n in the range $0 \le n \le B$, where $1 \le B < (A-1)/2$, then $\left(\frac{1-4A}{p}\right) = -1$ for all primes $p \le 2B+1$.

The class number one problem for even negative fundamental discriminants is not difficult:

Theorem 12.4. *If $h(d) = 1$ with $d = -4n$ for $n \in \mathbb{N}$, then $n = 1, 2, 3, 4,$ or 7.*

Proof. Suppose that $h(-4n) = 1$. Then n must be a prime power or else there exist coprime integers $1 < a \le c$ for which $ac = n$ and so $[a, 0, c]$ is a non-principal reduced form of discriminant $-4n$. Moreover $n+1$ must be an odd prime or a power of 2 or else there exist integers $1 < a \le c$ with $\gcd(a, 2, c) = 1$ for which $ac = n+1$ and so $[a, 2, c]$ is a non-principal reduced form of discriminant $-4n$.

[3] We therefore find ourselves in much the same situation as for class number one before Heegner's work, as discussed in the last footnote.

One of n and $n+1$ is even and hence must be a power of 2 (from the previous paragraph). If $n = 2^k$ with $k \geq 4$, then we have the non-principal reduced form $[4, 4, 2^{k-2}+1]$, and if $n+1 = 2^k$ with $k \geq 6$, then we have the non-principal reduced form $[8, 6, 2^{k-3}+1]$.

Therefore if $h(-4n) = 1$, then $n = 1, 2, 4$, or 8 or $n+1 = 2, 4, 8, 16$, or 32. We can rule out $n = 15$ (as 15 is composite) and $n = 8$ (as 9 is not an odd prime) and $n = 31$ (as $[5, 4, 7]$ is a non-principal reduced form of discriminant -124). We know that $h(-4n) = 1$ for $n = 1, 2, 3, 4$, and 7 by exercise 12.4.1. □

These discriminants have a beautiful property.

Corollary 12.5.2. *Let $n = 1, 2, 3, 4$, or 7. If p is a prime that does not divide $4n$, then p can be written as $u^2 + nv^2$ if and only if $\left(\frac{-n}{p}\right) = 1$.*

Proof. As we just discussed $h(-4n) = 1$, and so all binary quadratic forms of discriminant $-4n$ are equivalent to $x^2 + ny^2$. By Proposition 12.3.1, p can be represented by some form of discriminant $-4n$ if and only if $-4n$ is a square mod p, and the result follows. □

We had already discussed representations of p by $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$ in sections 9.1 and 9.2, and $x^2 + 4y^2 = x^2 + (2y)^2$ follows easily from $x^2 + y^2$. This leaves only the most interesting of the cases of Corollary 12.5.2:

$$p = x^2 + 7y^2 \text{ if and only if } p \equiv 1, 9, 11, 15, 23, \text{ or } 25 \pmod{28}.$$

Exercise 12.5.3. Let q be a prime $\equiv -1 \pmod 4$. Prove that $\left(\frac{p}{q}\right) = -1$ for all primes $p < \frac{q+1}{4}$ if and only if $h(-q) = 1$. This result suggests that finding a small prime p with $\left(\frac{p}{q}\right) = 1$ can be a deep problem (see appendix 8B for a discussion of small quadratic residues).

For much more on the values taken by binary quadratic forms, particularly the prime values, we recommend David Cox's wonderful book [**1**].

References for this chapter

[1] David A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, 1989.

[2] Dorian Goldfeld, *Gauss's class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. **13** (1985), 23–37.

Additional exercises

These last questions get considerably more involved but may be of interest to students interested in further pursuing number theory.

Exercise 12.6.1. Suppose that $f(x, y) = ax^2 + bxy + cy^2$ is a reduced binary quadratic form.

(a) Show that if $am^2 + bmn + cn^2 \leq a - |b| + c$ with $(m, n) = 1$, then $|m|, |n| \leq 1$.

(b) Prove that the least values properly represented by f are $a \leq c \leq a - |b| + c$, the first two properly represented twice, the last twice unless $b = 0$, in which case it is properly represented four times.

Exercise 12.6.2. We now use the results of exercise 12.6.1 to understand equivalences between primitive reduced binary quadratic forms. The idea is to recognize a reduced binary quadratic form by the smallest values it properly represents.

(a) Prove that:
- If $0 < |b| < a < c$, then $[a, b, c]$ properly represents a, c, and $a - |b| + c$ in exactly 2, 2, and 2 different ways, respectively.
- If $0 < |b| = a < c$, then $[a, b, c]$ properly represents a, and $c = a - |b| + c$ in exactly 2, and 4 different ways, respectively.
- If $0 < |b| < a = c$, then $[a, b, c]$ properly represents $a = c$, and $a - |b| + c$ in exactly 4, and 2 different ways, respectively.
- If $0 = |b| < a < c$, then $[a, b, c]$ properly represents a, c, and $a - |b| + c$ in exactly 2, 2, and 4 different ways, respectively.
- $[1, 1, 1]$ properly represents 1 in exactly six different ways.
- $[1, 0, 1]$ properly represents both 1 and 2 in exactly four different ways.

(b) Deduce that if $[a, b, c]$, and $[A, B, C]$ are equivalent primitive reduced binary quadratic forms, then $A = a$, $C = c$, and $B = b$ or $-b$.

(c) Use exercise 12.6.1(a) to show that the entries of a matrix representing such an equivalence must each be -1, 0, or 1.

(d) Prove that distinct primitive reduced binary quadratic forms are all inequivalent. Together with Theorem 12.1 this implies that every positive definite binary quadratic form is properly equivalent to a unique reduced form.

(e) Suppose that $M \in \mathrm{SL}(2, \mathbb{Z})$ transforms a primitive reduced binary quadratic form to itself (this is an *automorphism*). Show that $M = \pm I$, except in the following two cases:
- $[1, 1, 1]$ has automorphisms given by $\pm I$, $\pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, and $\pm \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$.
- $[1, 0, 1]$ has automorphisms given by $\pm I$ and $\pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Exercise 12.6.3. (a) Show that if $[A, B, C] \sim [a, b, c]$, then $[A, -B, C] \sim [a, -b, c]$.

(b) Use exercise 12.6.2(d) to show that if $[a, b, c]$ is reduced, then $[a, b, c] \sim [a, -b, c]$ if and only if $b = 0$, $b = a$, or $a = c$.

(c) Deduce that $[A, B, C] \sim [A, -B, C]$ if and only if they are equivalent to a quadratic form $[a, 0, c]$, $[a, a, c]$, or $[a, b, a]$.

(d) Prove that $[a, a, c] \sim [c, 2c - a, c]$.

(e) If $d < 0$ is odd, then show that the primitive reduced forms are given by taking each factorization $-d = rs$ with $0 < r \le s$ and $(r, s) = 1$,

$$\begin{cases} [a, a, c] & \text{if } s \ge 3r \text{ where } a = r \text{ and } c = (r + s)/4, \\ [a, b, a] & \text{if } s < 3r \text{ where } a = (r + s)/4 \text{ and } b = (s - r)/2. \end{cases}$$

(f) If $d < 0$ is even, then show that the primitive reduced forms are given by taking each factorization $-d/4 = rs$ with $0 < r \le s$ and $(r, s) = 1$,

$$\begin{cases} [a, 0, c] & \text{with } a = r \text{ and } c = s, \\ [a, a, c] & \text{if } s > 3r \text{ where } a = 2r \text{ and } c = (r + s)/2, \\ [a, b, a] & \text{if } s < 3r \text{ where } a = (r + s)/2 \text{ and } b = s - r. \end{cases}$$

Note that the last two cases hold only if $d/4$ is odd.

(g) Show that each binary quadratic form either represents both r and s, or both $2r$ and $2s$. (In (d), take $f(1, -2) = s$ in the first case; $f(1, 1) = s$, $f(1, -1) = r$ in the second case.)

(h) Deduce that if $d < 0$ is a fundamental discriminant, then there are exactly 2^{t-1} reduced binary quadratic forms for which $[a, b, c] \sim [a, -b, c]$, where t is the number of odd prime divisors of $|d|$, unless $4 \| d$ in which case there are 2^t.

Exercise 12.6.4.† (a) Prove that $x^2 + 6y^2$ and $2x^2 + 3y^2$ are the only binary quadratic forms, up to equivalence, of discriminant -24.

(b) Prove that prime p can be written in the form $a^2 + 6b^2$ if and only if $p \equiv 1$ or $7 \pmod{24}$.

(c) Prove that prime p can be written in the form $2u^2 + 3v^2$ if and only if $p = 2$ or 3, or $p \equiv 5$ or $11 \pmod{24}$.

We can refine this further:

(d) Prove that prime p can be written in the form $a^2 + 24B^2$ if and only if $p \equiv 1 \pmod{24}$.

(e) Prove that prime p can be written in the form $8U^2 + 3v^2$ if and only if $p = 3$, or $p \equiv 11 \pmod{24}$.

Automorphisms of binary quadratic forms.

Exercise 12.6.5. Suppose that $f \sim g$ via the transformation M and that G is the group of automorphisms of f.

(a) Prove that $M^{-1}GM$ is the group of automorphisms of g.

(b) Prove that MG is the set of transformations yielding g from f.

(c) Deduce that there are $\omega(d)$ automorphisms of every primitive quadratic form of discriminant d, where $\omega(-3) = 6, \omega(-4) = 4$, and $\omega(d) = 2$ for all other discriminants $d < 0$.

Exercise 12.6.6. (a) If $N = f(a, b)$, then $N = f(-a, -b)$. If $N = a^2 + b^2$, then $N = b^2 + (-a)^2 = (-a)^2 + (-b)^2 = (-b)^2 + a^2$. If $N = a^2 + ab + b^2$, then find five other representations of N by the quadratic form $x^2 + xy + y^2$.

(b) Explain how these representations correspond to the automorphisms of the quadratic form.

(c) Why did we not include $N = (-a)^2 + b^2$ in the representations in part (a)?

Exercise 12.6.7. (a) Let $\alpha, \beta, \gamma, \delta$ be given integers for which $\alpha\delta - \beta\gamma = 1$. Prove that β', δ' are integers for which $\alpha\delta' - \beta'\gamma = 1$ if and only if there exists an integer k such that

$$\begin{pmatrix} \alpha & \beta' \\ \gamma & \delta' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.$$

(b) If $A = f(\alpha, \gamma)$ with $(\alpha, \gamma) = 1$, then prove that there exists a unique pair of integers β, δ such that $f \sim [A, B, C]$ using the matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ for some integer B in the range $-A < B \le A$.

(c) Deduce that the proper representations of the integer A by reduced binary quadratic forms of discriminant d are in $\omega(d)$-to-1 correspondence with the solutions to $B^2 \equiv d \pmod{4A}$ with $-A < B \le A$.

Exercise 12.6.8. Let $f_1, \dots, f_h$ be the $h = h(d)$ distinct reduced binary quadratic forms of discriminant d, where $d \equiv 0$ or $1 \pmod 4$. Let $r_j(A)$ denote the number of proper representations of A by f_j. Prove that

$$r_1(A) + \cdots + r_h(A) = \frac{1}{2}\omega(d) \cdot \#\{B \pmod{4A} : \ B^2 \equiv d \pmod{4A}\}$$

and that this equals $\omega(d) \cdot \prod_{p|A} \left(1 + \left(\frac{d}{p}\right)\right)$ unless perhaps $4|(A, d)$.

Exercise 12.6.9. Suppose that p is an odd prime for which $(d/p) = 1$. Prove that p is properly represented either by only the principal form of discriminant d, or by only two non-principal, reduced, binary quadratic forms of discriminant d, one, say, $ax^2 + bxy + cy^2$, the other $ax^2 - bxy + cy^2$.

Transformations of the upper half-plane. Let $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ be the *upper half-plane*. We consider transformations with $M = \mathrm{SL}(2, \mathbb{Z})$ acting on $z \in \mathbb{C}$ by taking $M \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$ and considering this to be the map $z \to u/v$. In Theorem 1.2 we saw that that every matrix in $\mathrm{SL}(2, \mathbb{Z})$ can be represented as a product of the two fundamental matrices $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Exercise 12.6.10. Prove that S represents the transformation $z \to z + 1$ and that T represents the transformation $z \to -1/z$.

We define

$$\mathcal{F}=\left\{z\in\mathbb{C}:|z|>1 \text{ and } -\frac{1}{2}\le \mathrm{Re}(z)<\frac{1}{2}\right\}\cup\left\{z\in\mathbb{C}:|z|=1 \text{ and } -\frac{1}{2}\le \mathrm{Re}(z)\le 0\right\}.$$

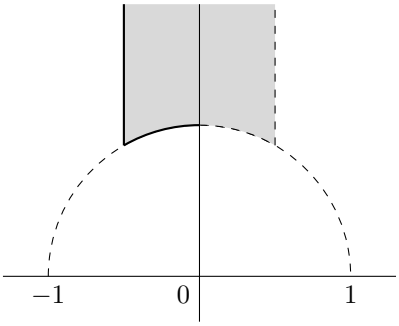
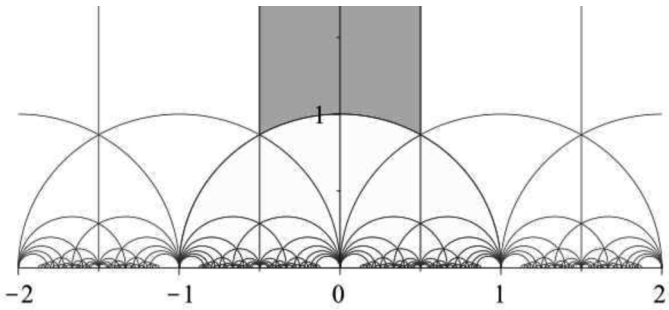


Figure 12.1. The shaded region is the *fundamental domain* $\mathcal{F}\subset\mathcal{H}$.

Exercise 12.6.11.† Prove that the binary quadratic form $ax^2+bxy+cy^2$ with discriminant $d<0$ is reduced if and only if $\frac{-b+\sqrt{d}}{2a}\in\mathcal{F}$.

Exercise 12.6.12.† Prove that for every $z\in\mathbb{C}$ there exists $M\in\mathrm{SL}(2,\mathbb{Z})$ such that $Mz\in\mathcal{F}$. Prove that M is unique.

Exercise 12.6.13.‡ Show that $\{M\mathcal{F}:\ M\in\mathrm{SL}(2,\mathbb{Z})\}$ is a partition of $\mathcal{H}$ into disjoint sets.



The shaded region is $\mathcal{F}$. Each enclosed region is a domain $M\mathcal{F}$ for some $M\in\mathrm{SL}(2,\mathbb{Z})$.

Appendix 12A. Composition rules: Gauss, Dirichlet, and Bhargava

We study generalizations of the identity (9.1.1), which leads to a notion of "multiplying" binary quadratic forms together, and hence to the group structure discovered by Gauss. We go on to study the reformulations of Dirichlet and Bhargava.

12.7. Composition and Gauss

In (9.1.1) we see that the product of any two integers represented by the binary quadratic form x^2+y^2 is also an integer represented by that binary quadratic form. We now look for further such identities. One easy generalization is given by

(12.7.1) $(u^2 + Dv^2)(r^2 + Ds^2) = x^2 + Dy^2$ where $x = ur + Dvs$ and $y = us - vr$.

Therefore the product of any two integers represented by the binary quadratic form $x^2 + Dy^2$ is also an integer represented by that binary quadratic form. For general *diagonal* binary quadratic forms (that is, having no "cross term" bxy) we have

(12.7.2) $(au^2 + cv^2)(ar^2 + cs^2) = x^2 + acy^2$ where $x = aur + cvs$ and $y = us - vr$.

Notice here that the quadratic form on the right-hand side is different from those on the left; that is, the product of any two integers represented by the binary quadratic form $ax^2 + cy^2$ is an integer represented by the binary quadratic form $x^2 + acy^2$.

One can come up with a similar identity no matter what the quadratic form, though one proceeds slightly differently depending on whether the coefficient b is odd or even. The discriminant $d = b^2 - 4ac$ has the same parity as b. If d is even,

then

$$(au^2+buv+cv^2)(ar^2+brs+cs^2) = x^2 - \frac{d}{4}y^2, \tag{12.7.3}$$

$$\text{where } x = aur + \tfrac{b}{2}(vr+us) + cvs \text{ and } y = rv - su.$$

If d is odd, then

$$(au^2+buv+cv^2)(ar^2+brs+cs^2) = x^2 + xy - \frac{d-1}{4}y^2, \tag{12.7.4}$$

$$\text{where } x = aur + \tfrac{b-1}{2}vr + \tfrac{b+1}{2}us + cvs \text{ and } y = rv - su.$$

That is, the product of two integers represented by the same binary quadratic form can be represented by the principal binary quadratic form of the same discriminant.

Exercise 12.7.1. (a) Prove that if n is represented by $ax^2+bxy+cy^2$, then an is represented by the principal form of the same discriminant.

(b) Suppose that $d<0$. Deduce that if d is a square mod $4n$, then there is a multiple an of n which is represented by the principal form of discriminant d, with $1 \le a \le \sqrt{|d|/3}$.

(c) We obtained the bound $1 \le a \le \sqrt{|d|}$ when d is even in section 9.6. Use that method to find a bound in the case that d is odd.

What about the product of the values of two different binary quadratic forms? If d is even, we have

$$(au^2+buv+cv^2)(r^2 - \tfrac{d}{4}s^2) = ax^2+bxy+cy^2, \tag{12.7.5}$$

$$\text{where } x = ur + \tfrac{b}{2}su + cvs \text{ and } y = vr - asu - \tfrac{b}{2}vs.$$

If d is odd, then

$$(au^2+buv+cv^2)(r^2 + rs - \tfrac{d-1}{4}s^2) = ax^2+bxy+cy^2, \tag{12.7.6}$$

$$\text{where } x = ur + \tfrac{b+1}{2}su + cvs \text{ and } y = vr - asu - \tfrac{b-1}{2}vs.$$

That is, the product of an integer that can be represented by a binary quadratic form f and an integer that can be represented by the principal binary quadratic form of the same discriminant can be represented by f.

Exercise 12.7.2. Suppose that a is a prime and $d=b^2-4ac$ is even. Let $D=-d/4$.

(a) Show that if a divides r^2+Ds^2, then a divides either $r+(b/2)s$ or $r-(b/2)s$.

(b) Prove that if $r^2+Ds^2 = an$, then there exist integers X, Y for which $n = aX^2+bXY+cY^2$.

If n is prime, then this result is true whether or not a is prime, but we will not prove that here. Assume though that is so.

(c) Suppose that $(d/p)=1$ and that ap is the smallest multiple of p that is represented by the principal form. Prove that a here must take the same value as in exercise 12.6.9.

(d) Prove that $1 \le a \le \sqrt{|d|/3}$ and then use exercises 12.4.4 and 12.6.1(b) to prove that if $p < \sqrt{|d|}/2$, then $a=p$.

What about two different binary quadratic forms with no particular structure? For example,

$$(4u^2+3uv+5v^2)(3r^2+rs+6s^2) = 2x^2+xy+9y^2$$

by taking $x = ur - 3us - 2vr - 3vs$ and $y = ur + us + vr - vs$. These are three inequivalent binary quadratic forms of discriminant -71. Gauss called this *composition*, that is, finding, for given binary quadratic forms f and g of the same

discriminant, a third binary quadratic form h of the same discriminant for which

$$f(u,v)g(r,s) = h(x,y),$$

where x and y are quadratic polynomials in u, v, r, and s.

These constructions suggest many questions. For example, are the identities that we found for two given quadratic forms the only possibility? Could the product of two sums of two squares always equal the value of some entirely different quadratic form? When we are given two quadratic forms of the same discriminant, is it true that there is always some third quadratic form of the same discriminant such that the product of the values of the first two always equals a value of the third? That is, is there always a composition of two given binary quadratic forms of the same discriminant? If so, can we determine the third quadratic form quickly?

Gauss proved that one *can always* find the composition of two binary quadratic forms of the same discriminant. The formulas above can mislead one into guessing that this is simply a question of finding the right generalization, but that is far from the truth. All of the examples, (12.7.1) through to (12.7.6), are so explicit only because they are very special cases in the theory. In Gauss's proof he had to prove that various other equations could be solved in integers in order to find h and the quadratic polynomials x and y (which are polynomials in u, v, r, and s). This was so complicated that some of the intermediate formulas took two pages to write down and are very difficult to make sense of.[4] We will prove Gauss's theorem though we will approach it in a somewhat different way.

Exercise 12.7.3. Given non-zero integers a, b, c, d prove that there exist integers m, n such that the set of integers that can be represented by $(ar+bs)(cu+dv)$ as r, s, u, v run over the integers is the same as the set of integers that can be represented by $mx+ny$ as x, y run over the integers.

We finish this section by presenting a fairly general composition.

Proposition 12.7.1. *Suppose that $a_ix^2 + b_ixy + c_iy^2$ for $i = 1, 2$ are binary quadratic forms of discriminant d such that $q = (a_1, a_2)$ divides $\frac{b_1+b_2}{2}$. Then*

$$(12.7.7) \quad (a_1x_1^2 + b_1x_1y_1 + c_1y_1^2)(a_2x_2^2 + b_2x_2y_2 + c_2y_2^2) = a_3x_3^2 + b_3x_3y_3 + c_3y_3^2$$

where $a_3 = a_1a_2/q^2$ and b_3 is any integer simultaneously satisfying the following (solvable) set of congruences:

$$b_3^2 \equiv d \pmod{4a_1a_2/q^2},$$
$$b_3 \equiv b_1 \pmod{2a_1/q}, \qquad b_3 \equiv b_2 \pmod{2a_2/q},$$
$$b_3(b_1+b_2) \equiv b_1b_2 + d \pmod{4a_1a_2/q},$$

and c_3 is chosen so that the discriminant of $a_3x_3^2 + b_3x_3y_3 + c_3y_3^2$ is d.

Exercise 12.7.4. Show that the above congruences for b_3 can be solved.

Proposition 12.7.1 implies that we can always compose two binary quadratic forms f and g of the same discriminant, whose leading coefficients are coprime.

[4] See article 234 and beyond in Gauss's book *Disquisitiones Arithmeticae* (1804).

Proof sketch. Computer software verifies that (12.7.7) holds taking $a_3 = a_1a_2/q^2$, for any integer q dividing (a_1, a_2), with

$$x_3 = qx_1x_2 + \frac{b_2 - b_3}{2a_2/q} \cdot x_1y_2 + \frac{b_1 - b_3}{2a_1/q} \cdot x_2y_1 + \frac{b_1b_2 + d - b_3b_1 - b_3b_2}{4a_1a_2/q} \cdot y_1y_2,$$

$$\text{and} \qquad y_3 = \frac{a_1}{q} \cdot x_1y_2 + \frac{a_2}{q} \cdot x_2y_1 + \frac{b_1 + b_2}{2q} \cdot y_1y_2.$$

To ensure that we are always working with integers, the coefficients of x_3 and y_3 must be integers. So this formula works if we can find integers q and b_3 for which q divides a_1, a_2, and $\frac{b_1+b_2}{2}$, and the above four congruences hold simultaneously for integer b_3. It is difficult to determine whether there is such a b_3 for an arbitrary q, but not so challenging if $q = (a_1, a_2)$ divides $\frac{b_1+b_2}{2}$. □

Corollary 12.7.1. *For any given integers a, b, c, h, k we have*

$$(ab, hk, ch) \cdot (ac, hk, bh) \sim (ah, hk, bc).$$

Proof. We multiply (ab, hk, ch) and $(ac, hk, bh) \sim (bh, -hk, ac)$ using the proof of Proposition 12.7.1. We take $q = b$ so that $a_3 = ah$ and $2q|b_1 + b_2 = 0$. Selecting $b_3 = hk$ we find that the congruences of Proposition 12.7.1 reduce to $d \equiv (hk)^2 \pmod{4abh}$, which follows from $d = (hk)^2 - 4abch$. Hence we have that $(ab, hk, ch) \cdot (ac, hk, bh) \sim (ab, hk, ch) \cdot (bh, -hk, ac) \sim (ah, hk, bc)$.

To get more symmetry in the statement of the result we note that $(ah, hk, bc) \cdot (bc, hk, ah) = 1$, and so

$$(ab, hk, ch) \cdot (ac, hk, bh) \cdot (bc, hk, ah) \sim 1. \qquad \square$$

12.8. Dirichlet composition

Dirichlet claimed that when he was a student, working with Gauss, he slept with a copy of *Disquisitiones* under his pillow every night for three years. It worked, as Dirichlet found a way to better understand Gauss's proof of composition, which amounts to a straightforward algorithm to determine the composition of two given binary quadratic forms f and g of the same discriminant.

Exercise 12.8.1. Given any primitive binary quadratic form $f(x, y) \in \mathbb{Z}[x, y]$ and non-zero integer A, prove that there exist integers r and s such that $f(r, s)$ is coprime to A. Deduce that there exists a binary quadratic form g, for which $f \sim g$, with $(g(1, 0), A) = 1$.

Exercise 12.8.2. Suppose that $f(x, y), F(X, Y)$ are two binary quadratic forms, with $\operatorname{disc}(f) \equiv \operatorname{disc}(F) \pmod 2$, for which $f(1, 0) = a$ is coprime to $F(1, 0) = A$. Prove that there exist quadratic forms $g = ax^2 + bxy + cy^2$ and $G = AX^2 + bXY + CY^2$ with the same middle coefficient, such that $f \sim g$ and $F \sim G$.

Now suppose we begin with two quadratic forms of the same discriminant. Let A be the leading coefficient of one of them. Then the other is equivalent to a quadratic form with leading coefficient a, for some integer a coprime to A, by exercise 12.8.1. Then these are equivalent to quadratic forms $g = ax^2 + bxy + cy^2$ and $G = AX^2 + bXY + CY^2$, respectively, by exercise 12.8.2. Since these have the

same discriminant we deduce that $ac = AC$ and so there exists an integer h for which

$$g(x,y) = ax^2 + bxy + Ahy^2 \quad \text{and} \quad G(x,y) = Ax^2 + bxy + ahy^2.$$

Then

$$H(m,n) = g(u,v)G(r,s) \text{ with } H(x,y) = aAx^2 + bxy + hy^2,$$
$$\text{where } m = ur - hvs \text{ and } n = aus + Avr + bvs.$$

Dirichlet went on to interpret this in terms of what we would today call *ideals*; and this in turn led to the birth of modern algebra by Dedekind. In this theory one is typically not so much interested in the identity, writing H as a product of g and G (which is typically very complicated and none too enlightening), but rather in how to determine H from g and G. Dirichlet's proof goes as follows:

The ideal $I\left(\frac{-b+\sqrt{d}}{2}, a\right)$ is associated to a given binary quadratic form $ax^2 + bxy + cy^2$ (see section 12.10 of appendix 12B). Therefore when we multiply together g and G, we multiply together their associated ideals to obtain

$$J := I\left(\frac{-b+\sqrt{d}}{2}, a\right) \cdot I\left(\frac{-b+\sqrt{d}}{2}, A\right),$$

which contains aA as well as both $a \cdot \frac{-b+\sqrt{d}}{2}$ and $A \cdot \frac{-b+\sqrt{d}}{2}$. Since $(a, A) = 1$ there exist integers r, s for which $ar + As = 1$ and so our new ideal contains

$$r \cdot a \cdot \frac{-b+\sqrt{d}}{2} + s \cdot A \cdot \frac{-b+\sqrt{d}}{2} = \frac{-b+\sqrt{d}}{2}.$$

Therefore

$$J = I\left(\frac{-b+\sqrt{d}}{2}, aA\right)$$

which is the ideal associated with the binary quadratic form H.

Defining the class group. We now know that we can multiply together the values of any two quadratic forms of the same discriminant and get another. Since there are only finitely many equivalence classes of binary quadratic forms of a given discriminant this might seem to lead to a group structure, under multiplication. To prove this we will need to know that the usual group properties hold (most importantly, associativity), and also that the values of a binary quadratic form classifies the form. Unfortunately this is not quite true. In exercise 12.6.2 we saw that the only issue in distinguishing between the values taken by forms is perhaps the values taken by $ax^2 + bxy + cy^2$ and $au^2 - buv + cv^2$. However there is an automorphism $u = x, v = -y$ between their sets of values so they cannot be distinguished in this way. On the other hand, the ideals

$$I\left(\frac{-b+\sqrt{d}}{2}, a\right) \quad \text{and} \quad I\left(\frac{b+\sqrt{d}}{2}, a\right)$$

are quite distinct, and so multiplying ideals (and therefore forms) using Dirichlet's technique leads one immediately to being able to determine a group structure. This is called the *class group*, since the group acts on equivalence classes of ideals (and

so of forms). In this approach, associativity follows easily, as multiplication of the numbers in the ideals multiply associatively, and it is similarly evident that the class group is commutative. Therefore the class group is a commutative group, acting on the ideal classes of a given discriminant, with identity element given by the class of principal ideals (which correspond to the principal form).

We will now give a useful criterion to determine how to take square roots inside the class group.

Proposition 12.8.1. *If f is a binary quadratic form of fundamental discriminant d which represents the square of an odd integer, then there exists a binary quadratic form g of discriminant d for which $g \cdot g \sim f$.*

Proof. We begin by squaring the primitive form $ax^2 + bxy + acy^2$. Then

$$J := I\left(\frac{-b+\sqrt{d}}{2}, a\right)^2$$

contains $a^2, a \cdot \frac{-b+\sqrt{d}}{2}$, and $(\frac{-b+\sqrt{d}}{2})^2 = -a^2c - b(\frac{-b+\sqrt{d}}{2})$. Therefore J contains $a \cdot \frac{-b+\sqrt{d}}{2}$ and $b \cdot \frac{-b+\sqrt{d}}{2}$. Now $(a, b) = 1$ or else our original form was not primitive, and so J contains $\frac{-b+\sqrt{d}}{2}$. Therefore

$$J = I\left(\frac{-b+\sqrt{d}}{2}, a^2\right)$$

and the corresponding binary quadratic form is $a^2x^2 + bxy + cy^2$.

One can justify this by finding a suitable multiplication of forms, namely,

$$(ar^2 + brs + acs^2)(au^2 + buv + acv^2) = a^2x^2 + bxy + cy^2,$$

where $x = ru - csv$ and $y = asu + arv + bsv$.

Now if f represents a^2 with $(a, d) = 1$, then there exist integers b, c such that the quadratic form $F := a^2x^2 + bxy + cy^2$ is equivalent to f. Note that $(a, b)^2$ divides $d = b^2 - 4a^2c$, which is a fundamental discriminant and so squarefree except perhaps a power of 2. However a is odd and so $(a, b) = 1$. Therefore we let $g = ax^2 + bxy + acy^2$ so that, as in the previous paragraph $g \cdot g \sim F \sim f$. □

12.9. Bhargava composition[5]

Let us begin with one further explicit composition, a tiny variant on (12.7.3) (letting $s \to -s$ there):

$$(au^2 + 2Buv + cv^2)(ar^2 - 2Brs + cs^2) = x^2 + (ac - B^2)y^2$$
$$\text{where } x = aur + B(vr - us) - cvs \text{ and } y = us + vr.$$

Combining this with the results of the previous section suggests that if the discriminant d is divisible by 4 (which is equivalent to b being even), then

$$F(u, v)G(r, s)H(m, -n) = P(x, y) \tag{12.9.1}$$

[5]Although there is no Nobel Prize in mathematics, there is the *Fields Medal*, awarded every four years, only to people 40 years of age or younger. In 2014, in Korea, one of the laureates was Manjul Bhargava for a body of work that begins with his version of composition, as discussed here, and allows us to much better understand many classes of equations, especially cubic.

where $P(x,y) = x^2 - \frac{d}{4}y^2$ is the principal form and x and y are cubic polynomials in m, n, r, s, u, v. Analogous remarks can be made if the discriminant is odd.

In 2004 Bhargava came up with an entirely new way to find all of the triples F, G, H of binary quadratic forms of the same discriminant for which (12.9.1) holds: We begin with a 2-by-2-by-2 cube, the corners of which are labeled with the integers a, b, c, d, e, f, g, h.

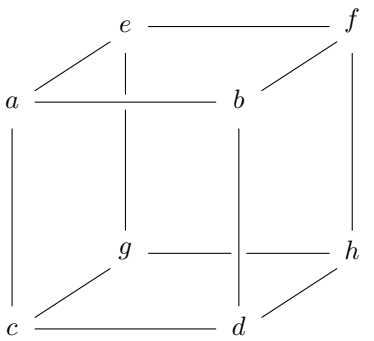


Figure 12.2. Bhargava's Rubik-type cube.

There are six faces of a cube, and these can be split into three parallel pairs. To each such parallel pair consider the pair of 2-by-2 matrices given by taking the entries in each face, those entries corresponding to opposite corners of the cube, always starting with a. Hence we get the pairs

$$M_1(x,y) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} x + \begin{pmatrix} e & f \\ g & h \end{pmatrix} y = \begin{pmatrix} ax+ey & bx+fy \\ cx+gy & dx+hy \end{pmatrix},$$
$$M_2(x,y) := \begin{pmatrix} a & c \\ e & g \end{pmatrix} x + \begin{pmatrix} b & d \\ f & h \end{pmatrix} y = \begin{pmatrix} ax+by & cx+dy \\ ex+fy & gx+hy \end{pmatrix},$$
$$M_3(x,y) := \begin{pmatrix} a & b \\ e & f \end{pmatrix} x + \begin{pmatrix} c & d \\ g & h \end{pmatrix} y = \begin{pmatrix} ax+cy & bx+dy \\ ex+gy & fx+hy \end{pmatrix},$$

where we have, in each, appended the variables, x, y, to create matrix functions of x and y. The determinant, $-Q_j(x,y)$, of each $M_j(x,y)$ is a quadratic form in x and y. Incredibly Q_1, Q_2, and Q_3 all have the same discriminant and their composition equals P, the principal form, just as in (12.9.1). We present two proofs. First, by substitution, one can exhibit that

$$Q_1(x,-y) = Q_2(x_2,y_2)Q_3(x_3,y_3)$$

where

$$y = \begin{pmatrix} x_3 & y_3 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \quad \text{and} \quad x = \begin{pmatrix} x_3 & y_3 \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Let's work though an example: Plot the cube in three dimensions, take the Cartesian coordinates of every corner (each 0 or 1), and then label the corner

(x, y, z), with $2^2x + 2y + z$, squared. Hence

$$a, b, c, d, e, f, g, h = 2^2, 6^2, 0^2, 4^2, 3^2, 7^2, 1^2, 5^2,$$

yielding the cube in Figure 12.3.

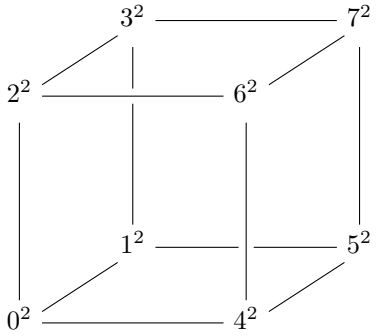


Figure 12.3. The construction of three binary quadratic forms using Bhargava's cube.

This cube leads to three binary quadratic forms of discriminant $-7 \cdot 4^4$: $Q_1 = -4^2(4x^2+13xy+11y^2)$, $Q_2 = -2^2(x^2-2xy+29y^2)$, and $Q_3 = 4^2(8x^2+5xy+y^2)$. After some work one can verify that

$$Q_1(m, n)Q_2(r, s)Q_3(u, v) = 4(x^2 + 4^3 \cdot 7y^2),$$

where x and y are the following cubic polynomials in m, n, r, s, u, v:

$$x = 8(-11mru - 3mrv + 25msu + 17msv - 17nru - 4nrv + 59nsu + 32nsv)$$

and $y = mru + mrv + 21msu + 5msv + 3nru + 2nrv + 31nsu + 6nsv$.

Bhargava proves his theorem, inspired by a 2-by-2-by-2 Rubik's cube. His idea is to apply one invertible linear transformation at a time, simultaneously to a pair of opposite sides, and to slowly "reduce" the numbers involved, while retaining the equivalence classes of Q_1, Q_2, and Q_3, until one reduces to a cube and a triple of binary quadratic forms with coefficients having a convenient structure.

Lemma 12.9.1. *If one applies an invertible linear transformation to a pair of opposite sides, then the associated binary quadratic form is transformed in the usual way, whereas the other two quadratic forms remain the same.*

Therefore we can act on our cube by such $\mathrm{SL}(2, \mathbb{Z})$-transformations, in each direction, and the three binary quadratic forms each remain in the same equivalence class.

Proof. If $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$, then we replace the face

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ by } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \beta; \text{ and } \begin{pmatrix} e & f \\ g & h \end{pmatrix} \text{ by } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \delta.$$

Then $M_1(x,y)$ gets mapped to

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\alpha + \begin{pmatrix} e & f \\ g & h \end{pmatrix}\beta\right\}x + \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\gamma + \begin{pmatrix} e & f \\ g & h \end{pmatrix}\delta\right\}y,$$

that is, $M_1(\alpha x+\gamma y, \beta x+\delta y)$. Therefore the quadratic form $Q_1(x,y)$ gets mapped to $Q_1(\alpha x+\gamma y, \beta x+\delta y)$ which is equivalent to $Q_1(x,y)$. Now $M_2(x,y)$ gets mapped to

$$\begin{pmatrix} a\alpha+e\beta & c\alpha+g\beta \\ a\gamma+e\delta & c\gamma+g\delta \end{pmatrix}x + \begin{pmatrix} b\alpha+f\beta & d\alpha+h\beta \\ b\gamma+f\delta & d\gamma+h\delta \end{pmatrix}y = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}M_2(x,y);$$

hence the determinant, $-Q_2(x,y)$, is unchanged. An analogous calculation reveals that $M_3(x,y)$ gets mapped to $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}M_3(x,y)$ and the determinant, $-Q_3(x,y)$, is also unchanged. □

The previous lemma allows one to proceed in "reducing" the three binary quadratic forms to equivalent forms that are easy to work with (rather as in Dirichlet's proof).

Proof of the Bhargava composition. We will simplify the entries in the cube by the following reduction algorithm:

• We select the corner that is to be a so that $a \neq 0$.

• We will transform the cube to ensure that a divides b, c, and e. If not, say a does not divide e, then select integers α, β so that $a\alpha + e\beta = (a,e)$, and then let $\gamma = -e/(a,e),\ \delta = a/(a,e)$. In the transformed matrix we have $a' = (a,e),\ e' = 0$, and $1 \leq a' \leq a-1$. It may well now be that a' does not divide b' or c', so we repeat the process. Each time we do this we reduce the value of a by at least 1; and since it remains positive this can only happen a finite number of times. At the end of the process a divides b, c, and e.

• We will transform the cube to ensure that $b = c = e = 0$. We already have that $a|b,c,e$. Now select $\alpha = 1,\ \beta = 0, \gamma = -e/a,\ \delta = 1$, so that $e' = 0, b' = b, c' = c$. We repeat this in each of the three directions to ensure that $b = c = e = 0$.

Replacing a by $-a$, we have that the three matrices are

$$M_1(x,y) := \begin{pmatrix} -a & 0 \\ 0 & d \end{pmatrix}x + \begin{pmatrix} 0 & f \\ g & h \end{pmatrix}y, \quad \text{so that } Q_1(x,y) = adx^2 + ahxy + fgy^2,$$

$$M_2(x,y) := \begin{pmatrix} -a & 0 \\ 0 & g \end{pmatrix}x + \begin{pmatrix} 0 & d \\ f & h \end{pmatrix}y, \quad \text{so that } Q_2(x,y) = agx^2 + ahxy + dfy^2,$$

$$M_3(x,y) := \begin{pmatrix} -a & 0 \\ 0 & f \end{pmatrix}x + \begin{pmatrix} 0 & d \\ g & h \end{pmatrix}y, \quad \text{so that } Q_3(x,y) = afx^2 + ahxy + dgy^2.$$

All three Q_j have discriminant $(ah)^2 - 4adfg$, and we observe that

$$Q_1(fy_2x_3 + gx_2y_3 + hy_2y_3, ax_2x_3 - dy_2y_3) = Q_2(x_2,y_2)Q_3(x_3,y_3)$$

where $x_1 = fy_2x_3 + gx_2y_3 + hy_2y_3$ and $y_1 = ax_2x_3 - dy_2y_3$. □

This brings to mind the twists of the Rubik's cube, though in that case one has only finitely many possible transformations, whereas here there are infinitely many possibilities, as there are infinitely many invertible linear transformations over $\mathbb{Z}$.

Appendices. The extended version of chapter 12 has the following additional appendices:

Appendix 12B. *The class group* is a group whose elements are the equivalence classes of quadratic forms with multiplication defined by composition as in appendix 12A. We will focus on classifying the all-important elements of order two.

Appendix 12C. *Binary quadratic forms of positive discriminant.* We have already explored at length the theory of binary quadratic forms of negative discriminant. Positive quadratic forms are quite a bit trickier, largely because there are infinitely many automorphisms of the solutions of a quadratic equation of this discriminant, corresponding to the solutions to Pell's equation, whereas for negative discriminants there is usually just the one non-trivial automorphism $(x, y) \to (-x, -y)$. Here we present some of that theory.

Appendix 12D. *Sums of three squares.* We discover here the connection between sums of three squares and class numbers and then develop Dirichlet's class number formula.

Appendix 12E. *Sums of four squares.* We give two proofs that every positive integer is the sum of four squares, including one via the theory of quaternions, and then discuss how many representations each integer has as the sum of four squares.

Appendix 12F. *Universality.* A quadratic form is universal if it takes all positive integer values. Although these were classified long ago by Ramanujan it was only recently that researchers found a much neater classification: simply verifying that the quadratic form represents every integer up to 290.

Appendix 12G. *Integers represented in Apollonian circle packings.* In appendix 9C we developed some of the mathematics of the curvatures inside a circle tiled by smaller circles. Now we show how some subset of the integers represented can be found by reducing the question to values of binary quadratic forms.

Hints for exercises

Exercises in chapter 0

Exercise 0.1.1(b). The key observation is that if $\alpha = \frac{1+\sqrt{5}}{2}$ or $\frac{1-\sqrt{5}}{2}$, then $\alpha^2 = \alpha + 1$ and so, multiplying through by α^{n-2}, we have $\alpha^n = \alpha^{n-1} + \alpha^{n-2}$ for all $n \geq 2$.

Exercise 0.1.3(b). Multiplying through by ϕ we have $\phi^{n+1} = F_n\phi^2 + F_{n-1}\phi$. Now use (a).

Exercise 0.1.5(b). Determine a and b in terms of α and then c and d in terms of α, x_0, and x_1.

Exercise 0.2.1(a). Note that $N^2 + (2N+1) = (N+1)^2$.

Exercise 0.3.1. In both parts use induction on n.

Exercise 0.4.2. Use (0.1.1) to establish that $|F_n - \phi^n/\sqrt{5}| < \frac{1}{2}$ for all $n \geq 0$.

Exercise 0.4.7. If the first character in a string in A_n is a 0, what must the subsequent string look like? What if the string begins with a 1?

Exercise 0.4.8. Use Gauss's trick to show that $\sum_{a<n\leq b} n = \binom{b+1}{2} - \binom{a+1}{2} = \frac{(b-a)(b+a+1)}{2}$, a product of two integers of opposite parity, both > 1. Show that if N is not a power of 2 (so that it has an odd divisor $m > 1$), then it is a product of two integers of opposite parity, both > 1. Determine a and b in terms of N and m.

Exercise 0.4.10(a). Verify this for $k = 1$ and 2, and then for larger k by induction.

(b) Select k and m as functions of n.

Exercise 0.4.16. By (0.1.1), $\sqrt{5}F_n = \phi^n - \overline{\phi}^n$, and so $(\sqrt{5}F_n)^k = \sum_{j=0}^k \binom{k}{j}(-1)^j\rho_j^n$ where $\rho_j := \overline{\phi}^j\phi^{k-j}$. Let $x^{k+1} - \sum_{i=0}^k c_i x^i = \prod_{j=0}^k (x - \rho_j)$. Therefore

$$\sum_{i=0}^k c_i(\sqrt{5}F_{n+i})^k = \sum_{j=0}^k \binom{k}{j}(-1)^j\rho_j^n \cdot \sum_{i=0}^k c_i\rho_j^i = \sum_{j=0}^k \binom{k}{j}(-1)^j\rho_j^n \cdot \rho_j^{k+1} = (\sqrt{5}F_{n+k})^k.$$

The result follows after dividing through by $(\sqrt{5})^k$.

Exercises in chapter 1

Exercise 1.1.1(a). Write $a = db$ for some integer d. Show that if $d \neq 0$, then $|d| \geq 1$. (b) Prove that if u and v are integers for which $uv = 1$, then either $u = v = 1$ or $u = v = -1$. (c) Write $b = ma$ and $c = na$ and show that $bx + cy = max + nay$ is divisible by a.

Exercise 1.1.2. Use Lemma 1.1.1 and induction on a for fixed b.

Exercise 1.2.1(a). By exercise 1.1.1(c) we know that d divides $au + bv$ for any integers u and v. Now use Theorem 1.1. (d) First note that a divides b if and only if $-a$ divides b. If $|a| = \gcd(a, b)$, then $|a|$ divides both a and b, and so a divides b. On the other hand if a divides b, then $|a| \leq \gcd(a, b) \leq |a|$ by (c).

Exercise 1.2.4(b). Let $g = \gcd(a, b)$ and write $a = gA, b = gB$ for some integers A and B. What is the value of $Au + Bv$? Now apply (a).

Exercise 1.2.5(a). Use Theorem 1.1.

Exercise 1.4.2. Use Lemma 1.4.1.

Exercise 1.7.5(e). Write $r = m + \delta$ where $0 < \delta < 1$, so that $[r] = m$ and $a - r = a - m - \delta$ so that $[a - r] =?$.

Exercise 1.7.10. Given any solution, determine u using Lemma 1.1.1.

Exercise 1.7.11. One might apply Corollary 1.2.2.

Exercise 1.7.14(d). Use exercise 1.7.10.

Exercise 1.7.22. For each given $m \geq 1$, prove that $x_m | x_{mr}$ for all $r \geq 1$, by induction on r, using exercise 0.4.10(a) with $k = rm$.

Exercise 1.7.23(a). Prove that $\gcd(x_n, b) = \gcd(ax_{n-1}, b)$ for all $n \geq 2$, and then use induction on $n \geq 1$, together with Corollary 1.2.2. (b) Prove that $\gcd(x_n, x_{n-1}) = \gcd(bx_{n-2}, x_{n-1})$ for all $n \geq 2$, and then use induction on $n \geq 1$, together with Corollary 1.2.2. (c) Use exercise 0.4.10(a) with $k = n - m$ and then (b). (d) Follow the steps of the Euclidean algorithm using (c).

Exercise 1.9.1. Use the matrix transformation for $(u_j, u_{j+1}) \to (u_{j+1}, u_{j+2})$.

Exercises in chapter 2

Exercise 2.1.4(b). Write the integers in the congruence class $a \pmod d$ as $a + nd$ as n varies over the integers, and partition the integers n into the congruences classes mod k.

Exercise 2.1.5. Write the congruence in terms of integers and then use exercise 1.1.1(c).

Exercise 2.1.6. Write the congruence in terms of integers and then use exercise 1.1.1(e).

Exercise 2.4.1(c). Factor 1001.

Exercise 2.5.4(a). Split the integers into k blocks of m consecutive integers, and use the main idea from the first proof of Theorem 2.1. (b) Write $N = km + r$ with $0 \leq r \leq m - 1$. Use (a) to get k such integers in the first km consecutive integers, and at most one in the remaining r. Compare k or $k + 1$ to the result required.

Exercise 2.5.6(b). Use the results for $m = 4$ from (a). (d) Use the same idea as in (c). (e) Study squares mod 8.

Exercise 2.5.9(b). Use that $\frac{1}{j}\binom{p-1}{j-1} = \frac{1}{p}\binom{p}{j}$.

Exercise 2.5.10(a). Treat the cases $a \geq b$ and $a < b$ separately. (b) Treat the cases $c \geq d$ and $c < d$ separately.

Exercise 2.5.13. Proceed by induction on $k \geq 1$.

Exercise 2.5.15(b). Use induction.

Exercise 2.5.16(a). Try a proof by contradiction. Start by assuming that the kth pigeonhole contains a_k letters for each k, and determine a bound on the total number of letters if each $a_k \leq 1$. (b) Use the pigeonhole principle. (c) Use induction.

Exercise 2.5.17(a). Use the pigeonhole principle on pairs $(x_r \pmod d), x_{r+1} \pmod d)$. (d) Use exercise 1.7.24.

Exercises in chapter 3

Exercise 3.0.1. The only divisors of p are 1 and p. Therefore $\gcd(p,a) = 1$ or p, and so $\gcd(p,a) = p$ if and only if p divides a. This implies that $\gcd(p,a) = 1$ if and only if p does not divide a.

Exercise 3.1.1. Use induction and the fact that every integer > 1 has a prime divisor, as proved in the "prerequisites" section. (The proof will appear as part of the proof of Theorem 3.2.)

Exercise 3.1.2(a). Apply Theorem 3.1 with $a = a_1 \cdots a_{k-1}$ and $b = a_k$, and if p divides a, then proceed by induction.

(b) p divides some q_j by (a), and as q_j only has divisors 1 and q_j, and as $p > 1$, we deduce that $p = q_j$.

Exercise 3.1.3(b). Write $n = 2^k m$ with m odd. Then n has an odd prime factor if and only if $m > 1$. Therefore if n has no odd prime factor, then $n = 2^k$.

Exercise 3.2.1. We have $[a,b] = ab$ by Corollary 3.2.2. The result follows from Lemma 1.4.1.

Exercise 3.3.1. Look at this first in the case that m and n are both powers of p, say, $m = p^a$ and $n = p^b$. If d divides m and n, then $d = p^c$, say, with $c \leq a$ and $c \leq b$. The maximum c that satisfies both of these inequalities is $\min\{a,b\}$. Similarly if m and n divide $L = p^e$, then $a \leq e$ and $b \leq e$ and so the minimum e that satisfies both of these inequalities is $\max\{a,b\}$. Now use this idea when m and n are arbitrary integers.

Exercise 3.3.5. Use exercise 3.3.3(d).

Exercise 3.3.7(c). Use exercise 3.3.3(c).

Exercise 3.5.1(a). Show that the $aj + b$ are distinct mod m.

Exercise 3.5.2. Prove that the $r_j \pmod m$ are all reduced residues, and then that they are distinct.

Exercise 3.5.3. If $ar \equiv c \pmod b$, then b divides $ar - c$. Therefore $\gcd(a,b)$ divides $ar - c$ and so c. In the other direction, we write $g = \gcd(a,b)$ and so $a = gA, b = gB, c = gC$, and we are looking for solutions to $Ar \equiv C \pmod B$. Then use exercise 3.5.1(b).

Exercise 3.5.5. Use the second proof of Corollary 3.5.2.

Exercise 3.6.4. If $am + bn = c$, then $am + bn \equiv c \pmod b$ (or indeed mod any integer $r \geq 1$). On the other hand if $au + bv \equiv c \pmod b$ and m is any integer $\equiv u \pmod b$, then $am \equiv au + bv \equiv c \pmod b$ and so there exists an integer n for which $am + bn = c$.

Exercise 3.7.2(a) We proceed by induction on the number of moduli using exercise 3.2.1.

(b) Replace m in (a) by $m - n$.

Exercise 3.7.8(a). Work with the prime power divisors of m and use the Chinese Remainder Theorem.

Exercise 3.8.3. Calculate the product mod p^e, for every prime power $p^e \| m$.

Exercise 3.9.1. Use exercise 1.7.20(a).

Exercise 3.9.3(a). If $2k+1 = n/m$, take $u = \alpha^m$ and $v = \beta^m$ in

$$\frac{u^{2k+1} + v^{2k+1}}{u+v} = (-uv)^k + \sum_{j=1}^{k} (-uv)^{k-j}(u^{2j} + v^{2j}),$$

so that y_n/y_m is a linear polynomial in the y_{2jm} with coefficients that are $\pm$ powers of b.

Exercise 3.9.6. Use exercise 3.3.7(c), and factor $gA^2 - gB^2$.

Exercise 3.9.7(a). Write $\frac{z^p - y^p}{z-y}$ as a polynomial in y and z.

Exercise 3.9.10(a). $\sqrt{2} + \sqrt{3}$ is a root of $x^4 - 10x^2 + 1$. Use Theorem 3.4.

(b) $\sqrt{a} + \sqrt{b}$ is a root of $x^4 - 2(a+b)x^2 + (a-b)^2$. Therefore the rational root $m = \sqrt{a} + \sqrt{b}$ must be an integer, and then m divides $a - b$. Writing $a = b + mk$ we have $k = \sqrt{a} - \sqrt{b}$ so that $b = (\frac{m-k}{2})^2$ and $a = (\frac{m+k}{2})^2$.

Exercise 3.9.11(b). Prove that $(\sqrt{d} + m)(\sqrt{d} - m)$ is an integer

Exercise 3.9.15(b). Use Corollary 2.3.1.

Exercise 3.9.17(b). Write $m = gM$ and $n = gN$ where $g = \gcd(m, n)$ so that $(M, N) = 1$, and then use exercise 3.7.7 (or exercise 3.9.16(b), for a less complete solution).

Exercise 3.10.2. Write the trinomial coefficient as the product of binomial coefficients.

Exercise 3.11.1. Prove this by induction on $n \geq 1$, using the observation in the paragraph immediately above.

Exercises in chapter 4

Exercise 4.0.1. One can proceed by induction on the number of distinct prime factors of n, using the definition of multiplicative.

Exercise 4.1.3. Pair m with $n - m$, and then m with n/m.

Exercise 4.1.5. If the prime factors of n are $p_1 < p_2 < \cdots < p_k$, then $p_j \geq k + j$ and so $\frac{\phi(n)}{n} = \prod_{j=1}^{k} \frac{p_j - 1}{p_j} \geq \prod_{j=1}^{k} \frac{k+j-1}{k+j} = \frac{k}{2k} = \frac{1}{2}$.

Exercise 4.2.2. Let $\ell = (d, a)$ so that $\ell | a$ and therefore $d/\ell | (a/\ell)b$ with $(d/\ell, a/\ell) = 1$ and therefore $m = d/\ell | b$.

Exercise 4.2.3(b). What is the power of 2 in $\sigma(n)$?

Exercise 4.2.4. Give a general lower bound on $\sigma(n)$.

Exercise 4.2.5(a). If $p^e \| n$, then $1 + \frac{1}{p} \leq \sigma(p^e)/p^e < 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots = \frac{p}{p-1}$.

(b) If n is a perfect number, then $\sigma(n)/n = 2$, and if it is odd with ≤ 2 prime factors, then $\prod_{p|n} \frac{p}{p-1} \leq \frac{3}{2} \cdot \frac{5}{4}$ which is < 2, contradicting (a).

Exercise 4.3.7(a). Use exercise 3.9.15(a).

Exercise 4.3.11(a). Prove this when a and b are both powers of a fixed prime and then use multiplicativity.

Exercise 4.3.12. In both parts write, for each $d | n$, the integers $m = an/d$ with $(a, d) = 1$. Use exercise 4.1.3.

Exercise 4.3.13(a). You could use the second part of exercise 4.1.3.

Exercise 4.3.15(b). Use multiplicativity. (e) Use exercise 4.2.5.

Exercise 4.5.1(a). Use the binomial theorem. (b) Let $m = \prod_{p|n} p$ and $x = -1$ in (a).

Exercise 4.5.2. Expand the right-hand side.

Exercise 4.6.2. Let $r = (a, m)$ and then $s = a/r$ and $t = m/r$ which therefore must be coprime. Now $a = rs$ divides $mn = rtn$, so that s divides tn and therefore s divides n as $(s, t) = 1$. Let $u = n/s$ and we finally deduce $b = mn/a = tu$.

Exercise 4.8.2. Use the expansion $\phi(n) = \sum_{d|n} \mu(n/d)d$ from the proof of Theorem 4.1 in section 4.4, and a similar expression for σ.

Exercises in chapter 5

Exercise 5.1.4. Show that if $2^{2^{n-1}} < x \le 2^{2^n}$, then there are $\ge n$ primes up to x. Then give a lower bound for n as a function of x.

Exercise 5.3.2. Show that if every prime factor of n is $\equiv 0$ or $1 \pmod 3$, then $n \equiv 0$ or $1 \pmod 3$.

Exercise 5.3.4. Consider splitting arithmetic progressions mod 3 into several arithmetic progressions mod 6.

Exercise 5.3.5. One might use exercise 3.1.4(b) in this proof.

Exercise 5.4.1(b). We wish to show that $\pi(x+\epsilon x) > \pi(x)$. By (5.4.2) (and footnote 14) we know that for any fixed $\delta > 0$ we have $(1-\delta)\frac{x}{\log x} < \pi(x) < (1+\delta)\frac{x}{\log x}$ if x is sufficiently large. The result will then follow if the middle inequality holds in

$$\pi(x) < (1+\delta)\frac{x}{\log x} < (1-\delta)\frac{x+\epsilon x}{\log(x+\epsilon x)} < \pi(x+\epsilon x).$$

Now $\frac{\log(x+\epsilon x)}{\log x} < 1 + \frac{\epsilon}{\log x}$ as $\log(1+\epsilon) < \epsilon$, and so the middle inequality follows if $1 + \frac{\epsilon}{\log x} < (1-\delta)(1+\epsilon)/(1+\delta)$. Selecting, say, $\delta = \epsilon/3$ this holds if x is sufficiently large.

Exercise 5.8.11. Use l'Hôpital's rule.

Exercise 5.8.12. First prove that $\left(\mathrm{Li}(x) - \frac{x}{\log x}\right) \Big/ \frac{x}{(\log x)^2} \to 1$ as $x \to \infty$.

Exercise 5.8.14(a). Use Corollary 2.3.1.

Exercise 5.9.1. Either use Kummer's Theorem (Theorem 3.7) or consider directly how often p divides the numerator and denominator of $\binom{2n}{n}$.

Exercise 5.9.3. Use induction to show that, for each $n \ge 6$, every integer in $[7, 2N+6]$ is the sum of distinct primes in $\{2, 3, \dots, 2N\}$, by induction on $N \ge 1$.

Exercise 5.9.6. Let p be a prime in $[2n, 4n]$. Now construct all the pairs you can that sum to p. Proceed.

Exercise 5.10.1. Maximize the log of the ratio using calculus.

Exercise 5.10.2. Use Proposition 5.10.1.

Exercise 5.10.3(a). If $r \le s/2$, then by Bertrand's postulate there is a prime $p \in (s/2, s] \subset (r, s]$. Otherwise $k = s - r \le r$. In either case, by Bertrand's postulate or the Sylvester-Schur Theorem, one term has a prime factor $p > k$, and so this is the only term that can be divisible by p.

Exercise 5.11.8(b). Use the Fundamental Theorem of Algebra mod p (see Lagrange's Theorem, Proposition 7.4.1).

Exercise 5.11.9(a). Can be proved by induction on k. For $k = 0$ this is trivial. For larger k, let $T \subset \{1, 2, \dots, m-1\}$ and we pair together the terms for $S = T$ and $S = T \cup \{m\}$ in our sum. The sum therefore becomes

$$\sum_{T \subset \{1,2,\dots,m-1\}} (-1)^{|T|} \left(\left(x_m + x_0 + \sum_{j \in T} x_j \right)^k - \left(x_0 + \sum_{j \in T} x_j \right)^k \right)$$
$$= \sum_{i=0}^{k-1} \binom{k}{i} x_m^{k-i} \sum_{T \subset \{1,2,\dots,m-1\}} (-1)^{|T|} (x_0 + \sum_{j \in T} x_j)^i$$

and the result follows by induction, as $m - 1 > k - 1 \ge i$.

(b) Let $x_0 = \log n$ and if n has prime factors $p_1, \dots, p_m$, then let $x_j = -\log p_j$ for each $j \geq 1$.

(c) We get $k! x_1 \dots x_k$ in (a) and so $(-1)^k k! \prod_{p|n} \log p$ in (b). We prove this by induction using the proof in (a), since in the induction step only the $i = k-1$ term remains, which is the result from the previous step multiplied by kx_k.

Exercises in chapter 6

Exercise 6.1.2. Study where lines of rational slope, going through the point $(2, 1)$, hit the curve again.

Exercise 6.1.5. Write down an equation that identifies when three given squares are in arithmetic progression.

Exercise 6.3.1(a). By (6.1.1) the area is $g^2 rs(r^2 - s^2)$ where $r > s \geq 1$ and $(r, s) = 1$. If this is a square, then each of r, s, and $r^2 - s^2$ must be squares; call them x^2, y^2, and z^2, respectively, so that $x^4 - y^4 = z^2$, which contradicts Theorem 6.2.

(c) Consider a right-angled triangle with sides $x^2, 2y^2, z$.

Exercise 6.5.3. Here b is the hypotenuse, and c is the area. Further hint: We need $b^2 - 4c$ and $b^2 + 4c$ to be integer squares, say, u^2 and v^2, so that $4c = b^2 - u^2 = v^2 - b^2$. Therefore $2b^2 = u^2 + v^2$, so u, v have the same parity and therefore $(\frac{u+v}{2})^2 + (\frac{u-v}{2})^2 = b^2$. This is our Pythagorean triangle, which has area $\frac{1}{2} \cdot \frac{u+v}{2} \cdot \frac{v-u}{2} = \frac{v^2 - b^2 + b^2 - u^2}{8} = c$.

Exercise 6.5.6. Let $\alpha = p/q$ with $(p, q) = 1$ so that $\alpha = (a\alpha + b)/\alpha = (ap + bq)/p$. Now $(p, q) = 1$ so comparing denominators we must have $q = 1$, and p divides $ap + bq$, so that p divides bq, and therefore b.

Exercise 6.5.7. By (6.1.1) the perimeter of such a triangle has length $2grs + g(r^2 - s^2) + g(r^2 + s^2) = 2gr(r + s)$ where $r > s > 0$. Therefore n has divisors r and $r + s$, where $r < r + s < 2r$. On the other hand if n has divisors d_1, d_2 for which $d_1 < d_2 < 2d_1$, then we may assume they are coprime, by dividing through by any common factor. Therefore $d_1 d_2$ divides n and so we can let $r = d_1$, $s = d_2 - d_1$, and $g = n/d_1 d_2$.

Exercise 6.5.9. Prove that if $n \geq 13$, then $(n+1)^2 + 128 < 2n^2$. Then proceed by induction on n for $m \in [n^2 + 129, 2n^2)$.

Exercise 6.5.10. What values can cubes take mod 9?

Exercises in chapter 7

Exercise 7.1.2(b). Use the technique in the proof of Lemma 7.1.1

Exercise 7.2.2. Let $k := \mathrm{ord}_m(a)$ and $A = \{1, a, a^2, \dots, a^{k-1} \pmod m\}$. Show that if b and b' are any two reduced residues mod m, then either bA and $b'A$ are disjoint or are equal. Therefore the sets of the form bA, where b is a reduced residue mod m, which are each of size k, partition the $\phi(m)$ reduced residues mod m. This implies that k divides $\phi(m)$ as desired.

Exercise 7.3.1. Let $k := \mathrm{ord}_q(2)$. We have $2^p \equiv 1 \pmod q$ and so k divides p by Lemma 7.1.2. Therefore $k = 1$ or p, but $k \neq 1$ as $2^1 \not\equiv 1 \pmod q$.

Exercise 7.4.1(a) If n is not of the form p or p^2, write $n = ab$ with $1 < a < b$. If $n = p^2$, then n divides $p \cdot 2p$.

Exercise 7.4.3(a). If $Q = \frac{p-1}{2}$, then

$$(p-1)!/Q! = (p-1)(p-2)\cdots(p-Q) \equiv (-1)(-2)\cdots(-Q) = (-1)^Q Q! \pmod p.$$

Exercise 7.5.2(b). As $(g^{\frac{p-1}{2}})^2 = g^{p-1} \equiv 1 \pmod p$, so $g^{\frac{p-1}{2}}$ is a square root of $1 \pmod p$; that is, $g^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod p$. But g has order $p-1$ and so $g^{\frac{p-1}{2}} \not\equiv 1 \pmod p$.

Exercise 7.10.2. Use Proposition 7.4.1.

Exercise 7.10.4. In every solution $n, n-1, n-2$ have prime factors $2, 3, p$ for some $p > 3$. At most one of these integers is divisible by p. Show that the other two lead to a solution to $2^n - 3^m = \pm 1$ and use exercise 7.10.3.

Exercise 7.10.5(b). Use Theorem 7.1.

(d) Make sure a is chosen so that $(q, a-1) = 1$.

Exercise 7.10.6(a). The trick is to write $z^p = ((z-y)+y)^p$ and then use the binomial theorem. One can also write $x_n = \frac{z^n - y^n}{z-y}$ and use exercise 2.5.20(a).

Exercise 7.10.12. Take the j and $p-j$ terms together.

Exercise 7.10.13. Let $M = a_0 + 1$ so that $a_n = 2^n M - 1$ for all $n \geq 0$. Let p be an odd prime dividing a_1. Then p divides a_p.

Exercise 7.10.16(b). Since n is not a Carmichael number, the subgroup in (a) is proper and so contains at most half the reduced residues. (c) Let $q = 2p - 1$. Now $n - 1 \equiv p - 1 \pmod{2p-2}$, so that if $(a, n) = 1$, then $a^{n-1} \equiv a^{p-1} \equiv 1 \pmod{p}$ and $a^{n-1} \equiv a^{p-1} \equiv a^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}$.

Exercise 7.10.17(a). $M_p - 1 = 2^p - 2$ is divisible by p.

Exercise 7.12.1(b). Let $f(x_1, \dots, x_p) = (x_2, \dots, x_p, x_1)$ in part (a).

Exercises in chapter 8

Exercise 8.1.2(b). Use Lemma 8.1.1.

Exercise 8.1.3(a). Use that $\left(\frac{b^2}{p}\right) = \left(\frac{b}{p}\right)^2 = (\pm 1)^2 = 1$.

Exercise 8.1.6(a). The residues $1, g^2, g^4, \dots, g^{p-3} \pmod{p}$ are evidently distinct and non-zero squares. As there are $\frac{p-1}{2}$ of them, they are all of the quadratic residues by Lemma 8.1.1.

(b) We see above that $g = g^1$ is not one of the quadratic residues.

Exercise 8.2.1. There are two solutions to $r^2 \equiv a \pmod{p}$, say, r and $-r \pmod{p}$, whose product is $r \cdot (-r) \equiv -a \pmod{p}$. Note also that $|S| = \frac{p-3}{2}$.

Exercise 8.4.1. r is the largest integer with $2r - 1 \leq \frac{q-1}{2}$; that is, $r \leq \frac{q+1}{4}$.

Exercise 8.4.5. Look at $(2/p)$.

Exercise 8.7.2(a). Use the Chinese Remainder Theorem and exercise 8.1.2(b).

Exercise 8.7.5. If a is odd, then $a = 1 + 2 \cdot \frac{a-1}{2}$, and so

$$1+2\cdot\frac{ab-1}{2} = ab = \left(1+2\cdot\frac{a-1}{2}\right)\left(1+2\cdot\frac{b-1}{2}\right) \equiv 1+2\cdot\left(\frac{a-1}{2}+\frac{b-1}{2}\right) \pmod{4}.$$

Exercise 8.7.6. Select $a^2 \equiv -2 \pmod{p}$ with a odd and minimal, so that $1 \leq a \leq p-1$. Write $a^2 + 2 = pr$. Evidently $pr \equiv a^2 + 2 \equiv 3 \pmod{8}$ and so $r \equiv 3p \equiv 5$ or $7 \pmod{8}$. But then $a^2 \equiv -2 \pmod{r}$ and so $\left(\frac{-2}{r}\right) = 1$ with $r = \frac{a^2+2}{p} < p$. This contradicts the induction hypothesis, and so $\left(\frac{-2}{p}\right) = -1$.

Exercise 8.8.1. Suppose that $k > \ell \geq 1$. If r is a quadratic residue mod p^k, then r is a quadratic residue mod p^ℓ, trivially. On the other hand if r is a quadratic residue mod p^ℓ, then it is a quadratic residue mod $p^{\ell+1}$ by Proposition 8.8.1, then mod $p^{\ell+2}$ by Proposition 8.8.1, etc., up to mod p^k. We take $\ell = 1$ if p is odd, and $\ell = 3$ if $p = 2$ and note that if r is a quadratic residue mod 8, then $r \equiv 1 \pmod{8}$.

Exercise 8.9.5(a). Write $n = 3^a m$ where $3 \nmid m$.

Exercise 8.9.9(a). Consider the size of the set of residues $\{a^2 \pmod p\}$ and of the set of residues $\{m - b^2 \pmod p\}$, as a and b vary.

(b) Take $m = -1$.

(c) Prove there is a solution u, v to $au^2 + bv^2 \equiv -c \pmod p$ and then multiply through by any $z \pmod p$.

Exercise 8.9.10(e). Apply Gauss's trick as in the proof of Corollary 7.5.2.

Exercise 8.9.12. For each solution to $y^2 \equiv b \pmod p$, consider whether there are solutions to $x^2 \equiv y \pmod p$.

Exercise 8.9.14. Let $b^2 \equiv -1 \pmod p$ and study $(1 + b)^2 \pmod p$.

Exercise 8.9.15. Show that if a has order $m \pmod p$, then $\sigma_{a,p}$ consists of $\frac{p-1}{m}$ cycles of length m.

Exercise 8.9.16(a). Use exercise 1.7.20(c). (b) Use exercise 1.7.20(b).

Exercise 8.9.17. Select integer m with $(m/n) = -1$. Consider the prime divisors of integers of the form $kn + m$ for well-chosen values of k.

Exercise 8.9.18(a). Modify the ideas in Euclid's proof that there are infinitely many primes. (b) $n = -3$. (c) Look at $4m^2 + 3$ with m odd. (d) $n = 3$. Note $(m^2 - 3)/2 \equiv 2 \pmod 3$. (e) $n = -4$. Note $m^2 + 4 \equiv 5 \pmod 8$. (f) $n = 2$. Note $m^2 - 2 \equiv 7 \pmod 8$. (g) $n = -2$. Note $m^2 + 2 \equiv 3 \pmod 8$. (h) $n = -4$ with $(m, 6) = 1$.

Exercise 8.9.24. Therefore $\left(\frac{2}{n}\right) = \left(\frac{2}{n-2}\right)$ if $n \equiv 1 \pmod 4$, and $\left(\frac{2}{n}\right) = -\left(\frac{2}{n-2}\right)$ if $n \equiv 3 \pmod 4$, and so the result follows by the induction hypothesis.

Exercise 8.10.2. If $N = pq + m$ where $0 \le m \le p - 1$, then $N - p[N/p] = N - pq = m$. If $r \ge 0$, then $m = r$; and if $r < 0$, then $m = p + r$.

Exercises in chapter 9

Exercise 9.1.2. If p does not divide a, then $(b/a)^2 \equiv -1 \pmod p$. Therefore $p = 2$ or $p \equiv 1 \pmod 4$. We get the same conclusion if p does not divide b and, otherwise, p divides (a, b).

Exercise 9.1.4. By induction on $k \ge 1$: It is trivial for $k = 1$ and otherwise let $n_k = a^2 + b^2$ and $n_1 \cdots n_{k-1} = c^2 + d^2$ (by the induction hypothesis), and then the result follows from (9.1.1).

Exercise 9.1.7(d). Use (a) to prove that $|ac - bd|, |ad - bc| < p$.

Exercise 9.3.1. Proceed as in the geometric proof of (6.1.1), or as in the proof of Proposition 9.1.2.

Exercise 9.7.2(b). Replace a and b by their absolutely least residues mod p.

Exercise 9.7.3(b). Select any b with $\left(\frac{b}{p}\right) = -1$ in (a), and let $m = r$ or s.

Exercise 9.7.7. We know that n is the length of the hypotenuse of a primitive Pythagorean triple iff there exist coprime integers r, s of different parity with $n = r^2 + s^2$. Hence all of n's prime factors are $\equiv 1 \pmod 4$, and we know we get at least two representations of n if it has at least two distinct prime factors.

Exercise 9.7.9. Since $m^2 \pm 2$ are odd they must be $\equiv 3 \pmod 4$, and so must be divisible by a prime $\equiv 3 \pmod 4$.

Exercise 9.7.10(a). In what domains do each of the ranges of ϕ lie? (b) We must be in the middle case (as $y, z \ne 0$) so that $x = y$ in which case $x(x + 4z) = p$. Since p can only be factored in one way into positive integers, we have $x = 1, z = \frac{p-1}{4}$; that is, $v = (1, 1, \frac{p-1}{4})$. (c) Pair up the elements of S using ϕ.

Exercise 9.9.2. Try $a = b = n = 1$.

Exercises in chapter 10

Exercise 10.3.2. Hopefully $n = pq$ and $\phi(n) = de - 1 = 29 \times 197 - 1 = 5712$; if so, then $p + q = n + 1 - \phi(n) = 180$. Therefore $(x - p)(x - q) = x^2 - 180x + 5891$ which we factor to obtain p and q.

Exercise 10.4.2(b). Use Corollary 7.5.3.

Exercise 10.7.5. Since n is a Carmichael number we know that it is squarefree and has prime divisors p and q, by Lemma 7.6.1. If $a^{(n-1)/2} \equiv -1 \pmod{n}$, then let $b \equiv 1 \pmod{p}$ and $b \equiv a \pmod{q}$, and determine the value of $b^{(n-1)/2} \pmod{pq}$.

Exercise 10.8.6(a). Factor $4x^4 + 1$ and substitute in $x = 2^n$.

Exercises in chapter 11

Exercise 11.2.1. If $y = 0$, then $m_1 n = n_1 m$. Now $(m, n) = (m_1, n_1) = 1$ and so $m_1 = m$ and $n_1 = n$ contradicting our construction of the pair m, n.

Exercise 11.2.5. Consecutive powerful numbers of the form 2^3a^2 followed by b^2, for some integers a and b.

Exercise 11.4.2. Use the product rule to compute the derivative.

Exercise 11.6.3. Given a smallest solution to $x^2 - dy^2 = 1$ expand $(x + \sqrt{d}y)^{\phi(d)} \pmod{d}$.

Exercise 11.6.11(c). Consider the example $1 + (2^n - 1) = 2^n$ with $m \geq 2/\epsilon$.

Exercises in chapter 12

Exercise 12.1.3. Suppose that d is a fundamental discriminant and $[a, b, c]$ is an imprimitive form of discriminant d. If $h|(a, b, c)$, then $h^2|d$, so that $h = 2$. But then $D = d/h^2 \equiv 0$ or $1 \pmod 4$, a contradiction. Now suppose that d is not a fundamental discriminant. Then there exists a prime p such that $d = p^2D$, where $D \equiv 0$ or $1 \pmod 4$. There is always a form g of discriminant D and so pg is an imprimitive form of discriminant d.

Exercise 12.1.4(c). Study the right-hand side of (12.1.2).

Exercise 12.1.5. Take determinants of both sides.

Exercise 12.1.6. First note that $b \equiv d \mod 2$, and that if $b = 2k+\delta$ with δ the least residue of $d \pmod 2$, then the change of variable $x \to x - ky$ shows that $[1, b, c] \sim [1, \delta, A]$, the principal form. The value of A must be $(\delta - d)/4$, so that the discriminant is $d = b^2 - 4c$.

Exercise 12.4.1. One example is $d = -171$. We begin by noting that $|b| \leq a \leq \sqrt{171/3} = \sqrt{57} < 8$ and b is odd. If $b = \pm 1$, then $ac = (1 + 171)/4 = 43$ with $a \leq c$ so that $a = 1$. If $b = \pm 3$, then $ac = (9 + 171)/4 = 45$ with $a \leq c$ so that $a = 1, 3, 5$ and $1 < |b|$. If $b = \pm 5$, then $ac = (25 + 171)/4 = 49$ with $a \leq c$ so that $a = 1, 7$ and $1 < |b|$. If $b = \pm 7$, then $ac = (49 + 171)/4 = 55$ with $a \leq c$ so that $a = 1, 5$ which are both $< |b|$, so we are left with $[1, 1, 43]$, $[3, 3, 15]$, $[5, 3, 9]$, $[5, -3, 9]$, $[7, 5, 7]$, and $[3, 3, 15]$ which is imprimitive.

Exercise 12.4.2. These are the smallest negative fundamental discriminants of class numbers 1 to 8:
For $d = -3$ we have $[1, 1, 1]$. For $d = -15$ we have $[1, 1, 4]$, $[2, 1, 2]$.
For $d = -23$ we have $[1, 1, 6]$, $[2, \pm 1, 3]$.
For $d = -39$ we have $[1, 1, 10]$, $[2, \pm 1, 5]$, $[3, 3, 4]$.
For $d = -47$ we have $[1, 1, 12]$, $[2, \pm 1, 6]$, $[3, \pm 1, 4]$.
For $d = -87$ we have $[1, 1, 22]$, $[2, \pm 1, 11]$, $[3, 3, 8]$, $[4, \pm 3, 6]$.
For $d = -71$ we have $[1, 1, 18]$, $[2, \pm 1, 9]$, $[3, \pm 1, 6]$, $[4, \pm 3, 5]$.
For $d = -95$ we have $[1, 1, 24]$, $[2, \pm 1, 12]$, $[3, \pm 1, 8]$, $[4, \pm 1, 6]$, $[5, 5, 6]$.

Exercise 12.4.3. These are the smallest even negative fundamental discriminants of class numbers 1 to 6: For $d = -4$ we have $[1, 0, 1]$; for $d = -20$ we have $[1, 0, 5]$, $[2, 2, 3]$; for

$d = -56$ we have $[1, 0, 14]$, $[2, 0, 7]$, $[3, \pm 2, 5]$; for $d = -104$ we have $[1, 0, 26]$, $[2, 0, 13]$, $[3, \pm 2, 9]$, $[5, \pm 4, 6]$.

Exercise 12.5.3. Use Rabinowicz's criterion, and quadratic reciprocity.

Exercise 12.6.1. Prove and use the inequality $am^2+bmn+cn^2 \geq am^2-|b|\max\{|m|,|n|\}^2+cn^2$.

Exercise 12.6.2(b). Use the smallest values properly represented by each form.

Exercise 12.6.5(c). Use exercise 12.6.2(e).

Exercise 12.6.7(c). Given a solution B, let $C = (B^2 - d)/4A$ and then $[A, B, C]$ represents A properly (by $(1, 0)$). Find reduced $f \sim [A, B, C]$ and use the transformation matrix to find the representation as in (b).

Exercise 12.8.1. Prove this one prime factor of A at a time and then use the Chinese Remainder Theorem. For each prime p, try $f(1, 0)$, $f(0, 1)$, and then $f(1, 1)$.

Exercise 12.8.2 If $f = [a, r, u]$, then the transformation $x \to x + ky, y \to y$ yields that $f \sim [a, b, c]$ where $b = r + 2ka$; that is, we can take b to be any value $\equiv r \pmod{2a}$. Similarly if $F = [A, s, v]$, then we can take b to be any value $\equiv s \pmod{2A}$. Such a b exists by the Chinese Remainder Theorem provided $r \equiv s \pmod 2$, and r and s have the same parity as the discriminants of f and F.

Recommended further reading

[AZ18] Martin Aigner and Günter M. Ziegler, *Proofs from The Book*, sixth ed., Springer, Berlin, 2018.

[Bak84] Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, Cambridge, 1984. MR781734

[BB09] Arthur T. Benjamin and Ezra Brown (eds.), *Biscuits of number theory*, The Dolciani Mathematical Expositions, vol. 34, Mathematical Association of America, Washington, DC, 2009. MR2516529

[Cas78] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. MR522835

[CG96] John H. Conway and Richard K. Guy, *The book of numbers*, Copernicus, New York, 1996. MR1411676

[Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. MR3236783

[CP05] Richard Crandall and Carl Pomerance, *Prime numbers: A computational perspective*, second ed., Springer, New York, 2005. MR2156291

[Dav80] Harold M. Davenport, *Multiplicative number theory*, Springer-Verlag, New York, 1980.

[Dav05] H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities*, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2005.

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[Edw01] H. M. Edwards, *Riemann's zeta function*, Dover Publications, Inc., Mineola, NY, 2001. MR1854455

[GG] Andrew Granville and Ben Green, *Additive combinatorics*, American Mathematical Society (to appear).

[Graa] Andrew Granville, *The distribution of primes: Analytic number theory revealed*, American Mathematical Society (to appear).

[Grab] Andrew Granville, *Rational points on curves: Arithmetic geometry revealed*, American Mathematical Society (to appear).

[GS] Andrew Granville and K. Soundararajan, *The pretentious approach to analytic number theory*, Cambridge University Press (to appear).

[Guy04] Richard K. Guy, *Unsolved problems in number theory*, third ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004. MR2076335

[HW08] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, Oxford, 2008. MR2445243

[IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716

[Knu98] Donald E. Knuth, *The art of computer programming. Vol. 2*, Seminumerical algorithms, third edition [of MR0286318], Addison-Wesley, Reading, MA, 1998. MR3077153

[LeV96] William J. LeVeque, *Fundamentals of number theory*, reprint of the 1977 original, Dover Publications, Inc., Mineola, NY, 1996. MR1382656

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers*, fifth ed., John Wiley & Sons, Inc., New York, 1991. MR1083765

[Rib91] Paulo Ribenboim, *The little book of big primes*, Springer-Verlag, New York, 1991. MR1118843

[Sha85] Daniel Shanks, *Solved and unsolved problems in number theory*, third ed., Chelsea Publishing Co., New York, 1985. MR798284

[ST15] Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, second ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR3363545

[Ste09] William Stein, *Elementary number theory: Primes, congruences, and secrets. A computational approach*, Undergraduate Texts in Mathematics, Springer, New York, 2009. MR2464052

[Tig16] Jean-Pierre Tignol, *Galois' theory of algebraic equations*, second ed., World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2016. MR3444922

[TMF00] Gérald Tenenbaum and Michel Mendès France, *The prime numbers and their distribution*, translated from the 1997 French original by Philip G. Spain, Student Mathematical Library, vol. 6, American Mathematical Society, Providence, RI, 2000. MR1756233

[VE87] Charles Vanden Eynden, *Elementary number theory*, The Random House/Birkhäuser Mathematics Series, Random House, Inc., New York, 1987. MR943119

[Wat14] John J. Watkins, *Number theory: A historical approach*, Princeton University Press, Princeton, NJ, 2014. MR3237512

[Zei17] Paul Zeitz, *The art and craft of problem solving*, third edition [of MR1674658], John Wiley & Sons, Inc., Hoboken, NJ, 2017. MR3617426

Index

Drawing by Robert J. Lewis. Courtesy of Princeton University Press.

Number Theory Revealed: An Introduction acquaints undergraduates with the "Queen of Mathematics". The text offers a fresh take on congruences, power residues, quadratic residues, primes, and Diophantine equations and presents hot topics like cryptography, factoring, and primality testing. Students are also introduced to beautiful enlightening questions like the structure of Pascal's triangle mod p and modern twists on traditional questions like the values represented by binary quadratic forms and large solutions of equations. Each chapter includes an "elective appendix" with additional reading, projects, and references.

An expanded edition, *Number Theory Revealed: A Masterclass*, offers a more comprehensive approach to these core topics and adds additional material in further chapters and appendices, allowing instructors to create an individualized course tailored to their own (and their students') interests.

About the Author:

Andrew Granville is the Canada Research Chair in Number Theory at the University of Montreal and professor of mathematics at University College London. He has won several international writing prizes for exposition in mathematics, including the 2008 Chauvenet Prize and the 2019 Halmos-Ford Prize, and is the author of *Prime Suspects* (Princeton University Press, 2019), a beautifully illustrated graphic novel murder mystery that explores surprising connections between the anatomies of integers and of permutations.

ISBN 978-1-4704-4157-9
9 781470 441579
MBK/126

For additional information and updates on this book, visit
www.ams.org/bookpages/mbk-126

AMS
www.ams.org