NUMBER THEORY

In the contemporary study of mathematics, number theory stands out as a peculiar branch for many reasons. Most of the development of mathematical thought is concerned with the identification of certain structures and relations in these structures. For example, the study of algebra is concerned with different types of operators on objects, such as the addition and multiplication of numbers or the permutation of objects or the transformation of geometric objects—and the study of algebra is concerned with the classification of the many such types of operators.

Similarly, the study of analysis is concerned with the properties of operators that satisfy conditions of continuity.

Number theory, however, is the study of the properties of those few systems that arise naturally, beginning with the natural numbers (which we shall usually denote $\mathbb{N}$), progressing to the integers ($\mathbb{Z}$), the rationals ($\mathbb{Q}$), the reals ($\mathbb{R}$), and the complex numbers ($\mathbb{C}$). Rather than identifying very general principles, number theory is concerned with very specific questions about these few systems.

For that reason, for many centuries, mathematicians thought of number theory as the purest form of inquiry. After all, it wasn't inspired by physics or astronomy or chemistry or other "applied" aspects of the physical universe. Consequently, mathematicians could indulge in number theoretic pursuits while being concerned only with the mathematics itself.

But number theory is a field with great paradoxes. This purest of mathematical disciplines, as we shall see, has served as the source for arguably the most important set of applications of mathematics in many years!

Another curious aspect of number theory is that it is possible for a very novice student of the subject to pose questions that can baffle the greatest minds. One example is the following: It is an interesting observation that there are many triples of natural numbers (in fact, an infinite number) that satisfy the equation $x^2 + y^2 = z^2$. For example, $3^2 + 4^2 = 5^2$; $5^2 + 12^2 = 13^2$; $7^2 + 24^2 = 25^2$; and so on.

However, one might easily be led to the question, can we find (nonzero) natural numbers x, y, and z such that $x^3 + y^3 = z^3$? Or, indeed, such that $x^n + y^n = z^n$, for any natural number $n > 2$ and nonzero integers x, y, and z?

The answer to this simple question was announced by the famous mathematician, Pierre Auguste de Fermat, in his last written work in 1637. Unfortunately, Fermat did not provide a proof but only wrote the announcement in the margins of his writing. Subsequently, this simply stated problem became known as Fermat's Last Theorem, and the answer eluded the mathematics community for 356 years, until 1993, when it was finally solved by Andrew Wiles.

The full proof runs to over one thousand pages of text and involves mathematical techniques drawn from a wide variety of disciplines within mathematics. It is thought to be highly unlikely that Fermat, despite his brilliance, could have understood the true complexity of his Last Theorem. (Lest the reader leave for want of the answer, what Wiles proved is that there are no possible nonzero x, y, z, and $n > 2$ that satisfy the equation.)

Other questions that arise immediately in number theory are even more problematic than Fermat's Last Theorem. For example, a major concern in number theory is the study of prime numbers—those natural numbers that are evenly divisible only by themselves and 1. For example, 2, 3, 5, 7, 11, 13 are prime numbers. Nine, 15, and any even number except 2 are not. (1, by convention, is not considered a prime.)

One can easily observe that small even numbers can be described as the sum of two primes: $2 + 2 = 4$; $3 + 3 = 6$; $3 + 5 = 8$; $3 + 7 = 5 + 5 = 10$; $5 + 7 = 12$; $7 + 7 = 14$; and so on. One could ask, can all even numbers be expressed as the sum of two primes? Unfortunately, no one knows the answer to this question. It is known as the *Goldbach Conjecture,* and fame and fortune await the person who successfully answers the question.

In this article, we will describe some of the principal areas of interest in number theory and then indicate what current research has shown to be an extraordinary application of this purest form of mathematics to several very current and very important applications.

Although this will in no way encompass all the areas of development in number theory, we will introduce:

Divisibility At the heart of number theory is the study of the multiplicative structure of the integers under multiplication. What numbers divide (i.e., are factors of) other numbers? What are all the factors of a given number? Which numbers are prime?

Multiplicative Functions In analyzing the structure of numbers and their factors, we are led to the consideration of functions that are *multiplicative:* In other words, a function is multiplicative if $f(a \times b) = f(a) \times f(b)$ for all a and b.

Congruence Two integers a and b are said to be congruent modulo n (where n is also an integer), and written $a \equiv b \pmod{n}$, if their difference is a multiple of n; alternatively, that a and b yield the same remainder when divided (integer division) by n. The study of the integers under congruence yields many interesting properties and is fundamental to number theory. The modular systems so developed are called modulo n arithmetic and are denoted either $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$.

Residues In $\mathbb{Z}_n$ systems, solutions of equations (technically, *congruences*) of the form $x^2 \equiv a \pmod{n}$ are often studied. In this instance, if there is a solution for x, a is called a quadratic residue of n. Otherwise, it is called a quadratic nonresidue of n.

Sums of Squares Beyond congruences of the form $x^2 \equiv a \pmod{n}$, we also consider sums of squares, that is equations of the form $x^2 + y^2 = n$.

Partitions Although, as we shall see, there is an essentially unique way of describing a natural number in terms of the ways by which other numbers can multiply together to form the number, the same is not true for addition. The study of partitions is the study of the number of ways a natural number can be reached by summing other natural numbers. This study also introduces some concepts from an-

J. Webster (ed.), *Wiley Encyclopedia of Electrical and Electronics Engineering*. Copyright © 2007 John Wiley & Sons, Inc.

other very vital branch, combinatorial mathematics.

Prime Numbers The prime numbers, with their special property that they have no positive divisors other than themselves and 1, have been of continuing interest to number theorists. In this section we will see, among other things, an estimate of how many prime numbers there are less than some fixed number n.

Continued Fractions The study of the division operations in $\mathbb{Q}$ has led to a branch of number theory studying repeated divisions and their relation to converging and diverging sequences. In general, a continued fraction is a finite or infinite sequence of the form

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cdots}}}$$

Algebraic and Transcendental Numbers More generally, number theory defines a class of real numbers that are obtainable by the solution of certain forms of polynomial equations. Numbers that can be so obtained (such as $\sqrt{2}$, a solution to $x^2 - 2 = 0$) are called *algebraic numbers.* Numbers that cannot be so determined are called *transcendental numbers.* It has proved to be enormously difficult to prove that certain common numbers, such as π and e, the base of natural logarithms, are transcendental. It is not yet known whether $\pi + e$ is transcendental!

Diophantine Equations The term *Diophantine equation* is used to apply to a family of algebraic equations in a number system such as $\mathbb{Z}$ or $\mathbb{Q}$. A good deal of research on this subject has been directed at polynomial equations with integer or rational coefficients, the most famous of which is the class of equations $x^n + y^n = z^n$, the subject of Fermat's Last Theorem.

Elliptic Curves A final area of discussion in number theory will be the theory of elliptic curves. Although generally beyond the scope of this article, this theory has been so important in contemporary number theory that some discussion of the topic is in order. An elliptic curve represents the set of points in some appropriate number system that are the solutions to an equation of the form $y^2z = x^3 + mxz^2 + nz^3$ when $m, n \in \mathbb{Z}$.

Applications The final section of this article will address several important applications in business, economics, engineering, and computing of number theory. It is remarkable that this, the purest form of mathematics, has found such important applications, often of theory that is hundreds of years old, to very current problems in these fields.

It should perhaps be noted here that many of the results indicated here are given without proof. Indeed, because of space limitations, proofs will be given only when they are especially instructive. A number of references will be given later in which proofs of all the results cited can be found.

DIVISIBILITY

Many of the questions arising in number theory have as their basis the study of the divisibility of the integers. An integer n is *divisible* by k if there exists another integer m, such that $k \times m = n$. We sometimes indicate divisibility of n by k by writing $k|n$, or $k\nmid n$ if n is not divisible by k.

A fundamental result is the *division algorithm.* Given $m, n \in \mathbb{Z}$, with $n > 0$, there exist unique integers c and d such that $m = c \times n + d$ and $0 \leq d < n$.

Equally as fundamental is the Euclidean algorithm.

Theorem 1 Let $m, n \in \mathbb{Z}$, both $m, n \neq 0$. There exists a unique integer c satisfying $c > 0$, $c|m$, $c|n$; and if $d|m$ and $d|n$, then $d|c$.

Proof Consider $\{d|d = am + bn, \forall a, b \in \mathrm{Z}\}$. Let c^* be the smallest natural number in this set. Then c^* satisfies the given conditions.

Clearly $c^* > 0$. $c^*|a$ because, by the division algorithm, there exists s and t such that $a = cs + t$ with $0 \leq t < u$. Thus $a = c^*s + t = ams + bns + t$, thus $a(1 - ms) + b(-ns) = t$. Because $t < c^*$, this implies that $t = 0$, and thus $a = c^*s$ or $c^*|a$. Similarly $c^*|b$. c^* is unique because if c' also meets the conditions then $c^*|c'$ and $c'|c^*$, so $c' = c^*$.

The *greatest common divisor* of two integers m and n is the largest positive integer [denoted GCD(m, n)] such that GCD(m, n)|m and GCD(m, n)|n.

Theorem 2 (Greatest Common Divisor) The equation $am + bn = r$ has integer solutions $a, b \Leftrightarrow$ GCD(m, n)|r.

Proof Let $r \neq 0$. It is not possible that GCD(m, n)|r since GCD(m, n)|m and GCD(m, n)|n, thus GCD(m, n)|($am + bn$) $= r$. By Theorem 1 this means that there exists a', b' such that $a'm + b'n =$ GCD(m, n).

Thus $a'' = ra'/$GCD(m, n), $b'' = rb'/$GCD(m, n) represents an integer solution to $am + bn = r$.

A related concept to the GCD is the LCM, or *least common multiple.*It can be defined as the smallest positive integer that m and n both divide. It is also worth noting that GCD(m, n) $\times$ LCM(m, n) $= m \times n$.

Primes

An integer $p > 1$ is called *prime* if it is divisible only by itself and 1. An integer greater than 1 and not prime is called *composite.* Two numbers m and n with the property that GCD(m, n) = 1 are said to *be relatively prime* (or sometimes *coprime*).

Here are two subtle results.

Theorem 3 Every integer greater than 1 is a prime or a product of primes.

Proof Suppose otherwise. Let n be the least integer that is neither; thus n is composite. Thus $n = ab$, and $a, b < n$. Thus a and b are either primes or products of primes, and thus so is their product n.

Theorem 4 There are infinitely many primes.

Proof (Euclid) If not, let $p_1, \ldots, p_n$ be a list of all the primes, ordered from smallest to largest. Then consider $q = (p_1p_2 \cdots p_n) + 1$. By the previous statement,

$$q = p'_1p'_2\cdots p'_k \tag{1}$$

p'_1 must be one of the $p_1, \ldots, p_n$, say p_j (because these were all the primes); but $p_j|q$, because it has a remainder of 1. This contradiction proves the theorem.

Theorem 5 (Unique Factorization) Every number can be expressed as a product of prime numbers in a unique manner.

Proof Let

$$\begin{aligned} a &= p_1^{\alpha_1}\cdots p_k^{\alpha_k} = P \\ &= q_1^{\beta_1}\cdots q_m^{\beta_m} = Q \end{aligned} \tag{2}$$

For each p_i, $p_i|Q \Rightarrow p_i|q^{\beta}{}_{ss}$ for some s, $1 \leq s \leq m$.

Because p_i and q_s are both primes, $p_i = q_s$. Thus $k = m$, and $Q = p_1^{\beta_1} \cdots p_k^{\beta}k$. We need to show only that the α_i and β_i are equal. Divide both decompositions P and Q by $p_i^{\alpha_i}$. If $\alpha_i \neq \beta_i$, on the one hand one decomposition $a/\, p_i^{\alpha_i}$ will contain p_i, and the other will not. This contradiction proves the theorem.

What has occupied many number theorists was a quest for a formula that would generate all the infinitely many prime numbers.

For example, Marin Mersenne (1644) examined numbers of the form $M_p = 2^p - 1$, where p is a prime. He discovered that some of these numbers were, in fact, primet. Generally, the numbers he studied are known as Mersenne numbers, and those that are prime are called Mersenne primes. For example, $M_2 = 2^2 - 1 = 3$ is prime; as are $M_3 = 2^3 - 1 = 7$; $M_5 = 2^5 - 1 = 31$; $M_7 = 2^7 - 1 = 127$. Alas, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ is not. Any natural number > 2 ending in an even digit 0, 2, 4, 6, 8 is divisible by 2. Any number > 5 ending in 5 is divisible by 5. There are also convenient tests for divisibility by 3 and 9—if the sum of the digits of a number is divisible by 3 or 9, then so is the number; and by 11—if the sum of the digits in the even decimal places of a number, minus the sum of the digits in the odd decimal places, is divisible by 11, then so is the number.

Several other Mersenne numbers have also been determined to be prime. At the current writing, the list includes 44 numbers:

M_n, where n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657. With current technology, particularly mathematical software packages such as *Mathematica* or *Maple,* many of these computations can be done rather easily. For example, a one-line program in Mathematica, 5.2, executing for 27.2 minutes on a Pentium 4 PC, with 1 GB of RAM and running at 2.8 GHz, was capable of verifying the primality of all M_n up to M_{10000}, and thus determining the first 22 Mersenne primes (up to M_{9941}).

It is not known whether an infinite number of the Mersenne numbers are prime.

It is known that $m^c - 1$ is composite if m ≥ 2 or if c is composite; for if $c = de$ we have

$$(m^e - 1)(m^{e(d-1)} + m^{e(d-1)} + \cdots + m^{e(d-1)} + 1)$$

We can also show that $a^c + 1$ is composite if m is odd, or if c has an odd factor. Certainly if m is odd, m^c is odd, and $m^c + 1$ is even and thus composite. If $c = d(2k + 1)$, then

$$m^c + 1 = (m^d + 1)(m^{2de} - m^{d(2e-1)} + m^{d(2e-2)} - \cdots + 1) \tag{4}$$

and $m^d + 1 > 1$.

Another set of numbers with interesting primality properties are the *Fermat numbers,* $F_n = 2^{2^n} + 1$. Fermat's conjecture was that they were primes. He was able to verify this for $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 2^{16} + 1 = 65537$. But then, Euler showed that

Theorem 6 $641|F_5$.

Proof $641 = 2^4 + 5^4 = 5 \times 2^7 + 1$; thus $2^4 = 641 - 5^4$. Because $2^{32} = 2^4 \times 2^{28} = 641 \times 2^{28} - (5 \times 2^7)^4 = 641 \times 2^{28} - (641 - 1)^4 = 641k - 1$.

To this date, no other Fermat numbers F_n with $n > 4$ have been shown to be prime. It has been determined that the other Fermat numbers through F_{20} are composite.

MULTIPLICATIVE FUNCTIONS

Functions that preserve the multiplicative structure of the number systems studied in number theory are of particular interest, not only intrinsically, but also for their use in determining other relationships among numbers.

A function f defined on the integers, which takes values in a set closed under multiplication, is called a *number-theoretic function.* If the function preserves multiplication for numbers that are relatively prime ($f(m) \times f(n) = f(m \times n)$), it is called a *multiplicative function;* it is called *completely multiplicative* if the restriction GCD(m, n) = 1 can be lifted.

Consider any number theoretic function f, and define a new function F by the sum of the values of f taken over the divisors of n,

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} f(n/d) \tag{5}$$

the latter being the former sum in reverse order.

Theorem 7 If f is a multiplicative function, then so is F.

Proof Let GCD(m, n) = 1; then $d|mn$ can be uniquely expressed as gh where $g|m$, $h|n$, with GCD(g, h) = 1.

$$
\begin{aligned}
F(mn) &= \sum_{d|mn} f(d) = \sum_{g|m}\sum_{h|n} f(gh) = \sum_{g|m}\sum_{h|n} f(g)f(h) \\
&= \sum_{g|m} f(g)f(h_1) + \cdots + \sum_{g|m} f(g)f(h_k) \qquad (6) \\
&= F(m)\left(\sum_{h|n} f(h)\right) = F(m)F(n)
\end{aligned}
$$

Two multiplicative functions of note are the divisor function $\tau(n)$, defined as the number of positive divisors of n; and the function $\sigma(n)$, defined as the sum of the positive divisors of n.

Theorem 8 τ and σ are multiplicative.

Proof Both τ and σ are the "uppercase" functions for the obviously multiplicative functions $1(n) = 1$ for all n, and $i(n) = n$ for all n. In other words,

$$\tau(n) = \sum_{d|n} 1(d) \qquad \text{and} \qquad \sigma(n) = \sum_{d|n} i(d) \qquad (7)$$

In order to compute τ and σ, for a prime p note that

$$\tau(p^n) = 1 + n$$

(because the divisors of p^n are $1, p, p^2,. . . ,p^n$); (8)

$$\sigma(p^n) = 1 + p + p^2 + \cdots + p^n = (p^{n+1} - 1)/(p - 1) \qquad (9)$$

Thus, for any $n = p_1a^{n_1}\, p_2a^{n_2} \ldots\, p_ka^{n_k}$,

$$\tau(n) = \prod_{i=1}^{k}(1 + n_i) \qquad \text{and}\, \sigma(n) = \prod_{i=1}^{k}(p_i^{n_i+1} - 1)/(p_i - 1) \quad (10)$$

In very ancient times, numbers were sometimes considered to have mystical properties. Indeed, the Greeks identified numbers that they called *perfect:* numbers that were exactly the sums of all their proper divisors, in other words, that $\sigma(n) = 2n$. A few examples are 6 = 1 + 2 + 3; 28 = 1 + 2 + 4 + 7 + 14; and 496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248. It is not known whether there are any odd perfect numbers or if an infinite number of perfect numbers exist.

Theorem 9 n is even and perfect $\Leftrightarrow n = 2^{p-1}(2^p - 1)$ where both p and $2^p - 1$ are primes.

In other words, there is one perfect number for each Mersenne prime.

Another multiplicative function of considerable importance is the Möbius function μ.

$\mu(1) = 1$; $\mu(n) = 0$ if n has a square factor; $\mu(p_1p_2 \cdots p_k) = (-1)^k$ if $p_1, \ldots, p_k$ are distinct primes.

Theorem 10 μ is multiplicative, and the "uppercase" function is 0 unless n =1, when it takes the value 1.

Theorem 11 (Möbius Inversion Formula) If f is a number theoretic function and $F(n) = \Sigma_{d|n} f(d)$, then

$$f(n) = \sum_{d|n} F(d)\mu(n/d) = \sum_{d|n} F(n/d)\mu(n) \qquad (11)$$

Proof

$$
\begin{aligned}
&\sum_{d|n} \mu(d)F(n/d) \\
&= \sum_{d_1d_2=n} \mu(d_1)F(n/d_2) \quad (\text{taking pairs } d_1d_2 = n) \qquad (12) \\
&= \sum_{d_1d_2=n} \left[\mu(d_1)\sum_{d|d_2} f(d)\right] \quad (\text{definition of } F) \qquad (13) \\
&= \sum_{d_1d|n} \mu(d_1)f(d) \quad (\text{multiplying the terms in brackets}) \qquad (14) \\
&= \sum_{d|n} f(d) \sum_{d_1|(n/d)} \mu(d_1) \quad [\text{collecting multiples of } f(d)] \\
&= f(n) \qquad (15)
\end{aligned}
$$

Theorem 12 If F is a multiplicative function, then so is f.

A final multiplicative function of note is the *Euler function, $\phi(n)$*. It is defined for n to be the number of numbers less than n and relatively prime to n. For primes p, $\phi(p) = p - 1$.

Theorem 13 ϕ is multiplicative.

CONGRUENCE

The study of congruence leads to the definition of new algebraic systems derived from the integers. These systems, called *residue systems,* are interesting in and of themselves, but they also have properties that allow for important applications to be discussed later.

Consider integers a, b, n with $n > 0$. Note that a and b could be positive or negative. We will say that *a is congruent to b, modulo n* [written $a \equiv b \pmod{n}$] $\Leftrightarrow n|(a - b)$. Alternatively, a and b yield the same remainder when divided by n. In such a congruence, n is called the modulus, and b is called a residue of a.

An algebraic system can be defined by considering classses of all numbers satisfying a congruence with fixed modulus. It is observed that congruence is an equivalence relation and that the definition of addition and multiplication of integers can be extended to the equivalence classes. Thus, for example, in the system with modulus 5 (also called mod 5 arithmetic), the equivalence classes are $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$, $\{\ldots, -9, -4, 1, 6, 11, \ldots\}$, $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$, $\{\ldots, -7, -2, 3, 8, 13, \ldots\}$, and $\{\ldots, -6, -1, 4, 9, 14, \ldots\}$. It is customary to denote the class by the (unique) representative of the class between 0 and $n - 1$. Thus the five classes in mod 5 arithmetic are denoted 0, 1, 2, 3, 4. Formally, the mod n system can be defined as the algebraic quotient of the integers $\mathbb{Z}$ and the subring defined by the multiples of $n(n\mathbb{Z})$. Thus the mod n system is often written $\mathbb{Z}/n\mathbb{Z}$. An alternative, and more compact notation, is $\mathbb{Z}_{\text{n}}$.

As mentioned earlier, addition and multiplication are defined naturally in $\mathbb{Z}_{\text{n}}$. Under addition, every $\mathbb{Z}_{\text{n}}$ forms an Abelian group [that is, the addition operation is closed, associative, and commutative; 0 is an identity; and each element has an additive inverse—for any $a, b = n - a$ always yields $a + b \equiv 0 \pmod{n}$].

In the multiplicative structure, however, only the closure, associativity, commutativity, and identity (1) are ensured. It is not necessarily the case that each element will have an inverse. In other words, the congruence $ax \equiv 1 \pmod{n}$ will not always have a solution.

Technically, an algebraic system with the properties described previously is called a *commutative ring with identity.* If it is also known that each (nonzero) element of $\mathbb{Z}_{\text{n}}$ has an inverse, the system would be called a *field.*

Theorem 14 Let a, b, n be integers with $n > 0$. Then $ax \equiv 1 \pmod{n}$ has a solution $\Leftrightarrow$ GCD$(a, n) = 1$. If x_0 is a solution, then there are exactly GCD(a, n) solutions given by $\{x_0, x_0 + n/\text{GCD}(a, n), x_0 + 2n/\text{GCD}(a, n), \ldots, x_0 + (\text{GCD}(a, n) - 1)n/\text{GCD}(a, n)\}$.

Proof This theorem is a restatement of Theorem 2.

In order for an element a in $\mathbb{Z}_{\text{n}}$ to have an inverse, alternatively to be a unit, by Theorem 14, it is necessary and sufficient for a and n to be relatively prime [i.e., GCD$(a, n) = 1$]. Thus, by the earlier definition of the Euler function, the number of units in $\mathbb{Z}_{\text{n}}$ is $\phi(n)$.

The set of units in $\mathbb{Z}_{\text{n}}$ is denoted $(\mathbb{Z}_{\text{n}})^*$, and it is easily verified that this set forms an Abelian group under multiplication. As an example, consider $\mathbb{Z}_{12}$ or $\mathbb{Z}/12\mathbb{Z}$. Note that $(\mathbb{Z}_{12})^* = \{1, 5, 7, 11\}$, and that each element is its own inverse: $1 \times 1 \equiv 5 \times 5 \equiv 7 \times 7 \equiv 11 \times 11 \equiv 1 \pmod{12}$. Furthermore, closure is observed because $5 \times 7 \equiv 11$, $5 \times 11 \equiv 7$, and $7 \times 11 \equiv 5 \pmod{12}$.

Theorem 15 If p is a prime number, then $\mathbb{Z}_{\text{p}}$ is a field with p elements. If n is composite, $\mathbb{Z}_{\text{n}}$ is not a field.

Proof If p is a prime number, every element $a \in (\mathbb{Z}_{\text{p}})^*$ is relatively prime to p, that is GCD$(a, p) = 1$. Thus $ax \equiv 1 \pmod{p}$ always has a solution. Because every element in $(\mathbb{Z}_{\text{p}})^*$ has an inverse, $(\mathbb{Z}_{\text{p}})^*$ is a field. If n is composite, there are integers $1 < k$, $1 < n$ such that $k1 = n$. Thus $k1 \equiv 0 \pmod{n}$, and so it is impossible that k could have an inverse. Otherwise, $l \equiv (k^{-1}k) \times l \equiv k^{-1}(\text{k} \times l) \equiv k^{-1} \times 0 \equiv 0 \pmod{n}$, which contradicts the assumption that $1 < n$.

One of the most important results of elementary number theory is the so-called *Chinese Remainder Theorem.* It is given this name because a version was originally derived by the Chinese mathematician Sun Tzu in the third century. The Chinese Remainder Theorem establishes a method of solving simultaneously a system of linear congruences in several modular systems.

Although there is a long history of the use of this term, it is perhaps a disservice to the discoverver not to coll it the Sun Tzu Theorem. After all, we do not call Fermat's Last Theorem the "French Last Theorem."

Theorem 16 (Chinese Remainder) Given a system $x \equiv a_{\text{i}}\ (\text{mod} n_{\text{i}})$, i = 1, 2, . . . , m. Suppose that for all $i \neq j$, GCD$(n_{\text{i}}, n_{\text{j}}) = 1$. Then there is a unique common solution modulo $n = n_1 n_2 \cdots n_{\text{m}}$.

Proof (by construction) Let $n'_{\text{i}} = n/n_{\text{i}}$, $i = 1, \ldots, m$. Note that GCD$(n_{\text{i}}, n'_{\text{i}}) = 1$. Thus there exists an integer n''_{i} such that $n'_{\text{i}} n''_{\text{i}} \equiv 1 \pmod{n_{\text{i}}}$. Then

$$x \equiv a_1 n'_1 n''_1 + a_2 n'_2 n''_2 + \cdots + a_m n'_m n''_m \pmod{n} \qquad (16)$$

is the solution. Because $n_{\text{i}} | n'_{\text{j}}$ if $i \neq j$, $x \equiv a_{\text{i}} n'_{\text{i}} n''_{\text{i}} \equiv a_{\text{i}} \pmod{n_{\text{i}}}$. The solution is also unique. If both x and y are common solutions, then $x - y \equiv 0 \pmod{n}$.

An interesting consequence of this theorem is that there is a 1–1 correspondence, preserved by addition and multiplication, of integers modulo n, and m-tuples of integers modulo n_{i}. Consider $\{n_1, n_2, n_3, n_4\} = \{7, 11, 13, 17\}$, and $n = 17017$. Then

$$\begin{aligned} 95 &\rightarrow (a_1, a_2, a_3, a_4) \\ &= (95 \bmod 7, 95 \bmod 11, 95 \bmod 13, 95 \bmod 17) \\ &= (4, 7, 4, 10) \end{aligned}$$

also

$$162 \rightarrow (1, 8, 6, 9)$$

Performing addition and multiplication tuple-wise:

$$\begin{aligned} &(4, 7, 4, 10) + (1, 8, 6, 9) \\ &\quad = (5 \bmod 7, 15 \bmod 11, 10 \bmod 13, 19 \bmod 17) \\ &\quad = (5, 4, 10, 2) \\ &(4, 7, 4, 10) \times (1, 8, 6, 9) \\ &\quad = (4 \bmod 7, 56 \bmod 11, 24 \bmod 13, 19 \bmod 17) \\ &\quad = (4, 1, 11, 5) \end{aligned}$$

Now verify that $95 + 162 = 257$ and $95 \times 162 = 15390$ are represented by $(5, 4, 10, 2)$ and $(4, 1, 11, 5)$ by reducing each number mod $n_1, \ldots, n_4$.

Another series of important results involving the products of elements in modular systems are the theorems of Euler, Fermat, and Wilson. Fermat's Theorem, although extremely important, is very easily proved—thus it is sometimes called the "Little Fermat Theorem" in contrast to the famous Fermat's Last Theorem described earlier.

Theorem 17 (Euler) If GCD$(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem 18 (Fermat) If p is prime, then $a^{\text{p}} \equiv a \pmod{p}$.

Proof (of Euler's Theorem) Suppose that $A = \{a_1, \ldots, a_{\phi(n)}\}$ is a list of the set of units in $\mathbb{Z}_{\text{n}}$. By definition, each of the a_{i} has an inverse, $a^{-1}{}_{\text{i}}$. Now consider the product, $b = a_1 a_2 \cdots a_{\phi(n)}$. It also has an inverse, in particular b^{-1}

= $a^{-1}{}_1 a^{-1}{}_2 \cdots a^{-1}{}_{\phi(n)}$. Choose any of the units—suppose it is a. Now consider the set $A' = \{aa_1, aa_2, aa_{\phi(n)}\}$. We need to show that as a set, $A' = A$. It is sufficient to show that the aa_i are all distinct. Because there are $\phi(n)$ of them, and they are all units, they represent all of the elements of A.

Suppose that $aa_\mathrm{i} \equiv aa_\mathrm{j}$ for some $i \neq j$. Then, because a is a unit, we can multiply by a^{-1}, yielding $(a^{-1}a)a_\mathrm{i} \equiv (a^{-1}a)a_\mathrm{j}$ or $a_\mathrm{i} \equiv a_\mathrm{j}$ (mod n), which is a contradiction. Thus the aa_i are all distinct, and $A = A'$.

Now compute

$$\prod_{i=1}^{\phi(n)} (aa_i) \equiv b \,(\mathrm{mod}\, n) \qquad \text{because } A = A' \tag{17}$$

$$\begin{aligned} a^{\phi(n)} b &\equiv b \,(\mathrm{mod}\, n) \\ a^{\phi(n)} bb^{-1} &\equiv bb^{-1} (\mathrm{mod}\, n) \quad \text{multiplying by } b^{-1} \\ a^{\phi(n)} &\equiv 1 (\mathrm{mod}\, n) \end{aligned} \tag{18}$$

Although the Chinese Remainder Theorem gives a solution for linear congruences, we would also like to consider nonlinear or higher degree polynomial congruences. In the case of polynomials in one variable, in the most general case,

$$f(x) \equiv 0 \,(\mathrm{mod}\, n) \tag{19}$$

If $n = p_1^{a_1} \cdots p_k^{a_k}$ is the factorization of n, then the Chinese Remainder Theorem ensures solutions of Eq. (24) ⇔ each of

$$f(x) \equiv 0 \,(\mathrm{mod}\, p_i^{a_i}) \qquad i = 1, 2, \ldots, k \tag{20}$$

has a solution.

Since $\phi(p) = p - 1$ for p a prime, Fermat's Theorem is a direct consequence of Euler's Theorem.

Solutions to Eq. (25) can be found by using a procedure to find solutions to $f(x) \equiv 0$ (mod p^k).

Suppose that x_0 is a solution to $f(x) \equiv 0$ (mod p^k). Then compute a Taylor expansion (using formal derivatives):

$$f(x_0 + tp^k) = f(x_0) + tp^k f'(x_0) + \cdots + 1/n![(tp^k)n] f^{(n)}(x_0) \tag{21}$$

where n is the degree of f and t is an integer. In mod $p^{k+1}(\mathbb{Z}_{p^{k+1}})$, all the terms after the second vanish. Thus x_0 + tp^k is a solution if and only if

$$tf'(x_0) \equiv -f(x_0)/p^k \,(\mathrm{mod}\, p) \tag{22}$$

By Theorem 14, if $p{+}f'_{-}(x_0)$, Eq. (27) has a unique solution, and so the solution x_0 of Eq. (27) gives rise to a unique solution $x_0 + tp^\mathrm{k}$ of Eq. (26). If $p|f'(x_0)$, then $f(x_0 + tp^\mathrm{k}) \equiv f(x_0)$ (mod $p^{\mathrm{k}+1}$); hence, either x_0 is also a solution of Eq. (26) in which case so is $x_0 + tp^\mathrm{k}$ for all t, or x_0 is not a solution in which case Eq. (26) has no solution satisfying $x \equiv x_0$ (mod $p^{\mathrm{k}+1}$).

Example Consider the congruence $f(x) = x^5 + 100x^4 + 112x^3 + 31x^2 + 67x + 64 \equiv 0$ (mod 125). Note that $f'(x) = 5x^4 + 400x^3 + 336x^2 + 62x + 67$. By the method described in the previous paragraph, we first examine the case $p = 5$.

Note that $f(1) \equiv 0$; $f(2) \equiv 0$; and $f(4) \equiv 0$ (mod 5). Thus we consider these for the case $p^2 = 25$.

$x = 1$: $f(1) \equiv 0$ (mod 25), and $f'(1) \equiv 20$; so 1 is a solution mod 25. Therefore, so are $1 + 5n$ (mod 25), that is, 6, 11, 16, 21.

$x = 2$: $f(2) \equiv 0$, and $f'(1) \equiv 15$; so 2 is a solution mod 25. Therefore, so are $2 + 5n$ (mod 25), that is, 7, 12, 17, 22.

$x = 4$: $f(4) \equiv 20 \not\equiv 0$ (mod 25), and $f'(4) \equiv 21$; thus compute $21t \equiv -20/5$ (mod 25) ⇒ $t = 1$. Therefore $4 + tp = 4 + 5 = 9$ is a solution,

Now finally consider $p^3 = 125$. The results are summarized in Table 1. Thus there are 21 roots of the congruence in all.

There are other important results in the theory of polynomial congruences.

Theorem 19 (Lagrange) If $f(x)$ is a nonzero polynomial of degree n, whose coefficients are elements of $\mathbb{Z}_\mathrm{p}$ for a prime p, then $f(x)$ cannot have more than n roots.

Theorem 20 (Chevalley) If $f(x_1, \ldots, x_\mathrm{n})$ is a polynomial with degree less than n, and if the congruence

$$f(x_1, x_2, \ldots, x_n) \equiv 0 (\mathrm{mod}\ p)$$

has either zero or at least two solutions.

The Lagrange Theorem can be used to demonstrate the result of Wilson noted earlier.

Theorem 21 (Wilson) If p is a prime then $(p - 1)! \equiv -1$ (mod p).

Proof If $p = 2$, the result is obvious. For p an odd prime, let

$$f(x) = x^{p-1} - (x-1)(x-2)\cdots(x-p+1) - 1$$

Consider any number $1 \leq k \leq p - 1$. Substituting k for x causes the term $(x - 1)(x - 2) \cdots (x - p + 1)$ to vanish; also, by Fermat's theorem, $k^{\mathrm{p}-1} \equiv 1$ (mod p). Thus, $f(k) \equiv 0$ (mod p). But k has degree less than $p - 1$; and so by the Lagrange Theorem, $f(x)$ must be identically zero, which means that all the coefficients must be divisible by p. The constant coefficient is

$$-1 - (p-1)! (\mathrm{mod}\ p)$$

and thus

$$(p-1)! \equiv -1 (\mathrm{mod}\ p)$$

QUADRATIC RESIDUES

Having considered general polynomial congruences, now we restrict consideration to quadratics. The study of quadratic residues leads to some useful techniques; additionally, they have important and perhaps surprising results.

Table 1

$f(x)$	Root?	$f'(x)$	More Roots?	Associated Roots $(x - 25n)$
1	Yes	$\neq 0$	Yes	1, 26, 51, 76, 101
2	No			
6	No			
7	Yes	$\not\equiv 0$	Yes	7, 32, 57, 82, 107
9	No	$\not\equiv 0$	Yes	solve $121t = -100/25 \pmod 5$, giving 34
11	No			
12	No			
16	Yes	$\not\equiv 0$	Yes	16, 41, 66, 91, 116
17	Yes	$\not\equiv 0$	Yes	17, 42, 67, 92, 117
21	No			
22	No			

The most general quadratic congruence (in one variable) is of the form $ax^2 + bx + c \equiv 0 \pmod m$. Such a congruence can always be reduced to a simpler form. For example, as indicated in the previous section, by the Chinese Remainder Theorem, we can assume that the modulus is a prime power. Also because in the case $p = 2$ we can easily enumerate the solutions, we will henceforth consider only odd primes. Finally, we can use the technique of "completing the square" from elementary algebra to transform the general quadratic to one of the form $x^2 \equiv a \pmod p$.

If $p+a$, then if $x^2 \equiv a \pmod p$ is soluble, a is called a *quadratic residue mod p;* if not, a is called a *quadratic nonresidue mod p.*

Theorem 22 Exactly half of the integers a, $1 \le a \le p - 1$, are quadratic residues mod p.

Proof Consider the set $\mathrm{QR} = \{1^2, 2^2, \ldots, ((p-1)/2)^2\}$. Each of these is a quadratic residue, and no two are congruent mod p. Because $t^2 - u^2 \equiv 0 \pmod p \Rightarrow t + u \equiv 0 \pmod p$ or $t - u \equiv 0 \pmod p$ and t and u are distinct, the second case is not possible; and since t and u must be both $<p - 1$, neither is the first case. Thus there are at least $(p - 1)/2$ quadratic residues.

If x_0 solves $x^2 \equiv a \pmod p$, then so does $p - x_0 = p^2 - 2px_0 + x^2{}_0 \equiv x^2{}_0 \equiv a \pmod p$, and $p - x_0 \not\equiv x_0 \pmod p$. Thus we have found $p - 1$ elements of $\mathbb{Z}_{\mathrm{p}}$ that square to elements of QR. Thus, there can be no more quadratic residues outside of QR, so the result is proved.

An important number theoretic function to evaluate quadratic residues is the *Legendre symbol.* For p an odd prime, the Legendre symbol for a

$$\left(\text{written alternatively } (a/p) \text{ or } \binom{a}{p}\right)$$

is

$$\binom{a}{p} = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue mod } p \\ 0 & \text{if } p \mid a \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p \end{cases}$$

One method of evaluating the Legendre symbol uses *Euler's criterion.* If p is an odd prime and $\mathrm{GCD}(a, p) = 1$, then

$$\binom{a}{p} = 1 \Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod p$$

Equivalently,

$$\binom{a}{p} \equiv a^{(p-1)/2} \pmod p$$

Here are some other charcteristics of the Legendre symbol.

Theorem 23

i. $\binom{ab}{p} = \binom{a}{p}\binom{b}{p}$:

ii. if $a \equiv b \pmod p$, then $\binom{a}{p} = \binom{b}{p}$:

iii. $\binom{a^2}{p} = 1$, $\binom{1}{p} = 1$:

iv. $\binom{-1}{p} = (-1)^{(p-1)/2}$.

Suppose that we want to solve $x^2 \equiv 518 \pmod{17}$. Then, compute

$$\binom{518}{17} = \binom{8}{17} = \binom{2}{17}$$

But

$$\binom{2}{17} = 1$$

because $6^2 = 36 \equiv 2 \pmod{17}$. Thus, $x^2 \equiv 518 \pmod{17}$ is soluble.

Computation of the Legendre symbol is aided by the following results. First, define an absolute least residue modulo p as the representation of the equivalence class of a mod p, which has the smallest absolute value.

Theorem 24 (Gauss' Lemma) Let $\mathrm{GCD}(a, p) = 1$. If d is the number of elements of $\{a, 2a, \ldots, (p - 1)a\}$ whose absolute least residues modulo p are negative, then

$$\binom{a}{p} = (-1)^{d}$$

Theorem 25 2 is a quadratic residue (respectively, quadratic nonresidue) of primes of the form $8k \pm 1$ (respectively, $8k \pm 3$). That is,

$$\binom{2}{p} = (-1)^{(p^2-1)/8}$$

Theorem 26

1. If $k > 1, p = 4k + 3$, and p is prime, then $2p + 1$ is also prime $\Leftrightarrow 2^{\mathrm{p}} \equiv 1 \pmod{2p + 1}$.
2. If $2p + 1$ is prime, then $2p + 1|M_{\mathrm{p}}$, the pth Mersenne number, and M_{p} is composite.

A concluding result for the computation of the Legendre symbol is one that, by itself, is one of the most famous—and surprising—results in all of mathematics. It is called *Gauss' Law of Quadratic Reciprocity.* What makes it so astounding is that it manages to relate prime numbers and their residues that seemingly bear no relationship to one another.

Suppose that we have two odd primes$p$ and q. Then, the Law of Quadratic Reciprocity relates the computation of their Legendre symbols; that is, it determines the quadratic residue status of each prime with respect to the other.

The proof, although derived from elementary principles, is long and would not be possible to reproduce here. Several sources for the proof follow.

Theorem 27 (Gauss' Law of Quadratic Reciprocity)

$$\binom{p}{q}\binom{q}{p} = (-1)^{(p-1)(q-1)/4}$$

A consequence of the Law of Quadratic Reciprocity follows.

Theorem 28 Let p and q be distinct odd primes, and $a \geq 1$. If $p \equiv \pm q \pmod{4a}$ then

$$\binom{a}{p} = \binom{a}{q}$$

An extension of the Legendre symbol is the *Jacobi symbol.* The Legendre symbol is defined only for primes p. By a natural extension, the Jacobi symbol, also denoted

$$\binom{a}{n}$$

is defined for any $n > 0$, assuming that the prime factorization of n is $p_1 \ldots, p_{\mathrm{k}}$, by

$$\binom{a}{n} \text{[Jacobi symbol]} = \binom{a}{p_1}\binom{a}{p_2}\cdots\binom{a}{p_k} \text{[Legendre symbols]}$$

SUMS OF SQUARES

A next step in the investigation of the properties of numbers is to consider sums of squares. In particular, we will consider a quadratic form $f(x_1, \ldots, x_{\mathrm{n}}) = a$, and look for solutions of this equation.

One technique that can often be employed here is the method of infinite descent. Infinite descent (although in fact a finite process) is a type of mathematical induction.

Given the form $f(x_1, \ldots, x_n) = a$ stated earlier, we seek a solution to

$$f(x_1, \ldots, x_n) = ka \tag{23}$$

for some positive integer k. We would seek this using congruence methods as described earlier. Then, given the solution to Eq. (23), we look for another solution $f(x_1, \ldots, x_n) = k'm$, with $0 < k' < k$. Then, by repeating the process, we may eventually find a solution to Eq. (23).

One of the first results of this technique is the result of Fermat.

Theorem 29 (Fermat) For a prime p, $x^2 + y^2 = p$ has a solution for x and $y \Leftrightarrow p = 2$ or $p \equiv 1 \pmod 4$.

Proof In the case $p = 2$, we have $1^2 + 1^2 = p$.

If $p \equiv 3 \pmod 4$, there can be no solution, because for $q \in \mathbb{Z}_4$, $q^2 \equiv 0$ or $1 \pmod 4$. Thus, we need to verify only the case $p \equiv 1 \pmod 4$. Using the method of infinite descent, by the Legendre symbol there exists an x such that $0 < x < p/2$ and $x^2 + 1 \equiv 0 \pmod p$. Hence, $x^2 + 1 = kp$ for some $k < p$.

Some related results follow.

Theorem 30 The equation $x^2 + y^2 = m$ has an integer solution $\Leftrightarrow$ each prime factor of m congruent to 3 modulo 4 occurs to an even power in the prime factorization of m.

Theorem 31 Let p be a prime. Then

1. $x^2 + 3y^2 = p$
2. $x^2 - xy + y^2 = p$

are both soluble in the integers $\Leftrightarrow p \equiv 1 \pmod 3$ or $p = 3$.

Theorem 2 Every nonnegative integer can be expressed as a sum of four squares.

Proof First, because of the following identity, it will be sufficient to prove the result for primes, as the product of two numbers expressible as the sum of four squares is also so expressible:

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)\\ &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2\\ &= (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \quad (24)\\ &= (x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2\\ &= (x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2\end{aligned}$$

Since the condition is satisfied for 1 and 2 ($1 = 1^2 + 0^2 + 0^2 + 0^2$; $2 = 1^2 + 1^2 + 0^2 + 0^2$), we need only prove it for odd primes. Consider $S = \{a^2 | a = 1, 2, \ldots, (p-1)/2\}$, and also $T = \{-1 - b^2 | b = 0, 1, \ldots, (p-1)/2\}$ for any odd prime p. No two elements of S are congruent mod p (by Theorem 22). The set $S \cup T$ has $p + 1$ elements. Thus there exists $a \in S$, $b \in T$ with $a, b < p/2$ and $a^2 \equiv -1 - b^2 \pmod p$. Thus $a^2 + b^2 + 1^2 + 0^2 \equiv 0 \pmod p$, and thus

$$x_1^2+x_2^2+x_3^2+x_4^2 = kp \text{ has a solution for some } k < p \qquad (25)$$

Now there are two cases to consider. Either k is even or odd. If k is even, then $x_1, \ldots, x_4$ are either all even, all odd, or two even. Thus $(x_1 + x_2)/2$, $(x_1 - x_2)/2$, $(x_3 + x_4)/2$, $(x_3 - x_4)/2$, after relabeling, are all integers. Thus, $[(x_1 + x_2)/2]^2 + [(x_1 - x_2)/2]^2 + [(x_3 + x_4)/2]^2 + [(x_3 - x_4)/2]^2 = kp/2$. Thus, we have successfully applied the principle of infinite descent.

If k is odd, let y_i be the absolute least residue mod k of x_i, so that

$$y_1^2+y_2^2+y_3^2+y_4^2 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \pmod k \text{ [by Eq. (25)]}$$

Thus $y^2{}_1 + y^2{}_2 + y^2{}_3 + y^2{}_4 = k_1k$, where $k_1 < k$. Let z_1, z_2, z_3, z_4 represent each of the right-hand side terms in Eq. (46). Then,

$$\begin{aligned}z_1^2+z_2^2+z_3^2+z_4^2 &= (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)\\ &= k^2k_1p\end{aligned} \qquad (26)$$

Also, each $z_i \equiv 0 \pmod k$. thus z_1/k, z_2/k, z_3/k, z_4/k are all integers. Thus we have the integer equation

$$(z_1/k)^2+(z_2/k)^2+(z_3/k)^2+(z_4/k)^2 = k_1p \qquad (27)$$

and infinite descent can be applied in this case as well, proving the result.

CONTINUED FRACTIONS

Part of the interest in studying the classical number systems lies in their interrelationships. In particular, because all real numbers can be approximated by limits of sequences of rational numbers, it is natural to consider methods of approximating real numbers through various sequences of rationals.

One type of rational sequence is called a *continued fraction.* A continued fraction is an expression of the form:

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cdots}}} \qquad (28)$$

where all the a_i, b_i are integers. If, in particular, the b_is are all equal to 1, and the a_is are all greater than or equal to 1, the continued fraction is called simple. We may also consider such a continued fraction with finitely many entries, with the last being any real number greater than or equal to 1.

An infinite continued fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \qquad (29)$$

henceforth to be denoted $[a_0, a_1, a_2, a_3, \ldots]$ is said to converge when the sequence $[a_0]$, $[a_0, a_1]$, $[a_0, a_1, a_2]$, . . . converges.

One fundamental result follows.

Theorem 33 Let $a_0, a_1, \ldots$ be a finite sequence of $n + 1$ positive integers, or an infinite sequence, except that a_0 can be zero; and let c_i and d_i be given by

$$\begin{array}{ll} c_0 = a_0 & d_0 = 1\\ c_1 = a_0a_1 + 1 & d_1 = a_1\\ \vdots & \vdots\\ c_{k+2} = c_{k+1}c_{k+2} = c_k & d_{k+2} = d_{k+1}a_{k+2} + d_k\end{array}$$

where $k \geq n$ if the sequence is finite. If $\alpha \in \mathbb{R}$ is greater than 1, then

$$\text{i. } [a_0, a_1, \ldots, a_k, \alpha] = \frac{\alpha c_k + c_{k-1}}{\alpha d_k + d_{k-1}} \quad \text{if } k > 0$$
$$\text{ii. } [a_0, a_1, \ldots, a_k] = c_k/d_k$$

Proof By induction. When $k = 1$,

$$a_0 + \frac{1}{a_1 + (1/\alpha)} = \frac{a_0a_1 + (a_0/\alpha) + 1}{a_1 + (1/\alpha)} = \frac{\alpha a_0a_1 + \alpha + a_0}{\alpha a_1 + 1} \qquad (30)$$

and

$$\frac{\alpha c_1 + c_0}{\alpha d_1 + d_0} = \frac{\alpha(a_0a_1 + 1) + a_0}{\alpha a_1 + 1} = \frac{\alpha a_0a_1 + \alpha + a_0}{\alpha a_1 + 1} \qquad (31)$$

For $k > 1$, $[a_0, \ldots, a_{k+1}, \alpha] = [a_0, \ldots, a_k, a_{k+1} + 1/\alpha]$

$$\begin{aligned}\frac{[a_{k+1} + (1/\alpha)]c_k + c_{k-1}}{[a_{k+1} + (1/\alpha)]d_k + d_{k-1}} &= \frac{a_{k+1}c_k + (1/\alpha)c_k + c_{k-1}}{a_{k+1}d_k + (1/\alpha)d_k + d_{k-1}}\\ &= \frac{\alpha(a_{k+1}c_k + c_{k-1}) + c_k}{\alpha(a_{k+1}d_k + d_{k-1}) + d_k} = \frac{\alpha c_{k+1} + c_k}{\alpha d_{k+1} + d_k}\end{aligned} \qquad (32)$$

Theorem 34 For $k > 0$,

1. $c_kd_{k+1} - c_{k+1}d_k = (-1)^{k+1}$
2. GCD$(c_k, d_k) = 1$
3. if $k > 0$ then $d_{k+1} > d_k$, so $d_k \geq k$
4. $c_0/d_0 < c_2/d_2 < c_{2k}/d_{2k} \cdots < c_{2k+1}/d_{2k+1} < \cdots < c_1/d_1$
5. all simple continued fractions converge.

Proof

1. Using the definition, $c_0d_1 - c_1d_0 = -1$; $c_kd_{k+1} - c_{k+1}d_k = -(c_{k-1}d_k - c_kd_{k-1})$. Use induction to complete the proof.
2. This follows from (i).
3. Again use the definition and induction, since $a_k \geq 1$, $\forall k$.
4. Substitute a_{k+1} for α in Theorem 33, to conclude that $a_{k+1} \geq 1$, c_{k+2}/d_{k+2} lies between c_k/d_k and c_{k+1}/d_{k+1}. But $c_0/d_0 < c_1/d_1$, so $c_0/d_0 < c_2/d_2 < c_1/d_1$. Prove the general result by induction.
5. By (i) and (iv), $\{c_k/d_k\}$ is a Cauchy sequence, and so converges.

Theorem 35 α is a rational number $\Leftrightarrow$ it has a finite continued fraction representation.

Proof Clearly if all the entries of a finite continued fraction are integers, then α is rational. On the other hand, if α is rational and can be expressed as s/t, we have $s/t = q_1 + 1/(t/r_1)$ if $r_1 > 0$, by the Euclidean algorithm and dividing by t. We can continue this process, next dividing (t/r_1), with the next remainder r_2, r_1. The process will eventually terminate, and the result is the desired continued fraction.

Example Consider $\alpha = 326/89$. Then,

$$\frac{326}{89} = 3 + \frac{79}{89} = 3 + \frac{1}{\frac{89}{79}} = 3 + \frac{1}{1 + \frac{1}{\frac{79}{10}}}$$

$$= \cdots = 3 + \cfrac{1}{1 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{9}}}}$$

Theorem 36 Let α be an irrational number. Then

1. $\lim_{n \to \infty} c_k/d_k = \alpha$.
2. $|\alpha - c_k/d_k| < 1/d_kd_{k+1} < 1/d^2_k$.

It can also be shown that continued fraction representations are unique.

For example, we can show that

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, \ldots]\text{: } \sqrt{2}]$$
$$= [1, 2, 2, 2, 2, \ldots]\text{: and } (1 + \sqrt{5})/2 = [1, 1, 1, 1, \ldots]$$

Two other interesting results follow.

Theorem 37 The continued fraction representation of α is eventually periodic $\Leftrightarrow$ α is a quadratic number, that is it solves a quadratic polynomial equation with rational coefficients.

Theorem 38 (Khinchin) $[a_0, a_1, a_2, \ldots]$ converges $\Leftrightarrow$ $\Sigma^{\infty}{}_{i=0}\, a_i$ diverges.

ALGEBRAIC AND TRANSCENDENTAL NUMBERS

Continuing in this theme, the study of number theory has also been concerned with discovering real (and complex) numbers that satisfy polynomial equations with coefficients that are algebraic numbers.

A complex number $c \in \mathbb{C}$, which is the solution of an equation $q_nc^n + q_{n-1}c^{n-1} + \cdots + q_1c + q_0 = 0$, where $q_0, \ldots, q_n \in \mathbb{Q}$, is called an *algebraic number.* If all the $q_0, \ldots, q_n \in \mathbb{Z}$, then c is called an *algebraic integer.*

Then, numbers that do not satisfy any such polynomial equation are called *transcendental.* In some ways, the transcendental numbers are the most intractable.

There is quite a lengthy history of research in number theory just to establish that several well-known numbers are transcendental. For example, it is known that if $\alpha \neq 0$ or 1 and is an algebraic number, then the following are transcendental:

$\pi, e^{\alpha}, \sin\alpha, \cos\alpha, \tan\alpha, \sinh\alpha, \cosh\alpha, \arcsin\alpha, \arccos\alpha, \ln\alpha$

However, it is unknown as to whether or not $e + \pi$, for example, is transcendental.

A major result in the theory of transcendental numbers is the Gelfond–Schneider theorem.

Theorem 39 (Gelfond–Schneider) If α and β are algebraic numbers, and $\alpha \neq 0$ or 1, and β is irrational, then α^{β} is transcendental.

PARTITIONS

We have been considering various questions arising from the properties of the ordinary arithmetic operators in the classical number systems. Within the natural numbers, another question of interest, for a natural number n, in how many ways can we find sums that will add to n?

Any such sum is called a *partition* of n, and the counting function that determines the number of such partitions is usually called $p(n)$. This function is one that, alas, does not admit to convenient algebraic properties. It is also one that grows very quickly. For example, although $p(5) = 7$, $p(10) = 42$, $p(15) = 176$, and $p(20) = 627$.

For S any subset of $\mathbb{N}$, $S \subseteqq \mathbb{N}$, let S' be the set of all partitions with parts only in S; and let S'_m be the set of those partitions in which no part is used more than m times. Further, let N' be the set of all partitions, and N'_1 the set of all partitions with no number repeated. Also, let $p(S', n)$ be the number of partitions of n with all summands in S.

Also, for any infinite sequence $\{a_0, a_1, a_2, \ldots\}$, let the power series $f(q) = \Sigma^{\infty}{}_{i=0}\, a_iq^i$ be called the generating function for the sequence $\{a_0, a_1, a_2, \ldots\}$.

Theorem 40 Let $S \subseteqq \mathbb{N}$, $m > 0$, and f and f_m be given by

$$f(q) = \sum_{i=0}^{\infty} p(S', i)q^i: \qquad f_m(q) = \sum_{i=0}^{\infty} p(S'_m, i)q^i$$

Then

$$f(q) = \prod_{i \in S} (1 - q^i)^{-1}$$

$$f_m(q) = \prod_{i \in H} (1 - q^{(m+1i})/(1 - q^i)$$

Proof We will ignore issues of convergence, which can be demonstrated. Consider

$$\prod_{n \in S} (1 - q^n)^{-1} = \prod_{n \in S} (1 + q^n + q^{2n} + \cdots + q^{kn} + \cdots) \\ = \sum{}^* q^{x1h1 + \cdots + xkhk} \tag{33}$$

where h_1, h_2, ... is an enumeration of H, and the sum is over all finite sequences of nonnegative x_i. q^n occurs each time $n = x_1h_1 + \cdots + x_kh_k \Rightarrow n$ has a partition in S'. Also each partition of n with parts in S will occur as an exponent in Σ^*. Thus

$$\prod_{i \in S} (1 - q^i)^{-1}: = \sum_{i=0}^{\infty} p(S'_m, i)q^i \tag{34}$$

and similarly for the other result.

Theorem 41 (Euler) Let O denote the set of odd positive integers, then

$$p(O', n) = \mathrm{p}(N'_1, n)$$

Proof

$$\sum_{i=0}^{\infty} p(O', i)q^i = \prod_{i=1}^{\infty} (1 - q^{2i-1})^{-1} \tag{35}$$

and

$$\sum_{i=0}^{\infty} p(N'_1, i)q^i = \prod_{i=1}^{\infty} (1 + q^i) \tag{36}$$

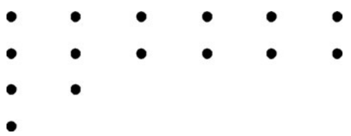
because

$$\prod_{i=1}^{\infty} (1 + q^i) = \prod_{i=1}^{\infty} (1 - q^{2i})/(1 - q^i) = \prod_{i=1}^{\infty} [1/(1 - q^{2i-1})] \tag{37}$$

We have the result.

Graphical Representation

Each partition of a number can be represented by a series of dots representing the summands. For example (ordering the summands in descending order), the partition of 15 given by 6 + 6 + 2 + 1 can be represented by



This dot pattern can be reflected along its diagonal; alternatively, it can be viewed vertically instead of horizontally, giving the partition 4 + 3 + 2 + 2 + 2 + 2. These two partitions are called conjugate.

Theorem 42 The number of partitions of n with at most m parts is equal to the number of partitions of m in which no part exceeds m.

Proof Consider the conjugates.

Next, we cite Euler's pentagonal number theorem, which gives an algorithm for enumerating $p(n)$. [A pentagonal number is one of the form $m(3m + 1)/2$ or $m(3m - 1)/2$.]

Theorem 43 Let $p_1(S, n)$ [respectively, $p_2(H, n)$] denote the number of partitions of n in H with an odd (respectively, even) number of parts. Then,

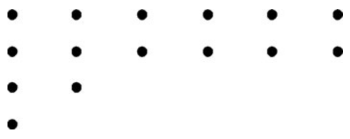
$$p_2(N_1, n) - p_1(N_1, n) = \begin{cases} (-1)^n & \text{if } n = r(3r \pm 1)/2 \\ 0 & \text{otherwise} \end{cases}$$

Proof Let a be a partition of n into r parts, $n = a_1 + \cdots + a_r$, with $a_i > a_{i+1}$ for all i. Let $s(a) = a_r$ (the smallest part); $t(a)$ the largest integer c. ∋. $a_1 = a_2 + 1, a_2 = a_3 + 1, \ldots, a_{c-1} = a_c + 1$; and let $t(a) = 1$ if $a_1 \neq a_2 + 1$.

CASE 1 $s(a) \leq t(a)$. Take a, add one to the first $s(a)$ parts, and delete the last part, yielding

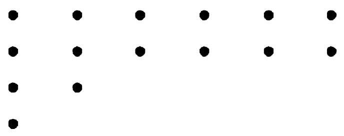
$$(a_1 + 1) + \cdots + (a_{s(a)} + 1) + a_{s(a)+1} + \cdots + a_{r-1} \tag{38}$$

Graphically,



CASE 2 $s(a) > t(a)$. Take a, subtract one from each of the first $t(a)$ parts, and add the new part $t(a)$. Then the new partition is

$$(a_1 + 1) + \cdots + (a_{t(a)} - 1) + a_{t(a)+1} + \cdots + a_r + t(a)$$



(39)

Because $a_{t(a)} - 1 > a_{t(a)} + 1$, $a_r > t(a)$, this is a partition into distinct parts.

These two cases provide a one-to-one correspondence between the partitions enumerated by $p_1(N_1, n)$ and $p_2(N_1, n)$, except in the following cases:

1. $s(a) = t(a) = r$ when

$$n = (2r-1) + (2r-2) + \cdots + r = r(3r-1)/2$$

and

2. $s(a) = t(a) + 1 = r + 1$ when

$$n = 2r + (2r-1) + \cdots + (r+1) = r(3r+1)/2$$

Theorem 44 (Euler Pentagonal Number Theorem) For $0 < q < 1$,

$$\prod_{n=1}^{\infty}(1-q^n) = 1 + \sum_{m=1}^{\infty}(-1)^m q^{m(3m-1)/2}(1+q^m)$$
$$= \sum_{m=-\infty}^{\infty}(-1)^m q^{m(3m-1)/2}$$

Proof

$$\sum_{m=-\infty}^{\infty}(-1)^m q^{m(3m-1)/2}$$
$$= 1 + \sum_{m=1}^{\infty}(-1)^m[q^{m(3m-1)/2} + q^{m(3m+1)/2}] \qquad (40)$$
$$= \sum_{n=0}^{\infty}[p_2(S'_1, n) - p_1(S'_1, n)]q^n$$

Also, as in Theorem 40,

$$\prod_{n=1}^{\infty}(1-q^n) = \sum{}^*(-1)^{a1+a2+\cdots}q^{a1+2a2+\cdots} \qquad (41)$$

$a_1 + 2a_2 + 3a_3 + \cdots$ is a partition into distinct parts, with an (odd) even number of parts $\Leftrightarrow$ $(-1)a_1 + \cdots + a_{\mathrm{k}} = -1$ (1, respectively); thus combining Eqs. (77) and (41),

$$\prod_{n=1}^{\infty}(1-q^n) = \sum_{n=1}^{\infty}(p_2(S'_1, n) - p_1(S'_1, n))q^n \qquad (42)$$

Theorem 45 If $n > 0$ then

$$p(n) - p(n-1) - p(n-2) + \cdots + (-1)^m p(n - m(3m-1)/2$$
$$+ (-1)^m p(n - m(3m+1)/2) + \cdots = 0$$

A further extension of the Euler Pentagonal Number Theorem follows.

Theorem 46 Let $N_{\mathrm{j},k}$ denote the set of all partitions with distinct parts in which each part is congruent to $-j$, 0, or j modulo $2k+1$. Then,

$$p_2(N_{j,k}, n) - p_1(N_{j,k}, n)$$
$$= (-1)^m \begin{cases} \text{for } n = [(2k \pm 1)m(m+1) \pm 2jm]/2 \\ 0 \quad \text{otherwise} \end{cases}$$

One of Ramanujan's remarkable results follows.

Theorem 47 $p(5n+4) \equiv 0 \pmod 5$.

Another important family of identities are the Rogers–Ramanujan identities.

Theorem 48 (Rogers–Ramanujan) The number of partitions of n with minimal difference 2 is equal to the number of partitions of the form $5m + 1$ and $5m + 4$, equivalently:

$$\prod_{n=0}^{\infty}\frac{1}{(1-x^{5n+1})(1-x^{5n+4})} = \sum_{n=1}^{\infty}\frac{x^{n^2}}{(1-x)(1-x^2)\cdots(1-x^n)}$$

Also, the number of partitions of n with parts not less than 2, and with minimal difference 2, is equal to the number of partitions of the form $5m + 2$ and $5m + 3$. Alternatively,

$$\prod_{n=0}^{\infty}\frac{1}{(1-x^{5n+2})(1-x^{5n+3})} = \sum_{n=1}^{\infty}\frac{x^{n(n+1)}}{(1-x)(1-x^2)\cdots(1-x^n)}$$

A further estimate on the size of the function $p(n)$ follows.

Theorem 49 For all $n > 1$,

$$2^{\sqrt{n}} < p(n) < e^{\pi\sqrt{(2n/3)}}$$

PRIME NUMBERS

The primes themselves have been a subject of much inquiry in number theory. We have seen earlier that there are an infinite number of primes, and that they are most useful in finite fields from modular arithmetic systems.

One subject of interest has been the development of a function to approximate the frequency of occurrence of primes. This function is usually called $\pi(n)$—it denotes the number of primes less than or equal to n.

In addition to establishing various estimates for $\pi(n)$, concluding with the so-called *Prime Number Theorem,* we will also state a number of famous unproven conjectures involving prime numbers.

An early estimate for $\pi(n)$, by Chebyshev, follows.

Theorem 50 (Chebyshev) If $n > 1$, then $n/(8 \log n) < \pi(n) < 6n/(\log n)$.

The Chebyshev result tells us that, up to a constant factor, the number of primes is of the order of $n/(\log n)$. In addition to the frequency of occurrence of primes, the greatest gap between successive primes is also of interest.

Theorem 51 (Bertrand's Partition) If $n \geq 2$, there is a prime p between n and $2n$.

Two other estimates for series of primes follow.

Theorem 52 $\Sigma_{p \le n} \log p/p = \log n + O(1)$.

Theorem 53 $\Sigma_{p \le n} 1/p = \log \log x + a + O(1/\log x)$.

Another very remarkable result involving the generation of primes is due to Dirichlet.

Theorem 54 (Dirichlet) Let a and b be fixed positive integers such that GCD(a,b) = 1. Then there are an infinite number of primes in the sequence $\{a + bn | n = 1, 2, \ldots\}$.

Finally, we have the best known approximation to the number of primes.

Theorem 55 (Prime Number Theorem) $\pi(n) \sim n/(\log n)$.

The conjectures involving prime numbers are legion, and even some of the simplest ones have proven elusive for mathematicians. A few examples are the Goldbach conjecture, the twin primes conjecture, the interval problem, the Dirichlet series problem, and the Riemann hypothesis.

Twin Primes Two primes p and q are called twins if $q = p + 2$. Examples are $(p, q) = (5,7); (11, 13); (17, 19); (521, 523)$. If $\pi_2(n)$ counts the number of twin primes less than n, the twin prime conjecture is that $\pi_2(n) \to \infty$ as $n \to \infty$. It is known, however, that there are infinitely many pairs of numbers (p, q), where p is prime, $q = p + 2$, and q has at most two factors.

Goldbach Conjecture Stated earlier, this conjecture is that every even number is the sum of two primes. What is known is that every large even number can be expressed as $p + q$ where p is prime and q has at most two factors. Also, it is known that every large odd integer is the sum of three primes.

Interval Problems It was stated earlier that there is always a prime number between n and $2n$. It is not known, however, whether the same is true for other intervals, for example such as n^2 and $(n + 1)^2$.

Dirichlet Series In Theorem 54, a series containing an infinite number of primes was demonstrated. It was not known if there are other series that have a greater frequency of prime occurrences, at least until recent research by Friedlander and Iwaniec, who showed that series of the form $\{a^2 + b^4\}$ not only have an infinite number of primes, but also that they occur more rapidly than in the Dirichlet series.

Riemann Hypothesis Although the connection to prime numbers is not immediately apparent, the Riemann hypothesis has been an extremely important pillar in the theory of primes. It states that, for the complex function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \qquad s = \sigma + it \in \mathbb{C}$$

there are zeros at $s = -2, -4, -6, \ldots$, and no more zeros outside of the [critical strip] $0 \le \sigma \le 1$. The Riemann hypothesis states that all zeros of ζ in the critical strip lie on the line $s = 1/2 + it$.

Examples of important number-theoretic problems whose answer depends on the Riemann hypothesis are: (i) the existence of an algorithm to find a nonresidue mod p in polynomial time; (ii) if n is composite, there is at least one b for which neither $b^{\mathrm{t}} \equiv 1 \pmod{n}$ nor $b^{2^r t} \equiv -1 \pmod{n}$. This latter is important in algorithms needed to find large primes.

DIOPHANTINE EQUATIONS

The term *Diophantine equation* is used to apply to a family of algebraic equations in a number system such as $\mathbb{Z}$ or $\mathbb{Q}$. To date, we have certainly seen many examples of Diophantine equations. A good deal of research in this subject has been directed at polynomial equations with integer or rational coefficients, the most famous of which being the class of equations $x^{\mathrm{n}} + y^{\mathrm{n}} = z^{\mathrm{n}}$, the subject of Fermat's Last Theorem.

One result in this study, due to Legendre, follows.

Theorem 56 Let $a, b, c \in \mathbb{Z}$ such that (i) $a > 0, b, c < 0$; (ii) a, b, and c are square-free; and (iii) GCD(a,b) = GCD(b,c) = GCD(a,c) = 1. Then

$$ax^2 + by^2 + cz^2 = 0$$

has a nontrivial integer solution ⇔

$$-ab \in \mathbf{QR}(c)$$
$$-bc \in \mathbf{QR}(a)$$
$$-ca \in \mathbf{QR}(b)$$

Example Consider the equation $3x^2 - 5y^2 - 7z^2 = 0$. With $a = 3, b = -5$, and $c = -7$, apply Theorem 56. Note that $ab \equiv 1 \pmod 7$, $ac \equiv 1 \pmod 5$, and $bc \equiv 1 \pmod 3$. Thus, all three products are quadratic residues, and the equation has an integer solution. Indeed, the reader may verify that $x = 3$, $y = 2$, and $z = 1$ is one such solution.

Another result, which, consequently, proves Fermat's Last Theorem in the case $n = 4$, follows. (Incidentally, it has also been long known that Fermat's Last Theorem holds for $n = 3$.)

Theorem 57 $x^4 + y^4 = z^2$ has no nontrivial solutions in the integers.

A final class of Diophantine equations is known generically as Mordell's equation: $y^2 = x^3 + k$. In general, solutions to Mordell's equation in the integers are not known. Two particular solutions follow.

Theorem 58 $y^2 = x^3 + m^2 - jn^2$ has no solution in the integers if

1. $j = 4$, $m \equiv 3 \pmod 4$ and $p \not\equiv 3 \pmod 4$ when $p|n$;

2. $j = 1, m \equiv 2 \pmod 4$, n is odd, and $p \not\equiv 3 \pmod 4$ when $p|n$.

Theorem 59 $y^2 = x^3 + 2a^3 - 3b^2$ has no solution in the integers if $ab \neq 0$, $a \not\equiv 1 \pmod 3$, $3 \nmid b$, a is odd if b is even, and $p = t^2 + 27u^2$ is soluble in integers t and u if $p|a$ and $p \equiv 1 \pmod 3$.

ELLIPTIC CURVES

Many of the recent developments in number theory have come as the by-product of the extensive research done in a branch of mathematics known as elliptic curve theory.

An elliptic curve represents the set of points in some appropriate number system that are the solutions to an equation of the form $y2z = x^3 + mxz^2 + nz^3$ when $m, n \in \mathbb{Z}$.

A major result in this theory is the theorem of Mordell and Weil. If K is any algebraic field, and $C(K)$ are the points with rational coordinates on an elliptic curve, then this object $C(K)$ forms a finitely generated Abelian group.

APPLICATIONS

To this point, all of our discussion has centered around the basic ideas in the development of number theory. We will conclude with three important and recent applications of this very pure mathematical theory in areas of enormous importance for business, government, engineering, and computing. These three areas are: (i) public-key cryptology (for secure computer network development); (ii) digital signatures and authentication (for electronic funds transfer and indeed all electronic communications requiring authentication); and (iii) multiple-radix arithmetic or residue number systems (for signal processing, error correction, and fault tolerance in computer and communications systems design).

Public-Key Cryptology

Despite other applications of number theory that have been discussed in recent years, there can be no doubt that the area of greatest application has been in the field of public-key cryptology.

Cryptology, literally the science of secret writing or code-making and code-breaking, is probably as old as writing itself. For much of its history, cryptology has been the province of the military forces of the world—and mathematical puzzlers. Only since the dawn of the computer era have the techniques involved in cryptology moved from simple mathematics involving permutations to the sophisticated approaches we now see in the computer era.

The fundamental model for any cryptologic system can be described as consisting of M, the message space, or set of finite strings defined over some alphabet; C, the ciphertext space, a set of finite strings over some (possibly different) alphabet; K, the key space, another set of finite strings over a possible third alphabet; and a family of invertible transformations, one for each $k \in K$, $t_k: M \to C$. All the security of the system must lie in the specific choice of key k.

A familiar form of simple cryptosystem is the one whose examples can often be found in daily newspapers under the heading "cryptogram." In this cryptosystem, the alphabet consists of the 26 letters of the Roman alphabet $\Sigma = \{a, b, c, \ldots, z\}$. M, the message space, is the set of all strings over Σ, as is C. Finally, the set $\{t_k\}$ consists of keys which are defined by all of the permutations of the 26 objects which are the symbols of Σ. Thus, $|\{t_k\}| = 26!$

This system is not very secure—otherwise it would not be very appealing as a challenge to daily newspaper readers—and the main technique in breaking this system arises from the knowledge that certain letters in English language text occur far more frequently than others.

A method devised in the early 1970s by Feistel at IBM and code named "Lucifer" evolved into what is now known as the Data Encryption Standard (*DES*). The DES is based on a complicated set of permutations and transpositions. In short, its formal description uses the alphabet $\Sigma = \{0,1\}$; the message space M_{64} consists of 64-bit strings, as does the ciphertext space C_{64}; the key space K_{56} consists of all 56-bit strings; and each t_k, for $k \in K_{56}$, is a composition of 18 transformations, $t_k = \mathrm{IP}^{-1} \circ T_{16} \circ T_{15} \circ \cdots \circ T_1 \circ \mathrm{IP}$, each of which maps 64-bit strings to 64-bit strings; and the individual components T^i depend on the specific choice of $k \in K_{56}$.

Although the DES has been the backbone of commercial data encryption for over 20 years, it has not been without detractors even from the time of its creation and adoption as a national standard.

The Public-Key Paradigm. For any number of reasons, the modern view of cryptology has indicated that the model that we have been using for cryptography has numerous weaknesses.

Historically, cryptology required that both the sending and the receiving parties possessed exactly the same information about the cryptosystem. Consequently, that information that they both must possess must be communicated in some way.

The Key Management Problem. Envision the development of a computer network consisting of one thousand subscribers where each pair of users requires a separate key for private communication. (It might be instructive to think of the complete graph on n vertices, representing the users; with the $n(n - 1)/2$ edges corresponding to the need for key exchanges. Thus in the 1000-user network, approximately 500,000 keys must be exchanged in some way, other than by the network!)

In considering this problem, Diffie and Hellman asked the following question: Is it possible to consider that a key might be broken into two parts, $k = (k_p, k_s)$, such that only kp is necessary for encryption, while the entire key $k = (k_p, k_s)$ would be necessary for decryption?

If it were possible to devise such a cryptosystem, then the following benefits would accrue. First of all, because the information necessary for encryption does not, a priori, provide an attacker with enough information to decrypt, then there is no longer any reason to keep it secret. Consequently, k_p can be made public to all users of the network. A cryptosystem devised in this way is called a public-key cryptosystem (or *PKC*).

Furthermore, the key distribution problem becomes much more manageable. Consider the hypothetical network of 1000 users, as before. For each user, choose a key $k_{\mathrm{i}} = (k_{\mathrm{p}i}, k_{\mathrm{s}i})$, $i = 1, \ldots, 1000$. In a system-wide public directory, list all of the "public" keys $k_{\mathrm{p}i}$, $i = 1, \ldots, 1000$. Then, to send a message m to user j, select the public key, k_{pi}, and apply the encryption transformation $c = T(k_{\mathrm{pi}}, m)$. Send the ciphertext c.

Only user *j* has the rest of the key necessary to compute $T[(k_{\mathrm{p}}, k_{\mathrm{s}}), c] = m$.

Thus, rather than having to manage the secret distribution of $O(n^2)$ keys in a network of n users, only n keys are required, and they need not be distributed secretly.

Therefore, if we could devise a PKC, it would certainly have most desirable features. But many questions remain to be asked. First of all, can we devise a PKC? What should we look for? Second, if we can find one, will it be secure? Will it be efficient?

In 1978, Rivest, Shamir, and Adelman described a public-key cryptosystem based on principles of number theory, with the security being dependent upon the inherent difficulty of factoring large integers.

Factoring. How hard is factoring numbers in any case? The method most often encountered in elementary courses relies upon generating all the prime numbers up to the square root of the number to be factored, using, for example, the Sieve of Eratosthenes.

If the number we sought to factor contained, let us say, 200 digits, then we would need to be able to generate all the prime numbers of $\leq$ 100 digits.

Then we would have to test each of these prime numbers for factorization. The direct approach will be $O(n)$, which is infeasible to compute when n is a 200-digit number.

The best general-purpose factoring algorithm is called the *number field sieve*. Its runtime is approximately $\mathrm{O}(\mathrm{e}^{1.9(\ln n)^{1/3}(\ln \ln \mathrm{n})^{2/3}})$, where n is the size of the number being factored.

In part to maintain momentum in factoring research, the security company RSA Security has issued various monetary challenges for the solution of selected factoring problems. The eight numbers in the challenge range from 174 to 617 decimal digits, and the prizes range from US$10,000 to US$200,000. The first six of the eight challenge numbers have been factored.

Rivest–Shamir–Adelman Algorithm. The basic idea of Rivest, Shamir, and Adelman (*RSA*) was to take two large prime numbers, p and q (for example, p and q each being $\sim 10^{100}$) and to multiply them together to obtain $n = pq$. n is published. Furthermore, two other numbers, d and e, are generated, where d is chosen randomly, but relatively prime to the Euler function, $\phi(n)$, in the interval $[\max(p, q) + 1, n - 1]$. As we have seen, $\phi(n) = (p - 1)(q - 1)$.

Key Generation.

1. Choose two 100-digit prime numbers randomly from the set of all 100-digit prime numbers. Call these p and q.
2. Compute the product $n = pq$.
3. Choose d randomly in the interval $[\max(p, q) + 1, n - 1]$, such that $\mathrm{GCD}[d, \phi(n)] = 1$.
4. Compute $e \equiv d^{-1}$ [modulo $\phi(n)$].
5. Publish n and e. Keep p, q and d secret.

Encryption.

1. Divide the message into blocks such that the bit-string of the message can be viewed as a 200-digit number. Call each block m.
2. Compute and send $c \equiv m^{\mathrm{e}}$ (modulo n).

Decryption. Compute

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\phi(n)+1} \equiv$$
$$m^{k\phi(n)} \times m \equiv 1 \times m \equiv m \quad (\text{modulo}\, n)$$

Note that the result $m^{\mathrm{k}\phi(n)} \equiv 1$ used in the preceding line is the Little Fermat Theorem.

Although the proof of the correctness and the security of RSA are established, there are a number of questions about the computational efficiency of RSA that should be raised.

1. Is it possible to find prime numbers of 200 decimal digits in a reasonable period of time?

   The Prime Number Theorem 55 assures us that after a few hundred random selections, we will probably find a prime of 200 digits.

   We can never actually be certain that we have a prime without knowing the answer to the Riemann hypothesis; instead we create a test (the Solovay–Strassen test), which, if the prime candidate passes, we assume the probability that p is not a prime is very low. We choose a number (say 100) numbers a_{i} at random, which must be relatively prime to p. For each a_{i}, if the Legendre symbol

   $$\begin{pmatrix} a \\ p \end{pmatrix} = a_i^{(p-1)/2} (\text{mod } p)$$

   then the chance that p is not a prime and passes the test is 1/2 in each case; if p passes all tests, the chances are $1/2^{100}$ that it is not prime.
2. Is it possible to find an e which is relatively prime to $\phi(n)$?

   Computing the $\mathrm{GCD}[e, \phi(n)]$ is relatively fast, as is computing the inverse of e mod n. Here is an example of a (3×2) array computation which determines both GCD and inverse. In each successive column $(k + 1)$, subtract the largest multiple m of column k less than the first row entry of column $(k - 1)$ to form the new column. When 0 is reached in the first row, both the inverse (if it exists) and the GCD are found.

m			4	4	1	2	17
$A[1,\bullet]$	1024	243	52	35	17	1	0
$A[2,\bullet]$	1	0	1	4	5	−14	
$A[3,\bullet]$	0	1	−4	17	−21	59	

Once $A[1, \bullet]$ becomes zero, the GCD is at $A[1, \bullet -1]$, and if it is 1, the desired inverse is the value of $A[3, \bullet -1]$, that is 59.

3. Is it possible to perform the computation $e \times d$ where e and d are themselves 200-digit numbers?

   Computing $m^e \pmod{n}$ consists of repeated multiplications and integer divisions. In Mathematica version 3.0, running on a Pentium machine, such a computation with 400-digit integers was done in 1.59 s.

   One shortcut in computing a large exponent is to use the "fast exponentiation" algorithm. Express the exponent as a binary, $e = b_n b_{n-1} \cdots b_0$. Then compute m^e as follows:

   ```
   ans = $m$

   for $i = n - 1$ to 0 do ans = ans × ans if $b_i = 1$ then ans = ans × $x$ end;
   ```

   The result is ans. Note that the total number of multiplies is proportional to the log of e.

Example Compute x^{123}.

$$123 = (1111011)_{\text{binary}}$$

So $n = 6$.

$$\begin{aligned}
& \text{ans} = x \\
i = 5 \quad & \text{ans} = \text{ans} \times \text{ans} \times (1 \times x) = x \times x \times x = x^3 \\
i = 4 \quad & \text{ans} = \text{ans} \times \text{ans} \times (1 \times x) = x^3 \times x^3 \times x = x^7 \\
i = 3 \quad & \text{ans} = \text{ans} \times \text{ans} \times (1 \times x) = x^7 \times x^7 \times x = x^{15} \\
i = 2 \quad & \text{ans} = \text{ans} \times \text{ans} \times (1 \times x) = x^{15} \times x^{15} \times x = x^{31} \\
i = 1 \quad & \text{ans} = \text{ans} \times \text{ans} = x^{31} \times x^{31} = x^{62} \\
i = 0 \quad & \text{ans} = \text{ans} \times \text{ans} \times (1 \times x) = x^{62} \times x^{62} \times x = x^{123}
\end{aligned}$$

In a practical version of the RSA algorithm, it is recommended by Rivest, Shamir, and Adelman that the primes p and q be chosen to be approximately of the same size, and each containing about 100 digits.

The other calculations necessary in the development of an RSA cryptosystem have been shown to be relatively rapid. Except for finding the primes, the key generation consists of two multiplications, two additions, one selection of a random number, and the computation of one inverse modulo another number.

The encryption and decryption each require is at most $2 \log_2 n$ multiplications (in other words, one application of the Fast Exponentiation algorithm) for each message block.

Digital Signatures

It seems likely that, in the future, an application similar to public-key cryptology will be even more widely used. With vastly expanded electronic communications, the requirements for providing a secure way of authenticating an electronic message will be required far more often than the requirement for transmitting information in a secure fashion.

As with public-key cryptology, the principles of number theory have been essential in establishing methods of authentication.

The authentication problem follows. Given a message m, is it possible for a user u to create a "signature," s_u, dependent on some information possessed only by u, so that the recipient of the message (m, s_u) could use some public information for u (a public key), to be able to determine whether or not the message was authentic.

Rivest, Shamir, and Adelman showed that their public-key encryption method could also be used for authentication. However, a number of other authors, particularly El Gamal and Ong–Schnorr–Shamir, developed more efficient solutions to the signature problem. More recently, in 1994, the National Institute for Standards and Technology, an agency of the US government, established such a method as a national standard, now called the *DSS* or Digital Signature Standard.

The DSS specifies an algorithm to be used in cases where a digital authentication of information is required. We assume that a message m is received by a user. The objective is to verify that the message has not been altered and that we can be assured of the originator's identity. The DSS creates for each user a public and a private key. The private key is used to generate signatures, and the public key is used in verifying signatures.

A DSS system begins with

1. The identification of a prime p, with $2^{N-1} < p < 2^N$, for $512 \leq N \leq 1024$, and N is a multiple of 64.
2. q, a prime number, is chosen, such that $q|(p-1)$, with $2^{159} < q < 2^{160}$.
3. $g \equiv h^{(p-1)/q} \pmod{p}$, is computed, where h is any integer such that $1 < h < p - 1$ and $h^{(p-1)/q} \pmod{p} > 1$; that is, g has order q mod p.
4. x is a randomly or pseudorandomly generated integer with $0 < x < q$.
5. $y \equiv g^x \pmod{p}$.
6. k is a randomly or pseudorandomly generated integer with $0 < k < g$.

p, q, and g can be public and common to a group of users. A user's private and public keys are x and y, respectively. In addition to x, k is also kept secret.

Signature Generation. For any message m, of arbitrary bit length, the signature of m is a triple, (m, r, s), where

$$r = (g^k \bmod p) \bmod q$$
$$s = k^{-1}[H(m) + xr)] \bmod q$$

where k^{-1} is the inverse of k mod q, and $H(m)$ is a 160-bit string computed by H, a secure hash algorithm. Note that r and s will each be 160 bits. Thus the length of (m, r, s) is 320 bits more than the length of m.

Signature Verification. If the received message is denoted (m', r', s'), then the verification proceeds as follows:

1. If $r' \leq 0$ or $r' \geq q$, then reject.
2. If $s' \leq 0$ or $s' \geq q$, then reject.
3. If (i) and (ii) are satisfied, then compute:

$$\begin{aligned} w &= (s')^{-1} \pmod q \\ u1 &= [H(m')w] \pmod q \\ u2 &= [r'w] \pmod q \\ v &= [(g^{u1}y^{u2}) \bmod p] \bmod q \end{aligned}$$

If $v = r'$, then the signature is verified; otherwise, the message should be considered invalid.

Proof of Correctness. If $m = m'$, $r = r'$, and $s = s'$, we need to show that $v = r$. First establish that with p, q, g, h as given,

$$\begin{aligned} g^q &\equiv (h^{(p-1/q})^q \equiv h^{p-1} \equiv 1 \pmod p \\ g^{m1} &\equiv g^{m2+1q} \equiv g^{m2}g^{1q} \equiv g^{m2} \pmod p \text{ by Eq. (43)} \end{aligned} \tag{43}$$

Now $y \equiv g^{x} \pmod p$, so by the Eq. (96)

$$\begin{aligned} v &= [(g^{u1}y^{u2}) \bmod p] \bmod q \equiv (g^{H(m)w}y^{rw} \bmod p) \bmod q \\ &\equiv [(g^{H(m)w}g^{xrw}) \bmod p] \bmod q \equiv (g^{H(m)w+xrw} \bmod p) \bmod q \end{aligned} \tag{44}$$

But $s \equiv [k^{-1}(H(m) + xr)] \pmod q$, and since $q = s^{-1}$, $w \equiv k[H(m) + xr]^{-1} \pmod q$. Then, by substitution in Eq. (97), obtain

$$v = (g^k \bmod p) \bmod q = r, \text{ by definition}$$

Secure Hash Function. The definition of a secure hash function, H, is that it is a function with the following properties:

1. H is a mapping of the set of all bit strings (in the DSS standard, limited to bitstrings of length, 2^{64}) to the set of all bit strings of length 160.
2. For any bitstring b, of length 160, it is computationally infeasible to find a message m such that $H(m) = b$.
3. It is computationally infeasible to find two distinct messages m, m' such that $H(m) = H(\mathrm{m}')$.

The secure hash function most commonly used in DSS is called SHA-1 or secure hash algorithm 1.

Security. Suppose a forger wants to forge a message, that is, alter the value of m, r, or s by the requirements of H, it will not be feasible to find another message m' such that $H(m) = H(m')$. Thus the forger must create an authentic r' and s'. Although p, q, and g are public, and r is transmitted, to solve $[(r = g^{k}) \bmod p] \bmod q$ is a problem known as the discrete log problem. Its solution is essentially equivalent to the problem of factoring large integers. Finally, because x is chosen at random and is kept secret, s is similarly infeasible to compute.

Despite the widespread use and acceptance of the Digital Signature Standard, in 2005 a number of efforts, led by Xiaoyun Wang, have seriously compromised major components of this United States federal standard. Dr. Wang has found "collisions" in the secure hash algorithm, SHA-1. A collision occurs when two different inputs hash to the same value. This could lead to the possibility of digital forgery. As of this writing, of the various secure Hash algorithm in the standard, SHA-0 is no longer felt to be secure. It may soon be joined by SHA-1. The remaining standards (SHA-224, SHA-256, SHA-384 and SHA-512) are considered secure, but their additional computational overhead would seem to lead to additional cost factors in the use of the DSS.

Multiple-Radix Arithmetic or Residue Number Systems

A final application of elementary number theory is the use of multiple-radix arithmetic or *MRA* systems, which is also known as residue number systems or *RNS*. Recall from the discussion of the Chinese Remainder Theorem 16 that for every product of distinct primes p_{i} (or, more generally, products of distinct numbers that are pairwise relatively prime) there is a one-to-one correspondence that preserves addition and multiplication between the subset of the integers defined by $[0, P - 1]$, where $P = \Pi\, p_{\mathrm{i}}$ and the product of rings $\mathbb{Z}_{\mathrm{p}1} \times \cdots \times \mathbb{Z}_{\mathrm{p}n}$, where the operation in this latter system is componentwise.

There are a growing number of applications where the rapid computation of $a \times b \pmod n$ or of $a^{\mathrm{b}} \pmod n$ is important. In addition to cryptology and signatures as described earlier, this computation is useful in digital signal processing as well.

On the assumption that a and b consist of n decimal digits, the number of one-digit multiplies represented by the normal multiplication algorithm is n^2. Although certain methods, such as the Karatsubo method, can reduce the algorithm to the order of n^{1+k}, for $k < 1$, this is still costly for large n.

Multiplication in an MRA or RNS system is $O(n)$. Consequently, this approach is very attractive in all the areas mentioned previously. Indeed, as we enter an era of more widespread parallel and distributed computing, an even more appealing use of MRA or RNS is to consider distributing large numbers, using their MRA representation, over many processors, with each processor P_{i} only required to perform those parts of the computation related to prime p_{i}.

There has been one barrier to the use of this computational method. Although $m \pm n$ and $m \times n$ are computationally efficient in MRA, it was thought that the computation of m mod n, or integer division of m by n, was essentially as costly as ordinary long division. However, some recent research of Abdelguerfi–Dunham–Patterson, and others has established a fast division algorithm.

To solve problems of computing A mod N in an MRA system, assume first that N is fixed. Furthermore, assume that $N^2 < P$. Then any product AB will be $< P$. We precompute

$$e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0) \quad f_i = e_i/P \in \mathbb{Q}$$
$$g_i = e_i (\mathrm{mod}\ N) h_i = g_i/N \in \mathbb{Q}$$

Also, precompute (P mod N)/N.

Let $A \rightarrow (a_1, a_2, \ldots, a_\mathrm{m})$ in the MRA system. Then

$$\begin{array}{ll} \sum a_i e_i = hP + a & (\in \mathbb{Z}) \\ \sum a_i f_i = h + (A/P) & (\in \mathbb{Q}) \end{array}$$

Therefore, $h = \Sigma\, a_\mathrm{i} f_\mathrm{i} - (A/P)$ = floor [$\Sigma\, a_\mathrm{i} f_\mathrm{i}$], where floor[ ] = greatest integer less than. Also,

$$\begin{array}{ll} \sum a_i e_i = hP + A (\in \mathbb{Z}) \Rightarrow & \\ \sum a_i (e_i \mathrm{mod} N) = h(P \mathrm{mod} N) + kN + Y & (0 \le Y < N) \Rightarrow \\ \sum a_i g_i /N = h(P \mathrm{mod} N)/N + k + Y/N & (\in \mathbb{Q}) \end{array}$$

Thus k = floor[$\Sigma\, a_\mathrm{i} h_\mathrm{I} - h(P \bmod N) - kN$].

After computing k, substitute to obtain $Y = \Sigma\, a_\mathrm{i} g_\mathrm{i} - h(P \bmod N) + kN$ in MRA. Because $Y < N$, and $X \equiv Y$ (mod N), the remainder is Y.

Example Use the system (p_1, p_2, p_3, p_4) = (7, 11, 13, 17); P = 17017.

Compute 395 mod 42. In the MRA system, this is (3, 10, 5, 4) mod (0, 9, 3, 8).

$$\begin{array}{llll} e_1 = 9724 & e_2 = 12376 & e_3 = 3927 & e_4 = 8008 \\ f_1 = 0.5714 & f_2 = 0.7273 & f_3 = 0.2308 & f_4 = 0.4706 \\ g_1 = 9724 \mathrm{mod}\, 42 & g_2 = 28 & g_3 = 21 & g_4 = 28 \\ \quad = 22 & & & \\ h_1 = 0.5238 & h_2 = 0.6667 & h_3 = 0.5000 & h_4 = 0.6667 \\ P \mathrm{mod} N = 7 & (P \mathrm{mod} N)/N = 0.1667 & & \end{array}$$

Then, h = floor[3 × 0.5714 + 10 × 0.7273 + 5 × 0.2308 + 4 × 0.4706] = 12; and k = floor[3 × 0.5238 + 10 × 0.6667 + 5 × 0.5000 + 4 × 0.6667 − 12 × 0.1667 − Y/N] = 11; therefore, 3 × (1,0,9,5) + 10 × (0,6,2,11) + 5 × (0,10,8,4) + 4 × (0,6,2,11) = 12 × (7,7,7,7) + 11 × (0,9,3,8) + Y, and so Y = (3,6,4,0). If one needed the standard form, one could note that Y in standard form is 17, as (17 mod 7, 17 mod 11, 17 mod 13, 17 mod 17) = 3, 6, 4, 0).

BIBLIOGRAPHY

Most of the references in this section discuss most of the topics contained in the main body of this article.

W. W. Adams L. J. Goldstein *Introduction to Number Theory*, Englewood Cliffs, NJ: Prentice-Hall, 1976.

A. Adler J. E. Coury *The Theory of Numbers: A Text and Source Book of Problems*, Boston: Jones and Bartlett, 1995.

W. S. Anglin *The Queen of Mathematics: An Introduction to Number Theory*, Boston: Kluwer, 1995.

A. Baker *A Concise Introduction to the Theory of Numbers*, Cambridge: Cambridge Univ. Press, 1984.

D. M. Burton *Elementary Number Theory*, New York: McGraw-Hill, 1998.

H. Cohen *A Second Course in Number Theory*, New York: Wiley, 1962.

L. E. Dickson *A History of the Theory of Numbers*, 3 Vols, Washington: Carnegie Inst., 1919–1923.

G. H. Hardy E. M. Wright *An Introduction to the Theory of Numbers*, 3rd ed., Oxford: Clarendon Press, 1954.

K. Ireland M. Rosen *A Classical Introduction to Modern Number Theory*, 2nd ed., New York: Springer-Verlag, 1990.

D. E. Flath *Introduction to Number Theory*, New York: Wiley, 1989.

R. K. Guy *Unsolved Problems in Number Theory*, New York: Springer-Verlag, 1994.

N. Koblitz *A Course in Number Theory and Cryptography*, New York: Springer-Verlag, 1994.

I. Niven H. S. Zuckerman *An Introduction to the Theory of Numbers*, 4th ed., New York: Wiley, 1991.

H. E. Rose *A Course in Number Theory*, Oxford: Oxford Univ. Press, 1988.

H. N. Shapiro *Introduction to the Theory of Numbers*, New York: Wiley-Interscience, 1983.

H. Stark *An Introduction to Number Theory*, Chicago: Markham, 1970.

Specialized references on Fermat's Last Theorem, elliptic curve theory, research on Dirichlet-like series, and Mersenne numbers can be found in these references.

C. K. Caldwell The Great Internet Mersenne Prime Search [Online]. Available www:http://www.utm.edu/research/primes/mersenne.shtml

J. Friedlander H. Iwaniec Using a parity-sensitive sieve to count prime values of a polynomial, *Proc. Natl. Acad. Sci. USA*, **94**: 1054–1058, 1997.

Great Internet Mersenne Prime Search, http://www.mersenne.org/.

N. Koblitz *Introduction to Elliptic Curves and Modular Forms*, New York: Springer-Verlag, 1984.

A. Wiles Modular elliptic curves and Fermat's last theorm, *Ann. Math.*, **141** (3): 443–551, 1995.

Mathematical software systems particularly useful in computational number theory are Maple and mathematica.

B. W. Char *et al.* Maple V language reference manual, New York: Springer-Verlag, 1991.

S. Wolfram *Mathematica: A system for doing mathematics by computer*, Redwood City, CA: Addison-Wesley, 1991.

References to Public-key cryptology and factoring include the following.

J. P. Buhler, H. W. Lenstra, and C. Pomerance, *The development of the number field sieve, Volume 1554 of Lecture Notes in Computer Science*, Springer-Verlag, 1994.

J. Buchmann, J. Loho, and J. Zayer, An implementation of the general number field sieve, *Advances in Cryptology - Crypto '93*, Springer-Verlag, 1994. 159–166.

W. Diffie M. E. Hellman New directions in cryptography, *IEEE Trans. Inf. Theory*, **IT-22**: 644–654, 1976.

H. Feistel Cryptography and computer privacy, *Scientific American*, **228** (5): 15–23, 1973.

National Bureau of Standards, Data Encryption Standard, FIPS PUB 46, January 1977.

W. Patterson *Mathematical Cryptology*, Totowa, NJ: Rowman and Littlefield, 1987.

R. L. Rivest A. Shamir L. Adelman A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, **21** (2): 120–126, 1978.

RSA Laboratories, The RSA Factoring Challenge, http://www.rsasecurity.com/rsalabs/node.asp?id=2092.

B. Schneier *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, New York: Wiley, 1994.

J. Seberry J. Pieprzyk *Cryptography: An Introduction to Computer Security*, New York: Prentice-Hall, 1989.

R. Solovay V. Strassen Fast Monte-Carlo tests for primality, *SIAM J. Comput.*, **6** (1): 84–85, 1977.

D. R. Stinson *Cryptography: Theory and and practice*, Boca Raton, FL: CRC Press, 1995.

The following references discuss the issues concerning digital signatures and their standards.

T. ElGamal A public key cryptosystem and a signature scheme based on discrete logarithms, Proc. Crypto 84, New York: Springer, 1985, pp. 10–18.

National Institute for Standards and Technology, Digital Signature Standard (DSS), Federal Inf. Processing Standards Publ. 186, May 19, 1994.

H. Ong C. P. Schnorr A. Shamir An efficient signature scheme based on polynomial equations, Proc. Crypto 84, New York: Springer, 1985, pp. 37–46.

X. Wang, Y. L. Yin and H. Yu, Finding Collisions in the Full SHA-1,*Advances in Cryptology, CRYPTO '05*, Springer-Verlag(2005),pp. 17–36.

And these references address multiple-radix arithmetic and residue number systems.

M. Abdelguerfi A. Dunham W. Patterson MRA: A computational technique for security in high-performance systems, Proc. IFIP/Sec '93, Internation Federation Inf. Processing Soc., World Symp. Comput. Security 1993, 1993, pp. 381–397.

G. Davida B. Litow Fast parallel arithmetic via modular representation, *SIAM J. Comput.*, **20** (4): 756–765, 1991.

M. A. Hitz E. Kaltofen Integer division in residue number systems, *IEEE Trans. Comput.*, **44**: 983–989, 1995.

H. Krishna *et al. Computational Number Theory and Digital Signal Processing: Fast Algorithms and Error Control Techniques*, Boca Raton, FL: CRC Press, 1994.

K. C. Posch R. Posch Modulo reduction in residue number systems, *IEEE Trans. Parallel Distrib. Syst.*, **6**: 449–454, 1995.

WAYNE PATTERSON
Howard University and the
National Science
Foundation, Washington, DC