Chapter 14
Partitions

Historical Introduction

The theory of numbers is that branch of mathematics which deals with properties of the whole numbers,

$$1, 2, 3, 4, 5, \ldots$$

also called the *counting numbers*, or *positive integers*.

The positive integers are undoubtedly man's first mathematical creation. It is hardly possible to imagine human beings without the ability to count, at least within a limited range. Historical record shows that as early as 3500 BC the ancient Sumerians kept a calendar, so they must have developed some form of arithmetic.

By 2500 BC the Sumerians had developed a number system using 60 as a base. This was passed on to the Babylonians, who became highly skilled calculators. Babylonian clay tablets containing elaborate mathematical tables have been found, dating back to 2000 BC.

When ancient civilizations reached a level which provided leisure time to ponder about things, some people began to speculate about the nature and properties of numbers. This curiosity developed into a sort of number-mysticism or numerology, and even today numbers such as 3, 7, 11, and 13 are considered omens of good or bad luck.

Numbers were used for keeping records and for commercial transactions for over 2000 years before anyone thought of studying numbers themselves in a systematic way. The first scientific approach to the study of integers, that is, the true origin of the theory of numbers, is generally attributed to the Greeks. Around 600 BC Pythagoras and his disciples made rather thorough studies of the integers. They were the first to classify integers in various ways:

Even numbers: 2, 4, 6, 8, 10, 12, 14, 16, . . .
Odd numbers: 1, 3, 5, 7, 9, 11, 13, 15, . . .
Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, . . .
Composite numbers: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, . . .

A *prime number* is a number greater than 1 whose only divisors are 1 and the number itself. Numbers that are not prime are called *composite*, except that the number 1 is considered neither prime nor composite.

The Pythagoreans also linked numbers with geometry. They introduced the idea of *polygonal numbers*: triangular numbers, square numbers, pentagonal numbers, etc. The reason for this geometrical nomenclature is clear when the numbers are represented by dots arranged in the form of triangles, squares, pentagons, etc., as shown in Figure I.1.

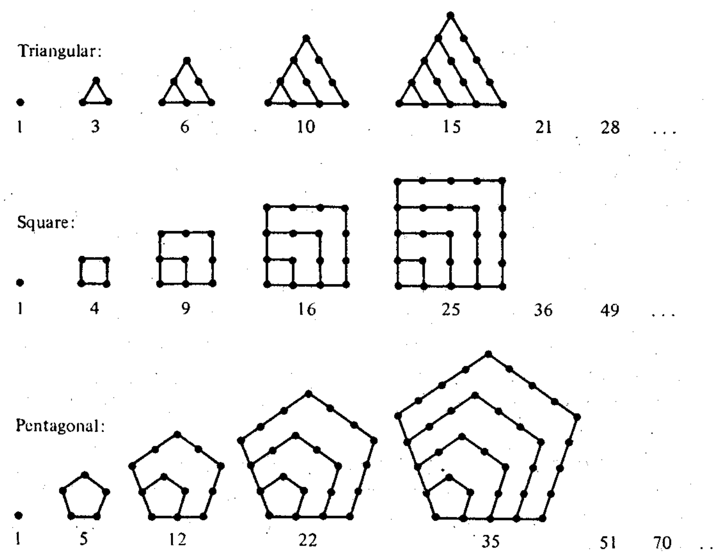

Figure I.1

Another link with geometry came from the famous Theorem of Pythagoras which states that in any right triangle the square of the length of the hypotenuse is the sum of the squares of the lengths of the two legs (see Figure I.2). The Pythagoreans were interested in right triangles whose sides are integers, as in Figure I.3. Such triangles are now called *Pythagorean triangles.* The corresponding triple of numbers (x, y, z) representing the lengths of the sides is called a *Pythagorean triple.*

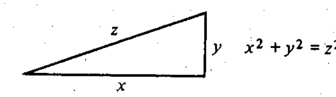

Figure I.2

A Babylonian tablet has been found, dating from about 1700 BC, which contains an extensive list of Pythagorean triples, some of the numbers being quite large. The Pythagoreans were the first to give a method for determining infinitely many triples. In modern notation it can be described as follows: Let n be any odd number greater than 1, and let

$$x = n, \qquad y = \tfrac{1}{2}(n^2 - 1), \qquad z = \tfrac{1}{2}(n^2 + 1).$$

The resulting triple (x, y, z) will always be a Pythagorean triple with $z = y + 1$. Here are some examples:

x	3	5	7	9	11	13	15	17	19
y	4	12	24	40	60	84	112	144	180
z	5	13	25	41	61	85	113	145	181

There are other Pythagorean triples besides these; for example:

x	8	12	16	20
y	15	35	63	99
z	17	37	65	101

In these examples we have $z = y + 2$. Plato (430–349 BC) found a method for determining all these triples; in modern notation they are given by the formulas

$$x = 4n, \qquad y = 4n^2 - 1, \qquad z = 4n^2 + 1.$$

Around 300 BC an important event occurred in the history of mathematics. The appearance of Euclid's *Elements*, a collection of 13 books, transformed mathematics from numerology into a deductive science. Euclid was the first to present mathematical facts along with rigorous proofs of these facts.

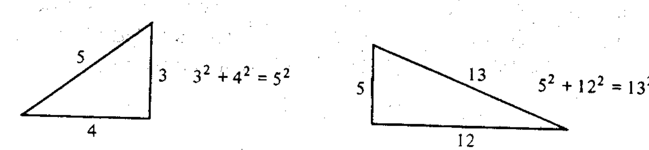

Figure I.3

Three of the thirteen books were devoted to the theory of numbers (Books VII, IX, and X). In Book IX Euclid proved that there are infinitely many primes. His proof is still taught in the classroom today. In Book X he gave a method for obtaining all Pythagorean triples although he gave no proof that his method did, indeed, give them all. The method can be summarized by the formulas

$$x = t(a^2 - b^2), \qquad y = 2tab, \qquad z = t(a^2 + b^2),$$

where t, a, and b, are arbitrary positive integers such that $a > b$, a and b have no prime factors in common, and one of a or b is odd, the other even.

Euclid also made an important contribution to another problem posed by the Pythagoreans—that of finding all perfect numbers. The number 6 was called a perfect number because $6 = 1 + 2 + 3$, the sum of all its proper divisors (that is, the sum of all divisors less than 6). Another example of a perfect number is 28 because $28 = 1 + 2 + 4 + 7 + 14$, and 1, 2, 4, 7, and 14 are the divisors of 28 less than 28. The Greeks referred to the proper divisors of a number as its "parts." They called 6 and 28 perfect numbers because in each case the number is equal to the sum of all its parts.

In Book IX, Euclid found all *even* perfect numbers. He proved that an even number is perfect if it has the form

$$2^{p-1}(2^p - 1),$$

where both p and $2^p - 1$ are primes.

Two thousand years later, Euler proved the converse of Euclid's theorem. That is, every even perfect number must be of Euclid's type. For example, for 6 and 28 we have

$$6 = 2^{2-1}(2^2 - 1) = 2 \cdot 3 \qquad \text{and } 28 = 2^{3-1}(2^3 - 1) = 4 \cdot 7.$$

The first five even perfect numbers are

$$6, 28, 496, 8128 \qquad \text{and } 33{,}550{,}336.$$

Perfect numbers are very rare indeed. At the present time (1983) only 29 perfect numbers are known. They correspond to the following values of p in Euclid's formula:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11,213, 19,937, 21,701, 23,209, 44,497, 86,243, 132,049

Numbers of the form $2^p - 1$, where p is prime, are now called *Mersenne numbers* and are denoted by M_p in honor of Mersenne, who studied them in 1644. It is known that M_p is prime for the 29 primes listed above and composite for all values of $p < 44{,}497$. For the following primes,

$$p = 137, 139, 149, 199, 227, 257$$

although M_p is composite, no prime factor of M_p is known.

No *odd* perfect numbers are known; it is not even known if any exist. But if any do exist they must be very large; in fact, greater than 10^{50} (see Hagis [29]).

We turn now to a brief description of the history of the theory of numbers since Euclid's time.

After Euclid in 300 BC no significant advances were made in number theory until about AD 250 when another Greek mathematician, Diophantus of Alexandria, published 13 books, six of which have been preserved. This was the first Greek work to make systematic use of algebraic symbols. Although his algebraic notation seems awkward by present-day standards, Diophantus was able to solve certain algebraic equations involving two or three unknowns. Many of his problems originated from number theory and it was natural for him to seek *integer* solutions of equations. Equations to be solved with integer values of the unknowns are now called *Diophantine equations*, and the study of such equations is known as *Diophantine analysis*. The equation $x^2 + y^2 = z^2$ for Pythagorean triples is an example of a Diophantine equation.

After Diophantus, not much progress was made in the theory of numbers until the seventeenth century, although there is some evidence that the subject began to flourish in the Far East—especially in India—in the period between AD 500 and AD 1200.

In the seventeenth century the subject was revived in Western Europe, largely through the efforts of a remarkable French mathematician, Pierre de Fermat (1601–1665), who is generally acknowledged to be the father of modern number theory. Fermat derived much of his inspiration from the works of Diophantus. He was the first to discover really deep properties of the integers. For example, Fermat proved the following surprising theorems:

Every integer is either a triangular number or a sum of 2 *or* 3 *triangular numbers; every integer is either a square or a sum of* 2, 3, *or* 4 *squares; every integer is either a pentagonal number or the sum of* 2, 3, 4, *or* 5 *pentagonal numbers*, and so on.

Fermat also discovered that every prime number of the form $4n + 1$ such as 5, 13, 17, 29, 37, 41, etc., is a sum of two squares. For example,

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2,$$
$$37 = 1^2 + 6^2, \quad 41 = 4^2 + 5^2.$$

Shortly after Fermat's time, the names of Euler (1707–1783), Lagrange (1736–1813), Legendre (1752–1833), Gauss (1777–1855), and Dirichlet (1805–1859) became prominent in the further development of the subject. The first textbook in number theory was published by Legendre in 1798. Three years later Gauss published *Disquisitiones Arithmeticae*, a book which transformed the subject into a systematic and beautiful science. Although he made a wealth of contributions to other branches of mathematics, as well as to other sciences, Gauss himself considered his book on number theory to be his greatest work.

In the last hundred years or so since Gauss's time there has been an intensive development of the subject in many different directions. It would be impossible to give in a few pages a fair cross-section of the types of problems that are studied in the theory of numbers. The field is vast and some parts require a profound knowledge of higher mathematics. Nevertheless, there are many problems in number theory which are very easy to state. Some of these deal with prime numbers, and we devote the rest of this introduction to such problems.

The primes less than 100 have been listed above. A table listing all primes less than 10 million was published in 1914 by an American mathematician, D. N. Lehmer [43]. There are exactly 664,579 primes less than 10 million, or about $6\frac{1}{2}\%$. More recently D. H. Lehmer (the son of D. N. Lehmer) calculated the total number of primes less than 10 billion; there are exactly 455,052,511 such primes, or about $4\frac{1}{2}\%$, although not all these primes are known individually (see Lehmer [41]).

A close examination of a table of primes reveals that they are distributed in a very irregular fashion. The tables show long gaps between primes. For example, the prime 370,261 is followed by 111 composite numbers. There are no primes between 20,831,323 and 20,831,533. It is easy to prove that arbitrarily large gaps between prime numbers must eventually occur.

On the other hand, the tables indicate that consecutive primes, such as 3 and 5, or 101 and 103, keep recurring. Such pairs of primes which differ only by 2 are known as *twin primes*. There are over 1000 such pairs below 100,000 and over 8000 below 1,000,000. The largest pair known to date (see Williams and Zarnke [76]) is $76 \cdot 3^{139} - 1$ and $76 \cdot 3^{139} + 1$. Many mathematicians think there are infinitely many such pairs, but no one has been able to prove this as yet.

One of the reasons for this irregularity in distribution of primes is that no simple formula exists for producing all the primes. Some formulas do yield many primes. For example, the expression

$$x^2 - x + 41$$

gives a prime for $x = 0, 1, 2, \ldots, 40$, whereas

$$x^2 - 79x + 1601$$

gives a prime for $x = 0, 1, 2, \ldots, 79$. However, no such simple formula can give a prime for all x, even if cubes and higher powers are used. In fact, in 1752 Goldbach proved that no polynomial in x with integer coefficients can be prime for all x, or even for all sufficiently large x.

Some polynomials represent infinitely many primes. For example, as x runs through the integers 0, 1, 2, 3, ..., the linear polynomial

$$2x + 1$$

gives all the odd numbers hence infinitely many primes. Also, each of the polynomials

$$4x + 1 \quad \text{and} \quad 4x + 3$$

represents infinitely many primes. In a famous memoir [15] published in 1837, Dirichlet proved that, if a and b are positive integers with no prime factor in common, the polynomial

$$ax + b$$

gives infinitely many primes as x runs through all the positive integers. This result is now known as Dirichlet's theorem on the existence of primes in a given arithmetical progression.

To prove this theorem, Dirichlet went outside the realm of integers and introduced tools of analysis such as limits and continuity. By so doing he laid the foundations for a new branch of mathematics called *analytic number theory*, in which ideas and methods of real and complex analysis are brought to bear on problems about the integers.

It is not known if there is any quadratic polynomial $ax^2 + bx + c$ with $a \neq 0$ which represents infinitely many primes. However, Dirichlet [16] used his powerful analytic methods to prove that, if a, $2b$, and c have no prime factor in common, the quadratic polynomial in two variables

$$ax^2 + 2bxy + cy^2$$

represents infinitely many primes as x and y run through the positive integers.

Fermat thought that the formula $2^{2^n} + 1$ would always give a prime for $n = 0, 1, 2, \ldots$ These numbers are called *Fermat numbers* and are denoted by F_n. The first five are

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257 \quad \text{and } F_4 = 65{,}537,$$

and they are all primes. However, in 1732 Euler found that F_5 is composite; in fact,

$$F_5 = 2^{32} + 1 = (641)(6{,}700{,}417).$$

These numbers are also of interest in plane geometry. Gauss proved that if F_n is a prime, say $F_n = p$, then a regular polygon of p sides can be constructed with straightedge and compass.

Beyond F_5, *no further Fermat primes have been found*. In fact, for $5 \leq n \leq 19$ each Fermat number F_n is composite. Also, F_n is known to be composite for the following further isolated values of n:

n = 21, 23, 25, 26, 27, 29, 30, 32, 36, 38, 39, 42, 52, 55, 58, 62, 63, 66, 71, 73, 77, 81, 91, 93, 99, 117, 125, 144, 147, 150, 201, 207, 215, 226, 228, 250, 255, 267, 268, 284, 287, 298, 316, 329, 416, 452, 544, 556, 692, 744, 1551, 1945, 2023, 2456, 3310, 4724, and 6537.

(See Robinson [59] and Wrathall [77]. More recent work is described in Gostin and McLaughlin, *Math. Comp.* 38 (1982), 645–649.)

It was mentioned earlier that there is no simple formula that gives all the primes. In this connection, we should mention a result discovered recently by Davis, Matijasevič, Putnam and Robinson. They have shown how to construct a polynomial $P(x_1, \ldots, x_k)$, all of whose positive values are primes for nonnegative integer values of $x_1, \ldots, x_k$ and for which the positive values run through all the primes but the negative values are composite. (See Jones, Sata, Wada and Wiens, *Amer. Math. Monthly* 83 (1976), 449–65 for references.)

The foregoing results illustrate the irregularity of the distribution of the prime numbers. However, by examining large blocks of primes one finds that their average distribution seems to be quite regular. Although there is no end to the primes, they become more widely spaced, on the average, as we go further and further in the table. The question of the diminishing frequency of primes was the subject of much speculation in the early nineteenth century. To study this distribution, we consider a function, denoted by $\pi(x)$, which counts the number of primes $\leq x$. Thus,

$$\pi(x) = \text{the number of primes } p \text{ satisfying } 2 \leq p \leq x.$$

Here is a brief table of this function and its comparison with $x/\log x$, where $\log x$ is the natural logarithm of x.

x	$\pi(x)$	$x/\log x$	$\pi(x) \Big/ \dfrac{x}{\log x}$
10	4	4.3	0.93
10^2	25	21.7	1.15
10^3	168	144.8	1.16
10^4	1,229	1,086	1.13
10^5	9,592	8,686	1.10
10^6	78,498	72,382	1.08
10^7	664,579	620,420	1.07
10^8	5,761,455	5,428,681	1.06
10^9	50,847,534	48,254,942	1.05
10^{10}	455,052,511	434,294,482	1.048

By examining a table like this for $x \leq 10^6$, Gauss [24] and Legendre [40] proposed independently that for large x the ratio

$$\pi(x) \Big/ \frac{x}{\log x}$$

was nearly 1 and they conjectured that this ratio would approach 1 as x approaches ∞. Both Gauss and Legendre attempted to prove this statement but did not succeed. The problem of deciding the truth or falsehood of this

conjecture attracted the attention of eminent mathematicians for nearly 100 years.

In 1851 the Russian mathematician Chebyshev [9] made an important step forward by proving that *if* the ratio did tend to a limit, then this limit must be 1. However he was unable to prove that the ratio *does* tend to a limit.

In 1859 Riemann [58] attacked the problem with analytic methods, using a formula discovered by Euler in 1737 which relates the prime numbers to the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for real $s > 1$. Riemann considered complex values of s and outlined an ingenious method for connecting the distribution of primes to properties of the function $\zeta(s)$. The mathematics needed to justify all the details of his method had not been fully developed and Riemann was unable to completely settle the problem before his death in 1866.

Thirty years later the necessary analytic tools were at hand and in 1896 J. Hadamard [28] and C. J. de la Vallée Poussin [71] independently and almost simultaneously succeeded in proving that

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$$

This remarkable result is called the *prime number theorem*, and its proof was one of the crowning achievements of analytic number theory.

In 1949, two contemporary mathematicians, Atle Selberg [62] and Paul Erdös [19] caused a sensation in the mathematical world when they discovered an elementary proof of the prime number theorem. Their proof, though very intricate, makes no use of $\zeta(s)$ nor of complex function theory and in principle is accessible to anyone familiar with elementary calculus.

One of the most famous problems concerning prime numbers is the so-called *Goldbach conjecture*. In 1742, Goldbach [26] wrote to Euler suggesting that every even number ≥ 4 is a sum of two primes. For example

$$4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 3 + 5,$$
$$10 = 3 + 7 = 5 + 5, \quad 12 = 5 + 7.$$

This conjecture is undecided to this day, although in recent years some progress has been made to indicate that it is probably true. Now why do mathematicians think it is *probably* true if they haven't been able to prove it? First of all, the conjecture has been verified by actual computation for all even numbers less than 33×10^6. It has been found that every even number greater than 6 and less than 33×10^6 is, in fact, not only the sum of two odd primes but the sum of two *distinct* odd primes (see Shen [66]). But in number theory verification of a few thousand cases is not enough evidence to convince mathematicians that something is *probably* true. For example, all the odd primes fall into two categories, those of the form $4n + 1$ and those of the form $4n + 3$. Let $\pi_1(x)$ denote all the primes $\leq x$ that are of the form $4n + 1$, and let $\pi_3(x)$ denote the number that are of the form $4n + 3$. It is known that there are infinitely many primes of both types. By computation it was found that $\pi_1(x) \leq \pi_3(x)$ for all $x < 26{,}861$. But in 1957, J. Leech [39] found that for $x = 26{,}861$ we have $\pi_1(x) = 1473$ and $\pi_3(x) = 1472$, so the inequality was reversed. In 1914, Littlewood [49] proved that this inequality reverses back and forth infinitely often. That is, there are infinitely many x for which $\pi_1(x) < \pi_3(x)$ and also infinitely many x for which $\pi_3(x) < \pi_1(x)$. Conjectures about prime numbers can be erroneous even if they are verified by computation in thousands of cases.

Therefore, the fact that Goldbach's conjecture has been verified for all even numbers less than 33×10^6 is only a tiny bit of evidence in its favor.

Another way that mathematicians collect evidence about the truth of a particular conjecture is by proving other theorems which are somewhat similar to the conjecture. For example, in 1930 the Russian mathematician Schnirelmann [61] proved that there is a number M such that every number n from some point on is a sum of M or fewer primes:

$$n = p_1 + p_2 + \cdots + p_M \qquad \text{(for sufficiently large } n\text{).}$$

If we knew that M were equal to 2 for all even n, this would prove Goldbach's conjecture for all sufficiently large n. In 1956 the Chinese mathematician Yin Wen-Lin [78] proved that $M \leq 18$. That is, every number n from some point on is a sum of 18 or fewer primes. Schnirelmann's result is considered a giant step toward a proof of Goldbach's conjecture. It was the first real progress made on this problem in nearly 200 years.

A much closer approach to a solution of Goldbach's problem was made in 1937 by another Russian mathematician, I. M. Vinogradov [73], who proved that from some point on every *odd* number is the sum of *three* primes:

$$n = p_1 + p_2 + p_3 \qquad (n \text{ odd, } n \text{ sufficiently large}).$$

In fact, this is true for all odd n greater than $3^{3^{15}}$ (see Borodzkin [5]). To date, this is the strongest piece of evidence in favor of Goldbach's conjecture. For one thing, it is easy to prove that Vinogradov's theorem is a consequence of Goldbach's statement. That is, if Goldbach's conjecture is true, then it is easy to deduce Vinogradov's statement. The big achievement of Vinogradov was that he was able to prove his result without using Goldbach's statement. Unfortunately, no one has been able to work it the other way around and prove Goldbach's statement from Vinogradov's.

Another piece of evidence in favor of Goldbach's conjecture was found in 1948 by the Hungarian mathematician Rényi [57] who proved that there is a number M such that every sufficiently large even number n can be written as a prime plus another number which has no more than M distinct prime factors:

$$n = p + A$$

where A has no more than M distinct prime factors (n even, n sufficiently large). If we knew that $M = 1$ then Goldbach's conjecture would be true for all sufficiently large n. In 1965 A. A. Buhštab [6] and A. I. Vinogradov [72] proved that $M \leq 3$, and in 1966 Chen Jing-run [10] proved that $M \leq 2$.

We conclude this introduction with a brief mention of some outstanding unsolved problems concerning prime numbers.

1. (Goldbach's problem). Is there an even number >2 which is not the sum of two primes?
2. Is there an even number >2 which is not the difference of two primes?
3. Are there infinitely many twin primes?
4. Are there infinitely many Mersenne primes, that is, primes of the form $2^p - 1$ where p is prime?
5. Are there infinitely many composite Mersenne numbers?
6. Are there infinitely many Fermat primes, that is, primes of the form $2^{2^n} + 1$?
7. Are there infinitely many composite Fermat numbers?
8. Are there infinitely many primes of the form $x^2 + 1$, where x is an integer? (It is known that there are infinitely many of the form $x^2 + y^2$, and of the form $x^2 + y^2 + 1$, and of the form $x^2 + y^2 + z^2 + 1$).
9. Are there infinitely many primes of the form $x^2 + k$, (k given)?
10. Does there always exist at least one prime between n^2 and $(n + 1)^2$ for every integer $n \geq 1$?
11. Does there always exist at least one prime between n^2 and $n^2 + n$ for every integer $n > 1$?
12. Are there infinitely many primes whose digits (in base 10) are all ones? (Here are two examples: 11 and 11,111,111,111,111,111,111,111.)

The professional mathematician is attracted to number theory because of the way all the weapons of modern mathematics can be brought to bear on its problems. As a matter of fact, many important branches of mathematics had their origin in number theory. For example, the early attempts to prove the prime number theorem stimulated the development of the theory of functions of a complex variable, especially the theory of entire functions. Attempts to prove that the Diophantine equation $x^n + y^n = z^n$ has no nontrivial solution if $n \geq 3$ (Fermat's conjecture) led to the development of algebraic number theory, one of the most active areas of modern mathematical research. Even though Fermat's conjecture is still undecided, this seems unimportant by comparison to the vast amount of valuable mathematics that has been created as a result of work on this conjecture. Another example is the theory of partitions which has been an important factor in the development of combinatorial analysis and in the study of modular functions.

There are hundreds of unsolved problems in number theory. New problems arise more rapidly than the old ones are solved, and many of the old ones have remained unsolved for centuries. As the mathematician Sierpinski once said, "... the progress of our knowledge of numbers is advanced not only by what we already know about them, but also by realizing what we yet do not know about them."

Note. Every serious student of number theory should become acquainted with Dickson's three-volume *History of the Theory of Numbers* [13], and LeVeque's six-volume *Reviews in Number Theory* [45]. Dickson's *History* gives an encyclopedic account of the entire literature of number theory up until 1918. LeVeque's volumes reproduce all the reviews in Volumes 1–44 of *Mathematical Reviews* (1940–1972) which bear directly on questions commonly regarded as part of number theory. These two valuable collections provide a history of virtually all important discoveries in number theory from antiquity until 1972.

1 The Fundamental Theorem of Arithmetic

1.1 Introduction

This chapter introduces basic concepts of elementary number theory such as divisibility, greatest common divisor, and prime and composite numbers. The principal results are Theorem 1.2, which establishes the existence of the greatest common divisor of any two integers, and Theorem 1.10 (the fundamental theorem of arithmetic), which shows that every integer greater than 1 can be represented as a product of prime factors in only one way (apart from the order of the factors). Many of the proofs make use of the following property of integers.

The principle of induction *If Q is a set of integers such that*

(a) $1 \in Q$,
(b) *$n \in Q$ implies $n + 1 \in Q$,*

then

(c) *all integers ≥ 1 belong to Q.*

There are, of course, alternate formulations of this principle. For example, in statement (a), the integer 1 can be replaced by any integer k, provided that the inequality ≥ 1 is replaced by $\geq k$ in (c). Also, (b) can be replaced by the statement $1, 2, 3, \ldots, n \in Q$ implies $(n + 1) \in Q$.

We assume that the reader is familiar with this principle and its use in proving theorems by induction. We also assume familiarity with the following principle, which is logically equivalent to the principle of induction.

The well-ordering principle *If A is a nonempty set of positive integers, then A contains a smallest member.*