3

Greek Number Theory

3.1 The Role of Number Theory

In Chapter 1 we saw that number theory has been important in mathematics for at least as long as geometry, and from a foundational point of view it may be more important. Despite this, number theory has never submitted to a systematic treatment like that undergone by elementary geometry in Euclid's *Elements*. At all stages in its development, number theory has had glaring gaps because of the intractability of elementary problems. Most of the really old unsolved problems in mathematics, in fact, are simple questions about the natural numbers $1, 2, 3, \ldots$. The nonexistence of a general method for solving Diophantine equations (Section 1.3) and the problem of identifying the primes of the form $2^{2^h} + 1$ (Section 2.3) have been noted. Other unsolved number theory problems will be mentioned in the sections that follow.

As a consequence, the role of number theory in the history of mathematics has been quite different from that of geometry. Geometry has played a stabilizing and unifying role, to the point of retarding further development at times and creating the popular impression that mathematics is a static subject. For those able to understand it, number theory has been a spur to progress and change. Only a minority of mathematicians have contributed to advances in number theory, but they include some of the greats—Diophantus, Fermat, Euler, Lagrange, and Gauss. This book stresses those advances in number theory that sprang from its deep connections with other parts of mathematics, particularly geometry, since these were the most significant for mathematics as a whole. Nevertheless, there are topics in number theory that are too interesting to ignore, even though they seem (at present) to be outside the mainstream. We discuss a few of them in the next section.

3.2 Polygonal, Prime, and Perfect Numbers

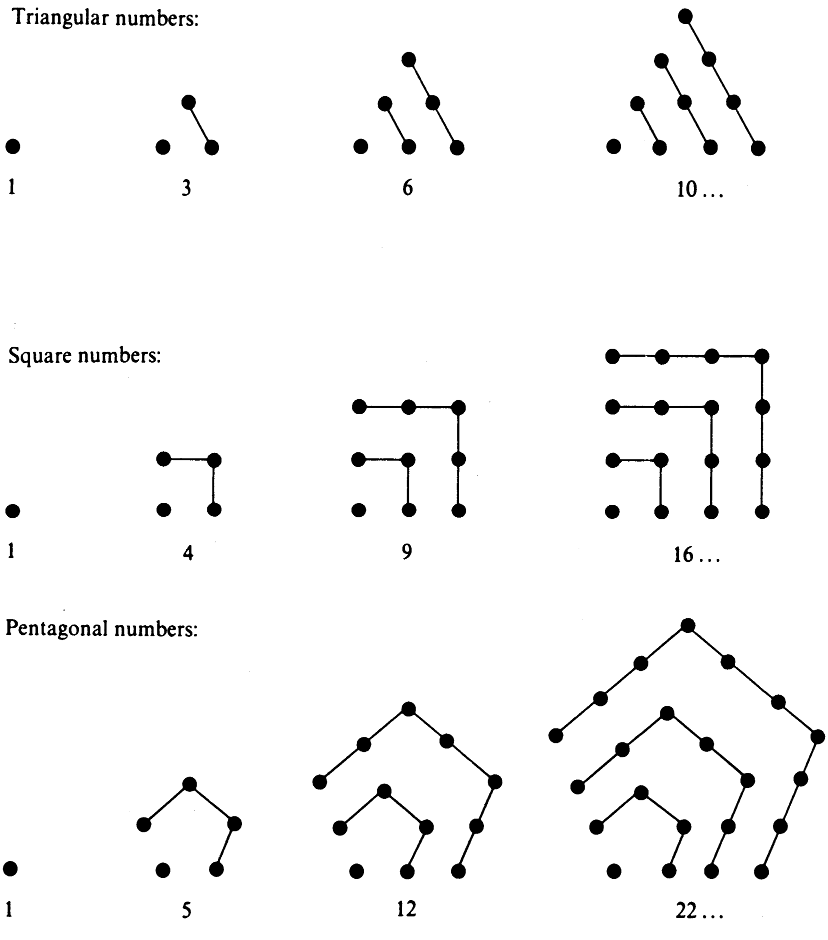

Figure 3.1: Polygonal numbers

The *polygonal numbers*, which were studied by the Pythagoreans, result from a naive transfer of geometric ideas to number theory. From Figure 3.1 it is an easy exercise to calculate an expression for the mth n-agonal number as the sum of a certain arithmetic series (Exercise 3.2.3) and to show, for example, that a square is the sum of two triangular numbers. Apart from Diophantus' work, which contains impressive results on sums of squares, Greek results on polygonal numbers were of this elementary type.

On the whole, the Greeks seem to have been mistaken in attaching much importance to polygonal numbers. There are no major theorems about them, except perhaps the following two. The first is the theorem conjectured by Bachet de Méziriac (1621) (in his edition of Diophantus' works) that every positive integer is the sum of four integer squares. This was proved by Lagrange (1770). A generalization, which Fermat (1670) stated without proof, is that every positive integer is the sum of n n-agonal numbers. This was proved by Cauchy (1813), though the proof is a bit of a letdown because all but four of the numbers can be 0 or 1. A short proof of Cauchy's theorem has been given by Nathanson (1987). The other remarkable theorem about polygonal numbers is the formula

$$\prod_{n=1}^{\infty}(1-x^n) = 1+\sum_{k=1}^{\infty}(-1)^k\left(x^{(3k^2-k)/2}+x^{(3k^2+k)/2}\right)$$

proved by Euler (1750) and known as Euler's pentagonal number theorem, since the exponents $(3k^2-k)/2$ are pentagonal numbers. [For a proof see Hall (1967), p. 33.]

(The four-square theorem and the pentagonal number theorem were both absorbed around 1830 into Jacobi's theory of theta functions, a much larger theory.)

The *prime numbers* were also considered within the geometric framework, as the numbers with no rectangular representation. A prime number, having no divisors apart from itself and 1, has only a "linear" representation. Of course this is no more than a restatement of the definition of prime, and most theorems about prime numbers require much more powerful ideas; however, the Greeks did come up with one gem. This is the proof that there are infinitely many primes, in Book IX of Euclid's *Elements*.

Given any finite collection of primes $p_1, p_2, \ldots, p_n$, we can find another by considering

$$p = p_1 p_2 \cdots p_n + 1.$$

This number is not divisible by $p_1, p_2, \ldots, p_n$ (each leaves remainder 1). Hence either p itself is a prime, and $p > p_1, p_2, \ldots, p_n$, or else it has a prime divisor $\neq p_1, p_2, \ldots, p_n$.

A *perfect number* is one that equals the sum of its divisors (including 1 but excluding itself). For example, $6 = 1+2+3$ is a perfect number, as is $28 = 1+2+4+7+14$. Although this concept goes back to the Pythagoreans, only two noteworthy theorems about perfect numbers are known. Euclid concludes Book IX of the *Elements* by proving that if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect (Exercise 3.2.5). These perfect numbers are of course even, and Euler (1849) (a posthumous publication) proved that every even perfect number is of Euclid's form. Euler's surprisingly simple proof may be found in Burton (1985), p. 504. It is not known whether there are any odd perfect numbers; this may be the oldest open problem in mathematics.

In view of Euler's theorem, the existence of even perfect numbers depends on the existence of primes of the form $2^n - 1$. These are known as Mersenne primes, after Marin Mersenne (1588–1648), who first drew attention to the problem of recognizing primes of this form. It is not known whether there are infinitely many Mersenne primes, though larger and larger ones seem to be found quite regularly. In recent years each new world-record prime has been a Mersenne prime, giving a corresponding world-record perfect number.

EXERCISES

Infinitely many natural numbers are not sums of three (or fewer) squares. The smallest of them is 7, and it can be shown as follows that no number of the form $8n+7$ is a sum of three squares.

3.2.1 Show that any square leaves remainder 0, 1, or 4 on division by 8.

3.2.2 Deduce that a sum of three squares leaves remainder 0, 1, 2, 3, 4, 5, or 6 on division by 8.

One reason polygonal numbers play only a small role in mathematics is that questions about them are basically questions about squares—hence the focus is on problems about squares.

3.2.3 Show that the k^{th} pentagonal number is $(3k^2 - k)/2$.

3.2.4 Show that each square is the sum of two consecutive triangular numbers.

Euclid's theorem about perfect numbers depends on the prime divisor property, which will be proved in the next section. Assuming this for the moment, it follows that if $2^n - 1$ is a prime p, then the proper divisors of $2^{n-1}p$ (those unequal to $2^{n-1}p$ itself) are

$$1, 2, 2^2, \ldots, 2^{n-1} \quad \text{and} \quad p, 2p, 2^2p \ldots, 2^{n-2}p.$$