Natural numbers and integers

Counting is presumably the origin of mathematical thought, and it is certainly the origin of difficult mathematical problems. As the great Hungarian problem-solver Paul Erdős liked to point out, if you can think of an open problem that is more than 200 years old, then it is probably a problem in number theory.

In recent decades, difficulties in number theory have actually become a virtue. Public key encryption, whose security depends on the difficulty of factoring large numbers, has become one of the commonest applications of mathematics in daily life.

At any rate, problems are the life blood of number theory, and the subject advances by building theories to make them understandable. In the present chapter we introduce some (not so difficult) problems that have played an important role in the development of number theory because they lead to basic methods and concepts.

- Counting leads to induction, the key to all facts about numbers, from banalities such as $a + b = b + a$ to the astonishing result of Euclid that there are infinitely many primes.
- Division (with remainder) is the key computational tool in Euclid’s proof and elsewhere in the study of primes.
- Binary notation, which also results from division with remainder, leads in turn to a method of “fast exponentiation” used in public key encryption.
- The Pythagorean equation $x^2 + y^2 = z^2$ from geometry is equally important in number theory because it has integer solutions.
In this chapter we are content to show these ideas at work in few interesting but seemingly random situations. Later chapters will develop the ideas in more depth, showing how they unify and explain a great many astonishing properties of numbers.

1.1 Natural numbers

Number theory starts with the natural numbers

\[ 1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots, \]

generated from 1 by successively adding 1. We denote the set of natural numbers by \( \mathbb{N} \). On \( \mathbb{N} \) we have the operations \(+\) and \(\times\), which are simple in themselves but lead to more sophisticated concepts.

For example, we say that \( a \) divides \( n \) if \( n = ab \) for some natural numbers \( a \) and \( b \). A natural number \( p \) is called prime if the only natural numbers dividing \( p \) are 1 and \( p \) itself.

Divisibility and primes are behind many of the interesting questions in mathematics, and also behind the recent applications of number theory (in cryptography, internet security, electronic money transfers etc.).

The sequence of prime numbers begins with

\[ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots \]

and continues in a seemingly random manner. There is so little pattern in the sequence that one cannot even see clearly whether it continues forever. However, Euclid (around 300 BCE) proved that there are infinitely many primes, essentially as follows.

**Infinitude of primes.** Given any primes \( p_1, p_2, p_3, \ldots, p_k \), we can always find another prime \( p \).

**Proof.** Form the number

\[ N = p_1 p_2 p_3 \cdots p_k + 1. \]

Then none of the given primes \( p_1, p_2, p_3, \ldots, p_k \) divides \( N \) because they all leave remainder 1. On the other hand, some prime \( p \) divides \( N \). If \( N \) itself is prime we can take \( p = N \), otherwise \( N = ab \) for some smaller numbers \( a \) and \( b \). Likewise, if either \( a \) or \( b \) is prime we take it to be \( p \), otherwise split \( a \) and \( b \) into smaller factors, and so on. Eventually we must reach a prime \( p \) dividing \( N \) because natural numbers cannot decrease forever. \( \square \)