CHAPTER 1

Introduction

God created the integers. All the rest is the work of man.

—Leopold Kronecker

If you look at zero you see nothing; but look through it and you will see the world.

—Robert Kaplan, *The Nothing That Is: A Natural History of Zero*

TO BE INVOLVED WITH MODERN cryptography is to dive willy-nilly into number theory, that is, the study of the natural numbers, one of the most beautiful areas of mathematics. However, we have no intention of becoming deep-sea divers who raise sunken treasure from the mathematical ocean floor, which in any case is unnecessary for cryptographic applications. Our goals are much more modest. On the other hand, there is no limit to the depth of involvement of number theory with cryptography, and many significant mathematicians have made important contributions to this area.

The roots of number theory reach back to antiquity. The Pythagoreans—the Greek mathematician and philosopher Pythagoras and his school—were already deeply involved in the sixth century B.C.E. with relations among the integers, and they achieved significant mathematical results, for example the famed Pythagorean theorem, which is a part of every school child's education. With religious zeal they took the position that all numbers should be commensurate with the natural numbers, and they found themselves on the horns of a serious dilemma when they discovered the existence of "irrational" numbers such as $\sqrt{2}$, which cannot be expressed as the quotient of two integers. This discovery threw the world view of the Pythagoreans into disarray, to the extent that they sought to suppress knowledge of the irrational numbers, a futile form of behavior oft repeated throughout human history.

Two of the oldest number-theoretic algorithms, which have been passed down to us from the Greek mathematicians Euclid (third century B.C.E.) and Eratosthenes (276–195 B.C.E.), are closely related to the most contemporary encryption algorithms that we use every day to secure communication across the Internet. The "Euclidean algorithm" and the "sieve of Eratosthenes" are both quite up-to-date for our work, and we shall discuss their theory and application in Sections 10.1 and 10.5 of this book.

Among the most important founders of modern number theory are to be counted Pierre de Fermat (1601–1665), Leonhard Euler (1707–1783), Adrien Marie Legendre (1752–1833), Carl Friedrich Gauss (1777–1855), and Ernst Eduard Kummer (1810–1893). Their work forms the basis for the modern development of this area of mathematics and in particular the interesting application areas such as cryptography, with its asymmetric procedures for encryption and the generation of digital signatures (cf. Chapter 17). We could mention many more names of important contributors to this field, who continue to this day to be involved in often dramatic developments in number theory, and to those interested in a thrilling account of the history of number theory and its protagonists, I heartily recommend the book *Fermat's Last Theorem*, by Simon Singh.

Considering that already as children we learned counting as something to be taken for granted and that we were readily convinced of such facts as that two plus two equals four, we must turn to surprisingly abstract thought constructs to derive the theoretical justification for such assertions. For example, set theory allows us to derive the existence and arithmetic of the natural numbers from (almost) nothing. This "almost nothing" is the empty (or null) set $\varnothing := \{\ \}$, that is, the set that has no elements. If we consider the empty set to correspond to the number 0, then we are able to construct additional sets as follows. The successor 0^+ of 0 is associated with the set $0^+ := \{\, 0 \,\} = \{\, \varnothing \,\}$, which contains a single element, namely the null set. We give the successor of 0 the name 1, and for this set as well we can determine a successor, namely $1^+ := \{\, \varnothing, \{\, \varnothing \,\} \,\}$. The successor of 1, which contains 0 and 1 as its elements, is given the name 2. The sets thus constructed, which we have rashly given the names 0, 1, and 2, we identify—not surprisingly—with the well-known natural numbers 0, 1, and 2.

This principle of construction, which to every number x associates a successor $x^+ := x \cup \{\, x \,\}$ by adjoining x to the previous set, can be continued to produce additional numbers. Each number thus constructed, with the exception of 0, is itself a set whose elements constitute its *predecessors*. Only 0 has no predecessor. To ensure that this process continues ad infinitum, set theory formulates a special rule, called the *axiom of infinity:* There exists a set that contains 0 as well as the successor of every element that it contains.

From this postulated existence of (at least) one so-called *successor set*, which, beginning with 0, contains all successors, set theory derives the existence of a minimal successor set $\mathbb{N}$, which is itself a subset of every successor set. This minimal and thus uniquely determined successor set $\mathbb{N}$ is called the set of *natural numbers*, in which we expressly include zero as an element.[1]

[1] It was not decisive for this choice that according to standard DIN 5473 zero belongs to the natural numbers. From the point of view of computer science, however, it is practical to begin counting at zero instead of 1, which is indicative of the important role played by zero as the neutral element for addition (additive identity).