CHAPTER 10

Basic Number-Theoretic Functions

> I am dying to hear about it, since I always thought number theory was the Queen of Mathematics—the purest branch of mathematics—the one branch of mathematics which has NO applications!
>
> —D. R. Hofstadter, *Gödel, Escher, Bach*

NOW THAT WE ARE FITTED out with a sturdy tool box of arithmetic functions that we developed in the previous chapters, we turn our attention to the implementation of several fundamental algorithms from the realm of number theory. The number-theoretic functions discussed in the following chapters form a collection that on the one hand exemplifies the application of the arithmetic of large numbers and on the other forms a useful foundation for more complex number-theoretic calculations and cryptographic applications. The resources provided here can be extended in a number of directions, so that for almost every type of application the necessary tools can be assembled with the demonstrated methods.

The algorithms on which the following implementations are based are drawn primarily from the publications [Cohe], [HKW], [Knut], [Kran], and [Rose], where as previously, we have placed particular value on efficiency and on as broad a range of application as possible.

The following sections contain the minimum of mathematical theory required to explicate the functions that we present and their possibilities for application. We would like, after all, to have some benefit from all the effort that will be required in dealing with this material. Those readers who are interested in a more thoroughgoing introduction to number theory are referred to the books [Bund] and [Rose]. In [Cohe] in particular the algorithmic aspects of number theory are considered and are treated clearly and concisely. An informative overview of applications of number theory is offered by [Schr], while cryptographic aspects of number theory are treated in [Kobl].

In this chapter we shall be concerned with, among other things, the calculation of the greatest common divisor and the least common multiple of large numbers, the multiplicative properties of residue class rings, the identification of quadratic residues and the calculation of square roots in

residue class rings, the Chinese remainder theorem for solving systems of linear congruences, and the identification of prime numbers. We shall supplement the theoretical foundations of these topics with practical tips and explanations, and we shall develop several functions that embody a realization of the algorithms that we describe and make them usable in many practical applications.

10.1 Greatest Common Divisor

> That schoolchildren are taught to use the method of prime factorization rather than the more natural method of the Euclidean algorithm to compute the greatest common divisor of two integers is a disgrace to our system of education.
>
> —W. Heise, P. Quattrocci, *Information and Coding Theory*

Stated in words, the greatest common divisor (gcd) of integers a and b is the positive divisor of a and b that is divisible by all common divisors of a and b. The greatest common divisor is thereby uniquely determined. In mathematical notation the greatest common divisor d of two integers a and b, not both zero, is defined as follows: $d = \gcd(a, b)$ if $d > 0$, $d \mid a$, $d \mid b$, and if for some integer d' we have $d' \mid a$ and $d' \mid b$, then we also have $d' \mid d$.

It is convenient to extend the definition to include

$$\gcd(0, 0) := 0.$$

The greatest common divisor is thus defined for all pairs of integers, and in particular for the range of integers that can be represented by `CLINT` objects. The following rules hold:

$$\begin{aligned}
&\text{(i)} && \gcd(a, b) = \gcd(b, a),\\
&\text{(ii)} && \gcd(a, 0) = |a| \text{ (the absolute value of } a),\\
&\text{(iii)} && \gcd(a, b, c) = \gcd(a, \gcd(b, c)),\\
&\text{(iv)} && \gcd(a, b) = \gcd(-a, b),
\end{aligned} \tag{10.1}$$

of which, however, only (i)–(iii) are relevant for `CLINT` objects.

It is obligatory first to consider the classical procedure for calculating the greatest common divisor according to the Greek mathematician Euclid (third century B.C.E.), which Knuth respectfully calls the grandfather of all algorithms (definitely see [Knut], pages 316 ff.). The Euclidean algorithm consists in a sequence of divisions with remainder, beginning with the reduction of $a \bmod b$, then $b \bmod (a \bmod b)$, and so on until the remainder vanishes.