Most of the topics reviewed in this chapter are probably well known to most readers. The purpose of the chapter is to recall the notation and facts from elementary number theory which we will need to have at our fingertips in our later work. Most proofs are omitted, since they can be found in almost any introductory textbook on number theory. One topic that will play a central role later — estimating the number of bit operations needed to perform various number theoretic tasks by computer — is not yet a standard part of elementary number theory textbooks. So we will go into most detail about the subject of time estimates, especially in §1.

1 Time estimates for doing arithmetic

Numbers in different bases. A nonnegative integer $n$ written to the base $b$ is a notation for $n$ of the form $(d_{k-1}d_{k-2}\cdots d_1d_0)_b$, where the $d$'s are digits, i.e., symbols for the integers between 0 and $b-1$; this notation means that $n = d_{k-1}b^{k-1} + d_{k-2}b^{k-2} + \cdots + d_1b + d_0$. If the first digit $d_{k-1}$ is not zero, we call $n$ a $k$-digit base-$b$ number. Any number between $b^{k-1}$ and $b^k$ is a $k$-digit number to the base $b$. We shall omit the parentheses and subscript $(\cdot\cdot\cdot)_b$ in the case of the usual decimal system $(b = 10)$ and occasionally in other cases as well, if the choice of base is clear from the context, especially when we're using the binary system $(b = 2)$. Since it is sometimes useful to work in bases other than 10, one should get used to doing arithmetic in an arbitrary base and to converting from one base to another. We now review this by doing some examples.
I. Some Topics in Elementary Number Theory

Remarks. (1) Fractions can also be expanded in any base, i.e., they can be represented in the form \((d_{k-1}d_{k-2}\cdots d_1d_0,d_{-1}d_{-2}\cdots)_b\). (2) When \(b > 10\) it is customary to use letters for the digits beyond 9. One could also use letters for all of the digits.

Example 1. (a) \((11001001)_2 = 201\).
(b) When \(b = 26\) let us use the letters A—Z for the digits 0—25, respectively. Then \((BAD)_{26} = 679\), whereas \((B.AD)_{26} = 1\frac{3}{676}\).

Example 2. Multiply 160 and 199 in the base 7. Solution:

\[
\begin{array}{rll}
316 &  \\
403 &  \\
1254 & \\
16030 & \\
161554 & \\
\end{array}
\]

Example 3. Divide \((11001001)_2\) by \((100111)_2\), and divide \((HAPPY)_{26}\) by \((SAD)_{26}\).

Solution:

\[
\begin{array}{c|c}
101 & 110 \\
\hline
100111 & 11001001 \\
100111 & SAD \\
101101 & HAPPY \\
100111 & GYBE \\
110 & COLY \\
\hline
\end{array}
\]

Example 4. Convert \(10^6\) to the bases 2, 7 and 26 (using the letters A—Z as digits in the latter case).

Solution. To convert a number \(n\) to the base \(b\), one first gets the last digit (the ones’ place) by dividing \(n\) by \(b\) and taking the remainder. Then replace \(n\) by the quotient and repeat the process to get the second-to-last digit \(d_1\), and so on. Here we find that

\[
10^6 = (11110100001001000000)_2 = (11333311)_{10} = (CEXHO)_{26}.
\]

Example 5. Convert \(\pi = 3.1415926\cdots\) to the base 2 (carrying out the computation 15 places to the right of the point) and to the base 26 (carrying out 3 places to the right of the point).

Solution. After taking care of the integer part, the fractional part is converted to the base \(b\) by multiplying by \(b\), taking the integer part of the result as \(d_{-1}\), then starting over again with the fractional part of what you now have, successively finding \(d_{-2}, d_{-3}, \ldots\). In this way one obtains:

\[
3.1415926\cdots = (11.001001000011111\cdots)_2 = (D.DRS\cdots)_{26}.
\]