

## 10 I. Some Topics in Elementary Number Theory

**Example 12.** Express in terms of the  $O$ -notation the time required to compute (a)  $n!$ , (b)  $\binom{n}{m}$  (see Examples 6 and 8).

**Solution.** (a)  $O(n^2 \log^2 n)$ , (b)  $O(m^2 \log^2 n)$ .

In concluding this section, we make a definition that is fundamental in computer science and the theory of algorithms.

**Definition.** An algorithm to perform a computation involving integers  $n_1, n_2, \dots, n_r$  of  $k_1, k_2, \dots, k_r$  bits, respectively, is said to be a *polynomial time* algorithm if there exist integers  $d_1, d_2, \dots, d_r$  such that the number of bit operations required to perform the algorithm is  $O(k_1^{d_1} k_2^{d_2} \cdots k_r^{d_r})$ .

Thus, the usual arithmetic operations  $+$ ,  $-$ ,  $\times$ ,  $\div$  are examples of polynomial time algorithms; so is conversion from one base to another. On the other hand, computation of  $n!$  is not. (However, if one is satisfied with knowing  $n!$  to only a certain number of significant figures, e.g., its first 1000 binary digits, then one can obtain that by a polynomial time algorithm using Stirling's approximation formula for  $n!$ .)

### Exercises

1. Multiply  $(212)_3$  by  $(122)_3$ .
2. Divide  $(40122)_7$  by  $(126)_7$ .
3. Multiply the binary numbers 101101 and 11001, and divide 10011001 by 1011.
4. In the base 26, with digits A—Z representing 0—25, (a) multiply YES by NO, and (b) divide JQVXHJ by WE.
5. Write  $e = 2.7182818\cdots$  (a) in binary 15 places out to the right of the point, and (b) to the base 26 out 3 places beyond the point.
6. By a "pure repeating" fraction of "period"  $f$  in the base  $b$ , we mean a number between 0 and 1 whose base- $b$  digits to the right of the point repeat in blocks of  $f$ . For example,  $1/3$  is pure repeating of period 1 and  $1/7$  is pure repeating of period 6 in the decimal system. Prove that a fraction  $c/d$  (in lowest terms) between 0 and 1 is pure repeating of period  $f$  in the base  $b$  if and only if  $b^f - 1$  is a multiple of  $d$ .
7. (a) The "hexadecimal" system means  $b = 16$  with the letters A—F representing the tenth through fifteenth digits, respectively. Divide  $(131B6C3)_{16}$  by  $(1A2F)_{16}$ .  
(b) Explain how to convert back and forth between binary and hexadecimal representations of an integer, and why the time required is far less than the general estimate given in Example 11 for converting from binary to base- $b$ .
8. Describe a subtraction-type bit operation in the same way as was done for an addition-type bit operation in the text (the list of five alternatives).