Algorithms and Data Structures
K. Mehlhorn and R. Seidel
Exercise 4

Summer 2008
Tu. Sept 2nd, afternoon

Motivation

These exercises are supposed to illustrate that certain restrictions that we put on our RAM model are really necessary, in the sense that if they are not imposed then some problems, that are believed to be very difficult, can be solved easily. In particular, you are to show that the problem of factoring a large integer into its prime components becomes quite easy, if no restriction on the sizes of integers stored in a RAM is made (or if you allow a floor function for a RAM with real numbers). Many methods in cryptography, e.g. the security of the RSA crypto system, rely on the assumption that factoring is hard.
The following sequence of subproblems should lead you to this result. The underlying model is an integer RAM with no size restriction and unit cost operations +,-,*,div.

1. Show that given integers A and N the number A^N can be computed in $O(\log N)$ time.
2. Show that given natural numbers N and K the binomial coefficient $\binom{N}{K}$ can be computed in $O(\log N)$ time.

   Hint: Consider $(A+1)^N$ for large A.
3. Show that given natural number N the number $N!$ can be computed in $O(\log^2 N)$ time.
4. Show that in $O(\log^2 N)$ time N can be tested whether it is a prime number.
5. Show that in $O(\log^3 N)$ time a non-trivial factor of N can be found, provided N is not prime. For this you may assume the existence of a routine that computes the GCD (Greatest Common Divisor) of two numbers X and Y in time $O(\log(\min\{X,Y\}))$.
6. Show that the prime factorization of N can be found in time $O(\log^4 N)$.

7. Can you improve some of the indicated asymptotic running times?

Have fun with the solution!