Algorithms and Data Structures
Winter Term 2015/16
Exercises for Units 1 and 2

1. This sequence of exercises is supposed to illustrate that certain restrictions that we put on our RAM model are really necessary. If they were not imposed then some problems that are believed to be very difficult could 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 restrictions on the sizes of integers stored in a RAM are 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 sub-problems should lead to this result. The underlying model is an integer RAM with no size restriction and unit cost operations $+,-,*,\text{div}$.

   a) Show that given integers A and N the number A^N can be computed in $O(\log N)$ time.

   b) Show that given natural numbers N and K the binomial coefficient $\binom{N}{K}$ can be compute in $O(\log N)$ time.
   Hint: Consider $(A+1)^N$ for large A.

   c) Show that given natural number N the number $N!$ can be computed in $O(\log^2 N)$ time.

   d) Show that in $O(\log^2 N)$ time it can be tested whether N is a prime number.

   e) 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 $O(\log(\min\{X,Y\}))$.

   f) Show that the prime factorization of N can be found in time $O(\log^4 N)$.

2. The following exercises are to remind you about asymptotic notation and some of its intricacies.

   a) Order the following functions by their asymptotic growth rate, and prove that this ordering is correct:

   $$n/1000 \quad n^{4/3} \quad 5^n \quad n\log n \quad n^{1-\varepsilon} \quad n/\log\log n \quad n^{4/3}\log n \quad (4/3)^n \quad n\cdot 2^{\sqrt{\log n}}$$

   Here, $0 < \varepsilon < 1$ is a fixed constant.

   b) We noted in class that $f \in O(g)$ can be viewed as analogous to $f \leq g$, and $f \in o(g)$ can be viewed as analogous to $f < g$, and similarly for $f \in \Omega(g)$ analogous to $f \geq g$ and $f \in \omega(g)$ analogous to $f > g$.

   - For numbers $x \not< y$ is the same as $x \geq y$. Is $f \notin o(g)$ the same as $f \in \Omega(g)$?
   - Is it possible that $f \notin o(g)$ and at the same time $g \notin o(f)$?
   - How about $f \notin O(g)$ and at the same time $g \notin O(f)$?