Aalto University
Department of Information and Computer Science
Petteri Kaski (tel. 23260)

T-79.4202 Principles of Algorithmic Techniques (5 cr)
Exam Thu 8 Mar 2012, 9–12 a.m.

Write down on each answer sheet:
- Your name, degree programme, and student number
- The text: "T-79.4202 Principles of Algorithmic Techniques 8.3.2012"
- The total number of answer sheets you are submitting for grading

Note: You can write down your answers in either Finnish, Swedish, or English.

1. Modular exponentiation.

   (a) Describe the repeated squaring algorithm for modular exponentiation.

   (b) How many multiplications does the repeated squaring algorithm use to compute $x^{15} \bmod N$? Is there a way to use fewer multiplications?

2. The *square* of a matrix A is its product with itself, AA.

   (a) Show that five multiplications are sufficient to compute the square of a 2×2 matrix.

   (b) Professor Boondoggle suggests the following algorithm for computing the square of an $n \times n$ matrix, for n a power of 2.

   > Use a divide-and-conquer approach as in Strassen's algorithm, except that instead of getting 7 subproblems of size $n/2$, we now get 5 subproblems of size $n/2$, thanks to part (a). Using the same analysis as Strassen's algorithm, we find that the algorithm runs in time $O(n^{\log_2 5})$.

   What is wrong with the algorithm?

3. Give an algorithm with running time $O(nt)$ for the following task.

   > *Input:* A list of n positive integers $a_1, a_2, \ldots, a_n$ and a positive integer t.
   > *Question:* Decide (output "yes" or "no") whether there is a subset of the a_i's whose sum is equal to t. Each a_i maybe used at most once.

4. Give an algorithm with running time $O(n+m)$ for the following task. The input is a set of n variables $x_1, x_2, \ldots, x_n$ and a set of m constraints, each of which is either an *equality* constraint of the form "$x_i = x_j$" or a *disequality* constraint of the form "$x_i \neq x_j$" for some $1 \leq i, j \leq n$. The task is to decide whether the variables can take integer values such that all the constraints are satisfied. For example, it is not possible to satisfy the four constraints

$$x_1 = x_2,\ x_2 = x_3,\ x_3 = x_4,\ x_1 \neq x_4.$$

   Hint: Use your knowledge of graph algorithms.

Grading: Each problem 12p, total 48p.