Course 02249, DTU Compute
Carsten Witt

Computationally Hard Problems – Fall 2016
Assignment 7

Date: 08.11.2016, **Due date**: 14.11.2016, 21:00

The following exercises are **not** mandatory:

Exercise 7.1: Let $\boldsymbol{x} = x_1x_2 \dots x_n \in \{0,1\}^n$ be a bit string, and let $m \le n$. Let $\boldsymbol{x}_j = x_jx_{j+1} \cdots x_{j+m-1}$ be the substring of length m starting at position j. Let $X_j = \sum_{i=0}^{m-1} x_{j+i}2^i$ be the natural number represented by $\boldsymbol{x}_j$. Show how to compute the numbers $X_1, X_2, \dots, X_{n-m+1}$ in this order with only $O(n+m)$ arithmetic operations.

End of Exercise 1

Exercise 7.2: Suppose you have a deterministic primality test that, given a natural number r, checks the number error-free for primality in time bounded by a polynomial in the input length $\log(r)$, say time at most $(\log(r))^c$ for some $c > 0$.
Given a natural number $t \ge 3$, your aim is to select a prime number **uniformly** over all prime numbers in the interval $[2, t]$. Describe a randomized algorithm that returns an output of the desired kind with probability at least $1/2$. The algorithm should have a running time that is polynomial in $\log t$ and be Las Vegas, i. e., if it fails to solve its task it should output "FAILED". Give arguments for the correctness and prove a bound on the running time.

Hint: Use

- the bound $\pi(t) \ge t/(2 \ln t)$ on the prime number function for $t \ge 3$,
- Lemma B.3 from the lecture notes.

End of Exercise 2

Exercise 7.3: Consider Algorithm 5.9 from the lecture notes. Suppose it is run on the following 3-SAT instance with variable set $\{x_1, \dots, x_3\}$ and clause set

$$x_1 \vee x_2 \vee x_3$$
$$\overline{x_1} \vee x_2 \vee x_3$$
$$x_1 \vee \overline{x_2} \vee x_3$$
$$x_1 \vee x_2 \vee \overline{x_3}$$
$$\overline{x_1} \vee \overline{x_2} \vee x_3$$
$$\overline{x_1} \vee x_2 \vee \overline{x_3}$$
$$x_1 \vee \overline{x_2} \vee \overline{x_3}.$$

a) Suppose the algorithm is run with $T = 1$. Find a choice of S such that the algorithm terminates with a satisfying assignment with probability at least $1/2$.

b) Suppose now $S = 1$ and that the random choice of the initial assignment in the algorithm results in $x_i = 0$ for $i \in \{1, \dots, 3\}$. Find a choice of T such that the algorithm terminates with a satisfying assignment with probability at least $1/2$.

Justify your choice in both parts. You need not find the smallest possible S and T.

Hint: Lemma A.2 and Inequality (A.10) from the lecture notes may be useful. In part b) you may define a pessimistic sequence of events that is guaranteed to lead to a satisfying assignment.

End of Exercise 3

The following exercise is **mandatory**:

Exercise 7.4: Show the computation of $\left[\frac{1543}{799}\right]$ (the Jacobi symbol of the two numbers) using the rules shown in the lecture notes. You may use that $\gcd(1543, 799) = 1$.

End of Exercise 4