Course 02249, DTU Compute
Carsten Witt

Computationally Hard Problems – Fall 2015
Assignment 7

Date: 10.11.2015, **Due date**: 16.11.2015, 23:59

The following exercises are **not** mandatory:

Exercise 7.1: Let $\boldsymbol{x} = x_1 x_2 \ldots x_n \in \{0,1\}^n$ be a bit string, and let $m \leq n$. Let $\boldsymbol{x}_j = x_j x_{j+1} \cdots x_{j+m-1}$ 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 $X_1, X_2, \ldots, X_{n-m+1}$ 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 $t \geq 3$, 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 $\pi(t) \geq t/(2 \ln t)$ on the prime number function for $t \geq 3$,
- Lemma B.3 from the lecture notes.

End of Exercise 2

Exercise 7.3: Let $G = (V, E)$ be a directed graph with vertex set $V = \{v_1, v_2, \ldots, v_n\}$ and edge set E. The graph does not have self-loops, i. e., there are no edges of the kind (v_i, v_i). A *directed cut* V_1, V_2 is a partition of the vertex set, i. e., $V_1, V_2 \subseteq V$, $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$. The *directed cut edge set* $C \subseteq E$ induced by the cut is the set of directed edges running from V_1 to V_2, formally $C = \{(v, w) \in E \mid v \in V_1 \text{ and } w \in V_2\}$. We construct such a directed cut with the following randomized algorithm: Every vertex is independently put into V_1 or V_2 according to the outcome of a random number generator.

```
for i ← 1 to n do
    if (rand(1,3) = 1)
      then
            put v_i into V_1
       else
            put v_i into V_2
    fi
od
```

a) Is the running time of the algorithm deterministic or can it vary due to the randomization?

b) What is the expected size of V_1? What is the expected size of V_2? The sizes should be expressed in terms of the size n of the set of vertices.

c) For an edge $e \in E$, what is the probability that it has both start and end point in V_1?

d) For an edge $e \in E$, what is the probability that it has its start point in V_1 and its end point in V_2?

e) What is the expected size of the directed cut edge set C, induced by this partition? The sizes should be expressed in terms of the size $|E|$ of the set of edges.

End of Exercise 3

The following exercise is **mandatory**:

Exercise 7.4: Show the computation of $\left[\frac{773}{1373}\right]$ (the Jacobi symbol of the two numbers) using the rules shown in the lecture notes. You may use that $\gcd(773, 1373) = 1$.

End of Exercise 4