Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

4. Exercise sheet
Hand in before Monday, 2005/11/28, 14^{00} in b-it 1.22.

Exercise 4.1 (Strong Pseudo Primality Test). (4+4 points)

Execute the Strong Pseudo Primality Test with

(i) $N = 41$, $a = 2$. $\boxed{1}$

(ii) $N = 57$, $a = 37$. $\boxed{1}$

(iii) $N = 1105$, $a = 47$. $\boxed{1}$

(iv) $N = 1105$, $a = 2$. $\boxed{1}$

It's ok to use MuPAD's `powermod` for computing the necessary powers.

(v*) Compute the number of Fermat liars for $N = 35$. $\boxed{+1}$

(vi*) Compute the number of Strong Pseudo Prime Test liars for $N = 35$. $\boxed{+1}$

(vii*) Do the same for $N = 561$. $\boxed{+2}$

Exercise 4.2 (Prime number theorem). (6 points)

Use MuPAD's `numlib::pi` to generate a plot (see `plot::Function2d`) over the ranges 1..100 (and 1..1000)

(i) with $\pi(x)/\frac{x}{\ln x}$, $\boxed{1}$

(ii) with the three functions in the prime number theorem (the bounds and π). (Use `Color=RGB::Green` to plot in green.) $\boxed{3}$

(iii) with the solution $c(x)$ of $\pi(x) = \frac{x}{\ln x}(1 + \frac{c(x)}{\ln x})$. $\boxed{2}$

Exercise 4.3 (Carmichael numbers & order). (4+2 points)

By Euler's theorem we know that $x^{\varphi(N)} = 1$ for all $x \in \mathbb{Z}_N^\times$. By Fermat's little theorem we know that $x^{N-1} = 1$ for all $x \in \mathbb{Z}_N^\times$ in case N is prime.

(i) Verify that for $N = 561 = 3 \cdot 11 \cdot 17$ we have of course $x^{2\cdot 10\cdot 16} = 1$ but also $x^{560} = 1$ for all $x \in \mathbb{Z}_N^\times$. $\boxed{3}$

(ii) Formulate and verify the corresponding statement for $N = 5 \cdot 13 \cdot 17$. $\boxed{1}$

(iii*) Suppose the factorization $N = p_1^{e_1} \cdot \cdots \cdot p_r^{e_r}$ (with pairwise different primes p_i and all $e_i \geq 1$) is given. Characterize Carmichael numbers: give a condition (on the p_i, e_i) characterizing when N is a Carmichael number without referring to elements in $\mathbb{Z}_N$. $\boxed{+2}$

Exercise 4.4 (Lagrange's theorem). (11 points)

We have seen that in a commutative group G we have $x^{\#G} = 1$ for $x \in G$. There is a more general version of the theorem which says more and works also for non-commutative groups.

Theorem (Lagrange). *Suppose G is a finite group.*

(a) If H is a subgroup of G, then $\#H$ divides $\#G$.

(b) If $x \in G$ then $x^{\#G} = 1$ in G.

We are going to prove the first part. Let $a \in G$ be arbitrary group elements. We consider the so-called *cosets* $aH = \{ah \,|\, h \in H\}$.

$\boxed{1}$ (i) Prove that there is a $c \in G$ such that $a \in cH$.

$\boxed{1}$ (ii) Consider the map $\lambda\colon H \to aH,\ x \mapsto ax$. Prove that it is bijective.

$\boxed{1}$ (iii) Conclude that $\#(aH) = \#H$ is independent of a.

$\boxed{2}$ (iv) Suppose we are given two group elements $a, b \in G$. Then only the following two cases are possible:

- $aH = bH$, or
- $aH \cap bH = \emptyset$.

In other words: it never happens that aH and bH have some but not all elements in common.

Prove this. [Hint: Suppose $x \in aH \cap bH$ (so we are not in the second case) and show that then $aH = bH$ (this is the first case).]

$\boxed{1}$ (v) Conclude that G is the disjoint union of all cosets.

$\boxed{1}$ (vi) Conclude that $\#H$ divides $\#G$.

We derive the second part from the first in the following steps:

$\boxed{1}$ (vii) Consider $\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$. Prove that this *is* a subgroup of G. It is called the *subgroup generated by a*.

$\boxed{2}$ (viii) Now let n be the *order* of a, that is $a^n = 1$ and $a^k \neq 1$ for all $0 < k < n$. Prove that $\langle a \rangle = \{1, a, \ldots, a^{n-1}\}$ and in particular $\# \langle a \rangle = n$.

$\boxed{1}$ (ix) Conclude that $a^{\#G} = 1$.

Exercise 4.5 (Loops). (0+9 points)

Consider an algorithm consisting of a single loop like this:

Algorithm.

1. Repeat
2. Perform some (constant time) computation involving random bits.
3. Until condition()

Suppose that the probability for condition() is p, that is prob(condition()) $= p$, and indepently in each iteration. Denote by X_i the random variable which equals 1 if condition() is true in the i-th iteration and 0 otherwise.

(i) Translate the assumption into $\boxed{+1}$

- prob$(X_i = 1) = p$,
- $(X_1, \ldots, X_n)$ are independent random variables.

(ii) Prove that the probability to have exactly one loop iteration, that is $X_1 = 1$, is p. $\boxed{+1}$

(iii) Prove that the probability to have exactly two loop iterations, that is $X_1 = 0$ and $X_2 = 1$, is $p(1-p)$. $\boxed{+1}$

Let K be the random variable that gives the number of loop iterations, that is $K = k$ iff $X_1 = 0$, $X_2 = 0, \ldots, X_{k-1} = 0$, and $X_k = 1$.

(iv) Prove that prob$(K = k) = p(1-p)^{k-1}$ and prob$(K \geq j) = (1-p)^{j-1}$. $\boxed{+2}$

The expected (or average) value $\mathrm{E}(K)$ is the weighted sum of the outcomes of K, that is $\mathrm{E}(K) = \sum_{k \in \mathbb{N}} \mathrm{prob}(K = k) \cdot k$.

(v) Rewrite that last formula into $\mathrm{E}(K) = \sum_{j \geq 1} \mathrm{prob}(K \geq j)$. $\boxed{+2}$

(vi) Prove that the expected running time, that is the expected value $\mathrm{E}(K)$ of the number of loop iterations, is $1/p$. $\boxed{+2}$

Hint: Use that $\sum_{j \in \mathbb{N}} x^j = \frac{1}{1-x}$ for $|x| < 1$.

Remark: To be prudent we should make sure that we only deal with finite probability spaces. This will be explained in the tutorial.