4. Exercise sheet
Hand in before Monday, 2005/11/28, 1400 in b-it 1.22.

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

(i) \( N = 41, a = 2 \).
(ii) \( N = 57, a = 37 \).
(iii) \( N = 1105, a = 47 \).
(iv) \( N = 1105, a = 2 \).

It’s ok to use MuPAD’s \texttt{powermod} for computing the necessary powers.

(v*) Compute the number of Fermat liars for \( N = 35 \).
(vi*) Compute the number of Strong Pseudo Prime Test liars for \( N = 35 \).
(vii*) Do the same for \( N = 561 \).

Exercise 4.2 (Prime number theorem). (6 points)
Use MuPAD’s \texttt{numlib::pi} to generate a plot (see \texttt{plot::Function2d}) over the ranges \( 1..100 \) and \( 1..1000 \)

(i) with \( \frac{x}{\pi(x)} \),

(ii) with the three functions in the prime number theorem (the bounds and \( \pi \)).
(Use \texttt{Color=RGB::Green} to plot in green.)

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

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 \( x \in \mathbb{Z}_N^\times \).

(ii) Formulate and verify the corresponding statement for \( N = 5 \cdot 13 \cdot 17 \).

(iii*) Suppose the factorization \( N = p_1^{e_1} \cdots p_r^{e_r} \) (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 \( \mathbb{Z}_N \).
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 \( aH = \{ah \mid h \in H\} \).

(i) Prove that there is a \( c \in G \) such that \( a \in cH \).

(ii) Consider the map \( \lambda : H \to aH, x \mapsto ax \). Prove that it is bijective.

(iii) Conclude that \( \#(aH) = \#H \) is independent of \( a \).

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

\[ \begin{align*}
\circ & \ aH = bH, \\
\circ & \ aH \cap bH = \emptyset.
\end{align*} \]

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).]

(v) Conclude that \( G \) is the disjoint union of all cosets.

(vi) Conclude that \( \# H \) divides \( \# G \).

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

(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 \( a \).

(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 \( \# \langle a \rangle = n \).

(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 \( \Pr(\text{condition}) = p \), and independently 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
- \( \Pr(X_i = 1) = p \)
- \( (X_1, \ldots, X_n) \) are independent random variables.

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

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

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 \( \Pr(K = k) = p(1-p)^{k-1} \) and \( \Pr(K \geq j) = (1-p)^{j-1} \).

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

(v) Rewrite that last formula into \( E(K) = \sum_{j \geq 1} \Pr(K \geq j) \).

(vi) Prove that the expected running time, that is the expected value \( E(K) \) of the number of loop iterations, is \( 1/p \).

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.