5. Exercise sheet
Hand in solutions until
Monday, 08 December 2008, 1159 am (deadline!).

Note that on Wednesday, 3 December 2008 there is the Dies Academicus in Bonn and we will have no lecture/tutorial. We will thus on Tuesday, 2 December 2008 have a special session in the tutorial that repeats some of the major concepts regarding groups, rings, fields and other mathematical basics (or anything else you ask for).

As usual: Any claim needs a proof or an argument.

Exercise 5.1 (Exponentiation & discrete logarithms). (15+3 points)
Suppose $G$ is a group and $g$ is an element of order $\ell$. In the course we have defined exponentiation as a map from the integers $\mathbb{Z}$ to some group $G$.

(i) Show that it makes sense to view it as a map

\[
\exp_g : \mathbb{Z}_\ell \to \langle g \rangle \subseteq G, \quad x \mapsto g^x.
\]

(ii) Let $G = \mathbb{Z}_{10001}^\times$, $g = 42$. Write a procedure to compute $\exp_g$ efficiently. [Group operations are allowed as primitives. Other predefined procedures may not be used.]

(iii) Same for $G = \mathbb{Z}_{241576501}^\times$, $g = 23$.

(iv) Now let $p = 241576501$, and $g = 23^{1500} = -46436978 \in \mathbb{Z}_p^\times$.

(a) Compute $g^{11^4}$ and $g^{11^5}$.

(b) Prove that the order of $g$ is $11^5$.

(c) Prepare a table with all powers of $h := g^{11^4} = 23^{(p-1)/11}$ in $\mathbb{Z}_p^\times$.

(d) Compute the discrete logarithm $x$ of $42^{1500} = 105868544 \in \mathbb{Z}_p^\times$ with respect to $g$. [Note that $(p-1) = 1500 \cdot 11^5$ and consider $42^{1500 \cdot 11^4} = g^{x \cdot 11^4}$...]

(e) What does the result tell us about the discrete logarithm of $42 \in \mathbb{Z}_p^\times$ with respect to the base $23 \in \mathbb{Z}_p^\times$?

Exercise 5.2 (High powers). (3 points)
Compute $3^{98765432101} \bmod 101$. 

3
Exercise 5.3 (Pollard’s $\varrho$ method). (9 points)

In class we discussed Pollard’s $\varrho$ method for computing the discrete logarithm in a group $\mathbb{Z}_p^\times$ of size $m$. In particular we defined the algorithm in the following way:

Assuming that we work on tuples $(\gamma, \delta, a^\gamma g^\delta)$ we looked at some in a sense randomly behaving function $f$ that mapped such tuples to other ones. This however is not efficient enough. [Why?] Thus we consider instead tuples $(\gamma, \delta, a^\gamma g^\delta)$ and the function $f$ defined as follows:

$$f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \times \mathbb{Z}_p^\times \rightarrow \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \times \mathbb{Z}_p^\times,$$

\[
(\gamma, \delta, x) \mapsto \begin{cases} 
(2\gamma, 2\delta, x^2) & x_1 = x_0 \\
(\gamma + 1, \delta, gx) & x_1x_0 = 01 \\
(\gamma + 1, \delta, ax) & x_1x_0 = 10 
\end{cases}
\]

(i) We start at $(\gamma_0, \delta_0, a^{\gamma_0} g^{\delta_0})$ with $\gamma_0, \delta_0 \in \mathbb{Z}_{p-1}$, and determine $(\gamma_i, \delta_i, x_i) = f^i(\gamma_0, \delta_0, a^{\gamma_0} g^{\delta_0})$. Show that $x_i = a^{\gamma_i} g^{\delta_i}$.

(ii) Show that with a collision in the third coordinate one can easily compute the discrete logarithm of $a$ to the base $g$.

(iii) Show that this can be done with heuristically expected $O(\sqrt{m})$ group operations. You may assume that $f$ indeed behaves randomly. Hint: Birthday-paradox.

(iv) Implement Pollard’s $\varrho$ algorithm and compute the discrete logarithm of your student registration number in the group $\mathbb{Z}_p^\times$ with $p = 10^8 + 37$ and base $g = 2$. Count the number of group operations needed. Additionally hand in the source code.

Exercise 5.4 (Order). (8+6 points)

Let $G$ be a (multiplicative) commutative group, $a$ an element of order 24 and $b$ an element of order 33. What is the order of $b^2, b^3, \ldots$? What are possible orders of $ab$?

Let us look at an example first: Take $G = \mathbb{Z}_{1321}^\times$, $a = 17$ and $b = 53$. We have $a^{24} = 1$ and $b^{33} = 1$ in $G$ and for all respective smaller positive exponents the result is not 1.

(i) Compute the order of $b^2, b^3, b^9, b^{10}, b^{11}$.

Now we want to investigate the general case:

(ii) Show: The order of the power $g^k$ of a group element $g \in G$ is the order of $g$ divided by the greatest common divisor of $k$ and that order, in formulae: $\text{ord}(g^k) = \text{ord}(g)/\gcd(k, \text{ord}(g))$. [Hint: Look at the special cases $\gcd(k, \text{ord}(g)) = 1$ and $k | \text{ord}(g)$ and derive the general solution from there.]
Consider again the example:

(iii) Compute the order of \(ab, ab^2, ab^3\).

\[\text{...and back to the general case:}\]

(iv) Show: The order of the product \(xy\) of two group elements \(g, h \in G\) in a commutative group \(G\) divides the least common multiple of the orders of \(g\) and \(h\), in formulae: \(\text{ord}(gh) | \text{lcm}(\text{ord}(g), \text{ord}(h))\).

(v*) Show: If the orders of two group elements \(g, h \in G\) are coprime, then the order of \(xy\) is actually equal to the the least common multiple of those orders, in formulae: \(\gcd(\text{ord}(g), \text{ord}(h)) = 1 \Rightarrow \text{ord}(gh) = \text{lcm}(\text{ord}(g), \text{ord}(h))\).

(vi*) Show that the following is true in general: If \(\text{ord}(g) = ms, \text{ord}(h) = mt\) where \(s\) and \(t\) are coprime, then \(st | \text{ord}(gh)\).

[Actually, \(st = \text{lcm}(\text{ord}(g), \text{ord}(h)) / \gcd(\text{ord}(g), \text{ord}(h))\).]