Security on the Internet, summer 2007

MICHAEL NÜSKEN

6. Exercise sheet
Hand in solutions until Thursday, 17 Mai 2007.

Any claim needs a proof or an argument.

Exercise 6.1 (High powers). (3 points)

Compute $3^{98765432101}$ in $\mathbb{Z}_{101}$. $\boxed{3}$

Exercise 6.2 (Finite sets and nice pictures). (5+5 points)

Use one of the introduced rings $\mathbb{Z}_N$.

(i) Start at $a_0 = 0 \in \mathbb{Z}_{43}$ and compute its square plus one: $a_1 = a_0^2 + 1$. Continue doing so. Draw a picture! $\boxed{1}$

(ii) Start at $a_0 = 0 \in \mathbb{Z}_{42}$ and compute its square plus one: $a_1 = a_0^2 + 1$. Continue doing so. Draw a picture! $\boxed{1}$

(iii) Start at a random point $a_0 \in_R \mathbb{Z}_{42}$, let $b_0 = a_0$, and compute $a_i = a_{i-1}^2 + 1$ and $b_i = (b_{i-1}^2 + 1)^2 + 1$. Compute $\gcd(a_i - b_i, 42)$. $\boxed{2}$

(iv) Play with further examples as in (iii) where N is a four digit number. $\boxed{+2}$

(v) What do you observe? $\boxed{1}$

$\boxed{+3}$

MuPAD-Hints: `R:=Dom::IntegerMod(`N`):` helps. To force a shorter output use `R::print := x->extop(x,1):`.

Exercise 6.3 (Exponentiation & discrete logarithms). (15+3 points)

Suppose G is a group and g is an element of order ℓ. 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 $\boxed{3}$

$$\exp_g : \begin{array}{ccc} \mathbb{Z}_\ell & \longrightarrow & G, \\ x & \longmapsto & g^x \end{array} .$$

(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.] $\boxed{3}$

(iii) Same for $G = \mathbb{Z}_{241576501}^{\times}$, $g = 23$. $\boxed{1}$

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

$\boxed{1}$ (a) Compute g^{11^4} and g^{11^5}.

$\boxed{3}$ (b) Prove that the order of g is 11^5.

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

$\boxed{3}$ (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 $42^{1500 \cdot 11^4} = g^{x \cdot 11^4} \ldots$]

$\boxed{+3}$ (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 6.4 (Diffie Hellman key exchange). (5+1 points)

Perform a toy example of a Diffie Hellman key exchange: Fix $p = 47$ and $g = 2 \in \mathbb{Z}_p^{\times}$.

$\boxed{1}$ (i) Show that the order of g is 23.

$\boxed{+1}$ [If you are clever then you only need to calculate g^{23}.]

$\boxed{1}$ (ii) Choose $x \in \mathbb{Z}_{23}$ (take $x \notin \{0, 1\}$ to get something interesting) and calculate $h_A := g^x$.

$\boxed{1}$ (iii) Choose $y \in \mathbb{Z}_{23}$ (take $y \notin \{0, 1, x\}$ to get something interesting) and calculate $h_B := g^y$.

$\boxed{2}$ (iv) Now compute h_B^x and h_A^y and compare.

Exercise 6.5 (Square and multiply). (0+5 points)

Use paper and pencil for this exercise. How many multiplications do you need to compute x^{382}?

$\boxed{+1}$ (i) Find an algorithm that uses 14 multiplications.

$\boxed{+2}$ (ii) Find an algorithm that uses 12 multiplications.

$\boxed{+2}$ (iii) Can you find an algorithm that uses 11 multiplitations?

Some side calculations: $382 = 101111110_2 = 112011_3 = 11332_4 = 3012_5 = 1434_6 = 1054_7 = 576_8$, $382 = 2 \cdot 191$, $190 = 2 \cdot 5 \cdot 19$, $189 = 7 \cdot 3^3$.