Electronic passport and biometrics, winter 2006

MICHAEL NÜSKEN

2. Exercise sheet
Hand in solutions until Tuesday, 14 November, $12^{\underline{15}}$.

Exercise 2.1 (Tool: The Extended Euclidean Algorithm). (4 points)

Integers: We can add, subtract and multiply them. And there is a division with remainder: Given any $a, b \in \mathbb{Z}$ with $b \neq 0$ there is a quotient $q \in \mathbb{Z}$ and a remainder $r \in \mathbb{Z}$ such that $a = q \cdot b + r$ and $0 \leq r < |b|$. (We write $a \operatorname{quo} b := q$, $a \operatorname{rem} b := r \in \mathbb{Z}$. If we want to calculate with the remainder in its natural domain we write $a \bmod b := r \in \mathbb{Z}_b$.) Using that we give an answer to the problem to find $s, t \in \mathbb{Z}$ with $sa + tb = 1$. Allowed answers are: "There is no solution." or "A solution is $s = ...$ and $t = ...$." Any answer needs a proof.

(i) Find $s, t \in \mathbb{Z}$ such that $s \cdot 17 + t \cdot 21 = 1$. 2

(ii) Find $s, t \in \mathbb{Z}$ such that $s \cdot 15 + t \cdot 21 = 1$. 2

PS: Guessing or trying all possibilities is not allowed here!

Exercise 2.2 (Tool: Groups). (6 points)

Consider the *additive group* $\mathbb{Z}_N^+ := (\mathbb{Z}_N, +)$ of the ring $\mathbb{Z}_N = (\mathbb{Z}_N, +, \cdot)$ of integers modulo N and for a prime p the *unit group* $\mathbb{Z}_p^\times := (\mathbb{Z}_p^\times, \cdot)$ of the ring $\mathbb{Z}_p = (\mathbb{Z}_p, +, \cdot)$ of integers modulo N. Compute (fast):

(i) $17 + 13$ in $\mathbb{Z}_{21}^+$.

(ii) $17 \cdot 13$ in $\mathbb{Z}_{67}^\times$. 1

(iii) -5 in $\mathbb{Z}_{15}^+$. 1

(iv) 5^{-1} in $\mathbb{Z}_{19}^\times$. 2

(v) $17 \cdot 5 := \underbrace{5 + \cdots + 5}_{17}$ in $\mathbb{Z}_{12}^+$. (Note that there is *no* multiplication available!) 1

(vi) $5^{17} := \underbrace{5 \cdot \ldots \cdot 5}_{17}$ in $\mathbb{Z}_{19}^\times$. 1

Exercise 2.3 (Tool: The exponentiation map). (10 points)

The group $G = \mathbb{Z}_p^\times$ has the $\#G = p - 1$ elements $\{1, 2, \ldots, p-1\}$. For any element $g \in G$ we get the exponentiation map

$$\mathrm{Exp}_g : \begin{array}{ccc} \mathbb{Z}^+ & \longrightarrow & \mathbb{Z}_p^\times, \\ a & \longmapsto & g^a. \end{array}$$

[1] (i) Consider the example $p = 7$, $g = 3$. Make a table of Exp_g for $0 \leq a < 2p$.

[1] (ii) Consider the example $p = 7$, $g = 2$. Make a table of Exp_g for $0 \leq a < p$.

[1] (iii) Consider the example $p = 11$, $g = 2$. Make a table of Exp_g for $0 \leq a < p$.

[1] (iv) Compute $2^{121110987654321}$ in $\mathbb{Z}_{11}^\times$.

[1] (v) Prove that the exponentiation map respects the group structure: for any $a, b \in \mathbb{Z}$ we have $g^a \cdot g^b = g^{a+b}$.

We have the following result:

Theorem (Lagrange). *If G is a finite group and $x \in G$ then $x^{\#G} = 1$.* □

Applied to our situation we obtain a new map:

[1] (vi) Prove that if $(a \bmod \#G) = (b \bmod \#G)$ then $g^a = g^b$.

[1] (vii) We obtain a well-defined map

$$\exp_g : \begin{array}{ccc} \mathbb{Z}_{\#G}^+ & \longrightarrow & \mathbb{Z}_p^\times, \\ a & \longmapsto & g^a \end{array}$$

(which by abuse of notation inherits the name from its parent).

[1] (viii) Make a table of $\exp_2$ and $\exp_3$ for $2, 3 \in \mathbb{Z}_{11}^\times$.

[1] (ix) Explain how to multiply 3 with 7 using the table for $\exp_2$.

[1] (x) Can you do the same using the table for $\exp_3$?

Exercise 2.4 (Tool: The Extended Euclidean Algorithm). (0+8 points)

If you want to know why the EEA works prove the following statements. [Notation: We assume that the first column contains *remainders* r_i, the second column *quotients* q_i and the other two *coefficients* s_i and t_i. The top row has $i = 0$, and the bottom row (the first with $r_i = 0$ and thus the last one) is row $\ell + 1$. There is no q_0 and no $q_{\ell+1}$, $r_0 = a$, $r_1 = b$. A division with remainder produces $q_i, r_{i+1} \in \mathbb{Z}$ with $r_{i-1} = q_i r_i + r_{i+1}$ with $0 \leq r_{i+1} < |r_i|$ $(0 < i < \ell)$.]

(i) For any row in the scheme we have $r_i = s_i a + t_i b$ $(0 \leq i \leq \ell + 1)$. +1

(ii) For any two neighbouring rows in the scheme we have that the greatest common divisor of r_i and r_{i+1} is the same $(0 \leq i \leq \ell)$. [A step leading there is $\gcd(r_i, r_{i+1}) = \gcd(r_{i-1}, r_i)$.] +2

(iii) The greatest common divisor of r_ℓ and 0 is r_ℓ. +1

(iv) We have $|r_{i+1}| < |r_i|$ $(1 \leq i \leq \ell)$, so the algorithm terminates. +1

(v) We have $|r_{i+1}| < \frac{1}{2}|r_{i-1}|$ $(2 \leq i \leq \ell)$, so the algorithm is fast, ie. $\ell \in \mathcal{O}(n)$ when a, b have at most n bits, ie. $|a|, |b| < 2^n$. +1

(vi) Put everything together and prove: +2

Theorem. *The EEA computes given $a, b \in \mathbb{Z}$ with at most n bits with at most $\mathcal{O}(n^3)$ bit operations the greatest common divisor g of a and b and a representation $g = sa + tb$ of it. In case $g = 1$ we thus have a solution of the equation $1 = sa + tb$. In case $g > 1$ there is no such solution.*

[Hint: A single multiplication or a single division with remainder of n bit numbers needs at most $\mathcal{O}(n^2)$ bit operations.]

Exercise 2.5 (Tool: elliptic curves). (0+12 points)

Let $p \geq 5$ be prime and $a, b \in \mathbb{Z}_p$ with $4a^3 + 27b^2 \neq 0$. Consider the elliptic curve E given $y^2 = x^3 + ax + b$, ie.

$$E = \left\{(x, y) \in \mathbb{Z}_p \,\middle|\, y^2 = x^3 + ax + b\right\} \dot\cup \{\mathcal{O}\}\,.$$

Choose any two points $P_1, P_2 \in E$. If $P_i = (x_i, y_i) \neq \mathcal{O}$ and $x_1 \neq x_2$ the line through them is given by an equation $y = m(x - x_1) + y_1$.

(i) Compute $P_3 = (x_3, y_3)$ which lies also on the line and the curve. [Hints: You only need to find x_3. If you know two solutions x_1, x_2 of a cubic equation $x^3 - Mx^2 + a'x + b' = 0$ then a third one exists and is equal to $M - x_1 - x_2$.] +2

Define $P_1 + P_2 = (x_3, -y_3)$ then. If $P_1 = -P_2$ then let $P_1 + P_2 := \mathcal{O}$. Further define $P_1 + \mathcal{O} = P_1$ and $\mathcal{O} + P_2 = P_2$ and $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

+2 (ii*) Find a suitable way to define $P_1 + P_1$.

+1 (iii) Prove that the so-defined operation is well-defined, has a neutral element, has inverses and is commutative. (PNIC)

+1 (iv*) Prove that the addition is associative at least in case all operations are of the first type. You may use a computer algebra system to perform tedious algebraic computations.

Consider an example: $p = 5$, $a = 2$, $b = 1$.

+1 (v) Make a list of all points of the defined curve. Draw a picture.

+1 (vi) Compute $(-2, 2) + (0, 1)$.

+1 (vii) Compute $2(0, 1) := (0, 1) + (0, 1)$.

+1 (viii) Compute $3(0, 1)$.

+1 (ix) Make a table of the map $\exp_{(0,1)}$ which maps $a \in \mathbb{Z}_7$ to $a \cdot (0, 1)$. [Hint: In $\mathbb{Z}_7$ we have $4 = -3$.]

+1 (x) Add $(-2, 2)$ and $(0, 1)$ using this table. Does it produce the same result as before? Should it?