Cryptographic passports & biometrics, summer 2009

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

3. Exercise sheet
Hand in solutions until Monday, 11 May 2009.

Any claim needs a proof or argument.

Exercise 3.1 (Tool: The exponentiation map). (7 points)

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

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

(i) Consider the example $p = 7$, $g = 3$. Make a table of Exp_g for $0 \leq a < 2p$. What is the subgroup $\langle g \rangle \subseteq G$ generated by g? $\boxed{1}$

(ii) Consider the example $p = 7$, $g = 2$. Make a table of Exp_g for $0 \leq a < p$. What is the subgroup $\langle g \rangle \subseteq G$ generated by g? $\boxed{1}$

(iii) Compute 2^{67649} in $\mathbb{Z}_{11}^\times$ using *Square and Multiply* (SaM). $\boxed{1}$

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

(v) Prove that if $(a \bmod \ell) = (b \bmod \ell)$ then $g^a = g^b$, where the *order ℓ of g* is the smallest positive integer ℓ such that $g^\ell = 1$. $\boxed{1}$

We obtain a well-defined map

$$\mathrm{exp}_g \colon \begin{array}{ccc} \mathbb{Z}_\ell^+ & \longrightarrow & \mathbb{Z}_p^\times, \\ a & \longmapsto & g^a \end{array}$$

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

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

Exercise 3.2 (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 $0 \leq r_{i+1} < |r_i|$ for $0 < i \leq \ell$.]

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

+2 (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 for $0 \leq i \leq \ell$. [A step leading there is $\gcd(r_i, r_{i+1}) = \gcd(r_{i-1}, r_i)$.]

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

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

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

+2 (vi) Put everything together and prove:

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 3.3 (Chinese Remainder Theorem). (10 points)

2 (i) Consider $21 = 3 \cdot 7$ and fill out a table to visualize the relation between the elements of $\mathbb{Z}_{21}$ and $\mathbb{Z}_7 \times \mathbb{Z}_3$.

1 (ii) Pick two elements $x, y \in \mathbb{Z}_{21}$ (to make it interesting: the sum of the representing integers shall be larger than 21). First, add them in $\mathbb{Z}_{21}$ and then map to $\mathbb{Z}_7 \times \mathbb{Z}_3$. Second, map both to $\mathbb{Z}_7 \times \mathbb{Z}_3$ and add afterwards. What do you observe?

1 (iii) Pick two elements $x, y \in \mathbb{Z}_{21}$ (to make it interesting: the product of the representing integers shall be larger than 21). First, multiply them in $\mathbb{Z}_{21}$ and then map to $\mathbb{Z}_7 \times \mathbb{Z}_3$. Second, map both to $\mathbb{Z}_7 \times \mathbb{Z}_3$ and multiply afterwards. What do you observe?

Note: a map having the properties observed in (ii) and (iii) is called a *ring homomorphism*.

(iv) Mark all the invertible elements in $\mathbb{Z}_7$, $\mathbb{Z}_3$, and $\mathbb{Z}_{21}$. What is their relationship? 2

Now consider two arbitrary relatively prime positive integers $m_1, m_2 \in \mathbb{Z}_{\geq 2}$.

(v) Let x be any integer and suppose $x \bmod m_1 m_2$ is invertible. Prove that $x \bmod m_1$ and $x \bmod m_2$ are also invertible. 1

(vi) Assume that an integer y is invertible modulo m_1 and modulo m_2. Prove that y is then invertible modulo $m_1 m_2$. 2

(vii) Conclude that there is a bijection between $\mathbb{Z}^\times_{m_1 m_2}$ and $\mathbb{Z}^\times_{m_1} \times \mathbb{Z}^\times_{m_2}$. 1

Exercise 3.4 (DLP in $(\mathbb{Z}_N, +)$). (4 points)

(i) What is the *Discrete Logarithm Problem* (DLP) in the additive group $(\mathbb{Z}_N, +)$. (Obviously, you are not allowed to use the function dlog to define the DLP.) 2

(ii) Show that the DLP in $(\mathbb{Z}_N, +)$ is *easy*, ie. can be computed with a number of bit operations polynomial in the bit-size of N. 2