Electronic elections, winter 2007

MICHAEL NÜSKEN

1. Exercise sheet
Hand in solutions until Sunday, 18 November 2007.

For future exercises it might be important to use b-it computers. So please register an account for the b-it. (Ask at the infodesk for the procedure.)

A word on the exercises. They are important. Of course, you know that. Just as an additional motivation, you will get a bonus for the final exam if you earn more than 60% or even more than 80% of the credits.

Exercise 1.1 (Secure email). (6 points)

(i) Send a digitally signed email with the subject "`[07ws-elect2] hello`" to me at `nuesken@bit.uni-bonn.de` from your personal account. The signature must be verifiable and correct, in particular, the mail body must be non-empty. [It is a good idea to verify this by sending a blind carbon copy (Bcc) to oneself.] 4

With Thunderbird I recommend using `enigmail` and `gpg`. In any case make sure to register your key eg. at `http://wwwkeys.de.pgp.net/`.

Choose yourself among this and possible other solutions. In any case use a pgp key pair.

Note: Future exercise hand-ins will only be accepted via *signed* email. Then a bonus point will be awarded for a correct signature and a malus for a missing or invalid signature.

Warning: If you loose your key, eg. because your computer crashed, then you have a serious problem. To prevent that store

- a revocation certificate and store that in a safe place. (To stop anybody from using it...)
- a copy of your secret key in a secure place. (To be able to restore it.)

Your own computer is not a safe place! (When the hard drive crashes...)

(ii) Send a second email with the subject "`[07ws-elect2] student id`" containing your student identification number. (How should that be secured?) You have only a single trial here! [If you need testing then test with yourself or with a friend.] 2

Deadline for earning these credits: Sunday, 18 November 2007, 23:59:59 (valid timestamp of your emails).

Exercise 1.2 (Trust). (4 points)

2 (i) Find the fingerprint of your own PGP key. Bring 20 printouts of it to the next tutorial. (Do not send me an email with it. Guess, why!)

2 (ii) Sign all your collegues' public keys and mine: The fingerprint of my up-to-date PGP key `0xB9670465` is

```
F753 FA1F 70C8 0B4A 0181 8B50 B6EF 9CA3 B967 0465
```

Find my key in your key management tool, after verification give it some or full trust, sign and submit your decision to the key server. (Make sure that things *are* visible on the server! Join with your fellow students to synchronize you.)

The deadline for this part is Sunday, 25 November 2007. (So you have two chances to fulfill the requirements: once in the tutorial and once in the course.)

Exercise 1.3 (Tool: The Extended Euclidean Algorithm). (8+8 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 (or at least a good argument).

We start with one example: Consider $a = 35 \in \mathbb{Z}$ and $b = 22 \in \mathbb{Z}$. Our aim is to find $s, t \in \mathbb{Z}$ such that $sa + tb$ is positive and as small as possible. By taking $s_0 = 1$ and $t_0 = 0$ we get $s_0 a + t_0 b = a$ (identity$_0$) and by taking $s_1 = 0$ and $t_1 = 1$ we get $s_1 a + t_1 b = b$ (identity$_1$). Given that we can combine the two identities with a smaller outcome if we use $a = q_1 b + r_2$ with r smaller than b (in a suitable sense); namely we form $1(\text{identity}_0) - q_1(\text{identity}_1)$ and obtain

$$\underbrace{(s_0 - q_1 s_1)}_{=:s_2} a + \underbrace{(t_0 - q_1 t_1)}_{=:t_2} b = \underbrace{a - q_1 b}_{=r_2}.$$

We arrange this in a table and continue with identity$_1$ and the newly found identity$_2$ until we obtain 0. This might be one step more than you think necessary, but the last identity is very easy to check and so gives us a cross-check of the entire calculation. For the example we obtain:

i	r_i	q_i	s_i	t_i	comment
0	$a = 35$		1	0	$1a + 0b = 35$
1	$b = 22$	1	0	1	$0a + 1b = 22, 35 = 1 \cdot 22 + 13$
2	13	1	1	-1	$1a - 1b = 13, 22 = 1 \cdot 13 + 9$
3	9	1	-1	2	$-1a + 2b = 9, 13 = 1 \cdot 9 + 4$
4	4	2	2	-3	$2a - 3b = 4, 9 = 2 \cdot 4 + 1$
5	**1**	4	**-5**	**8**	$-5a + 8b = 1, 4 = 4 \cdot 1 + 0$
6	0		22	-35	$22a - 35b = 0$, DONE, check ok!

We read off (marked in blue) that $1 = -5a + 8b$ and the greatest common divisor of a and b is 1. This implies that $8 \cdot 22 = 1$ in $\mathbb{Z}_{35}$, in other words: the multiplicative inverse of 22, often denoted 22^{-1} or $\frac{1}{22}$, in the ring $\mathbb{Z}_{35}$ of integers modulo 35 is 8. (Brute force is no solution! That is, guessing or trying all possibilities is not allowed here!)

(i) Find $s, t \in \mathbb{Z}$ such that $s \cdot 17 + t \cdot 35 = 1$. [2]

(ii) Find $s, t \in \mathbb{Z}$ such that $s \cdot 14 + t \cdot 35 = 1$. [2]

Actually, there are other things which can be added, subtracted, multiplied, and allow a division with remainder. For example, univariate polynomials with coefficients in a field form a *euclidean ring*. A concrete example is the ring $\mathbb{F}_2[X]$ of univariate polynomials with coefficients in the two element field $\mathbb{F}_2$. (The elements of $\mathbb{F}_2$ are 0 and 1, addition and multiplication are modulo 2, so $1 + 1 = 0$. The expression $1 + X + X^3 + X^4 + X^8$ is a typical polynomial with coefficients in $\mathbb{F}_2$; note that the coefficients know that '$1 + 1 = 0$' where they live. It's square is $1 + X^2 + X^6 + X^8 + X^{16}$, any occurance of $1 + 1$ during squaring yields 0.)

(iii) Find $s, t \in \mathbb{F}_2[X]$ such that $s \cdot (1 + X) + t \cdot (1 + X + X^3 + X^4 + X^8) = 1$. [4]

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

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

+2 (v) 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 $\gcd(r_i, r_{i+1}) = \gcd(r_{i-1}, r_i)$.]

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

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

+1 (viii) 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. $|a|, |b| < 2^n$.

+2 (ix) 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.]