The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

2. Exercise sheet

Prepare exercises 2.3, 2.4 for the tutorial on Tuesday, 22 April! Hand in solutions until Monday, 28 April 2008.

Exercise 2.1 (Playing with modular arithmetic). (5 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 the *unit group* $\mathbb{Z}_N^\times := (\mathbb{Z}_N^\times, \cdot)$ of the ring $\mathbb{Z}_N = (\mathbb{Z}_p, +, \cdot)$ of integers modulo N. Compute (fast):

(i) $17 + 13$ in $\mathbb{Z}_{21}^+$. $\boxed{0}$

(ii) $17 \cdot 5$ in $\mathbb{Z}_{12}$. $\boxed{0}$

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

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

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

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

Exercise 2.2 (Science). (6+5 points)

(i) Count the number of elements in $\mathbb{Z}_4^\times$, in $\mathbb{Z}_9^\times$, and in $\mathbb{Z}_{25}^\times$, respectively. $\boxed{1}$

Do you recognize a pattern? Can you prove your guess? $\boxed{+1}$

(ii) Prove that there are exactly 40 invertible elements in $\mathbb{Z}_{100}$. $\boxed{2}$

(iii) Prove with the help of Euler's theorem and Fermat's little theorem that we have the equation $\boxed{3}$

$$3^{3^{160}} = 3 \text{ in } \mathbb{Z}_{101}.$$

(iv) Prove that we have the equation $\boxed{+4}$

$$3^{2^{160}} = 3^{76} \text{ in } \mathbb{Z}_{101}.$$

Exercise 2.3 (More on the Extended Euclidean Algorithm). (6+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 $s = \ldots$ and $t = \ldots$." 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!)

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

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

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

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

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

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

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

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

(viii) We have $|r_{i+1}| < \frac{1}{2}|r_{i-1}|$ $(2 \le i \le \ell)$, 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

(ix) 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 2.4 (Euler totient function). (0 points)

Euler totient function is defined by

$$\varphi\colon \begin{array}{rcl} \mathbb{N}_{\geq 2} & \longrightarrow & \mathbb{N}, \\ N & \longmapsto & \#\mathbb{Z}_N^\times. \end{array}$$

Let $p \in \mathbb{N}$ be a prime number and $m, n \in \mathbb{N}_{\geq 2}$. Prove:

(i) If $p \in \mathbb{N}$ is prime then $\varphi(p) = p - 1$.

(ii) If $p \in \mathbb{N}$ is prime and $e \in \mathbb{N}_{\geq 1}$ then $\varphi(p^e) = p^{e-1}(p-1)$.

(iii) If $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$ then $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.