ETH Zürich, D-INFK
HS 2017, 7. November 2017

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik

Solution 7

7.1 Greatest common divisor

a) Let $a, b, u, v \in \mathbb{Z} \setminus \{0\}$ be such that $ua + vb = 1$ and let $d = \gcd(a, b)$. By the definition of gcd, we have $d \mid a$ and $d \mid b$. That is, there exist $k, l \in \mathbb{Z}$ such that $a = kd$ and $b = ld$. *(1 Point)*

Hence, $1 = ua + vb = ukd + vld = (uk + vl)d$. Thus, $d \mid 1$. *(1 Point)*

Since 1 is the only positive divisor of 1, it follows that $d = 1$. *(1 Point)*

b) Let $d \in \mathbb{N} \setminus \{0, 1\}$. Let $a := 3$, $b := 2$, $u := d$ and $v := -d$. *(1 Point)*

Then we have $ua + vb = 3d - 2d = d$ and $\gcd(a, b) = \gcd(3, 2) = 1 \neq d$. *(1 Point)*

7.2 Extended GCD Algorithm

a) The following table shows the values of s_1, s_2, u_1, u_2, v_1 and v_2 at the initialization and after each execution of the loop in the algorithm from Figure 4.1.

	s_1	s_2	u_1	u_2	v_1	v_2
after initialization	553	26	1	0	0	1
after execution 1	26	7	0	1	1	-21
after execution 2	7	5	1	-3	-21	64
after execution 3	5	2	-3	4	64	-85
after execution 4	2	1	4	-11	-85	234
after execution 5	1	0	-11	26	234	-553

By Theorem 4.6., it follows that $\gcd(553, 26) = 1$ and that the equation $553u + 26v = \gcd(553, 26)$ is satisfied by $u = -11$ and $v = 234$.

b) From the subtask a), we have $234 \cdot 26 - 11 \cdot 553 = 1$. Since $234 \cdot 26 \equiv_{26} 0$, by Lemma 4.18 (i) it follows that $-11 \cdot 553 \equiv_{26} 1$. Hence, $a = -11$ is a valid solution to the exercise. Analogously, we can choose $b = 234$.

c) From the proof in the lecture, we already know that the algorithm terminates and that it outputs the correct value $s_1 = \gcd(a, b)$. What is left to show is that at the end we have $u_1 a + v_1 b = s_1$.

Similarly to the proof from the lecture, we will show that two invariants hold throughout the execution of the algorithm: $u_1 a + v_1 b = s_1$ and $u_2 a + v_2 b = s_2$. Before the loop begins, we trivially have $1 \cdot a + 0 \cdot b = a = s_1$ and $0 \cdot a + 1 \cdot b = b = s_2$.

For a given execution of the loop, let us denote the variables at the beginning by $u_1', u_2', v_1', v_2', s_1', s_2'$ and the variables at the end by $u_1'', u_2'', v_1'', v_2'', s_1'', s_2''$. Assume that the invariants hold at the beginning of the loop, that is that $u_1'a + v_1'b = s_1'$ and $u_2'a + v_2'b = s_2'$. It follows that

$$\begin{aligned} u_2''a + v_2''b &= (u_1' - qu_2')a + (v_1' - qv_2')b \\ &= u_1'a - v_1'b + q(u_2'a - v_2'b) \\ &= s_1' - qs_2' && \text{(by the assumption)} \\ &= s_2'' && \text{(by the way } s_2'' \text{ was defined)} \end{aligned}$$

$$\begin{aligned} u_1''a + v_1''b &= u_2'a + v_2'b \\ &= s_2' && \text{(by the assumption)} \\ &= s_1'' && \text{(by the way } s_1'' \text{ was defined)} \end{aligned}$$

Therefore, the invariants also hold at the end of each execution of the loop. Hence, they hold at the end of the algorithm as well. This means that after the algorithm is finished, $u_1a + v_1b = s_1$.

7.3 Irrationality of logarithms

Assume for contradiction that $\log_7(11)$ is rational. That is, assume that there exist $a \in \mathbb{N}$, $b \in \mathbb{N} \setminus \{0\}$ such that $\log_7(11) = \frac{a}{b}$. It follows that $7^{\frac{a}{b}} = 11$ and further that $7^a = 11^b$. Hence, we found two ways to write the integer $i = 7^a$ as the product of primes, which is a contradiction to Theorem 4.8. Therefore, $\log_7(11)$ is irrational.

7.4 Congruences

a) Assume that $a \equiv_m b$ and $c \equiv_m d$. Thus, there exist $s, t \in \mathbb{Z}$ such that $a - b = ms$ and $c - d = mt$. That is, $a = ms + b$ and $c = mt + d$. It follows that

$$ac = (ms + b)(mt + d) = m^2st + msd + mtb + bd = m(mst + sd + tb) + bd$$

Therefore, $m \mid ac - bd$ and $ac \equiv_m bd$.

b) By the binomial theorem, we have

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}b^k.$$

It is enough to show that p divides $\binom{p}{k}$ for all $k \in \{1, \ldots, p-1\}$. For given k, consider the numerator and denominator of $\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$. The nominator contains the prime factor p. The denominator contains only factors strictly smaller than p, and thus not divisible by p. Hence, by Lemma 4.7, p does not divide the denominator. Since $\binom{p}{k} \in \mathbb{N}$, p must divide $\binom{p}{k}$.

7.5 Modular arithmetic

a) Let n be any non-negative even integer, that is $n = 2k$ for some $k \in \mathbb{N} \cup \{0\}$. By Lemma 4.18, we have $R_7(13^n + 6) = R_7((R_7(13))^n + R_7(6))$. Since $R_7(13) = R_7(-1)$, this is equal to $R_7((-1)^n + 6) = R_7((-1)^{2k} + 6) = R_7(7) = 0$. Hence, 7 must divide $13^n + 6$. *(2 Points)*

b) By Theorem 4.1, there exists a $q \in \mathbb{Z}$ such that $n = qe + R_e(n)$. Therefore,

$$\begin{aligned} R_m(a^n) &= R_m\left(a^{qe+R_e(n)}\right) \\ &= R_m\left((a^e)^q \cdot a^{R_e(n)}\right) \\ &= R_m\left(\left(R_m\left(a^e\right)\right)^q \cdot R_m\left(a^{R_e(n)}\right)\right), \end{aligned}$$

where the last step follows from Lemma 4.18 (applied multiple times). Since we assumed that $R_m(a^e) = 1$, it follows that $R_m(a^n) = R_m(a^{R_e(n)})$. *(2 Points)*

c) By the subtask b), we have $R_{11}(4^{2015}) = R_{11}(4^{R_{10}(2015)}) = R_{11}(4^5) = R_{11}(2^{10}) = 1$. *(1 Point)*

d) For an integer n, consider all possible remainders $R_{11}(n^5 + 7)$. By Lemma 4.18, we have $R_{11}(n^5 + 7) = R_{11}((R_{11}(n))^5 + 7)$. By considering all possibilities for $R_{11}(n)$, we get that $R_{11}(n^5 + 7)$ can only be equal to $6, 7$ or 8. Now for any integer m, consider all possible remainders $R_{11}(m^2)$. By reasoning analogous to the above, we can conclude that $R_{11}(m^2)$ can only be equal to $0, 1, 3, 4, 5$ or 9. Hence, $R_{11}(n^5 + 7)$ cannot be equal to $R_{11}(m^2)$ for any integers m and n. Therefore, $n^5 + 7$ cannot be equal to m^2.

7.6 The Chinese Remainder Theorem

a) $\Longrightarrow$: Assume that $a \equiv_{nm} b$. This means that there exists a $k \in \mathbb{Z}$ such that $a - b = k(nm)$. Therefore, $a - b = (km)n$ and, thus, $a \equiv_n b$. Analogously, we get $a \equiv_m b$.

$\Longleftarrow$: Assume that $a \equiv_n b \wedge a \equiv_m b$. Now consider the system of congruence equations $x \equiv_n R_n(b) \ \wedge \ x \equiv_m R_m(b)$. By Lemma 4.17, we have $a \equiv_n b \ \wedge \ a \equiv_m b \Longleftrightarrow a \equiv_n R_n(b) \ \wedge \ a \equiv_m R_m(b)$. Hence, by the assumption, $x = a$ is a solution to the system of congruence equations. Analogously, $x = b$ is also a valid solution.

Since $\gcd(n, m) = 1$, it follows from the Chinese Remainder Theorem that all solutions for x are congruent modulo nm. Therefore, we must have $a \equiv_{nm} b$.

b) Since m and n are not relatively prime, we cannot apply directly the Chinese Remainder Theorem. Therefore, we will transform the system of congruence equations.

By subtask a), the following system of congruence equations is equivalent:

$$x \equiv_a y_1 \tag{1}$$
$$x \equiv_b y_1 \tag{2}$$
$$x \equiv_a y_2 \tag{3}$$
$$x \equiv_c y_2 \tag{4}$$

If $y_1 \not\equiv_a y_2$, there are clearly no solutions. Otherwise, the equations (1) and (3) are equivalent and we can remove (3). By Lemma 4.17, we get the following equivalent system of congruence equations:

$$x \equiv_a R_a(y_1)$$
$$x \equiv_b R_b(y_1)$$
$$x \equiv_c R_c(y_2)$$

Since a, b, c are pairwise relatively prime, the Chinese Remainder Theorem guarantees that there exists a unique solution x_0 such that $0 \leq x_0 < abc$. All remaining solutions must be of the form $x_0 + k(abc)$ for $k \in \mathbb{N}$. Since $nm = a^2bc$, there exist exactly a solutions x such that $0 \leq x < nm$.