ETH Zürich, D-INFK
HS 2017, 30. October 2017

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik

Exercise 7

7.1 Greatest common divisor *(5 Points)*

Show that

a) ($\star\,\star$) For all $a, b, u, v \in \mathbb{Z} \setminus \{0\}$ such that $ua + vb = 1$, we have $\gcd(a, b) = 1$. *(3 Points)*

b) ($\star\,\star$) For all $d \in \mathbb{N} \setminus \{0, 1\}$, there exist $a, b, u, v \in \mathbb{Z} \setminus \{0\}$ such that $ua + vb = d$ and $\gcd(a, b) \neq d$. *(2 Points)*

7.2 Extended GCD algorithm

a) ($\star\,\star$) Use the extended GCD algorithm to compute $\gcd(553, 26)$ and numbers $u, v \in \mathbb{Z}$ such that $553u + 26v = \gcd(553, 26)$.

b) ($\star\,\star$) Find an $a \in \mathbb{Z}$ such that $a \cdot 553 \equiv_{26} 1$ and a $b \in \mathbb{Z}$ such that $b \cdot 26 \equiv_{553} 1$.

Hint: Use the solution to subtask a).

c) ($\star\,\star\,\star$) Finish the proof of Theorem 4.6 from the lecture. That is, prove that the algorithm in Figure 4.1 computes u and v such that $ua + vb = \gcd(a, b)$. You can assume that the algorithm outputs the correct value $d = s_1 = \gcd(a, b)$.

7.3 Irrationality of logarithms ($\star$)

Show that $\log_7(11)$ is irrational.

7.4 Congruences

a) ($\star\,\star$) Show that for all $m \in \mathbb{Z} \setminus \{0\}$ and for all $a, b, c, d \in \mathbb{Z}$ such that $a \equiv_m b$ and $c \equiv_m d$, we have $ac \equiv_m bd$.

b) ($\star\,\star$) Show that for all primes p and for all $a, b \in \mathbb{Z}$ we have:

$$(a + b)^p \equiv_p a^p + b^p$$

Hint: Use the binomial theorem.

7.5 Modular arithmetic ($\star\,\star$) *(5 Points)*

a) Show that for every even integer $n \geq 0$, we have 7 divides $13^n + 6$. *(2 Points)*

b) Let $a, e, m, n \in \mathbb{N} \setminus \{0\}$ be such that $R_m(a^e) = 1$. Show that $R_m(a^n) = R_m(a^{R_e(n)})$. *(2 Points)*

c) Knowing that $R_{11}(4^{10}) = 1$, compute $R_{11}(4^{2015})$. *(1 Point)*

d) ($\star\,\star\,\star$) Prove that there cannot exist an integer n such that $n^5 + 7$ is equal to m^2 for another integer m.

7.6 The Chinese Remainder Theorem

a) ($\star\,\star\,\star$) Show that for all $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{N} \setminus \{0\}$ such that $\gcd(n, m) = 1$ we have

$$a \equiv_{nm} b \;\Leftrightarrow\; a \equiv_n b \;\wedge\; a \equiv_m b$$

b) ($\star\,\star\,\star$) Let a, b, c be pairwise relatively prime integers. For $n = ab$, $m = ac$ and integers y_1, y_2 such that $0 \leq y_1 < n$ and $0 \leq y_2 < m$, consider the following system of congruence equations:

$$x \equiv_n y_1$$
$$x \equiv_m y_2$$

How many solutions $0 \leq x < nm$ does the above system of equations have, depending on a, b, c and y_1, y_2?

Due on 6. November 2017.
Exercises 7.1. and 7.5 (without d)) will be corrected.