ETH Zürich, D-INFK
HS 2023, 3. November 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Exercise 7

Exercise 7.3 gives **bonus points**, which can increase the final grade. The solution to these exercises must be your own work. You may not share your solutions with anyone else. See also the note on dishonest behavior on the course website: `https://crypto.ethz.ch/teaching/DM23/`.

7.1 The Greatest Common Divisor ($\star$)

If $d = \gcd(a, b)$ then one can write d as a linear combination of a and b (Corollary 4.5). In this exercise we show that when $d = 1$ the converse is also true. More formally, prove that for all $a, b, u, v \in \mathbb{Z} \setminus \{0\}$ such that $ua + vb = 1$, we have $\gcd(a, b) = 1$.

7.2 Geometric Interpretation of the Greatest Common Divisor ($\star\star$)

Let $a, b \in \mathbb{N}$. In the cartesian plane, consider the segment with endpoints $(0, 0)$ and (a, b). Show that the number of points with integer coordinates on this segment is $\gcd(a, b) + 1$.

7.3 Properties of Greatest Common Divisors ($\star$) *(8 Points)*

Prove that for all positive integers a, b, c

$$\gcd(a, \mathrm{lcm}(b, c)) = \mathrm{lcm}(\gcd(a, b), \gcd(a, c)).$$

Hint: use expressions from section 4.3.3.

7.4 Congruences

a) ($\star$) Prove that for all $m, n \in \mathbb{N}$, if $m \equiv_4 n$, then $123^m \equiv_{10} 33^n$.

b) ($\star$) Prove that for all $a, b, c, d, m \in \mathbb{Z}$ such that $m > 0$, if $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.

c) ($\star\star\star$) Prove that there do not exist $m, n \in \mathbb{Z}$, such that $n^5 + 7 = m^2$.

7.5 Modular Arithmetic ($\star$)

a) Prove that $7 \mid (13^n + 6)$ for every even integer $n \geq 0$.

b) Prove that for any $a, e, m, n \in \mathbb{N} \setminus \{0\}$, if $R_m(a^e) = 1$, then $R_m(a^n) = R_m(a^{R_e(n)})$.

c) Using the above fact and the fact that $R_{13}(2^{12}) = 1$, compute $R_{13}(2^{2023})$.

7.6 Multiplicative Inverses

a) ($\star$) Let $a, m \in \mathbb{N}$ with $m > 0$. Show how given any u and v such that $ua + vm = 1$, one can compute the multiplicative inverse of a modulo m.

b) ($\star\star$) Compute the multiplicative inverse of 142 modulo 553.

Hint: Use Lemma 4.2 to find $\gcd(142, 553)$, and, at the same time, u and v, such that $\gcd(142, 553) = 142u + 553v$.

7.7 Solution of a Congruence Equation ($\star\star$)

Prove that for all $a, b, m \in \mathbb{Z}$ such that $m > 0$, the equation $ax \equiv_m b$ has a solution $x \in \mathbb{Z}$ if and only if $\gcd(a, m) \mid b$.

7.8 The Chinese Remainder Theorem ($\star\star\star$)

a) 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

$$a \equiv_{nm} b \iff a \equiv_n b \ \land \ a \equiv_m b$$

b) 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:

$$\begin{aligned} x &\equiv_n y_1 \\ x &\equiv_m y_2 \end{aligned}$$

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 by 9. November 2023.
Exercise 7.3 is graded.