Diskrete Mathematik HS2025 — Prof. Dennis Hofheinz

Marian Dietz — Milan Gonzalez-Thauvin — Zoé Reinke

Exercise sheet 7

This is the exercise sheet number 7. The difficulty of the questions and exercises are rated from very easy ($\star$) to hard ($\star\star\star\star$) . The graded exercise is Exercise 7.2 and your solution has to be uploaded on the Moodle page of the course **by 06/11/2025, 23:59**. The solution to this exercise must be your own work, you may not share your solutions with anyone else. See also the note on dishonest behavior on the Moodle page.

Exercise 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 $\gcd(a, b) = 1$.

Exercise 7.2 Properties of GCD and LCM ($\star\star$) — GRADED *(8 points)*

Please upload your solution by 06/11/2025

1. (4 points) Prove that for all positive integers a, b, c: If a and b are relatively prime, then

$$\gcd(a \cdot b, c) = \gcd(a, c) \cdot \gcd(b, c) \ .$$

2. (4 points) Prove that lcm distributes over $\gcd$, i.e., prove that for all positive integers a, b, c:

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

Hint: Recall the definitions of GCD and LCM:

For any integers a and b (not both 0), an integer d is called a *greatest common divisor* of a and b if d divides both a and b and if every common divisor of a and b divides d, i.e., if

$$d|a \quad \land \quad d|b \quad \land \quad \forall c\big((c|a \quad \land \quad c|b) \to c|d\big).$$

The *least common multiple* l of two positive integers a and b, denoted $l = \mathrm{lcm}(a, b)$, is the common multiple of a and b which divides every common multiple of a and b, i.e.,

$$a|l \quad \land \quad b|l \quad \land \quad \forall m\big((a|m \quad \land \quad b|m) \to l|m\big).$$

For the proofs, the expressions from section 4.3.3 might be useful.

Exercise 7.3 Congruences

1. ($\star$) Prove that for all $m, n \in \mathbb{N}$, if $m \equiv_4 n$, then $123^m \equiv_{10} 33^n$.
2. ($\star$) 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 $ac \equiv_m bd$.
3. ($\star\star\star$) Prove that there do not exist $m, n \in \mathbb{Z}$, such that $n^5 + 7 = m^2$.

Exercise 7.4 Modular Arithmetic ($\star$)

1. Prove that $7 \mid (13^n + 6)$ for every even integer $n \geq 0$.
2. Prove that for any $a, e, m, n \in \mathbb{N} \setminus \{0\}$, if $R_m(a^e) = 1$, then $R_m(a^n) = R_m(a^{R_e(n)})$.
3. Using the above fact and the fact that $R_{13}(2^{12}) = 1$, compute $R_{13}(2^{2023})$.

Exercise 7.5 Multiplicative Inverses

1. ($\star$) 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.
2. ($\star\star$) 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 $\gcd(142, 553) = 142u + 553v$.

Exercise 7.6 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 $\gcd(a, m) \mid b$.

Exercise 7.7 The Chinese Remainder Theorem ($\star\star\star$)

1. 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

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

2. 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?

Exercise 7.8 Questions from exams HS 2023 and FS 2024 ($\star$)

These two questions are taken from exams of 2023 and 2024.

1. For the following tasks no justification is required.
   (a) Compute $R_{11}\left(9^{2024}\right)$.
   (b) Compute the prime factorization of $\operatorname{lcm}(9 \cdot 2^4, 3^6) \cdot \gcd(9^3, 12^2)$.
2. Let $a, b, c \in \mathbb{Z} \setminus \{0\}$. **Prove** that the equation $ax + by = c$ has solutions $(x, y) \in \mathbb{Z}^2$ if and only if $\gcd(a, b) \mid c$.

Due by 06/11/2025, 23:59.
Exercise 7.2 will be graded.