Diskrete Mathematik HS2025 — Prof. Dennis HOFHEINZ

Marian DIETZ — Milan GONZALEZ-THAUVIN — Zoé REINKE

Exercise sheet 9

This is the exercise sheet number 9. The difficulty of the questions and exercises are rated from very easy ($\star$) to hard ($\star\star\star\star$) . The graded exercise is Exercise 9.3 and your solution has to be uploaded on the Moodle page of the course **by 20.11.2025, 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 9.1 Diffie-Hellman ($\star\star$)

1. Since Alice can add much faster than she can multiply, she proposes to execute the Diffie-Hellman protocol using the group $\langle \mathbb{Z}_n; \oplus_n \rangle$ with a generator $g \in \mathbb{Z}_n$. Describe the messages exchanged between Alice and Bob in this case. Show that this protocol is insecure, that is, describe a way in which Eve, who eavesdrops on all exchanged messages, can recover the secret key.
2. Since, by question 1, the Diffie-Hellman protocol is insecure in the group $\langle \mathbb{Z}_n; \oplus_n \rangle$ and by Theorem 5.7 every cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus_n \rangle$, Bob concludes that the protocol is insecure in every cyclic group. Is he right?

Exercise 9.2 The Group $\mathbb{Z}_m^*$

1. ($\star$) Determine the order and the elements of the group $\langle \mathbb{Z}_{36}^*; \odot_{36} \rangle$.
2. ($\star$) Determine all generators of the group $\langle \mathbb{Z}_{11}^*; \odot_{11} \rangle$.
3. ($\star\star\star$) Prove that for any two relatively prime numbers $m, n > 0$, $\langle \mathbb{Z}_{nm}^*; \odot_{nm} \rangle$ is isomorphic to $\langle \mathbb{Z}_n^*; \odot_n \rangle \times \langle \mathbb{Z}_m^*; \odot_m \rangle$.

Exercise 9.3 Pitfalls of RSA ($\star\star$) — GRADED *(8 points)*

Please upload your solution by 20.11.2025

In this exercise you will look into different aspects of RSA.

1. **Small Moduli.** Security of RSA encryption depends crucially on the hardness of factoring the modulus n. Using small moduli that are easy to factor is therefore a bad idea. Consider RSA public key $(n, e) = (133, 25)$ and ciphertext $c \equiv_n m^e \equiv_n 9$.
   (a) Compute the decryption key d. Show your work.
   Hint: Use corollary 4.5 of the lecture notes and the fact that $1 = 13 \cdot 25 - 3 \cdot 108$.
   Note: A solution that requires testing many values of d does not give any points.

[1] The operation $\star$ on $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ is defined as $(a_1, b_1) \star (a_2, b_2) := (a_1 \odot_n a_2,\ b_1 \odot_m b_2)$.

(b) Recover plaintext message m from c. Show your work.
Note: All intermediate steps must be easily computable by hand. For example, your solution must not require entering 9^d into a calculator.

2. (4 points) **Modulus shared between multiple users.** If two or more users use the same modulus n, then RSA can become insecure in certain cases. Assume Alice and Bob have public keys (n, e_A) and (n, e_B) respectively such that $\gcd(e_A, e_B) = 1$. Now, Charlie encrypts the same message m to both Alice and Bob and sends the two ciphertexts $c_A \equiv_n m^{e_A}$ and $c_B \equiv_n m^{e_B}$ over an insecure network. Show that any third party Eve knowing public keys (n, e_A) and (n, e_B) as well as ciphertexts c_A and c_B can efficiently decrypt the ciphertexts, i.e. can recover the encrypted message m.

   Hint: Separately consider the case where both c_A and c_B are co-prime to n (i.e., $\gcd(c_A, n) = 1 = \gcd(c_B, n)$) and the case where at least one of the values is not co-prime to n. In the former case, Corollary 4.5 from the lecture notes may be useful, but take care about what happens if $\gcd(a, b) = ua + vb$ with at least one of u and v being negative.

Exercise 9.4 An Attack on RSA ($\star\star\star$)

Alice, Bob and Charlie use three different RSA keys $(n_1, 3)$, $(n_2, 3)$ and $(n_3, 3)$ respectively. A message m is encrypted for each one of them, resulting in ciphertexts c_1, c_2 and c_3. How can an adversary use these ciphertexts and the public keys to efficiently compute m?

Exercise 9.5 Properties of Commutative Rings ($\star$)

The goal of this exercise is to prove Lemma 5.19 (ii) and (iii). You cannot use lemmas from the lecture notes. Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a commutative ring and let $a, b, c \in R$. Show that:

1. If $a|b$, then $a|bc$ for all c.
2. If $a|b$ and $a|c$, then $a|(b + c)$.

Exercise 9.6 Ideals in Rings ($\star\star$)

We generalize the concept of *ideal* (Definition 4.4) to arbitrary rings. Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a commutative ring. A subset $I \subseteq R$ is an *ideal* of R if
- I is a subgroup of $\langle R; +, -, 0\rangle$.
- For all $x \in I$ and $r \in R$ it holds that $x \cdot r \in I$ (an ideal is closed under multiplication with elements of the ring).

1. Prove that for all $x \in \mathbb{Z}$ the subset $(x) = \{xz \mid z \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.
2. Let I be an ideal (with this new definition) of $\mathbb{Z}$. Prove that $I = (z)$ for some $z \in \mathbb{Z}$.
3. Let R be a commutative ring. Let $x, y \in R$. Prove that $(x, y) = \{xr + ys \mid r, s, \in R\}$ is an ideal of R.

4. Consider the ring $\mathbb{Z}[x]$ and the ideal $(2, x) = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$. Prove that there exists no element $p(x) \in \mathbb{Z}(x)$ such that [2]

$$(p(x)) = \{p(x)f(x) \mid f(x) \in \mathbb{Z}[x]\} = (2, x).$$

Why does the proof of question 2 break down in this setting?

Exercise 9.7 Group homomorphisms (exam FS 2025)

This exercise is taken from the spring exam of 2025.
Let $(G; \star, \hat{}, e)$ be a group.

1. ($\star$) **Prove** that G is commutative if and only if $g \mapsto \hat{g}$ is a group homomorphism.
2. ($\star \star \star$) Suppose that G is finite and suppose there exists an isomorphism $f : G \to G$ such that
   a. $f(g) = g \implies g = e$ for all $g \in G$,
   b. $f \circ f = \mathrm{id}_G$.

   Prove that G is commutative. *Hint: show that for all $g \in G$ there is $x \in G$ such that $g = \hat{x} \star f(x)$ and use part* 1.)

Due by 20.11.2025, 23:59.
Exercise 9.3 will be graded.

[2] Ideals which can be generated by a single element are called *principal* ideals. A ring in which all ideals are principal (like $\mathbb{Z}$, as you showed in question 2) are called *principal ideal rings*. Question 4 shows that the ring $\mathbb{Z}[x]$ is *not* a principal ideal ring.