ETH Zürich, D-INFK
HS 2023, 17. November 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Exercise 9

Exercise 9.4 gives **bonus points**, which can increase the final grade. 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 course website: `https://crypto.ethz.ch/teaching/DM23/`.

9.1 Diffie-Hellman

a) ($\star\star$) Since Alice can add much faster than she can multiply, she proposes to execute the Diffie-Hellman protocol using the group $\langle \mathbb{Z}_n; \oplus \rangle$ 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.

b) ($\star\star$) Since, by Subtask a), the Diffie-Hellman protocol is insecure in the group $\langle \mathbb{Z}_n; \oplus \rangle$ and by Theorem 5.7 every cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus \rangle$, Bob concludes that the protocol is insecure in every cyclic group. Is he right?

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

a) ($\star$) Determine the order and the elements of the group $\langle \mathbb{Z}_{36}^*; \odot \rangle$.

b) ($\star$) Determine all generators of the group $\langle \mathbb{Z}_{11}^*; \odot \rangle$.

c) ($\star\star\star$) Prove that for any two relatively prime numbers $m, n > 0$, $\langle \mathbb{Z}_{nm}^*; \odot \rangle$ is isomorphic to $\langle \mathbb{Z}_n^*; \odot \rangle \times \langle \mathbb{Z}_m^*; \odot \rangle$.

9.3 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?

9.4 Non-Minimality of Ring Axioms ($\star$) *(8 Points)*

In this exercise, you prove the remark in Chapter 5, Footnote 20 of the lecture notes.
Consider an algebra $\langle R; +, -, 0, \cdot, 1 \rangle$ such that

i) $\langle R; +, -, 0 \rangle$ is a group.

ii) $\langle R; \cdot, 1 \rangle$ is a monoid.

iii) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c, \in R$.

Prove that such an algebra satisfies Definition 5.18 in the lecture notes. Each step should consist of one or more applications of the given axioms, and the axioms used should be made explicit.
Hint: consider $(1 + 1)(a + b)$.

9.5 Elementary Properties of Rings ($\star\star$)

The goal of this exercise is to prove Lemma 5.17 (ii) and (iii). You can use only Lemma 5.17 (i), which is proved in the lecture notes. In Subtask b), you can use Subtask a).
Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a ring and let $a, b \in R$. Show that:

a) $(-a)b = -(ab)$

b) $(-a)(-b) = ab$

9.6 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:

a) If $a|b$, then $a|bc$ for all c.

b) If $a|b$ and $a|c$, then $a|(b + c)$.

9.7 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).

a) Prove that for all $x \in \mathbb{Z}$ the subset $(x) = \{xz \mid z \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.

b) Let I be an ideal (with this new definition) of $\mathbb{Z}$. Prove that $I = (z)$ for some $z \in \mathbb{Z}$.

c) 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.

d) 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 [1]

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

Why does the proof of subtask b) break down in this setting?

---

[1]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 subtask b)) are called *principal ideal rings*. Subtask d) shows that the ring $\mathbb{Z}[x]$ is *not* a principal ideal ring.

Due by 23. November 2023.
Exercise 9.4 is graded.