ETH Zürich, D-INFK
HS 2020, 6. November 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Exercise 9

Exercise 9.3 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/DM20/`.

9.1 Structure of Groups ($\star\,\star$)

a) List all subgroups of $\langle \mathbb{Z}_4; \oplus \rangle \times \langle \mathbb{Z}_5; \oplus \rangle$.

b) Let $\langle G; *, \widehat{\ }, e \rangle$ be a group, such that $a*a = e$ for all $a \in G$. Prove that G is commutative.

9.2 Isomorphisms Map Generators to Generators ($\star\,\star$)

Let ψ be a group isomorphism from $\langle G; *, \widehat{\ }, e \rangle$ to $\langle H; \star, \widetilde{\ }, e' \rangle$. Prove that if G is cyclic and g is a generator of G then $\psi(g)$ is a generator of H.

9.3 Applying Group Elements to Elements of Arbitrary Sets ($\star$) *(8 Points)*

Let $\langle G; *, \widehat{\ }, e \rangle$ be a group. For a given set S, let $\theta : G \times S \to S$ be a function such that

i) $\theta(e, s) = s$ for all $s \in S$, and

ii) $\theta(a * b, s) = \theta(a, \theta(b, s))$ for all $a, b \in G$ and all $s \in S$.

Prove the following two statements:

a) For any $a \in G$, the function $\psi_a : S \to S$ with $\psi_a(s) = \theta(a, s)$ is a bijection.

b) The relation $\sim$ defined by $s \sim t \overset{\text{def}}{\iff} \exists a \in G\ \theta(a, s) = t$ is an equivalence relation on S.

9.4 Rotations of a Cube ($\star$) (Optional)

Consider a sofa in the shape of a cube with corners labeled $0, 1, \ldots, 7$, standing in the corner of a room.

a) In how many ways can the sofa be placed in the corner?

Now one can take the sofa from the corner, rotate it in an arbitrary way and place it back in the corner. We distinguish two rotations b_1 and b_2 if the position of the sofa is different after the rotation b_1 and after b_2. Let R denote the set of such different rotations.

b) Determine $|R|$. Is it possible to describe each element of R as a rotation around a single axis? (For different elements the axes can be different.)

c) Let $b_2 \circ b_1$ denote applying to the sofa first the rotation b_1 and then the rotation b_2. Is $\langle R; \circ \rangle$ a group?

d) Is $\circ$ commutative?

9.5 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) ($\star\,\star\,\star$) 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?

9.6 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 $\langle \mathbb{Z}_n^*; \odot \rangle \times \langle \mathbb{Z}_m^*; \odot \rangle$.

d) ($\star\,\star$) Give an isomorphism from $\langle \mathbb{Z}_{15}^*; \odot \rangle$ to $\langle \mathbb{Z}_{20}^*; \odot \rangle$.

Hint: Use the statement proved in Subtask c).

9.7 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 we use these ciphertexts and the public keys to efficiently compute m?

Due by 17. November 2020.
Exercise 9.3 is graded.