ETH Zürich, D-INFK
HS 2017, 13. November 2017

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik

Exercise 9

9.1 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 $m, n > 0$, $\mathbb{Z}_{nm}^*$ is isomorphic to $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$.

d) ($\star\star$) Give an isomorphism from $\langle \mathbb{Z}_{15}^*; \odot \rangle$ to $\langle \mathbb{Z}_{20}^*; \odot \rangle$.
Hint: Use the statement you proved in Subtask c).

9.2 RSA attack ($\star\star\star$)

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?

9.3 Elementary properties of rings ($\star\star$) *(5 Points)*

In this exercise you will prove Lemma 5.17 (iii) and (iv). 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) $(-a)b = -(ab)$ *(2 Points)*

b) $(-a)(-b) = ab$ *(3 Points)*

9.4 Properties of commutative rings ($\star$)

In this exercise you will prove Lemma 5.18 (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 $a|(b + c)$.

9.5 System of linear equations ($\star$)

Consider the field $F = \{0, 1, A, B\}$ with 4 elements, described in Example 5.45. Solve the following system of linear equations over F:

$$\begin{aligned} A \cdot x + B \cdot y + B \cdot z &= A \\ x + A \cdot y + z &= 0 \\ B \cdot x + B \cdot y + z &= 1 \end{aligned}$$

Due on 20. November 2017.
Exercise 9.3 will be corrected.