ETH Zürich, D-INFK
HS 2020, 30. October 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Exercise 8

Exercise 8.2 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/`.

8.1 Multiplicative Inverses

a) ($\star$) 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.

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

8.2 Adding Digits of q-ary Numbers ($\star$) *(8 Points)*

We represent natural numbers in a q-ary system for $q \in \mathbb{N} \setminus \{0, 1\}$. That is, the sequence of digits $(a_0, \ldots, a_k) \in \{0, \ldots, q-1\}^* \setminus \{\epsilon\}$ represents the natural number

$$n = \sum_{i \in \{0,\ldots,k\}} q^i \cdot a_i.$$

a) Prove that for any natural number $n \in \mathbb{N}$ with q-ary representation $(a_0, \ldots, a_k)$ we have

$$R_{q-1}(n) = R_{q-1}\left(\sum_{i \in \{0,\ldots,k\}} a_i\right).$$

b) Let $n \in \mathbb{N}$ be arbitrary and let $(a_0, \ldots, a_k)$ and $(b_0, \ldots, b_k)$ be q-ary representations of n and $2n$, respectively. Prove that

$$\sum_{i \in \{0,\ldots,k\}} a_i = \sum_{i \in \{0,\ldots,k\}} b_i \quad \Longrightarrow \quad (q-1) \mid n.$$

8.3 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 $\gcd(a, m) \mid b$.

8.4 The Chinese Remainder Theorem ($\star\star\star$)

a) 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

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

b) 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?

8.5 Algebras ($\star$)

For each of the following algebras, decide whether it is a monoid, a group or neither. In case it is a monoid or a group, decide whether it is abelian. Justify your answers.

a) $\langle \mathbb{Z}; \star \rangle$, where $\star$ is defined by $a \star b := a^2 + b^2$ for any $a, b \in \mathbb{Z}$.

b) $\langle \mathcal{P}(X); \cup \rangle$, where X is a non-empty finite set.

8.6 Facts About Groups ($\star\star$)

In this exercise you are **not** allowed to use lemmas from the lecture notes (especially, Lemma 5.3). Let $\langle G; *, \widehat{\ }, e \rangle$ be a group.

a) Prove that the group axiom **G2** can be simplified (see also Section 5.2.4 of the lecture notes). That is, show that **G2** follows from the axioms **G1**, **G2**$'$ and **G3**, where

G2$'$ e is a right neutral element: $a * e = a$ for all $a \in G$.

b) Prove that $\widehat{a * b} = \widehat{b} * \widehat{a}$ for all $a, b, c \in G$.

c) Prove that $a * b = a * c \implies b = c$ for all $a, b, c \in G$.

Due by 10. November 2020.
Exercise 8.2 is graded.