ETH Zürich, D-INFK
HS 2020, 23. October 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Exercise 7

Exercise 7.3 gives **bonus points**, which can increase the final grade. The solution to these exercises 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/`.

7.1 Countability

Determine whether the following sets are countable or uncountable. Prove your answers.

i) ($\star$) The set of all Java programs.

ii) ($\star\star\star$) The set of all equivalence relations on $\mathbb{N}$.

7.2 The Diagonalization Argument ($\star\star$)

Let $\alpha_0, \alpha_1, \dots$ be an arbitrary sequence of semi-infinite binary sequences.

a) Define two different semi-infinite binary sequences $\alpha \neq \alpha'$ such that $\alpha \neq \alpha_i$ and $\alpha' \neq \alpha_i$ for all i.

Hint: See the proof of Theorem 3.21.

b) Let L be the set of all semi-infinite binary sequences α such that $\alpha \neq \alpha_i$ for all i. Is L countable? Justify your answer.

7.3 More Countability ($\star\star$) *(8 Points)*

Consider the set

$$S = \left\{ f \in \{0,1\}^{\mathbb{N}} \mid \forall x \, \exists y \, (x < y \wedge f(x) = f(y)) \right\}.$$

Prove or disprove that the set S is countable.

Hint: You can use results from the lecture notes.

Expectation: For this exercise, the claim that a certain function is injective (or bijective) has to be proved explicitly (if such a claim is part of the proof).

7.4 The Hunt for the Red October ($\star\star$)

You have to sink a submarine called the Red October. The submarine moves with the constant speed $v \in \mathbb{Z}$ and, at a given time $t \in \mathbb{N}$, it is located at the position $v \cdot t + s_0$, where

$s_0 \in \mathbb{Z}$ is the starting point. You do not know the values v and s_0. At each point in time you can fire a torpedo to one position $s \in \mathbb{Z}$. If at this moment the Red October can be found exactly at the position s, it sinks. Is there a strategy that allows to sink the Red October in a finite time?

7.5 The Greatest Common Divisor ($\star$)

Prove that for all $a, b, u, v \in \mathbb{Z} \setminus \{0\}$ such that $ua + vb = 1$, we have $\gcd(a, b) = 1$.

7.6 Congruences

Prove that:

a) ($\star$) For all $m, n \in \mathbb{N}$, if $m \equiv_4 n$, then $123^m \equiv_{10} 33^n$.

b) ($\star$) For all $a, b, c, d, m \in \mathbb{Z}$ such that $m > 0$, if $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.

c) ($\star \star \star$) There do not exist $m, n \in \mathbb{Z}$, such that $n^5 + 7 = m^2$.

7.7 Modular Arithmetic ($\star$)

a) Prove that $7 \mid (13^n + 6)$ for every even integer $n \geq 0$.

b) Prove that for any $a, e, m, n \in \mathbb{N} \setminus \{0\}$, if $R_m(a^e) = 1$, then $R_m(a^n) = R_m(a^{R_e(n)})$.

c) Using the above fact, and the fact that $R_{13}(4^6) = 1$, compute $R_{13}(4^{2020})$.

Due by 3. November 2020.
Exercise 7.3 is graded.