ETH Zürich, D-INFK
HS 2020, 20. November 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Exercise 11

Exercise 11.3 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/`.

11.1 Polynomials over a Field ($\star$)

a) Divide $x^5 + 6x^2 + 5$ by $5x^2 + 2x + 1$ over $\mathbb{Z}_7$ with remainders.

b) Determine all irreducible polynomials of degree 4 over $\mathrm{GF}(2)$.

c) Let $a(x)$ be a polynomial of degree 4 in $\mathrm{GF}(7)[x]$. We know that $a(x)$ has a double root at $x = 2$. Moreover, $a(3) = 2$, $a(4) = 3$ and $a(6) = 5$. Determine $a(0)$.

11.2 The Ring $F[x]_{m(x)}$ ($\star$)

a) Find all zero-divisors in the ring $\mathrm{GF}(3)[x]_{x^2+2x}$.

b) Determine all elements of $\mathrm{GF}(3)[x]_{x^2+2}$ and of the multiplicative group $\mathrm{GF}(3)[x]^*_{x^2+2}$.

c) Compute the inverse of the polynomial x in $\mathrm{GF}(3)[x]^*_{x^2+2}$.

11.3 Extension Fields ($\star$) *(8 Points)*

Let $F = \mathbb{Z}_5[x]_{x^2+3}$.

a) Prove or disprove that F is a field.

b) Compute the number of elements of the multiplicative group F^*. Justify your answer.

c) Consider the following matrix M over F

$$M = \begin{pmatrix} 3x+2 & 4x \\ 3x & x+1 \end{pmatrix}.$$

Compute the inverse M^{-1} of M.

Hint: $M^{-1} = (ad - bc)^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ for $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

11.4 Polynomials over Extension Fields ($\star\,\star$)

Factor the polynomial $a(y) = xy^3 + xy^2 + (x+1)y + x \in \mathrm{GF}(2)[x]_{x^2+x+1}[y]$ into irreducible polynomials.

11.5 Secret Sharing ($\star\star$)

A zookeeper takes care of n extremely intelligent monkeys, $M_1, \ldots, M_n$. He decides to store some frozen bananas in a safe, secured with a code $s \in \mathrm{GF}(q)$ (where $q > n$ is a prime). He would like to achieve the following goals ($1 \leq t < n$ is a parameter):

1. In case of an emergency, any t monkeys can open the safe and recover their food.
2. No clan of at most $t - 1$ greedy monkeys can steal the bananas.

In order to achieve this, the zookeeper does as follows. He first chooses n different public values $\alpha_i \in \mathrm{GF}(q) \setminus \{0\}$ and announces them to all monkeys. Then, he chooses at random the t coefficients $a_0, \ldots, a_{t-1} \in \mathrm{GF}(q)$ of a polynomial $a(x) = a_{t-1}x^{t-1} + \cdots + a_0$ of degree at most $t - 1$, and he locks the safe using $a_0 = a(0)$ as the code. Finally, he gives to each monkey M_i its secret share $s_i = a(\alpha_i)$.

a) How can t monkeys recover the code a_0, using their shares s_i?

b) Given $t - 1$ shares of a clan of greedy monkeys, how many possibilities are there for the secret code a_0?

Due by 1. December 2020.
Exercise 11.3 is graded.