ETH Zürich, D-INFK
HS 2017, 20. November 2017

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik

Exercise 10

10.1 Fields

a) ($\star$) Let $\langle F; +, \cdot \rangle$ be a field. Consider the algebra $\langle F \times F; \oplus, \otimes \rangle$ with the operations defined by

$$(a, b) \oplus (c, d) = (a + c, b + d)$$
$$(a, b) \otimes (c, d) = (a \cdot c, b \cdot d)$$

for all $(a, b), (c, d)$ in $F \times F$. Is the algebra $F \times F$ a field?

b) ($\star\star\star$) Show that in a finite field F with q elements, we have

$$x^{q-1} - 1 = \prod_{a \in F \setminus \{0\}} (x - a).$$

c) ($\star\star\star\star$) Let $\langle F; +, \cdot \rangle$ be a finite field with at least three elements. Show that the sum of all elements in F is equal to 0.

10.2 Computing on polynomials

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

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

c) ($\star$) 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 $a(0)$.

10.3 The ring $F[x]_{m(x)}$

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

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

10.4 Finite fields *(11 Points)*

a) ($\star$) Give an example of a field with 9 elements. Moreover, list all the elements of the constructed field. Justify your answer! *(6 Points)*

b) ($\star\star$) Find a generator of the multiplicative group of the field F from Subtask a). Prove that it is indeed a generator. *(5 Points)*

10.5 A safe in a monkey house ($\star\star$)

In a zoo, n extremely intelligent monkeys, $M_1, \ldots, M_n$ have access to a safe, in which a number of frozen bananas is stored for the case of emergency. The safe is secured with a secret code $s \in \mathrm{GF}(q)$ for some prime $q > n$. The knowledge of s is *shared* between the monkeys. Namely, a polynomial $a(x) \in \mathrm{GF}(q)[x]$ of degree at most $t-1$, such that $a(0) = s$, was randomly chosen by the zookeepers (by choosing uniformly at random all but one of the coefficients). Each monkey M_i got a unique value $\alpha_i \in \mathrm{GF}(q) \setminus \{0\}$ and its "share" $s_i = a(\alpha_i)$. The monkeys know all the values α_i, but they do not know the polynomial.

a) One night, all but t monkeys choose freedom and escape from the zoo. Show that the secret code s is not lost and that the remaining monkeys can still access the bananas.

b) A clan of $t-1$ greedy monkeys wants to steal the bananas without telling the others. Given their $t-1$ shares, how many possibilities are there for the secret code s? What does it mean for the clan of greedy monkeys?

Due on 27. November 2017.
Exercise 10.4 will be corrected.