ETH Zürich, D-INFK
HS 2023, 24. November 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Exercise 10

Exercise 10.5 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/DM23/`.

10.1 Warm-Up ($\star$)

a) What is the definition of a field?

b) What is the definition of a root of a polynomial $a(x) \in R[x]$?

c) Is the polynomial $b(x) = x^2 + 2 \in \mathrm{GF}(3)[x]$ irreducible? If not, give its factorization.

10.2 Integral Domains and Fields

a) ($\star$) Recall an example of an integral domain that is not a field.

b) ($\star\star\star$) Prove that every finite integral domain D is a field.

Hint: For an $a \in D \setminus \{0\}$, consider the function $f_a(x) = a \cdot x$.

10.3 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 $\mathrm{GF}(2)$.

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

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 $\mathrm{GF}(3)[x]^*_{x^2+2}$.

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

Let $F = \mathbb{Z}_5[x]_{x^2+4x+1}$.

a) Prove that F is a field.

b) Prove that $F^* = \langle x + 3 \rangle$. Show your work.

c) Write $a(y) = (2x+3)y^2 + (2x+1)y + 1 \in F[y]$ as a product of irreducible polynomials.
Hint: $2x + 1 \equiv_{x^2+4x+1} 2(x + 3)$ in $\mathbb{Z}_5[x]$.

10.6 Secret Sharing ($\star\star$)

We find ourselves on a lonely island, where the ballistic missile system can be activated with a secret key $s \in \mathrm{GF}(q)$ (where q is a prime). This key is distributed among $n < q$ generals $G_1, \ldots, G_n$ as follows: random coefficients $a_1, \ldots, a_{t-1} \in \mathrm{GF}(q)$ are chosen, such that

$$a(x) \stackrel{\text{def}}{=} a_{t-1}x^{t-1} + \ldots + a_1 x + s.$$

Each general G_i receives a *share* $s_i = a(\alpha_i)$, where $\alpha_1, \ldots, \alpha_n$ are publicly known and pairwise distinct values from $\mathrm{GF}(q) \setminus \{0\}$.

a) All except t generals die on a fishing trip. Show that the key is not lost, because it can be determined uniquely from t shares.

b) Mario (one of the generals) wants to resolve a dispute with his neighbor by using a ballistic missile. In order to determine the key s, he has collected a total of $t - 1$ shares (including her own share). How many values from $\mathrm{GF}(q)$ are still possible for the key, given $t - 1$ shares? Prove your answer.

10.7 Structure of Multiplicative Groups of Finite Fields ($\star\star\star$)

In this exercise we break down the proof of Theorem 5.40 from the lecture notes in smaller steps. Let F be a finite field and let $n = |F^*|$.

a) Let $a, b \in \mathbb{Z}$. Prove that $\gcd(a, b) = d \iff d \mid a$ and $d \mid b$ and $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

b) For $d \mid n$ define $A(d) = \{k \in \{1, \ldots, n\} \mid \gcd(k, n) = d\}$. Use subtask a) to prove that $|A(d)| = \varphi\left(\frac{n}{d}\right)$.

c) Use subtask b) to prove that $\sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$.

d) Use subtask c) to prove $n = \sum_{d|n} \varphi(n)$.

e) Let $B(d) = \{k \in F^* \mid \mathrm{ord}(k) = d\}$. Show that $|B(d)| \in \{0, \varphi(d)\}$.
Hint: consider the polynomial $x^d - 1 \in F[x]$.

f) Use subtasks d) and e) to show that if $d \mid n$ then $|B(d)| = \varphi(d)$.

g) Use subtask f) to conclude that F^* is cyclic.

Due by 30. November 2023.
Exercise 10.5 is graded.