Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Homework Sheet 2
Version 07.05.2020

Homework 1.

1. We consider the function $\varphi \in \mathcal{S}_5$ given as follows:

i	1	2	3	4	5
$\varphi(i)$	2	1	4	5	3

   Compute $\operatorname{ord}(\varphi)$ in $(\mathcal{S}_5, \circ)$.

2. We consider the function $\varphi \in \mathcal{S}_{10}$ given as follows:

i	1	2	3	4	5	6	7	8	9	10
$\varphi(i)$	2	1	4	5	3	8	10	9	7	6

   Compute $\operatorname{ord}(\varphi)$ in $(\mathcal{S}_{10}, \circ)$.

3. For $n \in \mathbb{N}$, we consider the cyclic left shift $\varphi \in \mathcal{S}_n$ given as follows:

i	1	2	...	$n-1$	n
$\varphi(i)$	2	3	...	n	1

   Compute $\operatorname{ord}(\varphi)$ in $(\mathcal{S}_n, \circ)$.

Homework 2.

Check whether the following structures $(\mathcal{R}, \oplus, \odot)$ are rings or even fields. In case of a ring, check whether it is zero-divisor free, i.e., whether the following property holds:

$$\forall x, y \in \mathcal{R}: \qquad x \odot y = o \quad \Longrightarrow \quad x = o \text{ or } y = o.$$

Above, o denotes the neutral element w.r.t. $\oplus$.

a) We consider the set $\mathcal{R} := \mathbb{Z}\times\mathbb{Z}$ of all pairs of integers equipped with the following binary operations:

$$\forall (a,b),(c,d) \in \mathbb{Z}\times\mathbb{Z}: \quad (a,b)\oplus(c,d) := (a+c, b+d) \qquad (a,b)\odot(c,d) := (a\cdot c, b\cdot d).$$

Above, $+$ and $\cdot$ denote the standard addition and multiplication in $\mathbb{Z}$.

b) Let $\mathcal{R}$ be the set of all subsets of $\mathbb{Z}$. We equip $\mathcal{R}$ with the following binary operations:

$$\forall A, B \in \mathcal{R}: \quad A \oplus B := A \cup B \qquad A \odot B := A \cap B.$$

Above, $\cup$ and $\cap$ denote the standard union and intersection operators for sets.

c) Let $\mathcal{R} \subset \mathcal{T}_{\mathbb{R}}$ be given by

$$\mathcal{R} := \{f \in \mathcal{T}_{\mathbb{R}} \,|\, \exists a \in \mathbb{R}\, \forall x \in \mathbb{R}: \; f(x) = ax\}.$$

We equip $\mathcal{R}$ with the binary operations defined by

$$\forall f, g \in \mathcal{R}\, \forall x \in \mathbb{R}: \quad (f \oplus g)(x) := f(x) + g(x) \qquad (f \odot g)(x) := g(f(x)).$$

Homework 3.

Solve the following systems of linear equations in the field $\mathbb{Z}_{23}$:

$$\begin{aligned} 3x_1 \quad\quad\quad + 19x_3 &= 11 \\ 2x_1 + 14x_2 + 12x_3 &= 2 \\ 17x_1 + 10x_2 + 5x_3 &= 17, \end{aligned} \qquad \begin{aligned} 9x_1 + 2x_2 + 20x_3 &= 9 \\ 2x_1 + 4x_2 + 20x_3 &= 9 \\ x_1 + 5x_2 + 3x_3 &= 14. \end{aligned}$$

Homework 4.

Compute the smallest natural number which solves the subsequently stated system of congruences:

$$\begin{aligned} x &\equiv 1 \mod 11 \\ x &\equiv 2 \mod 12 \\ x &\equiv 3 \mod 13. \end{aligned}$$