Fall 2019 – Math 328K – Florian Stecker

Homework 5

due Thursday, October 3, 11:00

Problem 1. We say that $\mathbb{Z}_m$ *has zero–divisors* if there are $x, y \in \mathbb{Z}_m$, both not $\overline{0}$, such that $xy = \overline{0}$.

a) For which $m \in \mathbb{N}$ does $\mathbb{Z}_m$ have zero–divisors? Give a proof.

b) Show that the cancellation law ($ac = bc$ implies $a = b$ for non–zero c) holds in $\mathbb{Z}_m$ if and only if $\mathbb{Z}_m$ has no zero–divisors.

Hint: To find a guess for a), look at the multiplication tables from the previous homework.

Problem 2. Prove Theorem 4.5: Let $m \in \mathbb{N}$. Then

1. $a + b = b + a$ and $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{Z}_m$,
2. $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{Z}_m$,
3. $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in \mathbb{Z}_m$,
4. $a + \overline{0} = a$ and $a \cdot \overline{1} = a$ for all $a \in \mathbb{Z}_m$. If $m > 1$, then $\overline{0} \neq \overline{1}$.
5. For every $a \in \mathbb{Z}_m$ there exists a unique additive inverse $-a \in \mathbb{Z}_m$ such that

$$a + (-a) = \overline{0}.$$

   If $a = \overline{x}$, then $-a = \overline{-x}$.

Problem 3. Show that the equation $x^2 = \overline{1}$ has one solution in $\mathbb{Z}_2$, two solutions in $\mathbb{Z}_4$ and four solutions in $\mathbb{Z}_{2^k}$ for all integers $k > 2$.

Problem 4. Let $a, b, c \in \mathbb{N}$ with

$$a \bmod c = b \bmod c.$$

Show that

$$(2^a - 1) \bmod (2^c - 1) = (2^b - 1) \bmod (2^c - 1).$$

Problem 5. Find inverses of $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ and $\overline{5}$ in $\mathbb{Z}_{8512}$, if they exist.