Fall 2021 – Math 328K – 55385

Homework 5

due Tuesday, October 5, 14:00

Problem 1. Find all solutions in $\mathbb{Z}/243\mathbb{Z}$ to the following equations:

a) $18x = 27$,

b) $3x = 3$,

c) $5x = 17$,

d) $6x = 19$.

Is it a valid strategy to simplify such an equation by dividing both sides by the greatest common divisor, for example replacing $18x = 27$ by $2x = 3$? Why/why not?

Problem 2. Let p be an odd prime and $a \in \mathbb{Z}/p\mathbb{Z}$ with $a \neq 0 \bmod p$. A *square root* of a is a solution $x \in \mathbb{Z}/p\mathbb{Z}$ of the equation $x^2 = a$.

a) Show that every $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0 \bmod p\}$ has either none or exactly two square roots.

b) Conclude that $\mathbb{Z}/p\mathbb{Z}$ has exactly two elements which are their own inverses.

c) Find the square roots of all elements of $\mathbb{Z}/7\mathbb{Z}$, if they exist.

d) Is the statement of a) still true if p is not prime?

Problem 3. Show that the equation $x^2 = 1$ has one solution in $\mathbb{Z}/2\mathbb{Z}$, two solutions in $\mathbb{Z}/4\mathbb{Z}$ and four solutions in $\mathbb{Z}/2^k\mathbb{Z}$ 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 [1], [2], [3], [4] and [5] in $\mathbb{Z}/8512\mathbb{Z}$, if they exist.