Second exam – Elementaire Getaltheorie

Lennart Meier

October 10, 2019

In all problems write your solution in detail. Each step has to be proven or cited from class. If you cannot solve part (a) or (b) of a problem, you are nevertheless allowed to use it in the following parts without proof.

Problem 1 (8 points)**.** *Determine* all odd *primes p such that*

$$x^2 \equiv 13 \mod p$$

has a solution with $x \in \mathbb{Z}$.

More precisely: Find an $n > 1$ and $a_1, \ldots, a_r \in \mathbb{Z}$ such that $x^2 \equiv 13 \mod p$ has a solution if and only if $p \equiv a_i \mod n$ for some $1 \leq i \leq r$.

Problem 2 (10 points)**.** *Decide for the following three congruences whether there are solutions. (Hint: You might want to determine first whether the numbers 101, 91 and 9991 are prime.)*

(a) $x^2 \equiv 91 \mod 101$

(b) $x^2 \equiv 5 \mod 91$

(c) $x^2 \equiv 2 \mod 9991$

Problem 3 (12 points)**.** *Let p be an odd prime.*

(a) Show that $1^k + 2^k + \cdots + (p-1)^k \equiv -1 \mod p$ if $(p-1)|k$.

(b) Let $\gcd(k, p-1) = 1$. Show that for every $a \in \mathbb{Z}$, there is an $x \in \mathbb{Z}$ with $x^k \equiv a \mod p$ and that any two such x are congruent to each other modulo p.

(c) Show that $1^k + 2^k + \cdots (p-1)^k \equiv 0 \mod p$ if $\gcd(p-1, k) = 1$.