Solutions for first midterm

Lennart Meier

October 10, 2019

In the solutions, I do not give all possible approaches, but just one or two. Please write to me if you find any typos or have other remarks.

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 $1 \leq i \leq r$.

There is a solution (namely $x = 0$) if $p = 13$. We note that $p = 13$ iff $p \equiv 0 \mod 13$.

Now assume that $p \neq 13$ is an odd prime. There is a solution of $x^2 \equiv 13 \mod p$ iff $\left(\frac{13}{p}\right) = 1$. By quadratic reciprocity, we have $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right)$ as $13 \equiv 1 \mod 4$. Thus $x^2 \equiv 13 \mod p$ has a solution iff p is a quadratic residue mod 13 (or $p = 13$).

The quadratic residues mod 13 are $\pm 1, \pm 3$ and ± 4 as a quick claculation shows. Thus, the p we are searching for are those that are congruent to $0, \pm 1, \pm 3$ or ± 4 modulo 13.

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

a) 101 is prime (not divisible by 2, 3, 5 and 7). We compute:

$$\left(\frac{91}{101}\right) = \left(\frac{101}{91}\right) = \left(\frac{101}{7}\right)\left(\frac{101}{13}\right) = \left(\frac{3}{7}\right)\left(\frac{10}{13}\right) = (-1) \cdot 1 = -1$$

Here we use quadratic reciprocity for Jacobi symbols and that we have computed the quadratic residues modulo 7 and 13 before. (For the last step, you could of course also use quadratic reciprocity again.)

b) Note $91 = 7 \cdot 13$. If $x^2 \equiv 5 \mod 91$ has a solution, then $x^2 \equiv 5 \mod 13$ has a solution as well. But 5 is not a quadratic residue modulo 13 as noted above. Thus, there is no solution.

c) We note $9991 = 10000 - 9 = 100^2 - 3^2 = 97 \cdot 103$. The numbers 97 and 103 are primes. Thus the Chinese Remainder Theorem implies that $x^2 \equiv 2 \mod 9991$ has a solution if and only if $x^2 \equiv 2 \mod 97$ and $x^2 \equiv 2 \mod 103$ have solution. As $97 \equiv 1 \mod 8$ and $103 \equiv -1 \mod 8$, we know that 2 is a quadratic residue modulo 97 and 103. Thus, $x^2 \equiv 2 \mod 9991$ also has a solution. (Alternatively, one can use the formula for the Jacobi symbol $\left(\frac{2}{9991}\right)$.)

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 $\gcd(p-1, k) = 1$.

a) Write $k = (p-1)l$. By Fermat's little theorem, we obtain $a^{p-1} \equiv 1 \mod p$ for every a not divisible by p and thus $a^k = \left(a^{p-1}\right)^l \equiv 1^l = 1 \mod p$. Thus,

$$1^k + \cdots (p-1)^k \equiv 1 + \cdots + 1 = (p-1) \equiv -1 \mod p.$$

b) If $a \equiv 0 \mod p$, the condition becomes $x^k \equiv 0 \mod p$, i.e. $p|x^k$. By Euclid's lemma, this is true if and only if $x \equiv 0 \mod p$. Thus assume a not divisible by p.

High-brow solution: The problem is equivalent to the following statement: For each $[a] \in (\mathbb{Z}/p)^\times$, there is a unique $[x] \in (\mathbb{Z}/p)^\times$ such that $[x]^k = [a]$. By the existence of a primitive root we know $(\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$ as abelian groups. Thus, the problem is equivalent to: For each $[b] \in \mathbb{Z}/(p-1)$ is there a unique $[c] \in \mathbb{Z}/(p-1)$ with $[k][c] = [b]$. This is true, as $[k]$ is invertible in $\mathbb{Z}/(p-1)$ and thus the unique solution is $[c] = [b][k]^{-1}$.

Alternative lower-brow solution: Let b be a primitive root modulo p. Thus $a \equiv b^m \mod p$ for some integer p. Choose $d, e \in \mathbb{Z}$ with $dk + e(p-1) = m$ (which is possible as $\gcd(k, p-1) = 1$). Set $x = b^d$. Then $x^k = b^{dk} = b^{m-e(p-1)}$. Note that $b^{e(p-1)} \equiv 1 \mod p$ as $b^{p-1} \equiv 1 \mod p$ by Fermat's theorem. Thus $x^k = x^k \cdot 1 \equiv b^m \equiv a \mod p$. This shows existence. For uniqueness suppose that $x_1^k \equiv a \equiv x_2^k \mod p$. Suppose $x_1 \equiv b^{d_1} \mod p$ and $x_2 \equiv b^{d_2} \mod p$. As b has order $(p-1)$, we see that $kd_1 \equiv kd_2 \mod (p-1)$. Because k is relative prime to $(k-1)$, it follows that $d_1 \equiv d_2 \mod (p-1)$. As $b^{p-1} \equiv 1 \mod p$, it follows that $x_1 \equiv b^{d_1} \equiv b^{d_2} \equiv x_2$.

c) For $1 \leq x \leq p-1$, let $a(x)$ be the remainder of x^k if dividing by p. Part (b) implies that

$$\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}, \qquad x \mapsto a(x)$$

is a bijection. Thus,

$$\begin{aligned} 1^k + \cdots + (p-1)^k &\equiv a(1) + \cdots a(p-1) \mod p \\ &= 1 + \cdots + (p-1) \\ &= \frac{p(p-1)}{2} \\ &= \frac{p-1}{2} \cdot p \end{aligned}$$

This is clearly congruent to 0 modulo p.