MEM204-Number Theory

15th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 22/05/2020

University of Crete

Answers of the 5th set

Exercise

Let $n = 2^r p_1^{n_1} \cdots p_k^{n_k}$, where $r \geq 0$ and $n_i \geq 0$, be the prime factorization of n. Further, let $(a, n) = 1$. Then

$$x^2 \equiv a \pmod{n}$$

is solvable if and only if $x^2 \equiv a \pmod{p_i^{n_i}}$ is solvable for $i = 1, \ldots, k$ and $x^2 \equiv a \pmod{2^r}$ is solvable (if $r \geq 2$).

Answer

We have that

$$\begin{aligned} x^2 \equiv a \pmod{n} \iff n \mid x^2 - a \iff p_i^{n_i} \mid x^2 - a \,\forall\, i \\ \iff x^2 \equiv a \pmod{p_i^{n_i}} \,\forall\, i. \end{aligned}$$

Exercise 3

Exercise

Let p be an odd prime, $r \geq 1$ and $p \nmid a$. Then $x^2 \equiv a \pmod{p^r}$ is solvable if and only if $x^2 \equiv a \pmod{p}$ is solvable.

Exercise 3

First, assume that $x^2 \equiv a \pmod{p^r}$ is solvable and let b be a solution. Then

$$b^2 \equiv a \pmod{p^r} \Rightarrow p^r \mid b^2 - a \Rightarrow p \mid b^2 - a \Rightarrow b^2 \equiv a \pmod{p},$$

hence $x^2 \equiv a \pmod{p}$ is solvable.

Next, assume that $x^2 \equiv a \pmod{p}$ is solvable and let b be a solution. We will show that b corresponds to a unique solution b_k of $f(x) \equiv 0 \pmod{p^k}$, for every $k \geq 1$, where $f(x) = x^2 - a$. We will use induction on k. For $k = 1$ the result is clear. Assume that it holds for $k = m$. Then, for $k = m + 1$, we have that $f'(b_m) = 2b_m \not\equiv 0 \pmod{p}$, since $p \nmid 2$ and $b_m^2 \equiv a \not\equiv 0 \pmod{p^m} \Rightarrow p \nmid b_m$. The result follows.

Exercise 4

Exercise

Let a be an odd number and $r \geq 3$. *Then* $x^2 \equiv a \pmod{2^r}$ *is solvable if and only if* $a \equiv 1 \pmod{8}$.

Exercise 4

It is not hard to confirm the statement for $r = 3$. Now, assume that $r > 3$ and $x^2 \equiv a \pmod{2^r}$ is solvable. Then $b^2 - a \equiv 0 \pmod{2^r}$, for some b. We have that

$$b^2 - a \equiv 0 \pmod{2^r} \Rightarrow 2^r \mid b^2 - a \Rightarrow 8 \mid b^2 - a,$$

that is, $x^2 \equiv a \pmod{8}$ is solvable. From the $r = 3$ case, this means that $a \equiv 1 \pmod{8}$.

We now focus on the other direction. Namely, assume that $a \equiv 1 \pmod{8}$. We will show that $x^2 \equiv a \pmod{2^r}$ is solvable for $r \geq 3$, using induction on r. We have already commented on the $r = 3$ case. Assume that $x^2 \equiv a \pmod{2^k}$ is solvable, where $k \geq 3$ and let x_0 be a solution. We will show that, for a suitable y, the number $x = x_0 + y2^{k-1}$ is a solution of

$$x^2 \equiv a \pmod{2^{k+1}}.$$

Exercise 4

The latter is equivalent to

$$x_0^2 + 2^k x_0 y + 2^{2k-2} y \equiv a \pmod{2^{k+1}}.$$

We have that $2k - 2 \geq k + 1$, for $k \geq 3$, hence $2^{2k-2} \equiv 0 \pmod{2^{k+1}}$. Furthermore, from the induction hypothesis, $2^k \mid x_0^2 - a$, that is $\frac{x_0^2 - a}{2^k} \in \mathbb{Z}$. We eventually get that

$$y x_0 \equiv \frac{x_0^2 - a}{2^k} \pmod{2^{k+1}}.$$

Since a is odd, the same goes for x_0, hence the above equation has a solution (for y). The result follows.

Exercise 5 – a characterization

By combining the last three exercises, we get the following.

Proposition

Let $n = 2^r p_1^{n_1} \cdots p_k^{n_k}$*, where* $r \geq 0$ *and* $n_i \geq 0$*, be the prime factorization of* n*. Further, let* $(a, n) = 1$*. Then*

$$x^2 \equiv a \pmod{n}$$

is solvable if and only if $\left(\frac{a}{p_i}\right) = 1$*, for all* $i = 1, \ldots, n$ *and*

$$a \equiv \begin{cases} 1 \pmod{8}, & \text{if } r \geq 3, \\ 1 \pmod{4}, & \text{if } r = 2. \end{cases}$$

Exercise 7 (items iii and iv)

Exercise

Compute the following symbols:

$$\left(\frac{100}{31}\right), \ \left(\frac{3}{23}\right).$$

Answer

$$\left(\frac{100}{31}\right) = \left(\frac{10^2}{31}\right) = \left(\frac{10}{31}\right)^2 = 1.$$

$$\left(\frac{3}{23}\right) = (-1)^{2\cdot 22/4}\left(\frac{23}{3}\right) = (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1.$$

Exercise 9

Exercise

Check whether $x^2 \equiv 7 \pmod{19}$ *is solvable.*

Answer

The above is solvable iff 7 is a quadratic residue modulo 19 and since 19 is a prime, it suffices to compute the symbol $\left(\frac{7}{19}\right)$. We have that

$$\begin{aligned}\left(\frac{7}{19}\right) &= (-1)^{6\cdot 18/4}\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) \\ &= -\left(\frac{-2}{7}\right) = \left(\frac{2}{7}\right) = (-1)^{(7^2-1)/8} = 1,\end{aligned}$$

thus the original congruence is solvable.

Exercise 10

Exercise

Find all the primes $10 < p < 100$*, such that* $p \mid n^2 + 1$*, for some n.*

Answer

We have that $p \mid n^2 + 1 \iff n^2 \equiv (-1) \pmod{p}$. The latter is solvable iff $\left(\frac{-1}{p}\right) = 1$, that is, iff $(p-1)/2$ is even, i.e., iff $p \equiv 1 \pmod{4}$. It follows that we are looking for all the primes of the form $4k + 1$, where $3 \leq k \leq 24$. These primes are:

$$13, 17, 29, 37, 41, 53, 61, 73, 89, 97.$$

Exercise 11

Exercise

Let p be prime, such that $p \equiv 3 \pmod 4$. If $a^2 + b^2 \equiv 0 \pmod p$, show that $a \equiv b \equiv 0 \pmod p$.

Answer

Assume that $a \not\equiv 0 \pmod p$. Then, clearly, $b \not\equiv 0 \pmod p$ and $a^2 \equiv -b^2 \pmod p$. Also, we get that

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

The latter implies that $(p-1)/2$ is even, i.e., that $p \equiv 1 \pmod 4$, a contradiction. It follows that $a \equiv 0 \pmod p$, which in turn implies $b \equiv 0 \pmod p$.

Stay safe!