UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
NUMBER THEORY - MEM204 (SPRING SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

5th exercise set - Answers

**Exercise 1.** Let $p$ be a prime and $m \in \mathbb{Z}_{>0}$. Prove that the congruence

$$x^m \equiv 0 \pmod{p^m}$$

has exactly $p^{m-1}$ solutions.

*Answer.* We will use induction on $m$. The statement is clear for $m = 1$ ($x \equiv 0 \pmod{p}$ is the sole solution).

Assume that $x^k \equiv 0 \pmod{p^k}$ has exactly $p^{k-1}$ solutions.

Let $f(x) = x^{k+1}$. In order to complete the proof, i.e., show that $f(x) \equiv 0 \pmod{p^{k+1}}$ has $p^k$ solutions, it suffices to prove two facts:

1. The solutions of $f(x) \equiv 0 \pmod{p^k}$ concide with the solutions of $x^k \equiv 0 \pmod{p^k}$ (hence there are $p^{k-1}$ of them from the induction hypothesis).
2. If $b$ is one of those solutions, then $f'(b) \equiv f(b) \equiv 0 \pmod{p^{k+1}}$ (hence each of them corresponds to $p$ solutions of $f(x) \equiv 0 \pmod{p^{k+1}}$).

Let $\nu_p(b)$ stand for the exponent of $p$ in the prime factorization of $b$. Then, if $f(b) \equiv 0 \pmod{p^k}$, we get that

$$p^k \mid b^{k+1} \iff \nu_p(b^{k+1}) \geq k \iff \nu_p(b) \geq 1 \iff p^\ell \mid b^\ell,$$

for all $\ell \geq 1$. For $\ell = k$, the above implies the Item 1, while, for $\ell = k$ and $\ell = k+1$, it implies Item 2. $\square$

**Exercise 2.** 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 $i = 1, \dots, k$ and $x^2 \equiv a \pmod{2^r}$ is solvable (if $r \geq 2$).

*Answer.* We have that

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

**Exercise 3.** 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.

*Answer.* 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. $\square$

**Exercise 4.** Let $a$ be an odd number and $r \geq 3$. Then $x^2 \equiv a \pmod{2^r}$ is solvable if and only if $a \equiv 1 \pmod{8}$.

*Answer.* 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

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

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

$$yx_0 \equiv \frac{x_0^2 - a}{2^k} \pmod{2^{k+1}}.$$

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

**Exercise 5.** 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

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

*Answer.* This follows as a corollary of Exercises 2-4. □

**Exercise 6.** Solve the congruence $4x^4 + 4x^3 + 6x^2 + 21x + 7 \equiv 0 \pmod{252}$.

*Answer.* Our first step is to factor the modulus into primes and split the problem into smaller ones. Here, we have that

$$252 = 2^2 3^2 7,$$

hence, if $f(x) = 4x^4 + 4x^3 + 6x^2 + 21x + 7$, it suffices to solve

$$f(x) \equiv 0 \pmod{2^2}, \tag{1}$$

$$f(x) \equiv 0 \pmod{3^2} \tag{2}$$

and

$$f(x) \equiv 0 \pmod 7. \tag{3}$$

First, we focus on (1). First we solve

$$f(x) \equiv 0 \pmod 2,$$

which is trivial to see that, 1 is its only solution $\pmod 2$. Then, we compute

$$f'(x) = 16x^3 + 12x^2 + 12x + 21,$$

that is $f'(1) \not\equiv 0 \pmod 2$. So, we conclude that there is a unique solution of (1), namely $x \equiv 3 \pmod 4$.

Then, we focus on (2). First, we consider $f(x) \equiv 0 \pmod 3$. We easily check that this is equivalent to $x^2 + x + 1 \equiv 0 \pmod 3$, that has the unique solution $1 \pmod 3$. Again, we confirm that $f'(1) \not\equiv 0 \pmod 3$, hence we have a unique solution for (2).

In order to find it, we compute $-f(1)/p^{2-1} = -42/3 = -14$ and $f'(1) = 61$, that is, we need to solve

$$61t \equiv -14 \pmod 3.$$

The above is equivalent to $t \equiv 1 \pmod 3$, so our (unique) solution is $x \equiv tp^{r-1} + b \equiv 4 \pmod 9$.

Finally, we focus on (3). One can easily see that this is equivalent to

$$2x^2(2x^2 + 2x + 3) \equiv 0 \pmod 7.$$

Since 7 is a prime, the latter yields that either $x \equiv 0 \pmod 7$, or $2x^2 + 2x + 3 \equiv 0 \pmod 7$. We explicitly check all values of $\mathbb{Z}_7$, and conclude that the second's congruence solutions are $1$ and $5 \pmod 7$.

In total, we have three solutions $x \equiv 0 \pmod 7$, $x \equiv 1 \pmod 7$ and $x \equiv 5 \pmod 7$.

To sum up, the solutions of the original congruence, are the solutions of the systems

$$\begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 9, \\ x \equiv 0 \pmod 7, \end{cases} \quad \begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 9, \\ x \equiv 1 \pmod 7, \end{cases} \quad \text{and} \begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 9, \\ x \equiv 5 \pmod 7. \end{cases}$$

The solutions of the above systems are

$$x \equiv 175,\ 211 \text{ and } 103 \pmod{252}$$

respectively. □

**Exercise 7.** Compute the following symbols:

$$\left(\frac{-14}{71}\right),\ \left(\frac{219}{383}\right),\ \left(\frac{100}{31}\right),\ \left(\frac{3}{23}\right).$$

*Answer.*

$$\begin{aligned} \left(\frac{-14}{71}\right) &= \left(\frac{-1}{71}\right)\left(\frac{2}{71}\right)\left(\frac{7}{71}\right) = (-1)^{\frac{70}{2}+\frac{71^2-1}{8}}\left(\frac{7}{71}\right) = (-1)\left(\frac{7}{71}\right) \\ &= (-1)\cdot(-1)^{\frac{70\cdot 6}{4}}\left(\frac{71}{7}\right) = \left(\frac{71}{7}\right) = \left(\frac{1}{7}\right) = 1. \end{aligned}$$

$$\begin{aligned} \left(\frac{219}{383}\right) &= \left(\frac{3}{383}\right)\left(\frac{73}{383}\right) = (-1)^{2\cdot 382/4}\left(\frac{383}{3}\right)(-1)^{72\cdot 382/4}\left(\frac{383}{73}\right) \\ &= (-1)\left(\frac{383}{3}\right)\left(\frac{383}{73}\right) = (-1)\left(\frac{2}{3}\right)\left(\frac{18}{73}\right) = \left(\frac{18}{73}\right) \\ &= \left(\frac{2}{73}\right)\left(\frac{3^2}{73}\right) = (-1)^{(73^2-1)/8}\cdot 1 = 1. \end{aligned}$$

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

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

□

**Exercise 8.** Check whether $x^2 - 6x - 13 \equiv 0 \pmod{127}$ is solvable.

*Answer.* The above is equivalent to $y^2 \equiv 22 \pmod{127}$, where $y = x-3$. In other words, the original congruence is solvable iff 22 is a quadratic residue modulo 127. Also, since 127 is prime, this means that if suffices to compute $\left(\frac{22}{127}\right)$. So, we have that

$$\begin{aligned}\left(\frac{22}{127}\right) &= \left(\frac{2}{127}\right)\left(\frac{11}{127}\right) = \left(\frac{11}{127}\right) = -\left(\frac{127}{11}\right) = -\left(\frac{6}{11}\right) \\ &= -\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1.\end{aligned}$$

It follows that the original congruence is solvable. $\square$

**Exercise 9.** 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

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

thus the original congruence is solvable. $\square$

**Exercise 10.** 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 $3 \le k \le 24$. These primes are:

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

**Exercise 11.** 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 $b \equiv 0 \pmod{p}$. $\square$

**Exercise 12.** Show that, if $n$ is a positive odd number,

$$\left(\frac{6}{n}\right) = \begin{cases} 1, & \text{if } n \equiv \pm 1 \text{ or } \pm 5 \pmod{24}, \\ -1, & \text{if } n \equiv \pm 7 \text{ or } \pm 11 \pmod{24}. \end{cases}$$

*Answer.* We have that

$$\left(\frac{6}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{3}{n}\right) = (-1)^{(n^2-1)/8}\left(\frac{3}{n}\right) = (-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}}\left(\frac{n}{3}\right).$$

The result follows from the facts

$$(-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}} = \begin{cases} 1, & \text{if } n \equiv 1 \text{ or } 3 \pmod 8, \\ -1, & \text{if } n \equiv -1 \text{ or } -3 \pmod 8, \end{cases}$$

$$\left(\frac{n}{3}\right) = \begin{cases} 1, & \text{if } n \equiv 1 \pmod 3, \\ -1, & \text{if } n \equiv -1 \pmod 3, \end{cases}$$

and the Chinese Remainder Theorem. □