# Math 328K. Fall 2025
## Some solutions to Homework # 6

*Prof. Hector E. Lomeli*

**Section 4.1. Exercise 14.** If $a \equiv b \pmod{c}$ then there exists $n \in \mathbb{Z}$ such that $a = b + nc$. This implies that

$$(a, c) = (b + nc, c) = (b, c).$$

**Section 4.1. Exercise 30.** Consider the following predicate

$$P(n) \Leftrightarrow 4^n \equiv 1 + 3n \pmod{9}.$$

We will use the PMI to prove that $P(n)$ is true for all $n \in \mathbb{N}$.

Clearly $P(1)$ is true. Let $n \in \mathbb{N}$ be arbitrarily chosen. We assume that $P(n)$ is true. We will show that $P(n+1)$ is also true. Given that $P(n)$ is true, we have that $4^n \equiv 1 + 3n \pmod{9}$. Multiplying by 4, we get that

$$4^{n+1} \equiv 4 + 12n \pmod{9}.$$

Clearly, $12 \equiv 4 \pmod{9}$. This implies that

$$4 + 12n \equiv 4 + 3n \equiv 1 + 3(n+1) \pmod{9}.$$

We conclude that $4^{n+1} \equiv 1 + 3(n+1) \pmod{9}$. This shows that $P(n+1)$ is true.
The PMI implies that $P(n)$ is true, for all $n \in \mathbb{N}$.

**Section 4.1. Exercise 34.** Clearly, if $x \equiv 0, 1 \pmod{p}$, then $x^2 \equiv x \pmod{p}$. Assume that we have a solution $x_0$ of the equation. Then $p | x_0^2 - x_0 = x_0(x_0 - 1)$. Using Euclid's theorem we find that either $p | x_0$ or $p | x_0 - 1$. Hence $x_0 \equiv 0 \pmod{p}$ or $x_0 \equiv 1 \pmod{p}$.

**5.** We have that there exist integers $k_1$ and $k_2$ such that

$$x_1 y_1 = 11k_1 + 1, \qquad x_2 y_2 = 7k_2 + 1.$$

This implies that

$$\begin{aligned} z\bar{z} - 1 &= -98x_1y_1 + 154x_2y_1 + 231x_1y_2 - 363x_2y_2 - 1 \\ &= -98\,(11k_1 + 1) - 363\,(7k_2 + 1) + 154x_2y_1 + 231x_1y_2 - 1 \\ &= -1078k_1 - 2541k_2 + 154x_2y_1 + 231x_1y_2 - 462 \\ &= 77\,(-14k_1 - 33k_2 + 2x_2y_1 + 3x_1y_2 - 6)\,. \end{aligned}$$

Given that $x_1, x_2, y_1, y_2, k_1, k_2$ are integers, we conclude that $77 \mid z\bar{z} - 1$.

**6.** Consider the following predicate

$$P(n) \Leftrightarrow x_n \equiv 15n + 9\,(-1)^n \pmod{45}.$$

We will use the PMI to prove that $P(n)$ is true for all $n \in \mathbb{N}$.

Clearly $P(1)$ is true. Let $n \in \mathbb{N}$ be arbitrarily chosen. We assume that $P(n)$ is true. We will show that $P(n+1)$ is also true. Given that $P(n)$ is true, we have that $x_n \equiv 15n + 9\,(-1)^n \pmod{45}$. Multiplying by 4 and adding 15, we get that

$$x_{n+1} = 4x_n + 15 \equiv 60n + 36\,(-1)^n + 15 \equiv 15n - 9\,(-1)^n + 15 = 15(n+1) + 9\,(-1)^{n+1} \pmod{45}.$$

We conclude that $x_{n+1} \equiv 15(n+1) + 9\,(-1)^{n+1} \pmod{45}$. This shows that $P(n+1)$ is true. The PMI implies that $P(n)$ is true, for all $n \in \mathbb{N}$.

**Section 4.2. Exercise 2b).** There are three incongruent solutions $x \equiv 2, 5, 8 \pmod{9}$.

**Section 4.2. Exercise 2c).** There is one incongruent solution $x \equiv 7 \pmod{21}$.

**Section 4.2. Exercise 2e).** There is one incongruent solution $x \equiv 812 \pmod{1001}$.

**Section 4.2. Exercise 2f).** There is one incongruent solution $x \equiv 1596 \pmod{1597}$.

**Section 4.2. Exercise 6.** First, we notice that $(12, 30) = 6$. To have a solution, we need $6|c$. The possible values of $c$ on the interval $0 \leq c < 30$ are 0, 6, 12, 18, 24.

**Section 4.2. Exercise 8.** If $\bar{a}$ denotes the inverse of $a$, we have the following values

| $a$ | 2 | 3 | 5 | 11 |
|---|---|---|---|---|
| $\bar{a}$ | 7 | 9 | 8 | 6 |

**Section 4.2. Exercise 10a).** The numbers $a$ for which an inverse modulo 14 exists are precisely the numbers that are relatively prime with 14. Therefore, the numbers $1 \leq a \leq 14$ that have an inverse are: 1, 3, 5, 9, 11, 13.

**Section 4.2. Exercise 10b).** If $\bar{a}$ denotes the inverse of $a$ modulo 14, we have the following values.

| $a$ | 1 | 3 | 5 | 9 | 11 | 13 |
|---|---|---|---|---|---|---|
| $\bar{a}$ | 1 | 5 | 3 | 11 | 9 | 13 |

**Section 4.2. Exercise 12.** The numbers $a, b, \bar{a}, \bar{b}$ satisfy

$$a\,\bar{a} \equiv 1 \pmod{m}, \qquad b\,\bar{b} \equiv 1 \pmod{m}.$$

Therefore $(a\,\bar{a})\,(b\,\bar{b}) \equiv 1 \pmod{m}$. This implies that $(a\,b)\,(\bar{a}\,\bar{b}) \equiv 1 \pmod{m}$. From this, we conclude that $\bar{a}\,\bar{b}$ is an inverse of $a\,b$ modulo $m$.

**Section 4.2. Exercise 18.** If the equation has a solution, then there exists a number $x_0$ such that

$$x_0^2 \equiv a \pmod{p}.$$

If $x_1$ is any other solution, then

$$x_1^2 \equiv a \equiv x_0^2 \pmod{p}.$$

This implies that

$$(x_1 - x_0)(x_1 + x_0) = x_1^2 - x_0^2 \equiv 0 \pmod{p}.$$

From this, we conclude that $p$ divides $x_1 - x_0$, or $p$ divides $x_1 + x_0$. Therefore, a solution $x_1$ satisfies

$$x_1 \equiv \pm x_0 \pmod{p}.$$

Given that $p$ does not divide $a$, we have that $p$ does not divide $x_0$. The two solutions $\pm x_0$ are incongruent, otherwise $p$ would divide $2x_0$, which is impossible.