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

4th exercise set - Answers

Exercise 1. Solve the following linear congruences:

1. $137x \equiv 4 \pmod{102}$.
2. $7x \equiv 8 \pmod{30}$.
3. $24x \equiv 22 \pmod{33}$.
4. $2086x \equiv -1624 \pmod{1729}$.

Answer.

1. Since $137 \equiv 35 \pmod{102}$, we can simplify the congruence as
$$35x \equiv 4 \pmod{102}.$$
Then, with the help of the euclidean algorithm, we compute $\overline{35}^{-1} = \overline{35}$. We multiply both sides of the congruence by $\overline{35}$ and we get
$$x \equiv 4 \cdot 35 \equiv 140 \equiv 38 \pmod{102}.$$

2. We will solve this congruence using Euler's theorem. Since $(7, 30) = 1$, Euler's theorem implies that
$$7^{\phi(30)} \equiv 1 \pmod{30} \Rightarrow 7^{-1} \equiv 7^{\phi(30)-1} \equiv 7^7 \pmod{30},$$
since $\phi(30) = 8$. We will now demonstrate an effective way for computing large powers.

   First write the exponent as a sum of powers of 2 (i.e., write it in binary). Here, $7 = 1 + 2 + 4$.

   Secondly compute the corresponding powers of the base (of course modulo the modulus), by constantly raising to the square. Here:
$$\begin{aligned} &7^1 \equiv 1 \pmod{30} \\ &7^2 \equiv 49 \equiv 19 \pmod{30} \\ &7^4 \equiv (7^2)^2 \equiv 19^2 \equiv 361 \equiv 1 \pmod{30}. \end{aligned}$$
Finally, multiply the corresponding powers as follows:
$$7^{-1} \equiv 7^7 \equiv 7^1 7^2 7^4 \equiv 7 \cdot 19 \cdot 1 \equiv 133 \equiv 13 \pmod{30}.$$
It follows that $7x \equiv 8 \pmod{30} \iff x \equiv 8 \cdot 13 \equiv 104 \equiv 14 \pmod{30}$.

3. The congruence is not solvable, since $(24, 33) = 3 \nmid 22$.

4. First, note that, in $\mathbb{Z}_{1729}$, $\overline{2086} = \overline{357}$ and $\overline{-1624} = \overline{105}$, so the congruence is equivalent to
$$357x \equiv 105 \pmod{1729}.$$
Next, we use the euclidean algorithm yields $(357, 1729) = 7$. However, $105 = 7 \cdot 15$. This implies that the congruence has exactly 7 solutions. Our next step is to identify one solution and, based on this, find the other 6.

Further, the euclidean algorithm yields
$$7 = 19 \cdot 1729 - 92 \cdot 357.$$
This implies
$$\begin{aligned} -92 \cdot 357 &\equiv 7 \pmod{1729} \\ \Rightarrow (-92 \cdot 15) \cdot 357 &\equiv 7 \cdot 15 \pmod{1729} \\ \Rightarrow 357 \cdot 349 &\equiv 105 \pmod{1729}. \end{aligned}$$
It follows that $\overline{349}$ is a solution of the congruence. If follows that all the solutions of the congruence are $x \equiv 349, 596, 843, 1090, 1337, 1584, 102 \pmod{1729}$. □

Exercise 2. A salesman is visiting a town every 5 months. Will he ever visit the town on March?

Answer. We label each month with its corresponding number, i.e., 3 stands for March. Assume that the first visit of the salesman to the city occurred on the month labeled a. The second visit will occur on the month labeled $a + 5 \pmod{12}$. The third on the month $a + 2 \cdot 5 \pmod{12}$ and so on.

Hence the question translates to whether there exists an x, such that $a + 5x \equiv 3 \pmod{12}$. This is equivalent to $5x \equiv (3 - a) \pmod{12}$, which has a unique solution $\pmod{12}$ (regardless a), since $(5, 12) = 1$. □

Exercise 3. Solve the following systems:

1. $\begin{cases} 3x \equiv -1 \pmod{10} \\ 2x \equiv 1 \pmod{5} \end{cases}$

2. $\begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 2 \pmod{4} \end{cases}$

3. $\begin{cases} x \equiv 1 \pmod{15} \\ x \equiv 7 \pmod{18} \end{cases}$

4. $\begin{cases} 2x \equiv 4 \pmod{5} \\ x \equiv -27 \pmod{22} \\ 3x \equiv 30 \pmod{39} \end{cases}$

Answer. 1. One easily checks that the system is equal to

$$\begin{cases} x \equiv 3 \pmod{10}, \\ x \equiv 3 \pmod{5}, \end{cases}$$

where, clearly, the first congruence implies the second. Hence the solution is $x \equiv 3 \pmod{10}$.

2. The system is impossible, since the first congruence's solutions are odd numbers and the second one's even.

3. Since $(15, 18) = 3 \mid 6 = 7-1$ and $\operatorname{lcm}(15, 18) = 90$, the system has a unique solution $\pmod{90}$. Let x_0 be a solution. The first congruence implies

$$x_0 = 1 + 15k,\ k \in \mathbb{Z}.$$

Now, the second congruence yields

$$\begin{aligned} & 1 + 15k \equiv 7 \pmod{18} \\ \iff & 15k \equiv 6 \pmod{18} \\ \iff & 5k \equiv 2 \pmod{6} \\ \iff & k \equiv 4 \pmod{6} \\ \iff & k = 4 + 6\ell,\ \ell \in \mathbb{Z}. \end{aligned}$$

It follows that $x_0 = 1 + 15k = 1 + 15(4 + 6\ell) = 61 + 90\ell$, $\ell \in \mathbb{Z}$. In other words $x_0 \equiv 61 \pmod{90}$.

4. First, we will simplify the three congruences, in order to get an equivalent system in the form of the statement of the Chinese Remainder Theorem. Towards this end, we solve the first congruence, using known methods, and get

$$x \equiv 2 \pmod{5}. \tag{1}$$

The second one can be rewritten as

$$x \equiv 17 \pmod{22}. \tag{2}$$

The third one does not have a unique solution modulo 39 (in fact it has three of them). Nonetheless, it is equivalent to the congruence

$$x \equiv 10 \pmod{13}. \tag{3}$$

Now the Chinese Remainder Theorem implies that the system has a unique solution $\pmod{1430}$. Let x be a solution. Congruence (1) implies

$$x = 2 + 5a, a \in \mathbb{Z}.$$

We replace this in (2) and get

$$2 + 5a \equiv 17 \pmod{22} \iff a \equiv 3 \pmod{22}.$$

It follows that $a = 3 + 22b$, that is,

$$x = 2 + 5(3 + 22b) = 17 + 110b,\ b \in \mathbb{Z}.$$

Finally, we replace the latter in (3) and get

$$17 + 110b \equiv 10 \pmod{13} \iff b \equiv 1 \pmod{13}.$$

It follows that $b = 1 + 13c$, that is,

$$x = 17 + 110(1 + 13c) = 127 + 1430c,\ c \in \mathbb{Z}.$$

In other words, we have shown that $x \equiv 127 \pmod{1430}$ is the solution of the system. □

Exercise 4 (Brahmagupta). A basket is full of eggs. When the eggs are taken out of a basket 2, 3, 4, 5, 6, 7 at a time, the remainders are 1, 2, 3, 4, 5 and 0 respectively. How many eggs were in the basket?

Answer. Let x be the number of eggs in the basket. From the statement we get that

$$\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{5}, \\ x \equiv 5 \pmod{6}, \\ x \equiv 0 \pmod{7}. \end{cases}$$

The third congruence implies the first and the fifth implies the second. Hence, the system can be simplified as

$$\begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{5}, \\ x \equiv 5 \pmod{6}, \\ x \equiv 0 \pmod{7}. \end{cases}$$

Now, notice that for each pair of the above congruences, the gcd of the moduluses divides the corresponding difference of factors, hence the system has a unique solution molulo $\operatorname{lcm}(4, 5, 6, 7) = 420$.

We easily check that the system

$$\begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 5 \pmod{6}, \end{cases}$$

is equivalent to $x \equiv 11 \pmod{12}$ and the system

$$\begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 0 \pmod{7}, \end{cases}$$

is equivalent to $x \equiv 28 \pmod{35}$.

From the above, the original system is reduced to

$$\begin{cases} x \equiv 11 \pmod{12}, \\ x \equiv 28 \pmod{35}, \end{cases}$$

whose unique solution is $x \equiv 203 \pmod{420}$. It follows that the basket contains $203+420k$ eggs, for some $k \geq 0$. □

Exercise 5 (The Chinese Cook Problem). In some looting, 17 pirates acquire a treasure of gold pieces. They decide to share the treasure and give the remainder to their Chinese cook. This way, the cook got 3 gold pieces. Later, at a naval battle, 6 of the pirates were killed and the remaining pirates decided to re-share the treasure in the same way. Now, the cook got 4 gold pieces. Later still, they had a shipwreck and only six of the original pirates (plus the cook) survived. They re-shared the treasure in the same way. Now, the Chinese cook got 5 gold pieces. While on shore, the cook poisoned the crew and got the whole treasure for himself. What is the minimum number of gold pieces that the Chinese cook has?

Answer. Let $x > 0$ be the total number of gold pieces of the treasure. The three consecutive sharings imply that

$$\begin{cases} x \equiv 3 \pmod{17}, \\ x \equiv 4 \pmod{11}, \\ x \equiv 5 \pmod{6}. \end{cases}$$

Since 17, 11 and 6 are pairwise co-prime, the Chinese Remainder Theorem implies that the above system has a unique solution modulo $17 \cdot 11 \cdot 6 = 1122$.

From the first congruence, we get that

$$x = 3 + 17\alpha,\ \alpha \in \mathbb{Z}.$$

We combine the above with the second congruence and get that

$$\begin{aligned} 3 + 17\alpha \equiv 4 \pmod{11} &\iff \alpha \equiv 2 \pmod{11} \\ &\iff \alpha = 2 + 11\beta,\ \beta \in \mathbb{Z}. \end{aligned}$$

It follows that

$$x = 3 + 17(2 + 11\beta) = 37 + 187\beta,\ \beta \in \mathbb{Z}.$$

We combine the latter expression for x with the third congruence and get

$$\begin{aligned} 37 + 187\beta \equiv 5 \pmod{6} &\iff \beta \equiv 4 \pmod{6} \\ &\iff \beta = 4 + 6\gamma,\ \gamma \in \mathbb{Z}. \end{aligned}$$

It follows that $x = 37 + 187(4 + 6\gamma) = 785 + 1122\gamma$, $\gamma \in \mathbb{Z}$, that is, the cook has at least 785 gold pieces. □

Exercise 6. On a 12-hour clock, we put a blue marble on position 1 and a red marble on position 2. Every hour we move the blue marble by 3 positions and the red marble by 1. Will the two marbles ever meet?

Answer. After x hours, the blue marble will be on the position $1+3x \pmod{12}$, while the red one on the position $2+x \pmod{12}$. Hence, the two marbles will meet if, for some x,

$$1+3x \equiv 2+x \pmod{12} \iff 2x \equiv 1 \pmod{12}.$$

However, since $(2,12)=2 \nmid 1$, the above congruence is not solvable. □

Exercise 7. Find a congruence equivalent with the system

$$\begin{cases} x \equiv 1 \pmod{4}, \\ x \equiv 2 \pmod{3}. \end{cases}$$

Answer. Since $(3,4)=1$, the Chinese Remainder Theorem implies that the above has a unique solution modulo 12. The first congruence implies that

$$x = 1+4k,\ k \in \mathbb{Z}.$$

Now, the second one yields

$$1+4k \equiv 2 \pmod{3} \Rightarrow k \equiv 1 \pmod{3} \Rightarrow k = 1+3\ell,\ \ell \in \mathbb{Z}.$$

It follows that

$$x = 1+4(1+3\ell) = 5+12\ell, \ell \in \mathbb{Z}.$$

It follows that the solution is $x \equiv 5 \pmod{12}$. □

Exercise 8. Solve $x^3+4x+8 \equiv 0 \pmod{15}$.

Answer. Let $f(x)=x^3+4x+8$. Since $15 = 3 \cdot 5$, The congruence $f(x) \equiv 0 \pmod{15}$ is solvable iff the congruences $f(x) \equiv 0 \pmod{3}$ and $f(x) \equiv 0 \pmod{5}$ are solvable.

We focus on $f(x) \equiv 0 \pmod{5}$. This is equal to

$$x^3 - x - 2 \equiv 0 \pmod{5}.$$

We check all the values $x = 0, \pm 1, \pm 2$ and verify that none is a solution, that is, the congruence is not solvable. We conclude that the congruence $f(x) \equiv 0 \pmod{15}$ is also not solvable. □

Exercise 9. Solve the following congruences:

1. $121x^5 + x^2 - 24x + 143 \equiv 0 \pmod{11}$.
2. $3x^7 + 2x^6 + x^5 + 2x^3 + 6 \equiv 0 \pmod{5}$.
3. $7x^7 + 16x^2 + 18 \equiv 0 \pmod{21}$.

Answer.

1. First, we replace the coefficients, in order to get a simpler expression of the original congruence as follows:

   $$x^2 - 2x \equiv 0 \pmod{11}.$$

   Then, we check the validity of the above for all the elements of $\mathbb{Z}_{11}$, i.e. $\{\bar{0}, \pm\bar{1}, \pm\bar{2}, \pm\bar{3}, \pm\bar{5}\}$ and easily see that the solutions are $\bar{0}$ and $\bar{2}$.

2. Fermat's theorem implies that for every $a \in \mathbb{Z}$, we have $a^5 \equiv a \pmod 5$. Hence

$$\begin{aligned} &a^7 \equiv a^5a^2 \equiv a \cdot a^2 \equiv a^3 \pmod 5, \\ &a^6 \equiv a^5a \equiv aa \equiv a^2 \pmod 5, \\ &a^5 \equiv a \pmod 5. \end{aligned}$$

   So, an equivalent congruence would be

$$3x^3 + 2x^2 + x + 2x^3 + 6 \equiv 5x^3 + 2x^2 + x + 6 \equiv 2x^2 + x + 1 \pmod 5.$$

   We easily check that the latter is not satisfied for $x = 0, \pm 1, \pm 2$, so we conclude that it has no solutions.

3. Since $21 = 3 \cdot 7$, we can instead study the congruences

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

   Lets begin with the first one. After employing Fermat's theorem, we check that $f(x) \equiv 0 \pmod 3$ is equivalent to $x^2 + x + 1 \equiv 0 \pmod 3$. We explicitly check $x \equiv 0, \pm 1 \pmod 3$ and we verify that $x \equiv 1 \pmod 3$ is the unique solution.

   Now, we turn our attention to the second one. We verify that $f(x) \equiv 0 \pmod 7$ is equal to $2x^2 + 3 \equiv 0 \pmod 7$. We explicitly check $x \equiv 0, \pm 1, \pm 2, \pm 3 \pmod 7$ and find the solutions $x \equiv \pm 3 \pmod 7$.

   It follows that the solutions of the original congruence are exactly the solutions of the following systems

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

   The Chinese Remainder Theorem ensures that both systems have a unique solution modulo 21. We explicitly solve both of them (using any method) and attain the solutions

$$x \equiv 10 \pmod{21} \text{ and } x \equiv 4 \pmod{21}. \qquad \square$$