# MEM204-Number Theory

## 4th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 08/04/2020

University of Crete

# Answers of the 3rd set

# Exercise 1

## Exercise

*Find* $13^{23}27^{41} \pmod 8$.

## Answer

*We have that* $13 \equiv 5 \pmod 8$ *and that* $27 \equiv 3 \pmod 8$.
*Moreover, given that* $\varphi(8) = 4$, *Euler's theorem implies*

$$13^{23} \equiv 5^{23} \equiv 5^{4\cdot 5+3} \equiv (5^4)^5 5^3 \equiv 1^5 125 \equiv 5 \pmod 8$$

*and*

$$27^{41} \equiv 3^{4\cdot 10+1} \equiv (3^4)^{10} 3^1 \equiv 1^{10} 3 \equiv 3 \pmod 8.$$

*It follows that* $13^{23}27^{41} \equiv 5 \cdot 3 \equiv 15 \equiv 7 \pmod 8$.

# Exercise 2

**Exercise**

*Prove that* $7 \mid 111^{333} + 333^{111}$.

**Answer**

*We have that* $111 \equiv -1 \pmod 7$ *and* $333 \equiv 4 \pmod 7$. *Moreover, Fermat's theorem implies* $4^6 \equiv 1 \pmod 7$. *It follows that*

$$333^{111} \equiv 4^{6\cdot 18+3} \equiv (4^6)^{18} 4^3 \equiv 1^{18} \cdot 64 \equiv 1 \pmod 7,$$

*hence*

$$111^{333} + 333^{111} \equiv (-1)^{333} + 1 \equiv -1 + 1 \equiv 0 \pmod 7.$$

*The result follows.*

## Exercise 3

### Exercise

*Prove that* $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$, *for* $n \geq 1$.

### Answer

*First, for* $n = 1$, $(-13)^2 \equiv 169 \pmod{181}$, *and* $(-13)^1 + (-13)^0 \equiv -13 + 1 \equiv 169 \pmod{181}$. *In other words, the statement holds for* $n = 1$.

*Now, assume that the statement holds for* $n = k$.

*For* $n = k + 1$, *we have that*

$$\begin{aligned}(-13)^{k+2} &\overset{I.H.}{\equiv} (-13)(-13)^{k+1} \equiv (-13)[(-13)^k + (-13)^{k-1}] \\ &\equiv (-13)^{k+1} + (-13)^k \pmod{181}.\end{aligned}$$

# Exercise 4

## Exercise

*Find the residue of* $4444^{4444}$ *divided by* $9$.

## Answer

*We easily see that the euclidean division between* $4444$ *and* $9$ *yields*

$$4444 = 493 \cdot 9 + 7,$$

*that is,* $4444 \equiv 7 \pmod 9$. *Moreover, since* $(7, 9) = 1$, *Euler's theorem implies that* $7^{\varphi(9)} = 7^6 \equiv 1 \pmod 9$. *Now, we compute*

$$\begin{aligned} 4444^{4444} \equiv 7^{440\cdot 6+4} \equiv (7^6)^{440} 7^4 \equiv 1^{440} \cdot 49^2 \equiv 4^2 \\ \equiv 16 \equiv 7 \pmod 9. \end{aligned}$$

# Exercise 7

**Exercise**

*Let* $m, n \in \mathbb{Z}$, *such that* $(m, n) = 1$. *Show that*

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

# Exercise 7

**Answer**

*The desired result is equivalent to* $mn \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$. *Since* $(m, n) = 1$, *the latter is equivalent to*

$$m \mid m^{\varphi(n)} + n^{\varphi(m)} - 1 \ \text{ and } \ n \mid m^{\varphi(n)} + n^{\varphi(m)} - 1.$$

*Furthermore, again because* $(m, n) = 1$, *we get*

$$m^{\varphi(n)} + n^{\varphi(m)} \overset{m \mid m^{\varphi(n)}}{\equiv} n^{\varphi(m)} \overset{Euler}{\equiv} 1 \pmod{m},$$

*or, equivalently* $m \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$. *Similarly,* $n \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$.

# Exercise 8

## Exercise

*Let $p, q$ be distinct primes such that*

$$a^p \equiv a \pmod q \text{ and } a^q \equiv a \pmod p.$$

*Show that $a^{pq} \equiv a \pmod{pq}$.*

## Answer

*We have that*

$$a^{pq} \equiv (a^p)^q \overset{a^p \equiv a \pmod q}{\equiv} a^q \overset{\text{Fermat}}{\equiv} a \pmod q.$$

*Similarly, $a^{pq} \equiv a \pmod p$. In other words both $p$ and $q$ divide $a^{pq} - a$, that is, since $(p, q) = 1$, $pq \mid a^{pq} - a$, which is equivalent to the desired result.*

# Exercise 9

**Exercise**

*Solve the following congruences:*

1. $34x \equiv 60 \pmod{98}$,
2. $255x \equiv 221 \pmod{391}$,
3. $-671x \equiv 121 \pmod{737}$.

# Exercise 9 - Answer - Item 1

We will solve this congruence using the euclidean algorithm explicitly. First, we use the euclidean algorithm to find whether we have a solution.

$$
\begin{aligned}
98 &= 2 \cdot 34 + 30 \qquad (1)\\
34 &= 30 + 4 \qquad (2)\\
30 &= 7 \cdot 4 + 2 \qquad (3)\\
4 &= 2 \cdot 2 + 0
\end{aligned}
$$

It follows that $(98, 34) = 2$. In addition, $60 = 30 \cdot 2$, that is, we have 2 solutions $\mod 98$ and if $x_0$ is one of them, the other will be $x_0 + \frac{98}{2} = x_0 + 49$. Now, the euclidean algorithm yields:

$$
\begin{aligned}
2 &\overset{(3)}{=} 30 - 7 \cdot 4 \overset{(2)}{=} 30 - 7(34 - 30) = -7 \cdot 34 + 8 \cdot 30\\
&\overset{(1)}{=} -7 \cdot 34 + 8(98 - 2 \cdot 34) = 8 \cdot 98 - 23 \cdot 34.
\end{aligned}
$$

We take this expression modulo 98 and get

$$
\begin{aligned}
&-23 \cdot 34 \equiv 2 \pmod{98} \\
\Rightarrow &34(-23 \cdot 30) \equiv 2 \cdot 30 \pmod{98} \\
\Rightarrow &34 \cdot 94 \equiv 60 \pmod{98}.
\end{aligned}
$$

It follows that the two solutions are $x_0 \equiv 94 \pmod{98}$ and $x_1 \equiv 45 \pmod{98}$.

# Exercise 9 - Answer - Item 2

We easily see that $(255, 391) = 17 \mid 221$. It follows that we have 17 solutions modulo 391. Also, $255x \equiv 221 \pmod{391} \iff 15x \equiv 13 \pmod{23}$. Moreover,

$$23 = 15 + 8 \tag{4}$$

$$15 = 8 + 7 \tag{5}$$

$$8 = 7 + 1, \tag{6}$$

that is,

$$1 \overset{(6)}{=} 8 - 7 \overset{(5)}{=} 8 - (15 - 8) = -15 + 2 \cdot 8 \overset{(4)}{=} -15 + 2(23 - 15) = 2 \cdot 23 - 3 \cdot 15.$$

From the latter, we get

$$15x \equiv 13 \pmod{23} \iff x \equiv 13 \cdot (-3) \equiv 7 \pmod{23}.$$

It follows that the solutions of the original congruence are the numbers $\mod 391$ that are $\equiv 7 \pmod{23}$, i.e.,

$$7, 7 + 23, 7 + 2 \cdot 23, \dots, 7 + 16 \cdot 23.$$

# Exercise 9 - Answer - Item 3

First, note that the congruence can be rewritten as

$$66x \equiv 121 \pmod{737}.$$

Like in the previous case, we have $(66, 737) = 11 \mid 121$, thus we have 11 solutions modulo 737, that are the solutions of $6x \equiv 11 \pmod{67}$. We compute that $x \equiv 13 \pmod{67}$. It follows that the solutions of the original congruence are

$$13, 13 + 67, \dots, 13 + 10 \cdot 67.$$

## Exercise 10

**Exercise**

*Find all the numbers* $n > 0$*, such that* $n^{13} \equiv n \pmod{1365}$.

# Exercise 10 - Answer

We will show that $n^{13} \equiv n \pmod{1365}$ for every $n > 0$. Take some $n > 0$. First, notice that $1365 = 3 \cdot 5 \cdot 7 \cdot 13$. It follows that it suffices to prove that $3 \mid n^{13} - n$, $5 \mid n^{13} - n$, $7 \mid n^{13} - n$ and $13 \mid n^{13} - n$.

- Fermat's theorem implies $n^3 \equiv n \pmod{3}$. It follows that

  $$n^{13} \equiv n^{3 \cdot 4 + 1} \equiv (n^3)^4 n \equiv n^4 n \equiv n^3 n^2 \equiv n^3 \equiv n \pmod{3},$$

  that is, $3 \mid n^{13} - n$.
- Fermat's theorem implies $n^5 \equiv n \pmod{5}$. It follows that

  $$n^{13} \equiv n^{5 \cdot 2 + 3} \equiv (n^5)^2 n^3 \equiv n^2 n^3 \equiv n^5 \equiv n \pmod{5},$$

  that is, $5 \mid n^{13} - n$.

# Exercise 10 - Answer

- Fermat's theorem implies $n^7 \equiv n \pmod{7}$. It follows that

  $$n^{13} \equiv n^{7+6} \equiv n^7 n^6 \equiv n \cdot n^6 \equiv n^7 \equiv n \pmod{7},$$

  that is, $7 \mid n^{13} - n$.
- Fermat's theorem implies $n^{13} \equiv n \pmod{13}$, that is, $13 \mid n^{13} - n$.

This concludes the proof.

# Exercise 11

**Exercise**

*Let p be an odd prime. Show that*

$$1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

# Exercise 11 - Answer

We have that

$$1^2 3^2 5^2 \cdots (p-2)^2 = (1 \cdot 3 \cdots (p-2))(1 \cdot 3 \cdots (p-2)).$$

However, since $p$ is odd, we have that, for $i$ odd, $p - i$ is even, while $i \equiv -(p-i) \pmod{p}$. It follows that

$$\begin{aligned} 1 \cdot 3 \cdots (p-2) &\equiv (-2) \cdot (-4) \cdots (-(p-1)) \\ &\equiv (-1)^{\frac{p-1}{2}} \cdot 2 \cdot 4 \cdots (p-1) \pmod{p}. \end{aligned}$$

A combination of the two above congruences yields

$$\begin{aligned} 1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p-1}{2}} (p-1)! &\overset{\text{Wilson}}{\equiv} (-1)^{\frac{p-1}{2}} (-1) \\ &\equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \end{aligned}$$

# A Chinese Problem

# 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?

## The Chinese cook problem - Answer

Let $x > 0$ be the total number of gold pieces of the treasure. The original sharing implies that

$$x \equiv 3 \pmod{17}, \tag{7}$$

the second one that

$$x \equiv 4 \pmod{11} \tag{8}$$

and the last one that

$$x \equiv 5 \pmod{6}. \tag{9}$$

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

## The Chinese cook problem - Answer

From (7), we get that

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

We combine the above with (8) 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

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

# The Chinese cook problem - Answer

We combine the latter expression for $x$ with (9) 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

$$x = 37 + 187(4 + 6\gamma) = 785 + 1122\gamma,\ \gamma \in \mathbb{Z}.$$

We conclude that the cook has at least 785 gold pieces.

**Exercise**

*Solve the Chinese cook problem with the other method for solving similar problems (the one that derives from the proof of the Chinese Remainder Theorem).*

Stay home, stay safe!