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

3rd exercise set - Answers

Exercise 1. 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 $\phi(8) = 4$, 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. 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. 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

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

□

Exercise 4. 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 $7^{\phi(9)} = 7^6 \equiv 1 \pmod 9$. Now, we compute

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

□

Exercise 5. Prove that $383838 \mid n^{37} - n$.
Hint: $383838 = 2 \cdot 3 \cdot 7 \cdot 13 \cdot 19 \cdot 37$.

Answer. We have that $383838 = 2 \cdot 3 \cdot 7 \cdot 13 \cdot 19 \cdot 37$. It follows that it suffices to show that $2 \mid n^{37} - n$, $3 \mid n^{37} - n$, $7 \mid n^{37} - n$, $13 \mid n^{37} - n$, $19 \mid n^{37} - n$ and $37 \mid n^{37} - n$. We will show each of these relations individually.

- – If $n \equiv 0 \pmod 2$, then $n^{37} - n \equiv 0 \pmod 2 \Rightarrow 2 \mid n^{37} - n$.
  – If $n \equiv 1 \pmod 2$, then $n^{37} - n \equiv 0 \pmod 2 \Rightarrow 2 \mid n^{37} - n$.

  Hence, in any case, $2 \mid n^{37} - n$.

- – If $n \equiv 0 \pmod 3$, then $n^{37} - n \equiv 0 \pmod 3 \Rightarrow 3 \mid n^{37} - n$.
  – If $n \not\equiv 0 \pmod 3$, then, $n \equiv \pm 1 \pmod 3 \Rightarrow n^2 \equiv 1 \pmod 3$. It follows that

  $$n^{37} - n \equiv n^{2 \cdot 18 + 1} - n \equiv (n^2)^{18} n - n \equiv n - n \equiv 0 \pmod 3.$$

  The latter implies $3 \mid n^{37} - n$.

  Hence, in any case, $3 \mid n^{37} - n$.

- – If $n \equiv 0 \pmod 7$, then $n^{37} - n \equiv 0 \pmod 7 \Rightarrow 7 \mid n^{37} - n$.
  – If $n \not\equiv 0 \pmod 7$, then, Fermat's theorem implies $n^6 \equiv 1 \pmod 7$, that is,

  $$n^{37} - n \equiv n^{6 \cdot 6 + 1} - n \equiv (n^6)^6 n - n \equiv n - n \equiv 0 \pmod 7.$$

  The latter implies $7 \mid n^{37} - n$.

  Hence, in any case, $7 \mid n^{37} - n$.

- – If $n \equiv 0 \pmod{13}$, then $n^{37} - n \equiv 0 \pmod{13} \Rightarrow 13 \mid n^{37} - n$.
  – If $n \not\equiv 0 \pmod{13}$, then, Fermat's theorem implies $n^{12} \equiv 1 \pmod{13}$, that is,

  $$n^{37} - n \equiv n^{12 \cdot 3 + 1} - n \equiv (n^{12})^3 n - n \equiv n - n \equiv 0 \pmod{13}.$$

  The latter implies $13 \mid n^{37} - n$.

  Hence, in any case, $13 \mid n^{37} - n$.

- – If $n \equiv 0 \pmod{19}$, then $n^{37} - n \equiv 0 \pmod{13} \Rightarrow 19 \mid n^{37} - n$.
  – If $n \not\equiv 0 \pmod{19}$, then, Fermat's theorem implies $n^{18} \equiv 1 \pmod{19}$, that is,

  $$n^{37} - n \equiv n^{18 \cdot 2 + 1} - n \equiv (n^{18})^2 n - n \equiv n - n \equiv 0 \pmod{19}.$$

  The latter implies $19 \mid n^{37} - n$.

  Hence, in any case, $19 \mid n^{37} - n$.

- Since 37 is a prime, Fermat's theorem implies that, for every n, $n^{37} \equiv n \pmod{37} \iff 37 \mid n^{37} - n$.

The proof is now complete. □

Exercise 6. Prove that the last two digits of $n^{22} - n^2$ are zeros.

Answer. It suffices to show that $100 \mid n^{22} - n^2 \iff 4 \mid n^{22} - n^2$ and $25 \mid n^{22} - n^2$.

- – If $n \equiv 0$ or $2 \pmod 4 \Rightarrow n^2 \equiv 0 \pmod 4 \Rightarrow n^2 2 - n^2 \equiv 0 \pmod 4 \Rightarrow 4 \mid n^{22} - n^2$.
  – If $n \equiv \pm 1 \pmod 4 \Rightarrow n^{22} - n^2 \equiv 1 - 1 \equiv 0 \pmod 4 \Rightarrow 4 \mid n^{22} - n^2$.

  In any case, $4 \mid n^{22} - n^2$.
- – If $n \equiv 0$ or $5 \pmod{25} \Rightarrow n^2 \equiv 0 \pmod{25} \Rightarrow n^2 2 - n^2 \equiv 0 \pmod{25} \Rightarrow 25 \mid n^{22} - n^2$.
  – If $n \not\equiv 0$ or $5 \pmod{25}$, then Euler's theorem implies $n^{\phi(25)} = n^{20} \equiv 1 \pmod{25}$. It follows that $n^{22} - n^2 \equiv n^{20} n^2 - n^2 \equiv n^2 - n^2 \equiv 0 \pmod{25} \Rightarrow 25 \mid n^{22} - n^2$.

  In any case, $25 \mid n^{22} - n^2$.

The result follows. □

Exercise 7. Let $m, n \in \mathbb{Z}$, such that $(m, n) = 1$. Show that

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

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

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

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

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

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

Exercise 8. 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. Solve the following congruences:

1. $34x \equiv 60 \pmod{98}$,

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

Answer. 1. We will solve this congruence using the euclidean algorithm explicitly. First, we use the euclidean algorithm to find whether we have a solution.

$$98 = 2 \cdot 34 + 30 \tag{1}$$
$$34 = 30 + 4 \tag{2}$$
$$30 = 7 \cdot 4 + 2 \tag{3}$$
$$4 = 2 \cdot 2 + 0$$

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 $x_1 \equiv 45 \pmod{98}$.

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.,

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

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

$$13, 13 + 67, \ldots, 13 + 10 \cdot 67. \qquad \square$$

Exercise 10. Find all the numbers $n > 0$, such that $n^{13} \equiv n \pmod{1365}$.

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

- 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, $13 \mid n^{13} - n$. $\square$

Exercise 11. Let p be an odd prime. Show that

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

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

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

A combination of the two above congruences yields

$$1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p-1}{2}} (p-1)! \overset{\text{Wilson}}{\equiv} (-1)^{\frac{p-1}{2}} (-1) \equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \quad \square$$