MEM204-Number Theory

9th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 01/05/2020

University of Crete

Answers of the 4th set

Exercise 1.2

Exercise

Solve $7x \equiv 8 \pmod{30}$.

We will solve this congruence using Euler's theorem. Since $(7, 30) = 1$, Euler's theorem implies that

$$7^{\varphi(30)} \equiv 1 \pmod{30} \Rightarrow 7^{-1} \equiv 7^{\varphi(30)-1} \equiv 7^7 \pmod{30},$$

since $\varphi(30) = 8$. We will now demonstrate an effective way for computing large powers.

Exercise 1.2

1. Write the exponent as a sum of powers of 2 (i.e., write it in binary). Here, $7 = 1 + 2 + 4$.
2. Compute the corresponding powers of the base (of course modulo the modulus), by constantly raising to the square. Here:

$$7^1 \equiv 7 \pmod{30}$$
$$7^2 \equiv 49 \equiv 19 \pmod{30}$$
$$7^4 \equiv (7^2)^2 \equiv 19^2 \equiv 361 \equiv 1 \pmod{30}.$$

3. 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 $7x \equiv 8 \pmod{30} \iff x \equiv 8 \cdot 13 \equiv 104 \equiv 14 \pmod{30}$.

Exercise 2

Exercise

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 4

Exercise (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?

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

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

Exercise 4

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 $\operatorname{lcm}(4, 5, 6, 7) = 420$.

Exercise 4

We easily check that the systems

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

are equivalent to $x \equiv 11 \pmod{12}$ and $x \equiv 14 \pmod{35}$ respectively.

From the above, the original system is reduced to

$$\begin{cases} x \equiv 11 \pmod{12}, \\ x \equiv 14 \pmod{35}, \end{cases}$$

whose unique solution is $x \equiv 119 \pmod{420}$. It follows that the basket contains $119 + 420k$ eggs, for some $k \geq 0$.

Exercise 6

Exercise

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

Exercise

Find a congruence equivalent with the system

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

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

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

Exercise 7

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

Exercise

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.

A few more exercises

A polynomial congruence modulo a prime power

Exercise

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.

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:

A polynomial congruence modulo a prime power

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 $f(x) \equiv 0 \pmod{p^{k+1}}$).

A polynomial congruence modulo a prime power

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

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

for all $\ell \geq 1$.

Equation (1), for $\ell = k$, implies the first item of the previous slide.

Equation (1), for $\ell = k$ and $\ell = k+1$, implies the second item of the previous slide.

Stay home, stay safe!