1

Consider a special case of a system like x = 2 (mod 5) and x = 2 (mod 7) What are the possible solutions for x? Is the solution unique? Unique modulo some number? Justify your answer.

Solutions include 2, 37, 72, 117.... and any number of the form 35k + 2. This should make sense as 35 is the lcm of 5 and 7.

Another way to think about this is: If x, y are two solutions, x-y=0 both mod 5 and 7, so 35 | (x-y). The solution is unique mod 35.

This means that 2 is a unique solution mod 35.

- Miah :)

2

2. Consider the system

$$x \equiv 2 \pmod 3 \text{ and } x \equiv 3 \pmod 7$$

Does the system have a solution? if so, is it unique? Unique modulo some number? Justify.

mod 3

For $x \equiv 2 \pmod 3$, The equivalence class $[2] = \{\ldots, 2, 5, 8, 11, 14, \mathbf{17}, 20, 23, 26, \ldots\} = 2 + 3\mathbb{Z}$

and for $x \equiv 3 \pmod 7$, The equivalence class $[3] = \{\ldots, 3, 10, \mathbf{17}, \ldots\} = 3 + 7\mathbb{Z}$

mod 7

$x \equiv 17 \pmod{lcm(3,7)}$

$x \equiv 17 \pmod{21}$.

Yes the system has a solution. Any integer x such that $x \equiv 17 \pmod{21}$.

Nice approach! To look at each individual equivalence class and to find the common elements!

Cy

3

No solution. If $x=3 \bmod 4$, then x must be odd. But $x=2 \bmod 6$ means x must be even. Contradiction.

4

Consider each of the residue classes a modulo 9. For each a, find the smallest positive k such that a^k ≡ 1 (mod 9).

The residue classes modulo 9 are: [0], [1], [2], [3], [4], [5], [6], [7], [8].

For a=1 the smallest possible k is 1. For a=2 the smallest possible k is 6. For a=4 the smallest possible k is 3.

For a=5 the smallest possible k is 6. For a=7 the smallest possible k is 3. For a=8 the smallest possible k is 2.

I was not able to find any positive k such that a^k=1(mod 9) for a=0, a=3, or a=6, because for these classes 9 divides a^k for any k>=2.

-Maggie

5

The order of 2 mod 13 is 12 because

2^12 = 4096 which is congruent to 1 mod 13.
315(13) + 1

But (-1)^12=1 mod 13 as well. Does that mean -1 has order 12 too?

1-12 did not result in 1 mod 13 as well???

Cian

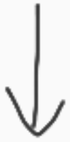
6

Suppose we know 5^96 == 1 (mod 357). How can you use this information to help find the order of 5 modulo 357?

We were given that if the order, k, modulo n of some integer, a, divides some h then a^h==1 (mod n). But we'd need the converse to be true for what I did.

We know the order must be at most 96. Assuming the converse of the statement is true, we could check all factors of 96 to see if they work as well.

If the converse is not true, we'd need to check all numbers less than 96. Doing this (programmatically) also shows 48 to be the order of 5 modulo 357



If they do, then the smallest that works is the order. If none do then 96 is the order. 48 works and no smaller factor of 96 does so I concluded that 48 is the order of 5 mod 357

-Nick

Last page