Modular Arithmetic

30/9/2024

Pre-Session Question: Why is 13 00 equal to 1 a.m.? Is there a general rule on how the hour on 24-hour clock relates to the 12-hour one?

Answer: $12 \mid (a - b)$ aka $a \equiv b \pmod{12}$. For e.g. $12 \mid (13 - 1)$, $12 \mid (14 - 2)$, …

" ≡ " Definition

$$a \equiv b \pmod{n}$$

if $n \mid (a - b)$

More examples:

$4 \equiv 10 \pmod{3}$

$32 \equiv -1 \pmod{11}$

$42 \equiv 98 \pmod{7}$

$-6 \equiv 2 \pmod{8}$

To note:

- Negative numbers are allowed.
- $a \equiv r \pmod{n}$ where r is the remainder of a when divided by n and $0 \le r < n$.

Some Modular Arithmetic Properties

- Addition: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$$a + c \equiv b + d \pmod{m}$$
$$a - c \equiv b - d \pmod{m}$$
In particular,
$$ka \equiv kb \pmod{m} \text{ for some integer } k$$

But why?

- Multiplication: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$$ac \equiv bd \pmod{m}$$
In particular,
$$a^k \equiv b^k \pmod{m} \text{ for some positive integer } k$$

- Division: If $ac \equiv bc \pmod{m}$,

$$a \equiv b \pmod{\frac{m}{\gcd(m,c)}}$$

In particular,

$$\text{if } ac \equiv bc \pmod m,\ \gcd(c, m) = 1, \text{ then } a \equiv b \pmod m$$

Complete System of Modulo n

By the division algorithm, any integer is just congruent to one of the numbers 0,1, ... , $n - 1$ modulo n and the n numbers 0,1, ... , $n - 1$ are not congruent each other modulo n. Therefore, there are totally n different classes modulo n.

Q1 : Prove that $6 \mid n (n+1) (2n+1)$ for n is a positive integer, using modular arithmetic.

Solution: $6 \mid n (n+1) (2n+1) \Leftrightarrow 2 \mid n (n+1) (2n+1)$ and $3 \mid n (n+1) (2n+1)$

$2 \mid n (n+1) (n+2)$ because either n or n+1 is even.

Then $3 \mid n (n+1) (2n+1)$?

$n \equiv 0$ or $n \equiv 1$ or $n \equiv 2 \pmod 3$ [Using the idea of complete system of modulo n]

Case 1: $n \equiv 0 \pmod 3 \Rightarrow 3 \mid n \Rightarrow 3 \mid n (n+1) (2n+1)$

Case 2: $n \equiv 1 \pmod 3 \Rightarrow 2n + 1 \equiv 2(1) + 1 \equiv 3 \equiv 0 \pmod 3 \Rightarrow 3 \mid n (n+1) (2n+1)$

Case 3: $n \equiv 2 \pmod 3 \Rightarrow n + 1 \equiv 2 + 1 \equiv 3 \equiv 0 \pmod 3 \Rightarrow 3 \mid n (n+1) (2n+1)$

We are done.

Some Modular Contradictions

$n^2 \equiv 0 \text{ or } 1 \pmod 3$

$n^2 \equiv 0 \text{ or } 1 \pmod 4$

$n^2 \equiv 0 \text{ or } \pm 1 \pmod 5$

$\text{odd}^2 \equiv 1 \pmod 8$

Proof: try the complete system of modulo n

As an example, we will try proving $n^2 \equiv 0 \text{ or } 1 \pmod 4$:

By the idea of complete system of modulo n, we know that any integer n belongs to any of the three categories:

$n \equiv 0 \pmod 4$; $n \equiv 1 \pmod 4$; $n \equiv 2 \pmod 4$); $n \equiv 3 \pmod 4$

Case 1: $n \equiv 0 \pmod 4 \Rightarrow n^2 \equiv 0^2 \equiv 0 \pmod 4$

Case 2: $n \equiv 1 \pmod 4 \Rightarrow n^2 \equiv 1^2 \equiv 1 \pmod 4$

Case 3: $n \equiv 2 \pmod 4 \Rightarrow n^2 \equiv 2^2 \equiv 4 \equiv 0 \pmod 4$

Case 4: $n \equiv 3 \pmod 4 \Rightarrow n^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod 4$

We only get $n^2 \equiv 0$ or $1 \pmod 4$ in all four cases. Therefore, we are done.

Q2: Assume that integers x, y and z satisfy

$$(x - y)(y - z)(z - x) = x + y + z.$$

Prove that $x + y + z$ is divisible by 27.

Solution: $x \equiv 0$ or $x \equiv 1$ or $x \equiv 2 \pmod 3$, and likewise with y and z.

Take a, b and c such that $x \equiv a$, $y \equiv b$ and $z \equiv c \pmod 3$ and $0 \le a,b,c \le 2$.

Since $(x - y)(y - z)(z - x) \equiv x + y + z \pmod 3$

$\Rightarrow (a - b)(b - c)(c - a) \equiv a + b + c \pmod 3$ – eq(1)

We will divide this problem into two cases:

1) Two of a,b,c are the same
2) None of a,b,c are the same, i.e. $(a,b,c) = (0,1,2)$

Case 1) If two of a,b,c are the same:

Let $a = b$.

LHS of eq(1) = 0

RHS of eq(1) = $a+b+c = 2a + c$.

Since $2a + c$ must be $0 \pmod 3$, $2a \equiv -c \pmod 3$. [Note that $2a \equiv -a$ because $3a \equiv 0 \pmod 3$.] Therefore, $-a \equiv -c \pmod 3 \Rightarrow a = c$.

Therefore, $a = b = c$.

Case 2) none of a,b,c are the same:

RHS of eq(1) = $3 \equiv 0 \pmod 3$

However, LHS will never be equivalent to 0 (mod 3).

So, case 2 is totally impossible.

Concluding both cases, only the scenario where a = b = c is possible.

Since a = b = c, 3 | x – y and 3 | y – z and 3 | z – x.

Therefore, 27 | (x-y)(y-z)(z-x). We are done.

Note: The solution is a little (just a little) different from what was explained in the lecture because this is way more efficient. In the lecture, I tried to focus more on the natural thought process and it was brute forced.

Two Equal Sets

Let p be a prime and consider S = {1, 2, . . . , p − 1} to be the set of non-zero remainder modulo p. Let a be any integer coprime to p (gcd (p,a) = 1). Then

$$\mathbf{aS \equiv S \pmod{p}}$$

For e.g. let p = 5 and a = 3.

Elements of S	1	2	3	4
Elements of 3S	3	6	9	12
Elements of 3S (mod 5)	3	1	4	2

Fermat's Little Theorem

1. Let a be any number. Then

$$\mathbf{a^p \equiv a \pmod{p}}$$

in which p is a prime.

2. Let a be a number co-prime to p. Then,

$$\mathbf{a^{p-1} \equiv 1 \pmod{p}}$$

(can be proven with two equal sets)

Proof: take S = {1,2,3,…,p-1} and aS = {a,2a,3a,…,(p-1)a}

aS ≡ S (mod p)

Multiplying all the elements on both side gives (this can be done because the two sets are identical at mod p):

a^{p-1} (p-1)! ≡ (p-1)! (mod p)

Since gcd((p-1)!, p) =1,

a^{p-1} ≡ 1 (mod p)

Wilson's Theorem

For a prime p,

$$(p-1)! \equiv -1 \pmod{p}$$

[Although I promised a proof, I decided not to add it because it used the idea of inverse.]

Q3(Myanmar TST 2024): Prove that if p is a prime number congruent to 1 (mod 4), then

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$$

Solution: Since p ≡ 1 (mod 4), let p = 4x + 1 for some x. $\frac{p-1}{2} = \frac{4x+1-1}{2} = 2x$.

Wilson's Theorem: (p-1)! ≡ -1 (mod p)

$1 \,.\, 2 \,.\, 3 \,.\, \ldots \,.\, (p-3) \,.\, (p-2).\, (p-1) \equiv -1 \pmod{p}$

$\text{LHS} = [1(p-1)] \,.\, [2(p-2]) \,.\, [3(p-3)] \,.\, \ldots \,.\, [(\frac{p-1}{2}).\, (\frac{p+1}{2})]$

$= (p - 1^2)\, (2p - 2^2)\, (3p - 3^2) \ldots ((\frac{p-1}{2})p - (\frac{p-1}{2})^2)$

$\equiv (-1^2)\, (-2^2)\, (-3^2) \ldots (-(\frac{p-1}{2})^2) \pmod{p}$ {p's can be eliminated because p-a ≡ -a (mod p)}

$\equiv ((-1)^{\wedge}\frac{p-1}{2})\, (1.2.3. \ldots .\frac{p-1}{2})^2 \pmod{p}$

$\equiv ((-1)^{2x})\, (\frac{p-1}{2}\,!)^2 \pmod{p}$

$\equiv ((\frac{p-1}{2})!)^2 \pmod{p}$

Therefore, $((\frac{p-1}{2})!)^2 \equiv -1 \pmod{p}$.

Q4(MOMC 2024 Senior Round 2): Find the remainder when 23 divides 3^{2023}.

Solution: By Fermat's Little Theorem, $3^{22} \equiv 1 \pmod{23}$

$3^{2023} = (3^{22})^{91} . 3^{21} \equiv 1^{91} . 3^{21} \equiv 3^{21} \pmod{23}$

$3^1 \equiv 3 \pmod{23}$

$3^2 \equiv 9 \pmod{23}$

$3^3 \equiv 27 \equiv 4 \pmod{23}$

$3^4 \equiv 3 . 3^3 \equiv 3 . 4 \equiv 12 \pmod{23}$

$3^7 \equiv 3^3 . 3^4 \equiv 4 . 12 \equiv 48 \equiv 2 \pmod{23}$

$3^{21} \equiv (3^7)^3 \equiv 2^3 \equiv 8 \pmod{23}$

Therefore, $3^{2023} \equiv 3^{21} \equiv 8 \pmod{23}$. The remainder is 8.