10-01-18 Modular Arithmetic

Basics

- In modulo 5, we count 0, 1, 2, 3, 4, 0. Imagine going around a clock.
- For -12 to 0 in mod 5: 3, 4, 0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0.

Notation & Introduction

- $n \equiv a \pmod{m}$ where $0 \leq a < m$ ∵ it's the remainder. It's described as "the residue of n".
- $\equiv$ means the remainders are the same. Read as "congruent to"
- Overall implication that...

$$a \equiv b \pmod{n} \text{ when } \frac{a-b}{n} \in \mathbb{Z}$$

∵ minusing no. from its remainder gives as its new remainder.

Examples

- $15 \equiv 11 \equiv 7 \equiv 3 \pmod{4}$
- $-2 \equiv 3 \pmod{5}$ ∵ count up from -5
- $311 \div 4 = 77 \text{ r } 3 \Rightarrow 311 \equiv 3 \pmod{4}$

Addition

- $17 \equiv 2 \pmod{5}$ & $6 \equiv 1 \pmod{5}$

$\Rightarrow 17 + 6 \pmod{5} \equiv 2 + 1 \bmod (5)$

Meaning... $a \equiv c \pmod{m}$ & $b \equiv d \pmod{m}$

$$a + b \equiv \underbrace{c + d}_{\text{the residue of } c \text{ \& } d \text{ combine}} \pmod{m}$$

Examples

- Find units of $2403 + 741 + 688 + 4839$

$\Rightarrow 2403 + 741 + 688 + 4839 \equiv 3 + 1 + 8 + 9 \equiv 21 \equiv 1 \pmod{10}$

Subtraction

- Similar to addition, subtraction is $a - c \equiv b - d \pmod{m}$ for $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$

Example

- What is the remainder of the difference between 60002 & 6001 when divided by 6?

$$60002 - 6001 \equiv 2 - 1 \equiv 1 \pmod{6}$$

Exponentiation & Multiplication

- $a^e \equiv b^e \pmod{m}$ ①

$\Rightarrow a^k \pmod{m} \equiv (a \pmod{m})^k$

$\Rightarrow a^c \pmod{m} \equiv a^k \pmod{m} \cdot a^j \pmod{m}$ where $c = j + k$

- $a \equiv c \pmod{m}$ & $b \equiv d \pmod{m} \Rightarrow a \cdot b \equiv c \cdot d \pmod{m}$ ②

The "Computer Method"

Find the remainder when 23^{18} is divided by 4.

$18 = 16 + 2$,

$23 \equiv 3 \pmod{4}$ (Always start here)

$23^2 \equiv 3^2 \equiv 1 \pmod{4}$ ①

$23^{16} \equiv 1^{16} \pmod{4}$

$\equiv 1 \pmod{4}$

$23^{16} \cdot 23^2 \equiv 1 \cdot 1 \pmod{4}$ ②

$\equiv \boxed{1} \pmod{4}$

Last digit of $7^{7^{1000}}$

Power... $7 \equiv -1 \pmod{4} \Rightarrow -1^{1000} = 1$ $\because$ 1000 is even

$\Rightarrow 7^1 \bmod 10 \equiv \boxed{7} \bmod 10$

Find the tens & units of 7^{1442}

$7^{1442} \bmod 100$

7^1	7^2	7^3	7^4
7	49	43	1

$\because 7^4 \bmod 100 = 1 \bmod 100$, we can have...

$$7^{4k} \equiv (7^4)^k \equiv 1^k \equiv 1 \bmod 100$$

$4 \times 485 = 1440$

$$\Rightarrow 7^{1440} \cdot 7^2 \bmod 100 \equiv 1 \times 49 \bmod 100 \equiv \boxed{49}$$

Last digit of 15^{12}?

$$\begin{aligned} 15^{12} \bmod 10 &\equiv (15 \bmod 10)^{12} \\ &\equiv (5 \bmod 10)^{12} \\ &\equiv 5^{12} \bmod 10 \\ &\equiv 5 \bmod 10 \end{aligned}$$

$\because$ anything 5^{∞} ends in 5

ALSO NOTE! $6^{\infty} \bmod 10 \equiv 6 \bmod 10$ $\because$ 6 to the power of anything ends in 6