Modular Arithmetic (Arithmetic of Remainders)

Congruence

Two numbers a and b are congruent modulo m if and only if m divides $(a - b)$.

Examples:

$31 \equiv 3 \pmod{7}$ because 7 divides $(31 - 3 = 28)$

$16 \equiv -4 \pmod{5}$ because 5 divides $(16 - (-4) = 20)$

Sample Problem 1

Are 13 and 47 congruent $(\text{mod } 17)$?

Sample Problem 2

Are 22 and -5 congruent $(\text{mod } 13)$?

Residue

We say that a is the modulo-m **residue** of b when $b \equiv a \pmod{m}$, and $0 \leq a < m$.

Sample Problem 3

Find the modulo 4 residue of 125.

Application

Find the value of i^{125}.

Arithmetic Rules

Consider four integers a, b, c, d and a positive integer m such that $a \equiv b\ (mod\ m)$ and $c \equiv d\ (mod\ m)$. In modular arithmetic, the following are true:

- Addition: $a + c \equiv b + d \pmod{m}$.
- Subtraction: $a - c \equiv b - d \pmod{m}$.
- Multiplication: $ac \equiv bd \pmod{m}$.
- Exponentiation: $a^n \equiv b^n \pmod{m}$ where n is a positive integer.

Sample Problem 4

Jerry has 44 boxes of soda in his truck. The cans of soda in each box are packed oddly so that there are 113 cans of soda in each box. Jerry plans to pack the sodas into cases of 12 cans to sell. After making as many complete cases as possible, how many sodas will Jerry have left over?

Application

How can I tell if a number is divisible by 3? by 9? by 11?

Application

Prove that the product of two odd numbers is odd, and that the product of an even number with any integer is even.

Math Challenge Exam Problem (4 points) Find the remainders of the following divisions. (Hint: look for patterns in the remainders of $a^1, a^2, a^3, \ldots$.)

a) (2 points) $3^{1000} \div 7$

$3^1 \div 7 \Rightarrow \text{remainder } 3$
$3^2 \div 7 = 3 \cdot 3 \div 7 \Rightarrow \text{remainder } 2$
$3^3 \div 7 = 2 \cdot 3 \div 7 \Rightarrow \text{remainder } 6$ **Method 1**
$3^4 \div 7 = 6 \cdot 3 \div 7 \Rightarrow \text{remainder } 4$
$3^5 \div 7 = 4 \cdot 3 \div 7 \Rightarrow \text{remainder } 5$
$3^6 \div 7 = 5 \cdot 3 \div 7 \Rightarrow \text{remainder } 1$

$3^{1000} \div 7 = (3^6)^{166} \cdot 3^4 \div 7 \quad \Rightarrow \quad \text{remainder } (1)^{166} \cdot 4 = \mathbf{4}$

OR

$3^3 = 27 \equiv -1 \pmod 7$
$3^{999} \equiv (3^3)^{333} \equiv (-1)^{333} \pmod 7$ **Method 2**
$3^{1000} \equiv 3^{999} \cdot 3 \equiv (-1) \cdot 3 \equiv -3 \equiv -3 + 7 \equiv \mathbf{4} \pmod 7$

b) (2 points) $7^{1000} \div 13$

a) $7^1 \div 13 \Rightarrow \text{remainder } 7$
$7^2 \div 13 = 7 \cdot 7 \div 13 \Rightarrow \text{remainder } 10$
$7^3 \div 13 = 10 \cdot 7 \div 13 \Rightarrow \text{remainder } 5$ **Method 1**
$7^4 \div 13 = 5 \cdot 7 \div 13 \Rightarrow \text{remainder } 9$
$7^5 \div 13 = 9 \cdot 7 \div 13 \Rightarrow \text{remainder } 11$
$7^6 \div 13 = 11 \cdot 7 \div 13 \Rightarrow \text{remainder } 12 \text{ or } -1$

$7^{1000} \div 13 = (7^6)^{166} \cdot 7^4 \div 13 \quad \Rightarrow \quad \text{remainder } (-1)^{166} \cdot 9 = \mathbf{9}$

OR

$7^2 = 49 \equiv -3 \pmod{13}$
$7^6 \equiv (7^2)^3 \equiv (-3)^3 = -27 \equiv -1 \pmod{13}$ **Method 2**
$7^{1000} \equiv (7^6)^{166} \cdot (7^2)^2 \equiv (-1)^{166} \cdot (-3)^2 \equiv 1 \cdot 9 \equiv \mathbf{9} \pmod{13}$