Newton School of Technology

Basic Arithmetic Foundations (Part 4)

By- Piyush Jain

CS01: Mathematics-I

Join the class

Newton School of Technology

Today’s Agenda

- Modular Inverse
- Divisibility rules

Quick Revision

- $a \equiv b \pmod{n}$
- It also indicates that n divides (a - b) which means that (a - b) is a multiple of n, i.e., (a - b) can be written as n * k for some integer k.

Quick Revision

- $\boldsymbol{a \equiv b}$ **(mod $\boldsymbol{n}$)**
- It also indicates that n divides (a - b) which means that (a - b) is a multiple of n, i.e., (a - b) can be written as n * k for some integer k.

- **Examples:**
  - 47 ≡ 12 (mod 5)
  - 13 ≡ 1 (mod 6)
  - 129 ≡ 9 (mod 8)

Properties of Modular Arithmetic

- **Modular Addition:**

  $$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$$

- **Modular Subtraction:**

  $$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$$

- **Modular Multiplication:**

  $$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$$

Properties of Modular Arithmetic

- **Modular Exponentiation:**

$$(a^b) \mod n = ((a \mod n)^b) \mod n$$

More Congruence Rules

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

- **Subtraction:** $a - c \equiv b - d \pmod{n}$
- **Multiplication:** $ac \equiv bd \pmod{n}$
- **Exponentiation:** $a^m \equiv b^m \pmod{n}$ for any positive integer m.

Example

- $16^3 \bmod 7$
- $23^3 \bmod 20$
- $92^{72} \bmod 13$
- $2^{1063} \bmod 3$

Modular Inverse

- For integers a and m (with m>1), the modular inverse of a modulo m is an integer x such that $\mathbf{a \cdot x \equiv 1 (mod\ m)}$.

- In other words:

When you multiply a with x, the product leaves remainder 1 when divided by m.

- We denote it as $\mathbf{a^{-1}\ (mod\ m) = x}$

Modular Inverse

Question:

What is the modular inverse of 3 modulo 7?

Modular Inverse

Question:

What is the modular inverse of 3 modulo 7?

Solution:

We want x such that:

$$3x \equiv 1 \pmod{7}$$

x = 5 satisfies the above condition.

So, the modular inverse of 3 (mod 7) is **5**.

- $3 \cdot 1 = 3 \equiv 3 \pmod{7}$
- $3 \cdot 2 = 6 \equiv 6 \pmod{7}$
- $3 \cdot 3 = 9 \equiv 2 \pmod{7}$
- $3 \cdot 4 = 12 \equiv 5 \pmod{7}$
- $3 \cdot 5 = 15 \equiv 1 \pmod{7}$ ✅

Modular Inverse

Question:

What is the modular inverse of 4 modulo 8?

Modular Inverse

Question:

What is the modular inverse of 4 modulo 8?

Solution:

Since 4 and 8 are not coprime, no modular inverse exists for 4 (mod 8). 🚫

The modular inverse of 4 modulo 8 does not exist.

$$4 \cdot 1 = 4 \equiv 4 \pmod 8$$

$$4 \cdot 2 = 8 \equiv 0 \pmod 8$$

$$4 \cdot 3 = 12 \equiv 4 \pmod 8$$

$$4 \cdot 4 = 16 \equiv 0 \pmod 8$$

Modular Inverse Existence Condition

- The modular inverse of **a (mod m)** exists if and only if **a** and **m** are **coprime**,i.e., **gcd(a,m) = 1**.

- If gcd(a,m) ≠ 1, then no inverse exists.

[Think about it. Explore! Share the reason in lab.]

Modular Inverse

Let's say the question is to find the modular inverse of **a (mod m)**.

Thought Process:

- We will find **x** such that **a.x ≡ 1 (mod m)**

Think about the following:

- While checking for modular inverse why do we check for x values from 0 to m-1 only?

Modular Inverse

Let's say the question is to find the modular inverse of **a (mod m)**.

Thought Process:

- We will find **x** such that **a.x ≡ 1 (mod m)**

Think about the following:

- While checking for modular inverse why do we check for x values from 0 to m-1 only?

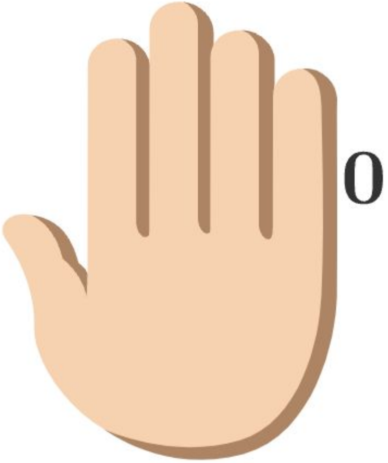
Note: Every number outside 0 to m−1 is equivalent to one inside that range. That's why we only need to check m values, not infinitely many.

Divisibility Rules

Example

Your friend writes down a five-digit number, and then covers all digits except the last digit, which is a 0, with his hand.

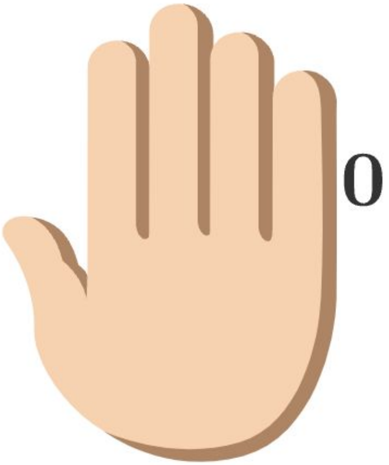
- Is this number divisible by 2?
- Is this number divisible by 4?
- Is this number divisible by 5?



Example

Your friend writes down a five-digit number, and then covers all digits except the last digit, which is a 0, with his hand.

- Is this number divisible by 2? Yes.
- Is this number divisible by 4? Not possible to be certain.
- Is this number divisible by 5? Yes.



Divisibility Rules

- A number is divisible by 2 if its last digit is divisible by 2.
- A number is divisible by 5 if its last digit is 0 or 5.
- A number is divisible by 10 if its last digit is 0.

Divisibility of 4

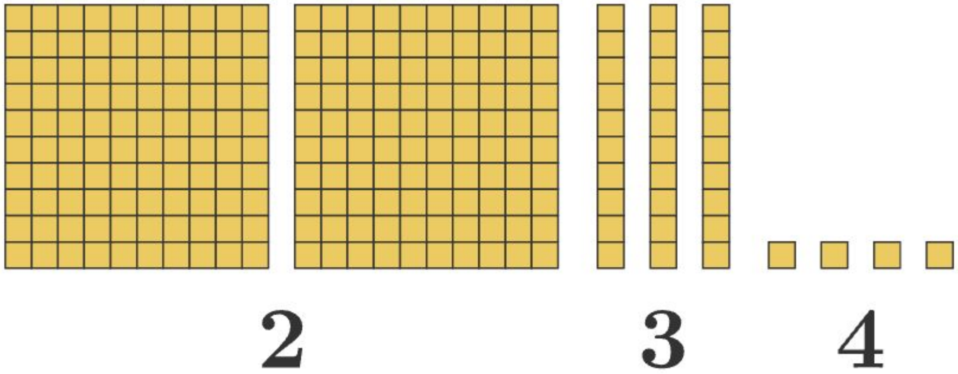
- What is divisibility rule of 4 ?

  A number is divisible by 4 if last 2 digits of the number are divisible by 4.

But why ?

Let’s Decode the Magic Technique

- Any number can be written as sum of hundreds, tens, and units.
    - Example: Check 234 is divisible by 4 or not



Determining if 234 is divisible by 4

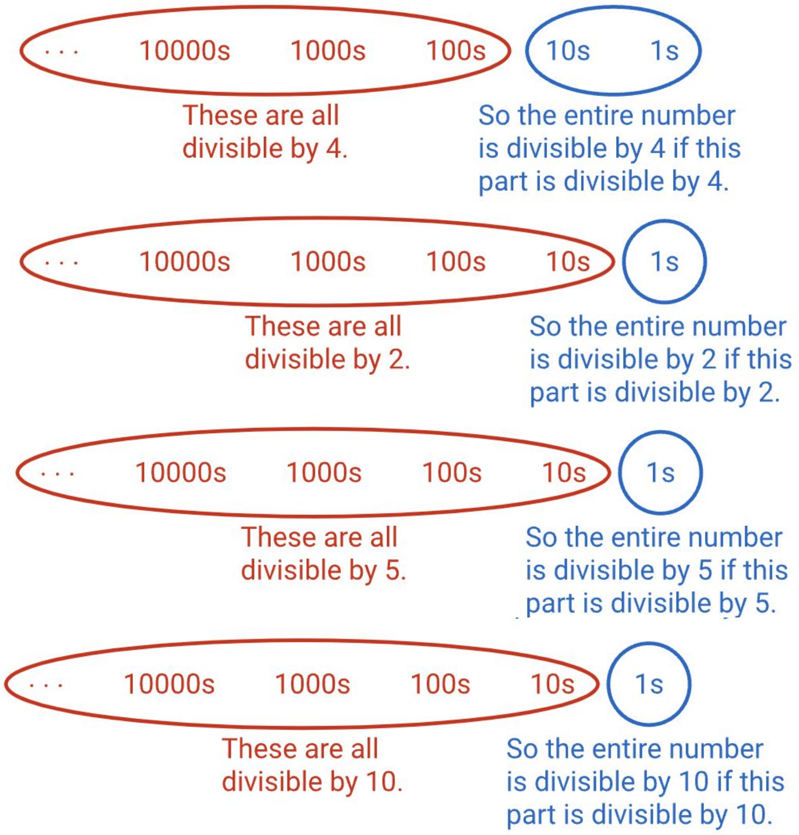
There are 2 sets of 100 squares, 3 sets of 10 squares, and 4 sets of 1 square each.

- Dividing 100 by 4 leaves a remainder of 0.
- Dividing 10 by 4 leaves a remainder of 2.
- Dividing 1 by 4 leaves a remainder of 1.

The sum of all these remainders is $(2\times0) + (3\times2) + (4\times1) = 10$.
Dividing 10 by 4 leaves a remainder of 2, which corresponds to the remainder when 234 is divided by 4.

Note: Since every power of 10 greater than 10 itself is divisible by 4, the remainder when a number is divided by 4 is the same as the remainder when the last two digits of the number are divided by 4.

Revisiting Divisibility Rule of 2,5,10



The Magic Technique

- To find out if a number n is divisible by another number m,
    - Do the division by m on each power of 10 in n separately, and
    - If there are remainders, add them together and determine whether this sum is divisible by m.

Example

A number is divisible by 8 if and only if the number formed by its last ________ digits are divisible by 8.

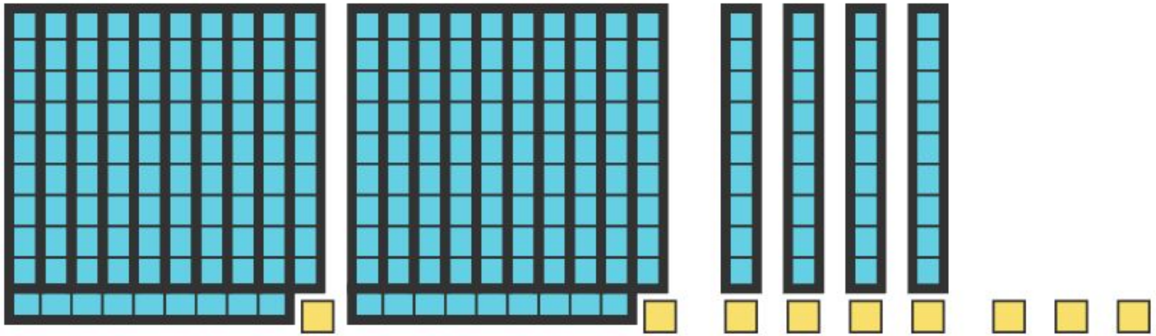
2 / 3 / 4 / 5

Divisibility Rule of 3

Check Divisibility of 243 with 3?

$243 = (2\times100) + (4\times10) + (3\times1)$

Sum of remainders = 2 + 4 + 3 = Sum of digits



Divisibility Rule of 9

Check Divisibility of 243 with 9?

$243 = (2\times100) + (4\times10) + (3\times1)$

Sum of remainders = 2 + 4 + 3 = Sum of digits

Divisibility Rule of 11

Check Divisibility of 51243 with 11?

Quiz Quiz Quiz


Feedback Time

See You Guys in Next Session :)