Newton School of Technology

Basic Arithmetic Foundations (Part 4)

By- Piyush Jain

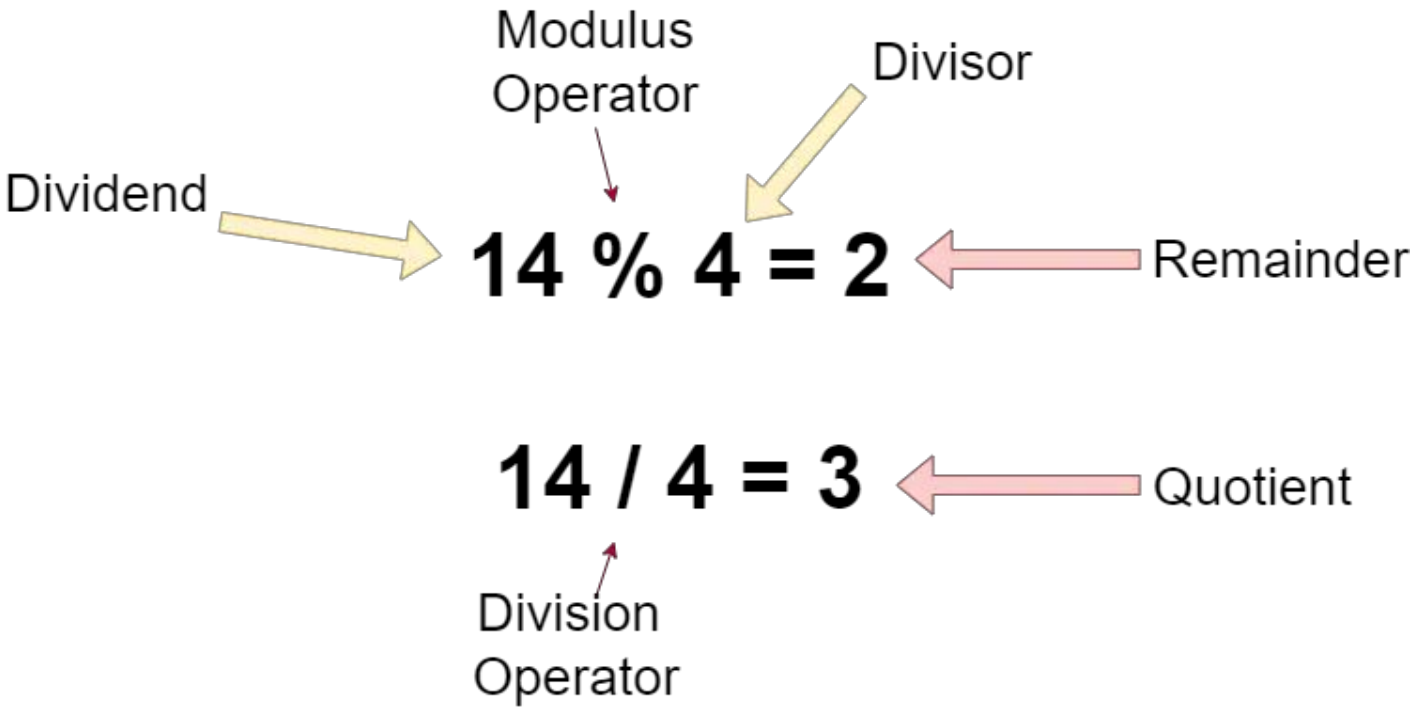
CS01: Mathematics-I

Newton School of Technology

Today’s Agenda

- Modular Arithmetic
    - Modular Addition
    - Modular Multiplication
    - Modular Subtraction
    - Modular Exponentiation

Modulus Operator



Rapid fire

What are the possible remainders when an integer n (positive or negative) is divided by 9?

Possible remainders:

{0, 1, 2, 3, 4, 5, 6, 7, 8}

0 <= (n mod 9) < 9

Cyclic Nature of Modulus

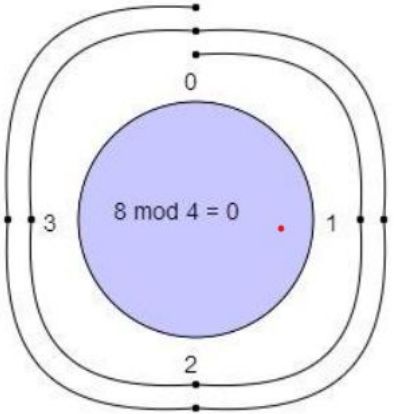
- 0%3 = 0
- 1%3 = 1
- 2%3 = 2
- 3%3 = 0
- 4%3 = 1
- 5%3 = 2
- 6%3 = 0

Note: The value of a%3 will always be either 0 or 1 or 2.

Example

What is the value of **8 mod 4**?

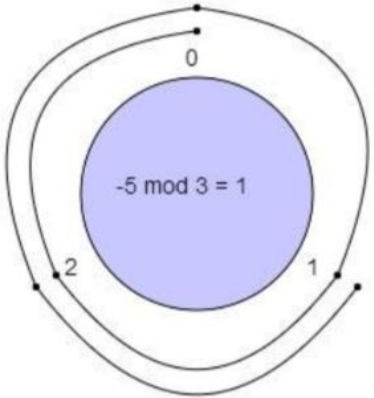
- With a modulus of 4, we make a clock with numbers 0, 1, 2, 3.
- We start at 0 and go through 8 numbers in a clockwise sequence 1, 2, 3, 0, 1, 2, 3, 0.
- We ended up at 0, So 8 mod 4 = **0**.



Example

What is the value of **-5 mod 3**?

- With a modulus of 3 we make a clock with numbers 0, 1, 2.
- We start at 0 and go through 5 numbers in **counter-clockwise** sequence.
- (5 is **negative**) 2, 1, 0, 2, 1.
- We ended up at **1** so -5 mod 3 = **1**



Example

What is the value of **-5 mod 3**?

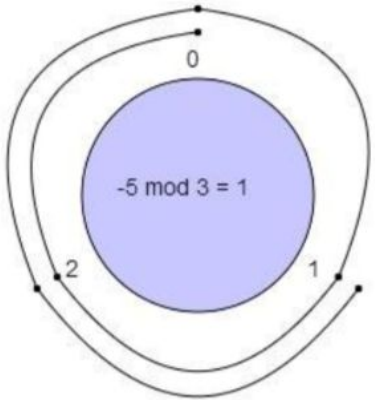
= (-5 + 3) mod 3.

= -2 mod 3

= (-2 + 3) mod 3

= 1 mod 3

= **1**



Note: m mod n = (m + k · n) mod n, where m, k, n are integers.

Logic to find m mod n when m < 0

Newton School of Technology

We need to find smallest positive integer ‘k’ such that **$m + k \cdot n \geq 0$**.

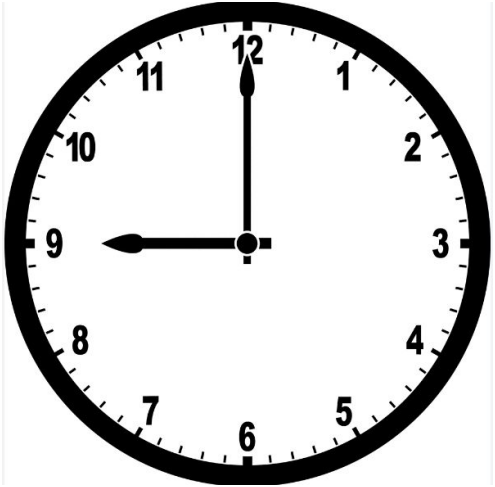
The value of **$m + k \cdot n$** will be the result of **m mod n**.

Note: $m \bmod n = (m + k \cdot n) \bmod n$

Example

In a 12-hour clock, what time is it 35 hours after 9 o’clock?

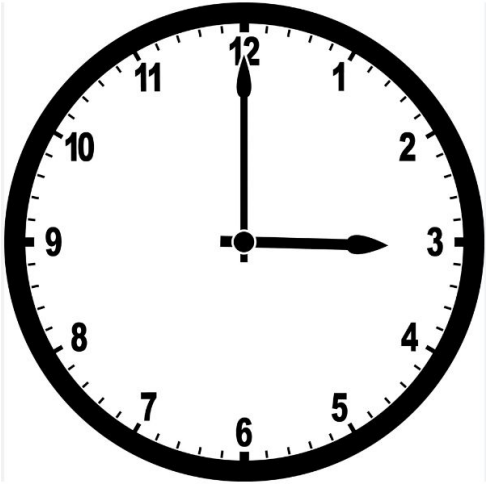
Ans: (9+35) mod 12 = 44 mod 12 = 8 o’clock



Example

In a 12-hour clock, What time is it 8 hours before 3 o’clock?

Ans: (3-8) mod 12 = -5 mod 12 = 7 o’clock



Traditional Division v/s Modulo Perspective

- **Traditional:** $\frac{a}{n}$ process focuses on quotient q.
- **Modulo Perspective:** Focus shifts to the remainder.
- When a is divided by n, we get remainder r_1:

$$a = qn + r_1$$

- Similarly, when b is divided by n, we might get remainder r_2:

$$b = q'n + r_2$$

What happens when Remainders are Equal?

- If $r_1 \neq r_2$ when a and b are divided by n (where n is a positive integer), then it's NOT INTERESTING.

- If $r_1 = r_2$ when a and b are divided by n (where **n is a positive integer**), we use the notation:

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

- This is read as "**a is congruent to b modulo n**".

Congruence: Not a New Concept

Newton School of Technology

- The word ”congruent” is familiar from school

(e.g., congruent triangles, $\triangle ABC \cong \triangle PQR$).

- In number theory, congruence is between remainders of a and b when divided (reduced) by n.

From Remainders to Divisibility

- From **$a = q_1 n + r$** and **$b = q_2 n + r$**:

$$a - q_1 n = r$$

$$b - q_2 n = r$$

- Equating the remainders: **$a - q_1 n = b - q_2 n$**
- Rearranging: **$a - b = (q_1 - q_2)n$**
- **This implies $a - b = kn$ for some integer k.**
- Therefore, n divides (a − b), written as **$n|(a - b)$**.

General Notation

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

- **Examples:**
  - 7 ≡ 2 (mod 5) because 7 - 2 = 5, and 5 divides 5.
  - 13 ≡ 1 (mod 6) because 13 - 1 = 12, and 6 divides 1.
  - 25 ≡ 1 (mod 8) because 25 - 1 = 24, and 8 divides 24.

Even and Odd Numbers

- **a and b are congruent modulo 2** (**a ≡ b (mod 2)**):
  - This means 2|(a − b).
    - **Case 1:** If **a and b are both even** (2k, 2t), then

      a − b = 2k − 2t = 2(k − t), so **2|(a − b).**
    - **Case 2:** If **a and b are both odd** (2k + 1, 2t + 1), then

      a − b = (2k + 1) − (2t + 1) = 2k − 2t = 2(k − t), so **2|(a − b).**
    - **Case 3:** If **one is even and one is odd**, a − b is odd, and **2 ∤ (a − b)**.

Remainders 0, 1, or 2

- When a and b are congruent modulo 3, i.e., **a ≡ b (mod 3)**:
  - This means 3|(a − b).
- **Case 1:** Both a and b leave remainder 0 (e.g., 3m, 3n).
- **Case 2:** Both a and b leave remainder 1 (e.g., 3m + 1, 3n + 1).
- **Case 3:** Both a and b leave remainder 2 (e.g., 3m + 2, 3n + 2).

Question: What can you say about the following cases?

a) (3m + 3, 3n + 3)

b) (3m + 4, 3n + 4)

c) (3m + 5, 3n + 5)

Remainders 0, 1, or 2

- When a and b are congruent modulo 3, i.e., **a ≡ b (mod 3)**:
  - This means 3|(a − b).
- **Case 1:** Both a and b leave remainder 0 (e.g., 3m, 3n).
- **Case 2:** Both a and b leave remainder 1 (e.g., 3m + 1, 3n + 1).
- **Case 3:** Both a and b leave remainder 2 (e.g., 3m + 2, 3n + 2).

Question: What can you say about the following cases?

a) (3m + 3, 3n + 3) → Same as **Case 1** → Remainder 0.

b) (3m + 4, 3n + 4) → Same as **Case 2** → Remainder 1.

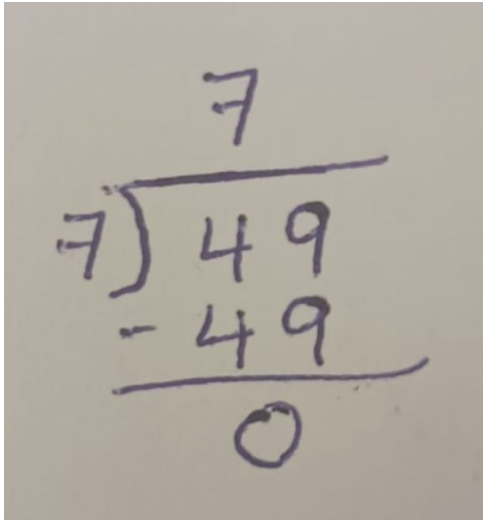
c) (3m + 5, 3n + 5) → Same as **Case 3** → Remainder 2.

Simple Modulo Calculation

- When somebody asks **49 (mod 7)**, they are asking about the **remainder of 49 divided by 7**.

- We know **49 = 7 × 7 + 0**.

- So, **49 ≡ 0 (mod 7)**.



Newton School of Technology

Properties of Modular Arithmetic

- **Modular Addition:**

  (a + b) mod n = [(a mod n) + (b mod n)] mod n

  Try out (17 + 23) mod 5

- **Modular Subtraction:**

  (a - b) mod n = [(a mod n) - (b mod n)] mod n

  Try out (17 - 23) mod 5

- **Modular Multiplication:**

  (a x b) mod n = [(a mod n) x (b mod n)] mod n

  Try out (17 x 23) mod 5

Properties of Modular Arithmetic

- **Modular Exponentiation:**

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

Modular Exponentiation

- It refers to finding the result of a number raised to a certain power and then taking the remainder when divided by a modulus. In mathematical terms, it calculates:

  $$\mathbf{x = a^b \bmod n}$$

- When the exponent **b** is large, calculating $\mathbf{a^b}$ directly would result in an extremely large number, potentially leading to overflow or inefficiency. Modular exponentiation efficiently handles these large numbers by reducing intermediate results modulo **n**

- **Note:** $a^b \bmod n = [(a \bmod n)^b] \bmod n$

Example (Try it yourself)

- **Try to prove the following using modular multiplication property:**

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

Ans. $a^b \bmod n$
$= (a \times a \times a \times \ldots. \times a) \bmod n \quad \Rightarrow$ (here, a x a x a …. x a will be b times)
$= [(a \bmod n) \times (a \bmod n) \times (a \bmod n) \times (a \bmod n) \times \ldots. \times (a \bmod n)] \bmod n \Rightarrow$ (using modular multiplication property)

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

Newton School of Technology

Modular Exponentiation In Programming

Python provides a built-in function pow(a, b, m) for modular exponentiation, which is highly optimized.

```
a = 2
b = 10
m = 1000
result = pow(a, b, m)
print(result)  # Output: 24
```

If a ≡ b (mod n) and c ≡ d (mod n)

- **Property:** $a + c \equiv b + d \pmod{n}$
- **Proof:**
  - Given $a \equiv b \pmod{n} \Rightarrow a - b = kn$ for some $k \in \mathbb{Z}$.
  - Given $c \equiv d \pmod{n} \Rightarrow c - d = tn$ for some $t \in \mathbb{Z}$.
  - Consider $(a + c) - (b + d) = (a - b) + (c - d)$
  - Substitute: $(a + c) - (b + d) = kn + tn = (k + t)n$.
  - Since $(k + t)$ is an integer, $n|((a + c) - (b + d))$.
  - Therefore, $a + c \equiv b + d \pmod{n}$.

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.

Cancellation in Modular Arithmetic

▸ **Question:**

If **ac ≡ bc (mod n)**, can we say **a ≡ b (mod n)**?

▸ **Answer:**

Yes/No? Justify your answer.

- If **Yes**, then **rethink**.
- If **No**, then what condition **c** must satisfy to be cancelled from the following equation **ac ≡ bc (mod n)** ?

When Cancellation in Modular Arithmetic is Allowed?

- If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{\frac{n}{\gcd(c,n)}}$.
- If $\gcd(c, n) = 1$ (i.e., c and n are coprime), then we can cancel c:

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

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

Sum of Factorials Modulo 12

- **Problem:** Find the remainder when 1! + 2! + 3! + · · · + 100! is divided by 12.

$$(1! + 2! + 3! + \cdots + 100!) \pmod{12}$$

*Solve in SNAP!

Sum of Factorials Modulo 12

- Without modulo, this is very cumbersome.
- Observe $4! = 4 \times 3 \times 2 \times 1 = 24$.
- $24 \equiv 0 \pmod{12}$.
- This means for any $k \geq 4$, $k!$ will contain $4!$ as a factor, so $k! \equiv 0 \pmod{12}$.
- Out of 100 terms, $4! + 5! + \cdots + 100!$ all go to $0 \pmod{12}$.
- We are left with:

$$\begin{aligned} 1! + 2! + 3! + 4! + \cdots + 100! &\equiv (1! + 2! + 3!) \pmod{12} \\ &\equiv (1 + 2 + 6) \pmod{12} \\ &\equiv 9 \pmod{12} \end{aligned}$$

- Hence, the remainder is 9 when $1! + 2! + 3! + \cdots + 100!$ is divided by 12.

Example

Check whether the given statement is True or False:

$$41 \mid (2^{20} - 1), \text{ i.e., } 2^{20} - 1 \equiv 0 \pmod{41}$$

Newton School of Technology

Homework

1. Find the remainders when 2^{50} and 4^{65} are divided by 7.
2. Find $(1^5 + 2^5 + 3^5 + 4^5 + \cdots + 100^5) \pmod 4$.
3. Show that $53^{103} + 103^{53}$ is divisible by 39.
4. Show that $111^{333} + 333^{111}$ is divisible by 7.

Newton School of Technology

See You Guys in Next Session :)