An Introduction to Modular Arithmetic

Exploration of Number Theory

Kazi Istiak Uddin Toriqe
Fahad Ahmed Akash
Arko Sikder

Department of CSE, BUET

December 9, 2023

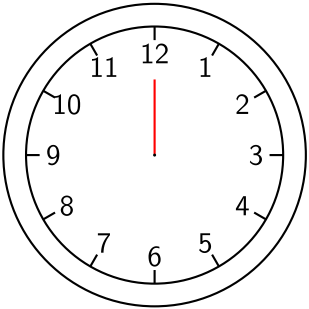
Modular

Arithmetic

Think!

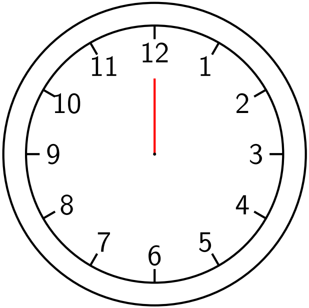
Think about a fact. When we are telling a time, we wouldn't say 13 o'clock rather we would say 1 o'clock.

Clock - 12 modulo system

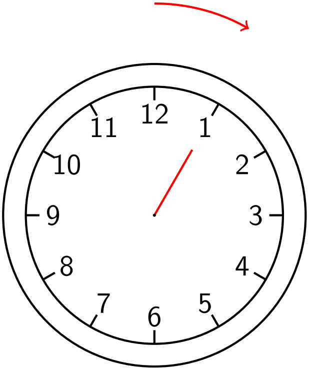


12 o'clock

Clock - 12 modulo system



12 o'clock



13 == 1 o'clock

Remainder

The remainder when we divide 13 by 12 is **1**.

$$13 \equiv 1 \pmod{12}$$

Remainder

The remainder when we divide 13 by 12 is **1**.

$$13 \equiv 1 \pmod{12}$$

$$13 = 12 * 1 + 1$$

Remainder

The remainder when we divide 14 by 12 is **2**.

$$13 \equiv 1 \pmod{12}$$

$$14 \equiv 2 \pmod{12}$$

$$13 = 12 * 1 + 1$$

Remainder

The remainder when we divide 14 by 12 is **2**.

$$13 \equiv 1 \pmod{12}$$

$$14 \equiv 2 \pmod{12}$$

$$13 = 12 * 1 + 1$$

$$14 = 12 * 1 + 2$$

Remainder

The remainder when we divide 25 by 12 is **1**.

$$13 \equiv 1 \pmod{12}$$

$$14 \equiv 2 \pmod{12}$$

$$25 \equiv 1 \pmod{12}$$

$$13 = 12 * 1 + 1$$

$$14 = 12 * 1 + 2$$

Remainder

The remainder when we divide 25 by 12 is **1**.

$$13 \equiv 1 \pmod{12}$$

$$14 \equiv 2 \pmod{12}$$

$$25 \equiv 1 \pmod{12}$$

$$13 = 12 * 1 + 1$$

$$14 = 12 * 1 + 2$$

$$25 = 12 * 2 + 1$$

Modular Arithmetic

If divide **a** by **n** gets quotient **q** and remainder **r**

$$\mathbf{a} = \mathbf{qn} + \mathbf{r}$$

Modular Arithmetic

$$a = qn + r$$

quotient

remainder

Modular Arithmetic

$$\mathbf{a} = \mathbf{q}\mathbf{n} + \mathbf{r} \qquad\qquad \mathbf{a} \equiv \mathbf{r} (\mathbf{mod}\ \mathbf{n})$$

quotient

remainder

a is congruent to r mod n

Residue

Remainder r often referred to as Residue. A small amount of something that remains after the main part has been taken is called residue.

Residue

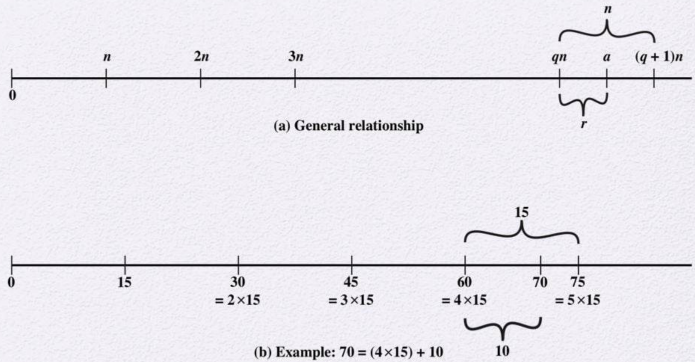
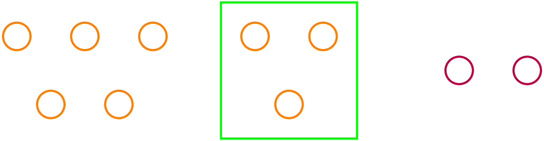


Figure 4.1 **The Relationship** $a = qn + r;\ 0 \le r < n$

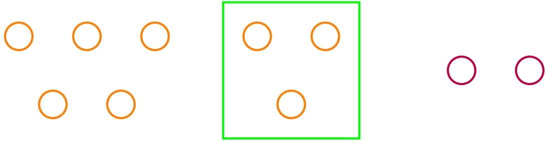
Think!

Now it is time to explore some properties!

Properties

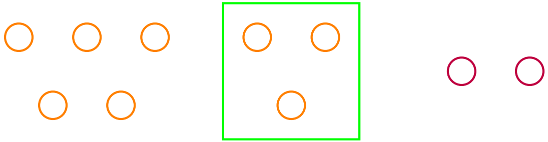


Properties

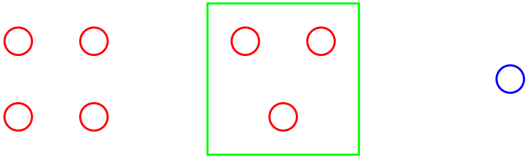


$$5 \equiv 2 \pmod{3}$$

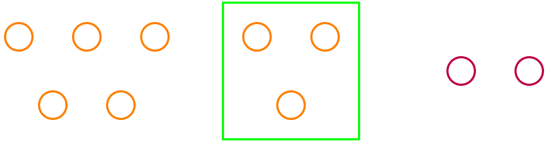
Properties



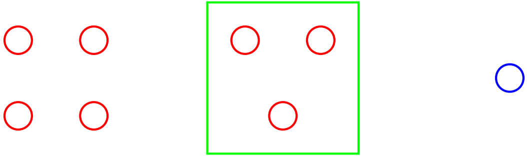
$$5 \equiv 2 \pmod{3}$$



Properties

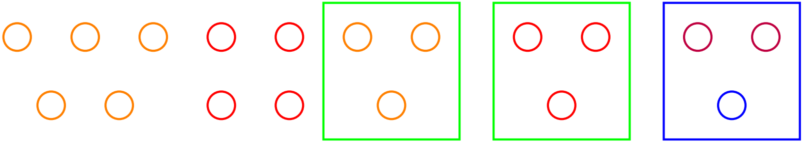


$$5 \equiv 2 \pmod{3}$$

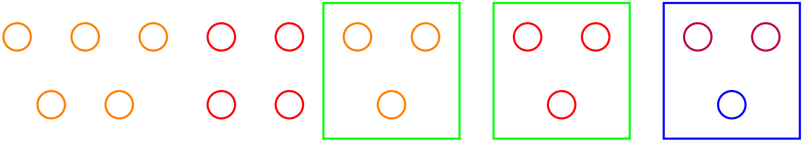


$$4 \equiv 1 \pmod{3}$$

Add



Add



Add

$$9 \equiv 0 \pmod{3}$$

Sub

Sub

Sub

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

Addition and Subtraction

$$a_1 \equiv b_1 \pmod{m}$$

$$a_2 \equiv b_2 \pmod{m}$$

$$a_1 + a_2 \equiv (b_1 + b_2) \pmod{m}$$

$$a_1 - a_2 \equiv (b_1 - b_2) \pmod{m}$$

Proof

$$a_1 \equiv b_1 \pmod{p}$$

Proof

$$a_1 \equiv b_1 \pmod{p}$$

$$\boldsymbol{a_1 = mp + b_1}$$

Proof

$$a_1 \equiv b_1 \pmod{p}$$

$$a_2 \equiv b_2 \pmod{p}$$

$$a_1 = mp + b_1$$

Proof

$$a_1 \equiv b_1 \pmod{p}$$

$$a_1 = mp + b_1$$

$$a_2 \equiv b_2 \pmod{p}$$

$$\boldsymbol{a_2 = np + b_2}$$

Proof

$$a_1 \equiv b_1 \pmod{p} \qquad a_2 \equiv b_2 \pmod{p}$$

$$a_1 = mp + b_1 \qquad a_2 = np + b_2$$

$$a_1 \pm a_2 = (mp + b_1) \pm (np + b_2)$$

Proof

$$a_1 \equiv b_1 \pmod{p} \qquad a_2 \equiv b_2 \pmod{p}$$

$$a_1 = mp + b_1 \qquad a_2 = np + b_2$$

$$\begin{aligned} a_1 \pm a_2 &= (mp + b_1) \pm (np + b_2) \\ &= (m \pm n)p + (b_1 \pm b_2) \end{aligned}$$

Proof

$$a_1 \equiv b_1 \pmod{p} \qquad a_2 \equiv b_2 \pmod{p}$$

$$a_1 = mp + b_1 \qquad a_2 = np + b_2$$

$$\begin{aligned} a_1 \pm a_2 &= (mp + b_1) \pm (np + b_2) \\ &= (m \pm n)p + (b_1 \pm b_2) \\ X &= Ap + Y \end{aligned}$$

Proof

$$a_1 \equiv b_1 \pmod{p} \qquad a_2 \equiv b_2 \pmod{p}$$

$$a_1 = mp + b_1 \qquad a_2 = np + b_2$$

$$\begin{aligned} a_1 \pm a_2 &= (mp + b_1) \pm (np + b_2) \\ &= (m \pm n)p + (b_1 \pm b_2) \\ X &= Ap + Y \end{aligned}$$

$$X \equiv Y \pmod{p}$$

Proof

$$a_1 \equiv b_1 \pmod{p} \qquad a_2 \equiv b_2 \pmod{p}$$

$$a_1 = mp + b_1 \qquad a_2 = np + b_2$$

$$\begin{aligned} a_1 \pm a_2 &= (mp + b_1) \pm (np + b_2) \\ &= (m \pm n)p + (b_1 \pm b_2) \\ X &= Ap + Y \end{aligned}$$

$$X \equiv Y \pmod{p}$$

$$a_1 \pm a_2 \equiv (b_1 \pm b_2) \pmod{p} \quad \textbf{[QED]}$$

Multiplication

$$5 \equiv 2 \pmod{3}$$

$$4 \equiv 1 \pmod{3}$$

Multiplication

$$5 \equiv 2 \pmod 3$$
$$4 \equiv 1 \pmod 3$$

Multiply

$$20 \equiv 2 \pmod 3$$

Multiplication

$$a_1 \equiv b_1 \pmod{m}$$

$$a_2 \equiv b_2 \pmod{m}$$

$$\boldsymbol{a_1 a_2 \equiv b_1 b_2 \pmod{m}}$$

Multiplication

$$a_1 \equiv b_1 \pmod{m}$$

$$a_2 \equiv b_2 \pmod{m}$$

$$\boldsymbol{a_1 a_2 \equiv b_1 b_2 \pmod{m}}$$

Can be easily proved just as before!

Power

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

Power

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

If we put $a_1 = a_2 = a$,

$$a^2 \equiv b^2 \pmod{m}$$

Power

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

If we put $a_1 = a_2 = a$,

$$a^2 \equiv b^2 \pmod{m}$$

If we keep multiplying,

Power

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

If we put $a_1 = a_2 = a$,

$$a^2 \equiv b^2 \pmod{m}$$

If we keep multiplying,

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

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

Sol^n :

$$7^{2023}$$

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

Sol^n :

$$7^{2023} \equiv 7^{2022} \cdot 7 \pmod{10}$$

An Interesting Problem

Find the last digit of $(2 + 0 + 2 + 3)^{2023}$

Sol^n :

$$\begin{aligned} 7^{2023} &\equiv 7^{2022} \cdot 7 \pmod{10} \\ &\equiv (7^2)^{1011} \cdot 7 \pmod{10} \end{aligned}$$

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

Sol^n :

$$\begin{aligned} 7^{2023} &\equiv 7^{2022}\cdot 7 \pmod{10} \\ &\equiv (7^2)^{1011}\cdot 7 \pmod{10} \\ &\equiv (49)^{1011}\cdot 7 \pmod{10} \end{aligned}$$

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

Sol^n :

$$\begin{aligned} 7^{2023} &\equiv 7^{2022} \cdot 7 \pmod{10} \\ &\equiv (7^2)^{1011} \cdot 7 \pmod{10} \\ &\equiv (49)^{1011} \cdot 7 \pmod{10} \\ &\equiv (-1)^{1011} \cdot 7 \pmod{10} \end{aligned}$$

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

Sol^n :

$$\begin{aligned} 7^{2023} &\equiv 7^{2022} \cdot 7 \pmod{10} \\ &\equiv (7^2)^{1011} \cdot 7 \pmod{10} \\ &\equiv (49)^{1011} \cdot 7 \pmod{10} \\ &\equiv (-1)^{1011} \cdot 7 \pmod{10} \\ &\equiv (-1) \cdot 7 \pmod{10} \end{aligned}$$

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

Sol^n :

$$\begin{aligned} 7^{2023} &\equiv 7^{2022}\cdot 7 \pmod{10} \\ &\equiv (7^2)^{1011}\cdot 7 \pmod{10} \\ &\equiv (49)^{1011}\cdot 7 \pmod{10} \\ &\equiv (-1)^{1011}\cdot 7 \pmod{10} \\ &\equiv (-1)\cdot 7 \pmod{10} \\ &\equiv -7 \pmod{10} \end{aligned}$$

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

Sol^n :

$$\begin{aligned}
7^{2023} &\equiv 7^{2022} \cdot 7 \pmod{10} \\
&\equiv (7^2)^{1011} \cdot 7 \pmod{10} \\
&\equiv (49)^{1011} \cdot 7 \pmod{10} \\
&\equiv (-1)^{1011} \cdot 7 \pmod{10} \\
&\equiv (-1) \cdot 7 \pmod{10} \\
&\equiv -7 \pmod{10} \\
&\equiv 3
\end{aligned}$$

An Interesting Problem

Find the last digit of $(2+0+2+3)^{2023}$

Sol^n :

$$
\begin{aligned}
7^{2023} &\equiv 7^{2022}\cdot 7 \pmod{10}\\
&\equiv (7^2)^{1011}\cdot 7 \pmod{10}\\
&\equiv (49)^{1011}\cdot 7 \pmod{10}\\
&\equiv (-1)^{1011}\cdot 7 \pmod{10}\\
&\equiv (-1)\cdot 7 \pmod{10}\\
&\equiv -7 \pmod{10}\\
&\equiv 3
\end{aligned}
$$

So the last digit of 7^{2023} is 3

Modular Arithmetic for Division

- Can we do modular operations for division algorithms ?

Modular Arithmetic for Division

- Can we do modular operations for division algorithms ?
- The answer is no . Division algorithm doesn't work like that way all the time .

Modular Arithmetic for Division

- Can we do modular operations for division algorithms ?
- The answer is no . Division algorithm doesn't work like that way all the time .
- Why ?

Modular Arithmetic for Division

- Can we do modular operations for division algorithms ?
- The answer is no . Division algorithm doesn't work like that way all the time .
- Why ?
- Remember what we know !! we cannot divide anything by 0 .

Modular Arithmetic for Division

- Can we do modular operations for division algorithms ?
- The answer is no . Division algorithm doesn't work like that way all the time .
- Why ?
- Remember what we know !! we cannot divide anything by 0 .
- Even if , $a \equiv 0 \pmod{b}$

Modular Arithmetic for Division

- We can't determine it simply by writing

$$\left(\frac{a}{b}\right) \equiv \frac{a \equiv d_1 \pmod{m}}{b \equiv d_2 \pmod{m}}$$

Modular Arithmetic for Division

- We can't determine it simply by writing

$$(\frac{a}{b}) \equiv \frac{a \equiv d_1 \pmod{m}}{b \equiv d_2 \pmod{m}}$$

- Because there's a possibility of the denominator d_2 becoming 0 again!!

Modular Arithmetic for Division

- Let's see another example for more clear picture

$$15 \equiv 6 \pmod 9 \tag{1}$$

$$3 \equiv 3 \pmod 9 \tag{2}$$

Modular Arithmetic for Division

- Let's see another example for more clear picture

$$15 \equiv 6 \pmod 9 \tag{1}$$

$$3 \equiv 3 \pmod 9 \tag{2}$$

- if we use the distribution law for division , We will get

$$5 \equiv 2 \pmod 9$$

Modular Arithmetic for Division

- Let's see another example for more clear picture

$$15 \equiv 6 \pmod 9 \tag{1}$$

$$3 \equiv 3 \pmod 9 \tag{2}$$

- if we use the distribution law for division , We will get

$$5 \equiv 2 \pmod 9$$

- Which emerges a disastrous question to our knowledge about division !!

How do we know it ?

Modular Multiplicative Inverse

$$5.5^{-1} \equiv 1 \pmod{9}$$

Modular Multiplicative Inverse

$$5.5^{-1} \equiv 1 \pmod{9}$$

$$\Rightarrow 5b \equiv 1 \pmod{9}$$

Modular Multiplicative Inverse

$$5.5^{-1} \equiv 1 \pmod{9}$$

$$\Rightarrow 5b \equiv 1 \pmod{9}$$

$$\Rightarrow 5.2 \equiv 1 \pmod{9}$$

Modular Multiplicative Inverse

$$5.5^{-1} \equiv 1 \pmod{9}$$

$$\Rightarrow 5b \equiv 1 \pmod{9}$$

$$\Rightarrow 5.2 \equiv 1 \pmod{9}$$

2 is the modular multiplicative inverse of **5**, modulo **9**

Modular Multiplicative Inverse

Let's Solve a problem !

$$(\frac{20}{5}) \pmod 9$$

Modular Multiplicative Inverse

Let's Solve a problem !

$$(\frac{20}{5}) \pmod 9$$

2 is the modular multiplicative inverse of **5**, modulo **9**

$$20.\frac{1}{5} \equiv (20 * 2) \equiv 4 \pmod 9$$

Modular Multiplicative Inverse

Let's Solve a problem !

$$\left(\frac{20}{5}\right) \pmod{9}$$

2 is the modular multiplicative inverse of **5**, modulo **9**

$$20.\frac{1}{5} \equiv (20 * 2) \equiv 4 \pmod{9}$$

- $ab \equiv 1 \pmod{p}$ and $\mathbf{gcd(a,p)} = 1$

Modular Multiplicative Inverse

Let's Solve a problem !

$$(\frac{20}{5}) \pmod 9$$

2 is the modular multiplicative inverse of **5**, modulo **9**

$$20.\frac{1}{5} \equiv (20 * 2) \equiv 4 \pmod 9$$

- $ab \equiv 1 \pmod p$ and $\mathbf{gcd(a,p)} = 1$
- **b** is called the modular multiplicative inverse of **a** modulo **p**

Modular Multiplicative Inverse

- A modular multiplicative inverse of a positive integer **a** modulo **p** is always unique

Modular Multiplicative Inverse

- A modular multiplicative inverse of a positive integer **a** modulo **p** is always unique
- Otherwise **a** and **b** must not be relatively-prime

Modular Multiplicative Inverse

- A modular multiplicative inverse of a positive integer **a** modulo **p** is always unique
- Otherwise **a** and **b** must not be relatively-prime

Proof :

- suppose $\exists \mathbf{c} \in Z^{+}, \mathbf{c}$ is a solution

Modular Multiplicative Inverse

- A modular multiplicative inverse of a positive integer **a** modulo **p** is always unique
- Otherwise **a** and **b** must not be relatively-prime

Proof :

- suppose $\exists \mathbf{c} \in Z^+, \mathbf{c}$ is a solution
- $ab \equiv ac \equiv 1 \pmod{p}$

Modular Multiplicative Inverse

- A modular multiplicative inverse of a positive integer **a** modulo **p** is always unique
- Otherwise **a** and **b** must not be relatively-prime

Proof :

- suppose $\exists \mathbf{c} \in Z^+, \mathbf{c}$ is a solution
- $ab \equiv ac \equiv 1 \pmod{p}$
- $a(b - c) \equiv 0 \pmod{p}$

Modular Multiplicative Inverse

Proof Continues :

- Either $a \equiv 0 \pmod{p}$

Modular Multiplicative Inverse

Proof Continues :

- Either $a \equiv 0 \pmod{p}$
- or $(b - c) \equiv 0 \pmod{p}$

Modular Multiplicative Inverse

Proof Continues :

- Either $a \equiv 0 \pmod{p}$
- or $(b - c) \equiv 0 \pmod{p}$
- $a \equiv 0 \pmod{p}$

Modular Multiplicative Inverse

Proof Continues :

- Either $a \equiv 0 \pmod{p}$
- or $(b - c) \equiv 0 \pmod{p}$
- $a \equiv 0 \pmod{p}$
- Therefore $gcd(a, p) \neq 1$ which is a contradiction

Modular Multiplicative Inverse

Proof Continues :

- Either $a \equiv 0 \pmod{p}$
- or $(b - c) \equiv 0 \pmod{p}$
- $a \equiv 0 \pmod{p}$
- Therefore $gcd(a, p) \neq 1$ which is a contradiction
- So, $(b - c) \equiv 0 \pmod{p}$

Modular Multiplicative Inverse

Proof Continues :

- Either $a \equiv 0 \pmod{p}$
- or $(b - c) \equiv 0 \pmod{p}$
- $a \equiv 0 \pmod{p}$
- Therefore $gcd(a, p) \neq 1$ which is a contradiction
- So, $(b - c) \equiv 0 \pmod{p}$
- $b = c \pmod{p}$

Exercise

Some interesting problem may become food for your brain!

- Josephus problems
- Extended GCD

Recommended books -

- Art and Craft of Problem Solving
- 102 Number Theory Problems

Q/A

Questions?

Thank you!