CRYPTOGRAPHY AND ENCRYPTION (CY 371)

Dr Eric Affum

Abstract Algebra and Number Theory

- Every secure transaction depends on modern cryptography
- Plaintext and Ciphertext
- Most encryption is based heavily on number theory and Abstract algebra

Concepts

- The Division Algorithm –Helps to generate quotient and remainder
- The Euclidian Algorithm – Finding the GCD
- Extended Euclidian algorithm- To find multiplicative inverse
- Modular Arithmetic –
- Groups, rings, Field and Finite Fields
- Polynomial Arithmetic for better security
- Prime Numbers- RSA, Elliptic curve , Diffie Helman Algorithm
- Fermat's and Euler's Theorem
- Testing for Primality.
- The Chinese Remainder Theorem.
- Discrete Logarithm

- NB: All these are for the cryptography for classical computers

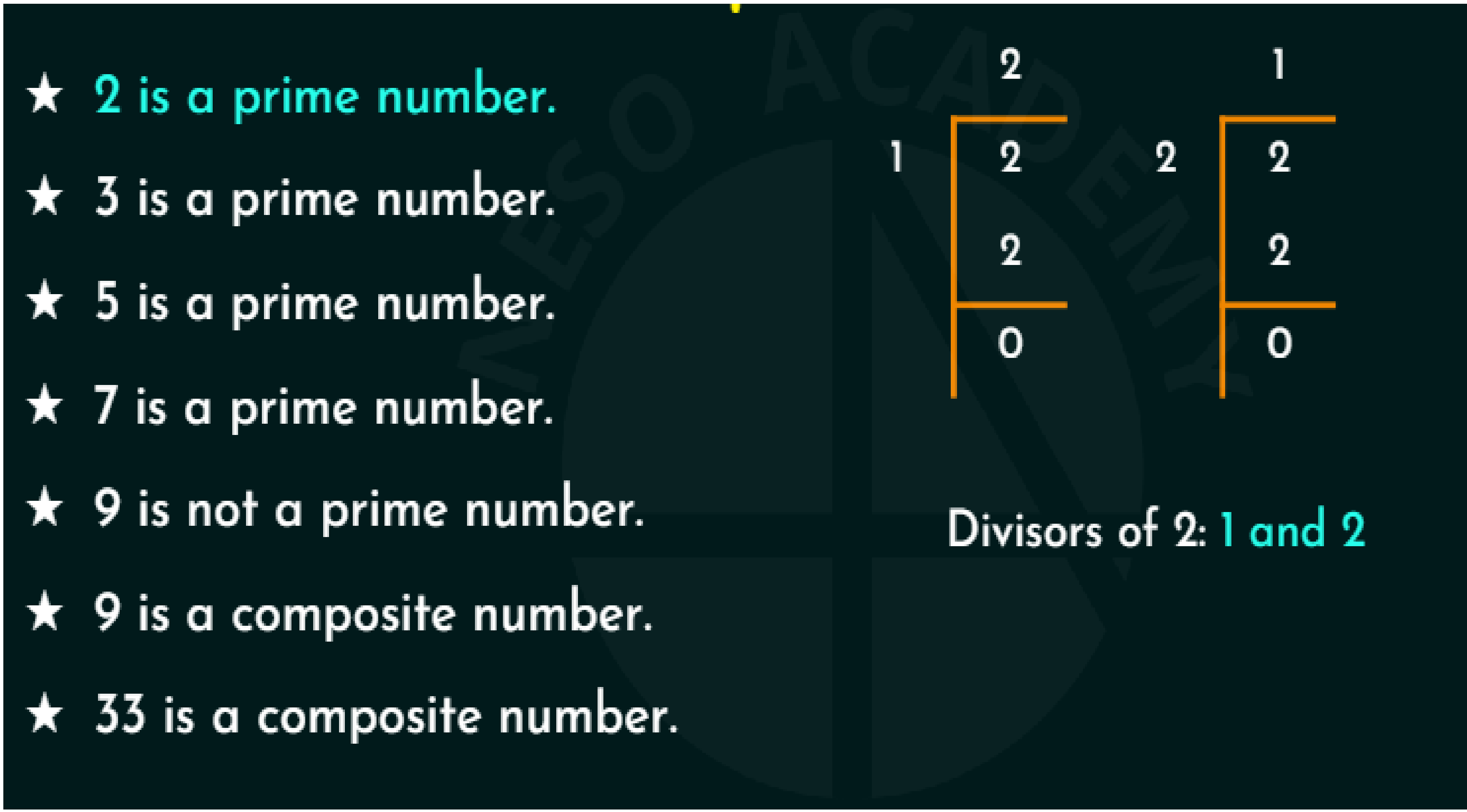
Prime Numbers

- Prime Numbers: Has exactly two divisors
- If N is a prime number, then the divisors are 1 and N.
- All numbers have prime factors.

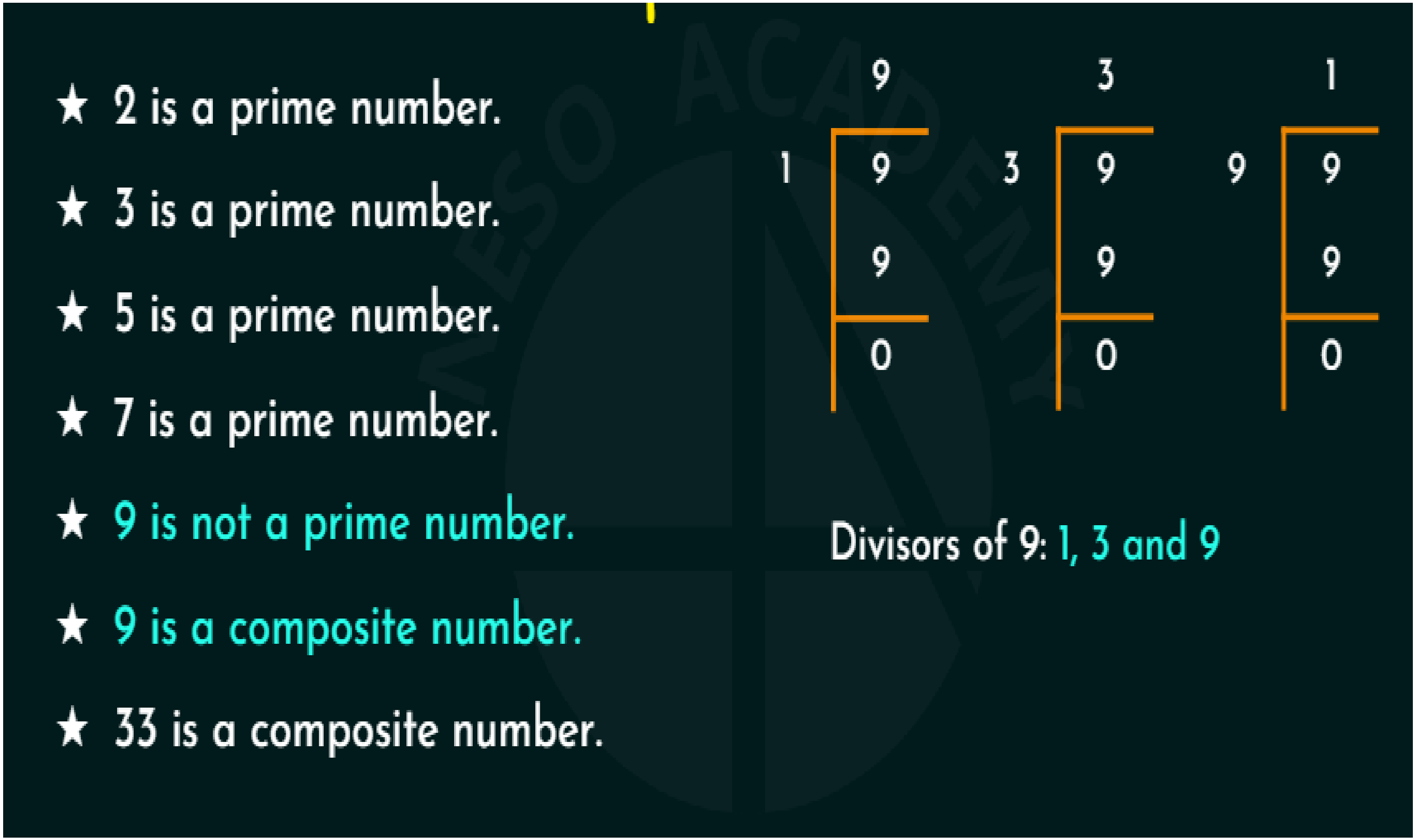
Numbers	10	11	100	37	308	14688
Prime Factorization	$2^1 \times 5^1$	$1^1 \times 11^1$	$2^2 \times 5^2$	$1^1 \times 37^1$	$2^2 \times 7^1 \times 11^1$	$2^5 \times 3^3 \times 17^1$
Prime Numbers	2, 5	1, 11	2, 5	1, 37	2, 7, 11	2, 3, 17

- A prime number is a number greater than 1 with only two factors- itself and one
- It cannot be divided further by any other numbers without leaving a remainder

Prime Numbers – Example



Prime Numbers – Example



Facts About Primes

- Only even prime : 2
- Smallest prime number: 2
- Is 1 a prime number? No

Why prime numbers in cryptography

- Many encryption algorithms are based on prime numbers

- Very fast to multiply two large prime numbers

- Extremely computer-intensive to do reverse.

- Factoring very large prime numbers is very hard. i.e. takes computers a long time.

Are they prime numbers?

- 5393
- 27644437
- 4398042316799
- 1125899839733759
- 18014398241046527
- 1298074214633706835075030044377087

Note: Cryptographic algorithms use large prime numbers.

Modular Arithmetic

- System of arithmetic for integers.
- Wrap around after reaching a certain value called modulus.

- Central mathematical concept in cryptography

Modular Arithmetic

- define **modulo operator** "`a mod n`" to be remainder when a is divided by n
  - where integer *n* is called the **modulus**
- *b* is called a **residue** of *a* mod *n*
  - since with integers can always write: `a = qn + b`
  - usually chose smallest positive remainder as residue
    - ie. `0 <= b <= n-1`
  - process is known as **modulo reduction**
    - `eg. -12 mod 7 = -5 mod 7 = 2 mod 7 = 9 mod 7`
- *a* & *b* are **congruent** if: `a mod n = b mod n`
  - when divided by *n,* a & b have same remainder
  - eg. 100 = 34 mod 11

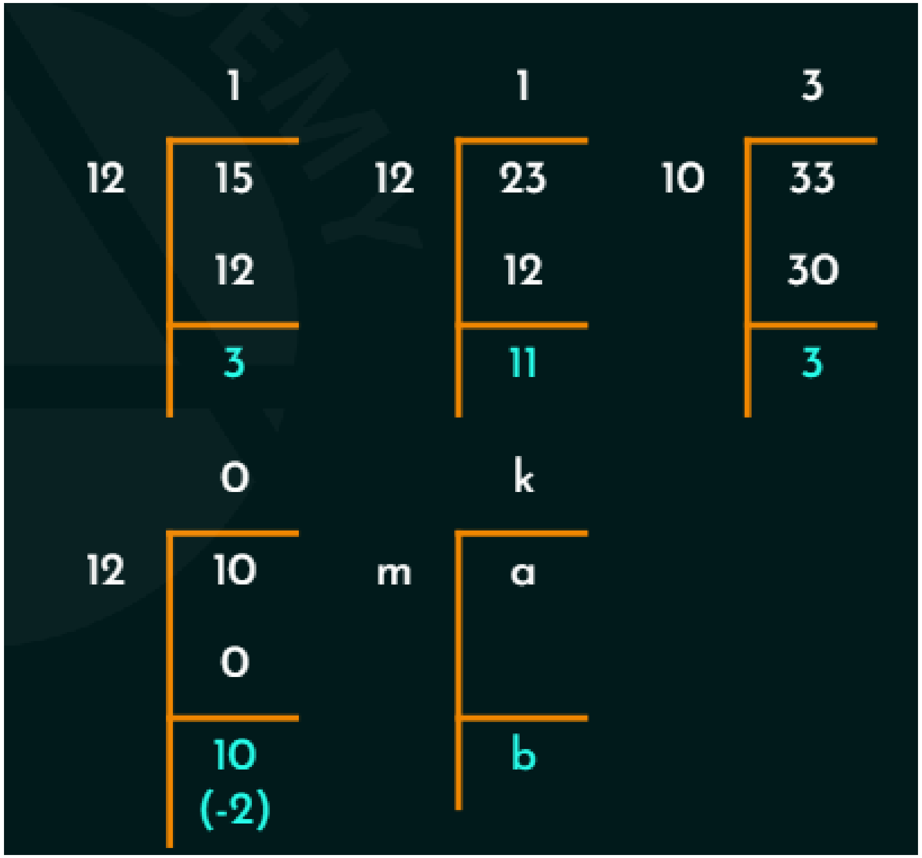
Modular Arithmetic Operations

- can perform arithmetic with residues
- uses a finite number of values, and loops back from either end

  $Z_n = \{0, 1, . . . , (n – 1)\}$
- modular arithmetic is when do addition & multiplication and modulo reduce answer
- can do reduction at any point, ie
  - `a+b mod n = [a mod n + b mod n] mod n`

Congruence

- In cryptography, congruence (≡) instead of equality (=).
- Example:
- $15 \equiv 3 \pmod{12}$
- $23 \equiv 11 \pmod{12}$
- $33 \equiv 3 \pmod{10}$
- $10 \equiv -2 \pmod{12}$
- $a \equiv b \pmod{m}$
- i.e. $a \equiv km + b$



- Why ≡ ?

Congruence

- Valid and Invalid Congruence

★ $38 \equiv 2 \pmod{12}$ ✓

★ $38 \equiv 14 \pmod{12}$ ✓

★ $5 \equiv 0 \pmod{5}$ ✓

★ $10 \equiv 2 \pmod{6}$ ✗

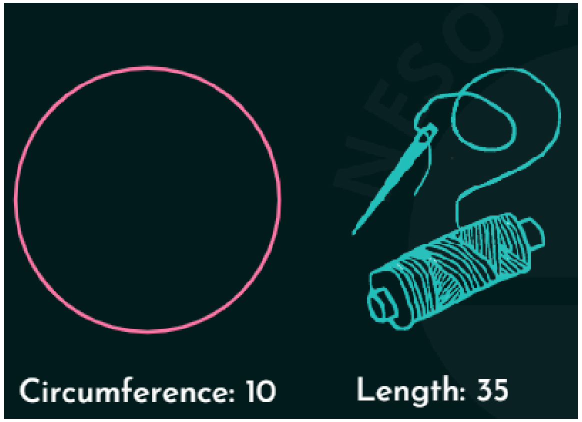
★ $13 \equiv 3 \pmod{13}$ ✗

★ $2 \equiv -3 \pmod{5}$ ✓

★ $-8 \equiv 7 \pmod{5}$

★ $-3 \equiv -8 \pmod{5}$

Congruence



No. of Wraps (Quotient)	Remaining thread (Remainder)	Congruence
1	25	$35 \equiv 25 \bmod 10$
2	15	$35 \equiv 15 \bmod 10$
3	5	$35 \equiv 5 \bmod 10$

Properties of Modular Arithmetic Operations

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

e.g.

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2 (11 + 15) mod 8
= 26 mod 8
= 2

[(11 mod 8) – (15 mod 8)] mod 8 = –4 mod 8 = 4 (11 – 15) mod 8
= –4 mod 8
= 4

[(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 = 5 (11 x 15) mod 8
= 165 mod 8
= 5

Modulo 8 Addition Example

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Modulo 8 Multiplication

+	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Modular Arithmetic Properties

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Modular Arithmetic Properties

Properties of Modular Arithmetic

Property	Expression
Commutative Laws	$(a + b) \bmod n = (b + a) \bmod n$ $(a \times b) \bmod n = (b \times a) \bmod n$
Associative Laws	$[(a + b) + c] \bmod n = [a + (b + c)] \bmod n$ $[(a \times b) \times c] \bmod n = [a \times (b \times c)] \bmod n$
Distributive Laws	$[a \times (b + c)] \bmod n = [(a \times b) + (a \times c)] \bmod n$
Identities	$(0 + a) \bmod n = a \bmod n$ $(1 \times a) \bmod n = a \bmod n$
Additive Inverse	For each $a \in Z_n$, there exists a '$-a$' such that $a + (-a) \equiv 0 \bmod n$

Modular Exponentiation

- It is a type of exponentiation performed over modulus
- **a^b mod m** or **a^b (mod m)**

- **Examples:**

- **2^{33} mod 30**

- **3^{100} mod 29**

Example

Solve $23^3 \bmod 30$.

$$
\begin{aligned}
23^3 \bmod 30 &= -7^3 \bmod 30 \;||\; 23 \bmod 30 \text{ can be } 23 \text{ or } -7.\\
&= -7^3 \bmod 30\\
&= -7^2 \times -7 \bmod 30\\
&= 49 \times -7 \bmod 30\\
&= -133 \bmod 30\\
&= -13 \bmod 30\\
&= 17 \bmod 30
\end{aligned}
$$

$23^3 \bmod 30 = 17$

Example 2

Solve 31^{500} mode 30

Example 2

Solve $31^{500} \bmod 30$.

$$
\begin{aligned}
31^{500} \bmod 30 &= 1^{500} \bmod 30 \\
&= 1 \bmod 30 \\
&= 1
\end{aligned}
$$

$$31^{500} \bmod 30 = 1$$

Example 3

Solve $242^{329} \bmod 243$.

$$
\begin{aligned}
242^{329} \bmod 243 &= -1^{329} \bmod 243 \\
&= -1^{329} \bmod 243 \;||\; -1^{328} \times -1^{1} \\
&= -1 \bmod 243 \\
&= 242
\end{aligned}
$$

$242^{329} \bmod 243 = 242$

Example 4

Solve $11^7 \bmod 13$.

$$
\begin{aligned}
11^7 \bmod 13 &= 11 \bmod 13 \times 11 \bmod 13 \times 11 \bmod 13 \times 11 \bmod 13 \times 11 \bmod 13 \times 11 \bmod 13 \times 11 \bmod 13 \\
&= -2 \times -2 \times -2 \times -2 \times -2 \times -2 \times -2 \bmod 13 \\
&= -128 \bmod 13 \\
&= -11 \bmod 13 \\
&= 2
\end{aligned}
$$

$11^7 \bmod 13 = 2$

(or)

$11^7 \bmod 13 = (-2)^7 \bmod 13$

Example 5

Solve $88^7 \bmod 187$.

$88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 88^1 \times 88^1 \bmod 187 = 88 \times 88 = 7744 \bmod 187 = 77$

$88^4 \bmod 187 = 88^2 \times 88^2 \bmod 187 = 77 \times 77 = 5929 \bmod 187 = 132$

$88^7 \bmod 187 = 88^4 \times 88^2 \times 88^1 \bmod 187 = (132 \times 77 \times 88) \bmod 187$

$= 894{,}432 \bmod 187$

$88^7 \bmod 187 = 11$

Example 5

What is "the last two digits" of 29^5?

$$
\begin{aligned}
29^1 \bmod 100 &= 29 \text{ or } -71 \\
29^2 \bmod 100 &= 29^1 \times 29^1 \bmod 100 = 29 \times 29 = 841 \bmod 100 = 41 \text{ or } -59 \\
29^4 \bmod 100 &= 29^2 \times 29^2 \bmod 100 = 41 \times 41 = 1681 \bmod 100 = 81 \text{ or } -19 \\
29^5 \bmod 100 &= 29^4 \times 29^1 \bmod 100 \\
&= -19 \times 29 \bmod 100 \\
&= -551 \bmod 100 \\
&= -51 \bmod 100 \\
&= 49
\end{aligned}
$$

$$29^5 \bmod 100 = 49$$

Example 6

Solve $3^{100} \bmod 29$.

$3^1 \bmod 29 = 3 \bmod 29 = 3$ or -26.

$3^2 \bmod 29 = 3^1 \times 3^1 \bmod 29 = 3 \times 3 \bmod 29 = 9 \bmod 29 = 9$ or -20.

$3^4 \bmod 29 = 3^2 \times 3^2 \bmod 29 = 9 \times 9 \bmod 29 = 81 \bmod 29 = 23$ or -6.

$3^8 \bmod 29 = 3^4 \times 3^4 \bmod 29 = -6 \times -6 \bmod 29 = 36 \bmod 29 = 7$ or -22.

$3^{16} \bmod 29 = 3^8 \times 3^8 \bmod 29 = 7 \times 7 \bmod 29 = 49 \bmod 29 = 20$ or -9.

$3^{32} \bmod 29 = 3^{16} \times 3^{16} \bmod 29 = -9 \times -9 \bmod 29 = 81 \bmod 29 = 23$ or -6.

$3^{64} \bmod 29 = 3^{32} \times 3^{32} \bmod 29 = -6 \times -6 \bmod 29 = 36 \bmod 29 = 7$ or -22.

$$
\begin{aligned}
3^{100} \bmod 29 &= 3^{64} \times 3^{32} \times 3^{4} \bmod 29. \\
&= 7 \times -6 \times -6 \bmod 29 \\
&= 252 \bmod 29
\end{aligned}
$$

$3^{100} \bmod 29 = 20$

Greatest Common Divisor (GCD)

- A common problem in number theory
- GCD (a,b) of a and b is the largest integer that divides evenly into both a and b
  - eg GCD(60,24) = 12
- Define gcd(0, 0) = 0
- Often want **no common factors** (except 1) define such numbers as **relatively prime**
  - eg GCD(8,15) = 1
  - hence 8 & 15 are relatively prime

GCD

	12	33
Divisors	1, 2, 3, 4, 6, 12	1, 3, 11, 33
Common Divisors	1, 3	
Greatest Common Divisor (GCD)	3	

$\therefore$ GCD(12, 33) = 3

GCD

	25	150
Divisors	1, 5, 25	1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150
Common Divisors	1, 5, 25	
Greatest Common Divisor (GCD)	25	

$\therefore$ GCD(25, 150) = 25

GCD

	13	31
Divisors	1, 13	1, 31
Common Divisors	1	
Greatest Common Divisor (GCD)	1	

$\therefore GCD(13, 31) = 1$

GCD- Euclidean Algorithm

Find the GCD(12, 33).

Q	A	B	R
	33	12	

$$\begin{array}{r|l} & 2 \\ \hline 12 & 33 \\ & 24 \\ \hline & 9 \end{array}$$

GCD- Euclidean Algorithm

Find the GCD(12, 33).

Q	A	B	R
2	33	12	9

$$\begin{array}{r|l} & 2 \\ 12 & 33 \\ & 24 \\ \hline & 9 \end{array}$$

GCD- Euclidean Algorithm

Find the GCD(12, 33).

Q	A	B	R
2	33	12	9
	12	9	

GCD- Euclidean Algorithm

Find the GCD(12, 33).

Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0
X	3	0	X

GCD- Euclidean Algorithm

Find the GCD(12, 33).

Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0
X	$\boxed{3}$	0	X

GCD- Euclidean Algorithm

GCD(750, 900) = 150.

Q	A	B	R
1	900	750	150
5	750	150	0
X	150	0	X

GCD- Euclidean Algorithm

GCD(252, 105) = 21.

Q	A	B	R
2	252	105	42
2	105	42	21
2	42	21	0
X	$\boxed{21}$	0	X

0 | 21

Euclid’s Algorithm for finding GCD

- Prerequisite: a>b
- Euclid_GCD (a, b)
- If b = 0 then
- Return a;
- Else
- Return Euclid’s_GCD (b, a mod b)

Euclid’s Algorithm

Example 1: Find the GCD (50, 12).

Solution:

Here a=50, b=12

GCD (a, b) = GCD (b, a mod b)

GCD (50, 12) = GCD (12, 50 mod 12) = GCD(12, 2)

GCD (12, 2) = GCD (2, 12 mod 2) = GCD(2, 0) = 2

GCD (50, 12) = 2

Euclid’s Algorithm

Example 2: Find the GCD (83, 19).

Solution:

Here a=83, b=19

GCD (a, b) = GCD (b, a mod b)

GCD (83, 19) = GCD (19, 83 mod 19) = GCD(19, 7)

GCD (19, 7) = GCD (7, 19 mod 7) = GCD(7, 5)

GCD (7, 5) = GCD (5, 7 mod 5) = GCD(5, 2)

GCD (5, 2) = GCD (2, 5 mod 2) = GCD(2, 1)

GCD (2, 1) = GCD (1, 2 mod 1) = GCD(1, 0) = 1

GCD (83, 19) = 1

Relatively prime numbers

- A number is said to be relatively prime if they have no prime factor in common, and their only prime factor is 1

- If **GCD(a, b)=1**, then **a** and **b** are relatively prime numbers

- Co-prime

Relatively prime numbers

Question 1: Are 4 and 13 relatively prime?

Solution:

	4	13
Divisors	1, 2, 4	1, 13
Common Divisors	1	
Greatest Common Divisor (GCD)	1	

GCD(4, 13) = 1

Yes, 4 and 13 are relatively prime numbers.

Relatively prime numbers

Question 2: Are 15 and 21 relatively prime?

Solution:

	15	21
Divisors	1, 3, 5, 15	1, 3, 7, 21
Common Divisors	1, 3	
Greatest Common Divisor (GCD)	3	

GCD(15, 21) = 3

No, 15 and 21 are not relatively prime numbers.

Relatively prime numbers

a	b	GCD(a, b)	Relatively Prime?	Remarks
11	17	1	Yes	'a' and 'b' are prime
11	21	1	Yes	'a' is prime and 'b' is composite
12	77	1	Yes	'a' and 'b' are composite

Euler’s Totient Function

Denoted as $\Phi(n)$.

$\Phi(n)$ = Number of positive integers less than ‘n’ that are relatively prime to n.

Euler’s Totient Function
Relatively prime numbers

- Manual Approach when the number is small

Example 3: Find $\Phi(8)$.

Solution:

Here n=8.

Numbers less than 8 are 1, 2, 3, 4, 5, 6, and 7.

GCD	Relatively Prime?
GCD (1, 8) = 1	✓
GCD (2, 8) = 2	✗
GCD (3, 8) = 1	✓
GCD (4, 8) = 4	✗

GCD	Relatively Prime?
GCD (5, 8) = 1	✓
GCD (6, 8) = 2	✗
GCD (7, 8) = 1	✓

$\therefore \Phi(8) = 4.$

Euler’s Totient Function

	Criteria of ‘n’	Formula
$\Phi(n)$	‘n’ is prime.	$\Phi(n) = (n-1)$
	$n = p \times q$. ‘p’ and ‘q’ are primes.	$\Phi(n) = (p-1) \times (q-1)$
	$n = a \times b$. Either ‘a’ or ‘b’ is composite. Both ‘a’ and ‘b’ are composite.	$\Phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots$ where $p_1, p_2, \ldots$ are distinct primes.

Euler’s Totient Function

Example 1: Find $\Phi(5)$.

Solution:

Here n=5.

‘n’ is a prime number.

$\Phi(n) \quad = (n-1)$

$\Phi(5) \quad = (5-1)$

$\Phi(5) \quad = 4$

So, there are 4 numbers that are lesser than 5 and relatively prime to 5.

Euler’s Totient Function

Example 3: Find $\Phi(35)$.

Solution:

Here n=35.

‘n’ is a product of two prime numbers 5 and 7.

Let us assign p=5 and q=7.

$\Phi(n) = (p-1) \times (q-1)$

$\Phi(35) = (5-1) \times (7-1)$

$\Phi(35) = 4 \times 6$

$\Phi(35) = 24$

So, there are 24 numbers that are lesser than 35 and relatively prime to 35.

Euler’s Totient Function

Example 4: Find $\Phi(1000)$.

Solution:

Here $n = 1000 = 2^3 \times 5^3$.

Distinct prime factors are 2 and 5.

$$\Phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots .$$

$$\Phi(1000) = 1000 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$

$$\Phi(1000) = 1000 \times \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)$$

$$\Phi(1000) = 400$$

Euler’s Totient Function

Example 5: Find $\Phi(7000)$.

Solution:

Here $n = 7000 = 2^3 \times 5^3 \times 7^1$

Distinct prime factors are 2, 5 and 7.

$$\Phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\ldots$$

$$\Phi(7000) = 7000 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$$

$$\Phi(7000) = 7000 \times \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)$$

$$\Phi(7000) = 2400$$

Fermat’s Little Theorem

- If ‘p’ is a prime number and ‘a’ is a positive integer not divisible by ‘p’ then $a^{p-1} \equiv 1 \ (mod\ p)$

Fermat’s Little Theorem

Example 1: Does Fermat's theorem hold true for p=5 and a=2?

Solution:

Given: p=5 and a=2.

$a^{p-1} \equiv 1 \pmod{p}$

$2^{5-1} \equiv 1 \pmod{5}$

$2^{4} \equiv 1 \pmod{5}$

$16 \equiv 1 \pmod{5}$

Therefore, Fermat's theorem holds true for p=5 and a=2.

Fermat’s Little Theorem

Example 2: Prove Fermat's theorem holds true for p=13 and a=11.

Solution:

$a^{p-1} \equiv 1 \pmod{p}$

$11^{13-1} \equiv 1 \pmod{13}$

$11^{12} \equiv 1 \pmod{13}$

$-2^{12} \equiv 1 \pmod{13}$

$-2^{4x3} \equiv 1 \pmod{13}$

$3^3 \equiv 1 \pmod{13}$

$27 \equiv 1 \pmod{13}$

Therefore, Fermat's theorem holds true for p=13 and a=11.

Fermat’s Little Theorem

Example 3: Prove Fermat’s theorem does not hold for p=6 and a=2.

Solution:

$a^{p-1} \equiv 1 \pmod{p}$

$2^{6-1} \equiv 1 \pmod{6}$

$2^{5} \equiv 1 \pmod{6}$

$32 \equiv 1 \pmod{6}$

$32 \equiv 1 \pmod{6}$

Therefore, Fermat’s theorem does not hold true for p=6 and a=2.

Euler’s Theorem

- For every positive integer ‘a’ and ‘n’, which are said to be relatively prime, then

$$a^{1} \equiv 1 \ (mod\ n)$$

Euler’s Theorem

Example 1: Prove Euler’s theorem hold true for a=3 and n=10.

Solution:

Given: a=3 and n=10.

$a^{\Phi(n)} \equiv 1 \pmod{n}$

$3^{\Phi(10)} \equiv 1 \pmod{10}$

$\Phi(10) = 4$

$3^4 \equiv 1 \pmod{10}$

$81 \equiv 1 \pmod{10}$

Therefore, Euler’s theorem holds true for a=3 and n=10.

Euler’s Theorem

Example 2: Does Euler’s theorem hold true for a=2 and n=10?

Solution:

Given: a=2 and n=10.

$a^{\Phi(n)} \equiv 1 \pmod{n}$

$2^{\Phi(10)} \equiv 1 \pmod{10}$

$\Phi(10) = 4$

$2^4 \equiv 1 \pmod{10}$

$16 \equiv 1 \pmod{10}$

Therefore, Euler’s theorem does not hold for a=2 and n=10.

Euler's Theorem

Example 3: Does Euler's theorem hold true for a=10 and n=11?

Solution:

Given: a=10 and n=11.

$a^{\Phi(n)} \equiv 1 \pmod{n}$

$10^{\Phi(11)} \equiv 1 \pmod{11}$

$\Phi(11) = 10$

$10^{10} \equiv 1 \pmod{11}$

$-1^{10} \equiv 1 \pmod{11}$

$1 \equiv 1 \pmod{11}$

Therefore, Euler's theorem holds for a=10 and n=11.

Primitive Root

- A number α is a primitive root modulo n if every number coprime to n is congruent to a power of α modulo n

- Def.
- ‘α’ is said to be a primitive root of prime number ‘p’, if

$\alpha^1 \, mod \, p, \alpha^2 \, mod \, p, \ldots\ldots\ldots \alpha^{p-1} \, mod \, p$ are distinct.

NB: this concept is important for Diffie helman key exchange algorithm.

Primitive Root

Example 1: Is 2 a primitive root of prime number 5?

Solution:

2^1 mod 5	2 mod 5	2	✓
2^2 mod 5	4 mod 5	4	✓
2^3 mod 5	8 mod 5	3	✓
2^4 mod 5	16 mod 5	1	✓

Yes, 2 is a primitive root of prime number 5.

Primitive Root

Example 3: Is 2 a primitive root of prime number 7?

Solution:

2^1 mod 7	2 mod 7	2	✓
2^2 mod 7	4 mod 7	4	✓
2^3 mod 7	8 mod 7	1	✓
2^4 mod 7	16 mod 7	2	✗
2^5 mod 7	4 mod 7	4	✗
2^6 mod 7	8 mod 7	1	✗

No, 2 is not a primitive root of 7.

Multiplicative Inverse

- Let’s understand multiplicative inverse
- $5 \times 5^{-1} = 1$
- $5 \times \frac{1}{5} = 1$
- $\mathrm{A} \times \frac{1}{A} = 1$
- $\mathrm{A} \times A^{-1} = 1$

Multiplicative Inverse

- Real change comes when modulus arithmetic is involved

- Under mod n

- $\mathrm{A} \times A^{-1} \equiv 1 \; mod \; n$

- 3 x ? ≡ 1 mod 5

- 2 is the multiplicative inverse of 1 mod 5

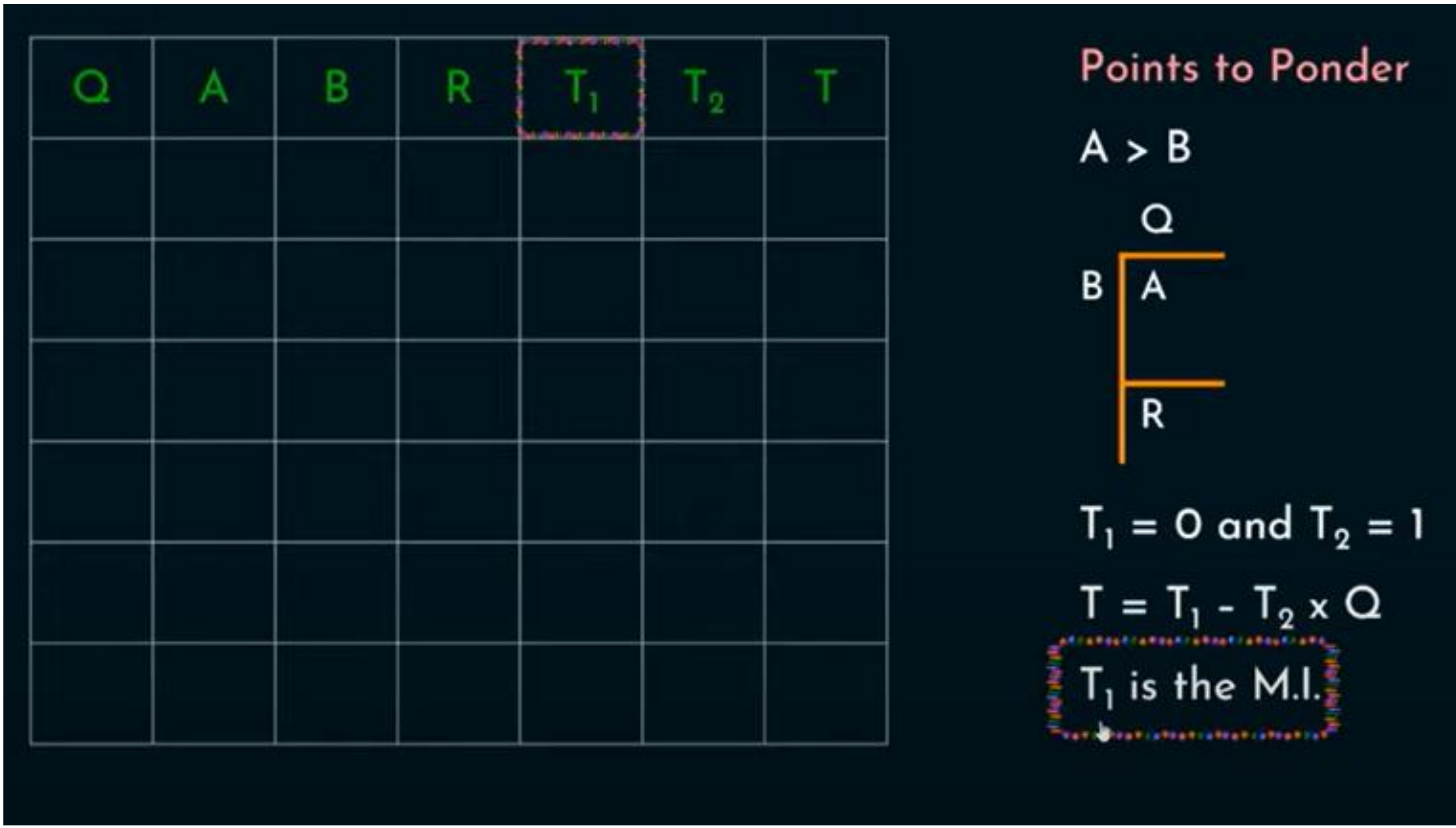
- 3 x 2 ≡ 1 mod 5

2 x ? ≡ 1 mod 11

5 x ? ≡ 1 mod 10

- NB: numbers which are not reactively prime have no multiplicative invers

Multiplicative Inverse Using Extended Euclidian Algorithm



Multiplicative Inverse Using Extended Euclidian Algorithm

- Example: What is the multiplicative index of 11 mod 13

Q	A	B	R	T_1	T_2	T
	13	11				

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2			

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	

$T_1 = 0$ and $T_2 = 1$

$T = T_1 - T_2 \times Q$

$T = 0 - 1 \times 1$

$T = 0 - 1$

$T = -1$

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
	11	2		1	-1	

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	

$$T = T_1 - T_2 \times Q$$

$$T = 1 - (-1) \times 5$$

$$T = 1 - (-5)$$

$$T = 1 + 5$$

$$T = 6$$

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	6

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	6
2	2	1	0	-1	6	-13
	1	0		6	-13	

Multiplicative Inverse Using Extended Euclidian Algorithm

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	6
2	2	1	0	-1	6	-13
X	1	0	X	6	-13	X

- Therefore 6 is the M.I of 11 mod 13

Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below:

$X \equiv a_1 \pmod{m_1}$

$X \equiv a_2 \pmod{m_2}$

. . .

$X \equiv a_n \pmod{m_n}$

CRT states that the above equations have a unique solution of the moduli are relatively prime.

$$\boxed{X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \ldots + a_n M_n M_n^{-1}) \bmod M}$$

Multiplicative Inverse Using Extended Euclidian Algorithm

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod{3}$

$X \equiv 3 \pmod{5}$

$X \equiv 2 \pmod{7}$

Solution:

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$X \equiv a_1 \pmod{m_1}$	$X \equiv 2 \pmod{3}$
$X \equiv a_2 \pmod{m_2}$	$X \equiv 3 \pmod{5}$
$X \equiv a_3 \pmod{m_3}$	$X \equiv 2 \pmod{7}$

Solution:

$$X = (a_1M_1 M_1^{-1} + a_2M_2M_2^{-1} + a_3M_3M_3^{-1}) \bmod M$$

Given		To Find		
$a_1 = 2$	$m_1 = 3$	M_1	M_1^{-1}	M
$a_2 = 3$	$m_2 = 5$	M_2	M_2^{-1}	
$a_3 = 2$	$m_3 = 7$	M_3	M_3^{-1}	

Given		To Find		
$a_1 = 2$	$m_1 = 3$	M_1	M_1^{-1}	
$a_2 = 3$	$m_2 = 5$	M_2	M_2^{-1}	$M=105$
$a_3 = 2$	$m_3 = 7$	M_3	M_3^{-1}	

Solution:

$M = m_1 \times m_2 \times m_3$

$M = 3 \times 5 \times 7$

$M = 105$

Given		To Find		
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	M_1^{-1}	$M=105$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	M_2^{-1}	
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	M_3^{-1}	

$$M_1 = \frac{M}{m_1}$$

$$M_1 = \frac{105}{3}$$

$$M_1 = 35$$

$$M_2 = \frac{M}{m_2}$$

$$M_2 = \frac{105}{5}$$

$$M_2 = 21$$

$$M_3 = \frac{M}{m_3}$$

$$M_3 = \frac{105}{7}$$

$$M_3 = 15$$

Given		To Find		
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	M_1^{-1}	
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	M_2^{-1}	$M=105$
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	M_3^{-1}	

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$35 \times M_1^{-1} = 1 \bmod 3$

$35 \times 2 = 1 \bmod 3$

$M_1^{-1} = 2$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$21 \times M_2^{-1} = 1 \bmod 5$

$21 \times 1 = 1 \bmod 5$

$M_2^{-1} = 1$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$15 \times M_3^{-1} = 1 \bmod 7$

$15 \times 1 = 1 \bmod 7$

$M_3^{-1} = 1$

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	$M=105$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

Solution:

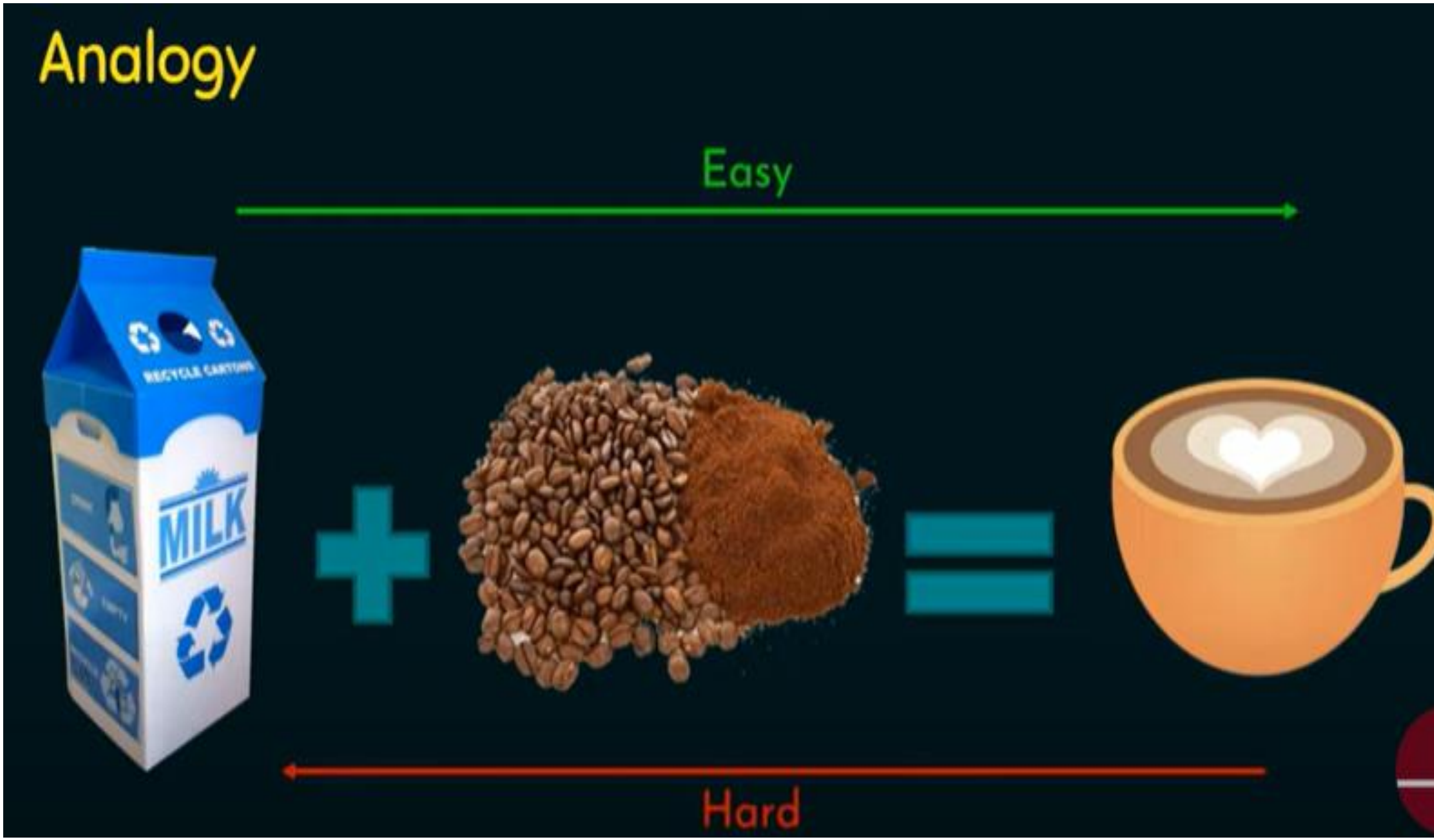
$X = (a_1M_1 M_1^{-1} + a_2M_2M_2^{-1} + a_3M_3M_3^{-1}) \bmod M$

$= (2x35x2 + 3x21x1 + 2x15x1) \bmod 105$

$= 233 \bmod 105$

$X = 23$

Discrete Logarithm Problem

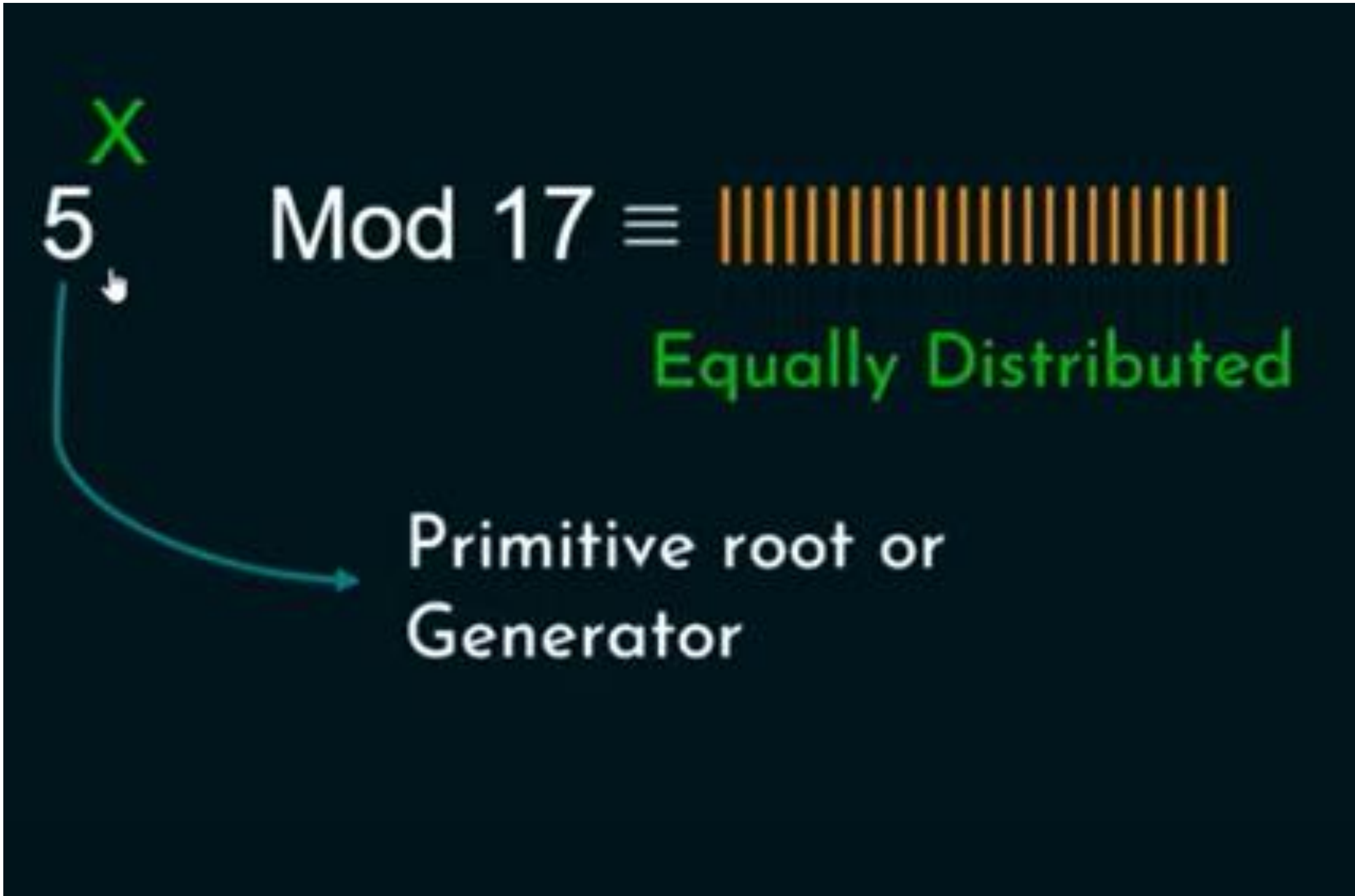


Discrete Logarithm Problem

Understanding the DLP

$5^{1} \bmod 17$	$5^{9} \bmod 17$
$5^{2} \bmod 17$	$5^{10} \bmod 17$
$\boxed{5^{3} \bmod 17}$	$5^{11} \bmod 17$
$5^{4} \bmod 17$	$5^{12} \bmod 17$
$5^{5} \bmod 17$	$5^{13} \bmod 17$
$5^{6} \bmod 17$	$5^{14} \bmod 17$
$5^{7} \bmod 17$	$5^{15} \bmod 17$
$5^{8} \bmod 17$	$5^{16} \bmod 17$

Discrete Logarithm Problem



Discrete Logarithm Problem

- 5 power 9, 25, 41, 57, 71 …..=12
- One direction is easy, and one direction is difficult.
- i.e. Important property of one way function.

Discrete Logarithm Problem

- g^x **mod p**
- 2^x **mod 7 = 4; X=2, 5, etc.,**
- For smaller value of '**p**' is may be easy to find **X**
- If '**p**' is very large, then the finding '**X**' is hard
- If '**p**' is large, then the time and the effort to find '**X**' is very hard.
- The strength of one-way function is depending on how much time it takes to break it .

Discrete Logarithm Problem

Example 1: Solve $\log_2 9 \bmod 11$.

Solution:

Here p=11, g=2, X=9

$\log_g X \equiv n \pmod{p}$

$X \equiv g^n \pmod{p}$

$9 \equiv 2^n \pmod{11}$

Try 'n' = 1, 2, 3, ...

$9 \equiv 2^6 \pmod{11}$

Answer is 6.

Factoring- Fermant's Algorithm

- Used to find prime factors of a number

- To factor '10'
- n= X . Y

- Works well when X and Y are close

- n= $\boldsymbol{X^2 - Y^2}$

- $\boldsymbol{X^3 = n + Y^2}$
- $X = \sqrt{n + \boldsymbol{Y^2}}$
- Try different value of Y from 1 up

Factoring- Fermant’s Algorithm

Question 1: Factor n = 187.

Solution:

$X = \sqrt{n + Y^2}$

$X = \sqrt{187 + Y^2}$

$X = \sqrt{187 + 1^2} = \sqrt{188} \neq$ Integer

$X = \sqrt{187 + 2^2} = \sqrt{191} \neq$ Integer

$X = \sqrt{187 + 3^2} = \sqrt{196} = 14$

$X = 14$ and $Y = 3$

Recall:

$n = X^2 - Y^2$

$n = (X+Y)\,(X-Y)$

$n = (14+3)\,(14-3)$

$n = (17)\,(11)$

$187 = 17 \times 11$

The prime factors of 187 are 17 and 11.

Fermat’s Primality Test

- To test if a given number is prime number or not.

Is ‘p’ prime?

Test:

$a^p - a \longrightarrow$ ‘p’ is prime if this is a multiple of ‘p’ for all $1 \leq a < p$.

- Drawback-Time consuming

Fermat’s Primality Test

Question 1: Is 5 prime?

Solution:

$a^p - a \longrightarrow$ ‘p’ is prime if this is a multiple of ‘p’ for all $1 \le a < p$.

$1^5 - 1 \quad = 1 - 1 \quad = 0$

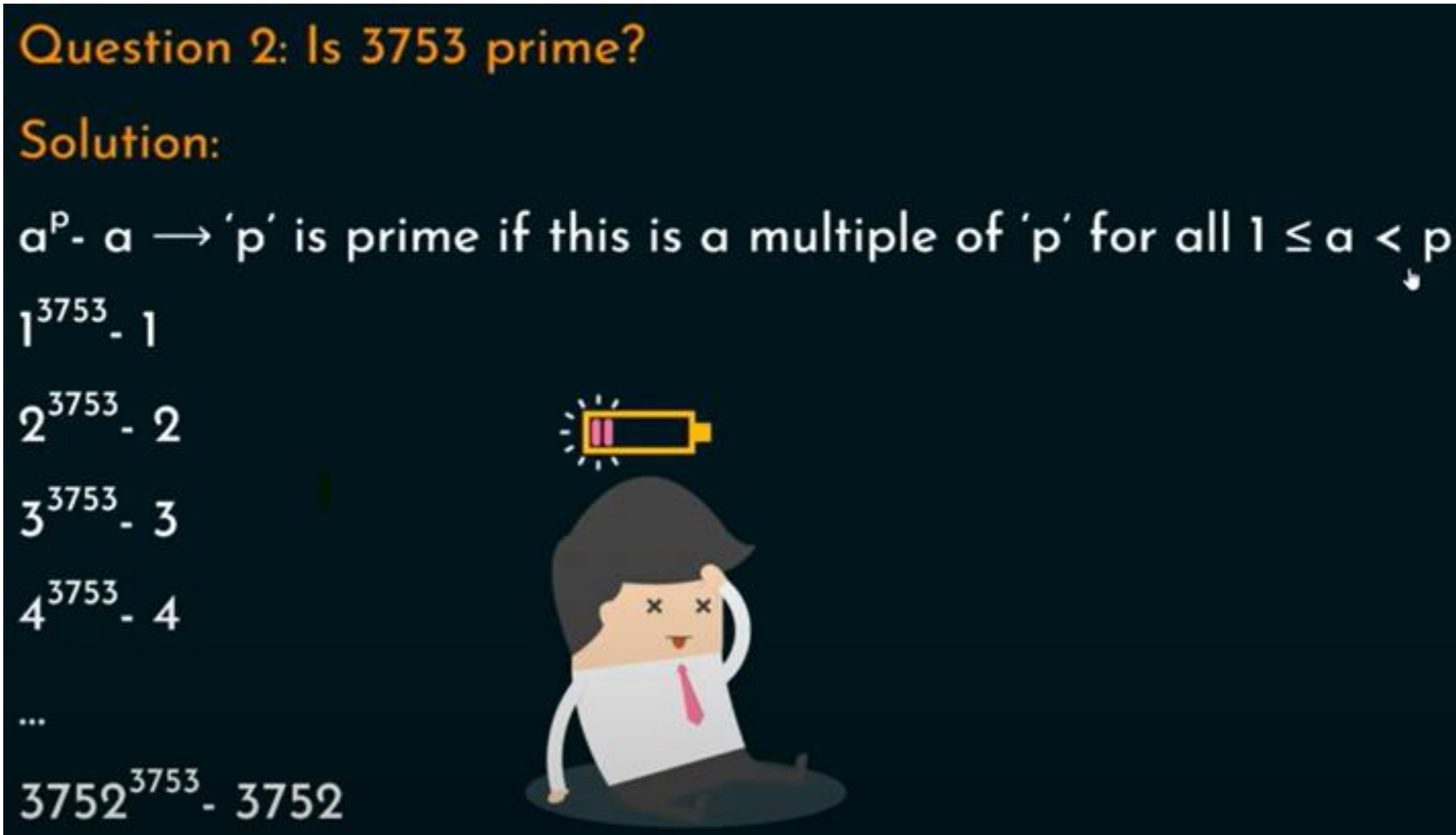
$2^5 - 2 \quad = 32 - 2 \quad = 30$

$3^5 - 3 \quad = 243 - 3 \quad = 240$

$4^5 - 4 \quad = 1024 - 4 \quad = 1020$

$\therefore$ 5 is prime

Fermat’s Primality Test



Group

- A group G denote by {G, .}, is a set under some operation (.) of elements or “numbers”if the following properties
  - Closure
  - associative law: $(a.b).c = a.(b.c)$
  - has identity e: $e.a = a.e = a$
  - has inverses a^{-1}: $a.a^{-1} = e$

  It may be finite or infinite

- if commutative $a.b = b.a$
  - then forms an **abelian group**

Groups and Abelian Groups

<table>
<tr><th colspan="3">Property</th><th>Explanation</th></tr>
<tr><td rowspan="5">Abelian Group</td><td rowspan="4">Group</td><td>Closure</td><td>$a, b \in G$, then $(a \bullet b) \in G$.</td></tr>
<tr><td>Associative</td><td>$a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c \in G$.</td></tr>
<tr><td>Identity element</td><td>$(a \bullet e) = (e \bullet a) = a$ for all $a, e \in G$.</td></tr>
<tr><td>Inverse element</td><td>$(a \bullet a') = (a' \bullet a) = e$ for all $a, a' \in G$.</td></tr>
<tr><td colspan="2">Commutative</td><td>$(a \bullet b) = (b \bullet a)$ for all $a, b \in G$.</td></tr>
</table>

Group

Question: Is (Z, +) a group?

Solution:

$Z = \{ ...., -3, -2, -1, 0, 1, 2, 3, ...\}$

CAIN Property	Explanation	Satisfied?
Closure	If $a, b \in G$, then $(a \bullet b) \in G$. If $a = 5, b = -2 \in Z$ then $(a + b) = -3 \in Z$	✓
Associative	$a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c \in G$. $5 + (3 + 7) = (5 + 3) + 7 \in Z$	✓
Identity element	$(a \bullet e) = (e \bullet a) = a$ for all $a \in G$. $(5 + 0) = (0 + 5) = 5$ for all $a \in G$.	✓
Inverse element	$(a \bullet a') = (a' \bullet a) = e$ for all $a, a' \in G$. $(5 + -5) = (-5 + 5) = 0$ for all $5, -5 \in Z$	✓
Commutative	$(a \bullet b) = (b \bullet a)$ for all $a, b \in G$.	

Group and **Abelian group**

Solution:

$Z = \{ ...., -3, -2, -1, 0, 1, 2, 3, ...\}$ is an abelian group.

CAIN Property	Explanation	Satisfied?
Closure	If $a, b \in G$, then $(a \bullet b) \in G$. If $a = 5, b = -2 \in Z$ then $(a + b) = -3 \in Z$	✓
Associative	$a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c \in G$. $5 + (3 + 7) = (5 + 3) + 7 \in Z$	✓
Identity element	$(a \bullet e) = (e \bullet a) = a$ for all $a \in G$. $(5 + 0) = (0 + 5) = 5$ for all $a \in G$.	✓
Inverse element	$(a \bullet a') = (a' \bullet a) = e$ for all $a, a' \in G$. $(5 + -5) = (-5 + 5) = 0$ for all $5, -5 \in Z$	✓
Commutative	$(a \bullet b) = (b \bullet a)$ for all $a, b \in G$. $(5 + 9) = (9 + 5)$ for all $9, 5 \in Z$.	✓

Notations

$N \longrightarrow$ Set of all natural numbers.

$W \longrightarrow$ Set of all whole numbers.

$Z \longrightarrow$ Set of all integers.

$C \longrightarrow$ Set of all complex numbers.

$Q \longrightarrow$ Set of all rational numbers.

$R \longrightarrow$ Set of all real numbers.

$Z^{+} \longrightarrow$ Set of all positive integers.

$Z^{-} \longrightarrow$ Set of all negative integers.

Cyclic Group

A group G denoted by {G, •}, is said to be a cyclic group, if it contains at-least one generator element.

Cyclic Group

Question 1: Prove that $(G, *)$ is a cyclic group, where $G = \{1, \omega, \omega^2\}$.

Solution:

Composition Table

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$1^1 = 1$
$1^2 = 1*1 = 1$
$1^3 = 1*1*1 = 1$
$1^4 = 1*1*1*1 = 1$

Cyclic Group

Question 1: Prove that $(G, *)$ is a cyclic group, where $G = \{1, \omega, \omega^2\}$.

Solution:

Composition Table

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$1^1 = 1$

$1^2 = 1*1 = 1$

$1^3 = 1*1*1 = 1$

$1^4 = 1*1*1*1 = 1$

$\omega^1 = \omega$

$\omega^2 = \omega*\omega = \omega^2$

$\omega^3 = \omega^2*\omega = 1$

$\omega^4 = \omega^3*\omega = \omega$

Cyclic Group

Question 1: Prove that (G, *) is a cyclic group, where $G = \{1, \omega, \omega^2\}$.

Solution:

Composition Table

*	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$1^1 = 1$
$1^2 = 1*1 = 1$
$1^3 = 1*1*1 = 1$
$1^4 = 1*1*1*1 = 1$

$\omega^1 = \omega$
$\omega^2 = \omega*\omega = \omega^2$
$\omega^3 = \omega^{2}*\omega = 1$
$\omega^4 = \omega^{3}*\omega = \omega$

$(\omega^2)^1 = \omega^2$
$(\omega^2)^2 = \omega^4 = \omega^{3}*\omega = \omega$
$(\omega^2)^3 = \omega^6 = \omega^{3}*\omega^3 = 1$
$(\omega^2)^4 = \omega^8 = \omega^{3}*\omega^{3}*\omega^2 = \omega^2$

Question 1: Prove that $(G, *)$ is a cyclic group, where $G = \{1, \omega, \omega^2\}$.

Solution:

Composition Table

*	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$1^1 = 1$
$1^2 = 1*1 = 1$
$1^3 = 1*1*1 = 1$
$1^4 = 1*1*1*1 = 1$

Not a Generator

$\omega^1 = \omega$
$\omega^2 = \omega*\omega = \omega^2$
$\omega^3 = \omega^2*\omega = 1$
$\omega^4 = \omega^3*\omega = \omega$

Generator

$(\omega^2)^1 = \omega^2$
$(\omega^2)^2 = \omega^4 = \omega^3*\omega = \omega$
$(\omega^2)^3 = \omega^6 = \omega^3*\omega^3 = 1$
$(\omega^2)^4 = \omega^8 = \omega^3*\omega^3*\omega^2 = \omega^2$

Generator

The generators of $(G, *)$ are ω and ω^2.

$\therefore (G, *)$ is a cyclic group.

Cyclic Group

Question 2: When does group G with operation 'x', is said to be a cyclic group?

Solution:

Let us take an element x

$G = \{ \quad x^{-1}, 1, x, \quad \}$

Cyclic Group

Question 2: When does group G with operation 'x', is said to be a cyclic group?

Solution:

Let us take an element x

$G = \{ \ldots, x^{-4}, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, x^4, \ldots \}$

$\quad$ = Group generated by x

If $G = \langle x \rangle$ for some x, then we call G a cyclic group.

Cyclic Group

Question 1: Prove that $(G, *)$ is a cyclic group, where $G = \{1, \omega, \omega^2\}$.

Solution:

Composition Table

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Cyclic Group

Question 3: When does group G with operation '+', is said to be a cyclic group?

Solution:

Let us take an element y

$G = \{ \quad -y, 0, y, \quad \}$

Cyclic Group

Question 3: When does group G with operation '+', is said to be a cyclic group?

Solution:

Let us take an element y

$G = \{\ldots\ldots, -4y, -3y, -2y, -y, 0, y, 2y, 3y, 4y, \ldots\ldots\}$

$\quad = \text{Group generated by } y$

If $G = \langle y \rangle$ for some y, then we call G a cyclic group.

Rings

A ring R denoted by $\{R, +, *\}$, is a set of elements with two binary operations, called addition and multiplication, such that for all $a, b, c \in R$ the following axioms are obeyed:

- Group (A1-A4), Abelian Group(A5).
- Closure under multiplication (M1): If $a, b \in R$ then $ab \in R$
- Associativity of multiplication (M2): $a (bc) = (ab) c$ for all $a, b, c \in R$
- Distributive laws (M3) :

$$a (b + c) = ab + ac \quad \text{for all } a, b, c \in R$$

$$(a + b) c = ac + bc \quad \text{for all } a, b, c \in R$$

Commutative Rings

A ring is said to be commutative, if it satisfies the following additional condition:

Commutativity of multiplication (M4): $ab = ba$ for all $a, b \in R$

Integral Domain

An integral domain is a commutative ring that obeys the following axioms:

Multiplicative identity (M5): There is an element $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$.

No zero divisors (M6): If $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$.

Fields

A field F , sometimes denoted by {F, +,* }, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c $\in$ F the following axioms are obeyed:

(A1-M6): F is an integral domain; that is, F satisfies axioms A1 - A5 and M1 - M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that

$$aa^{-1} = (a^{-1})a = 1$$

Note: $a/b = a(b^{-1})$.

Familiar examples of Fields:

- Rational numbers
- Real numbers
- Complex numbers

Groups, Rings and Fields

Finite Fields

- A finite field or Galois field (so-named in honor of Évariste Galois) is a field that contains a finite number of elements.
- As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules.
- The most common examples of finite fields are given by the integers (mod p) when p is a prime number.

Application areas:

- Mathematics and computer science - Number theory, Algebraic geometry, Galois theory, Finite geometry, Cryptography and Coding theory.

Thank You!