Introduction to Number Theory

Prime Numbers

★ Prime Numbers: Has exactly two divisors.

★ If 'N' is prime, 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

Prime Numbers – Example

- ★ 2 is a prime number.
- ★ 3 is a prime number.
- ★ 5 is a prime number.
- ★ 7 is a prime number.
- ★ 9 is not a prime number.
- ★ 9 is a composite number.
- ★ 33 is a composite number.

Divisors of 2: 1 and 2

Facts about primes

- ★ Only even prime : 2
- ★ Smallest prime number : 2
- ★ Is 1 a prime number? No.
- ★ Except for 2 and 5, all prime numbers end in the digit 1, 3, 7 or 9.

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 the reverse.
- ★ Factoring very large prime numbers is very hard i.e. take computers a long time.

Congruence

★ In cryptography, congruence(≡) instead of equality(=).

Examples:

$15 \equiv 3 \pmod{12}$

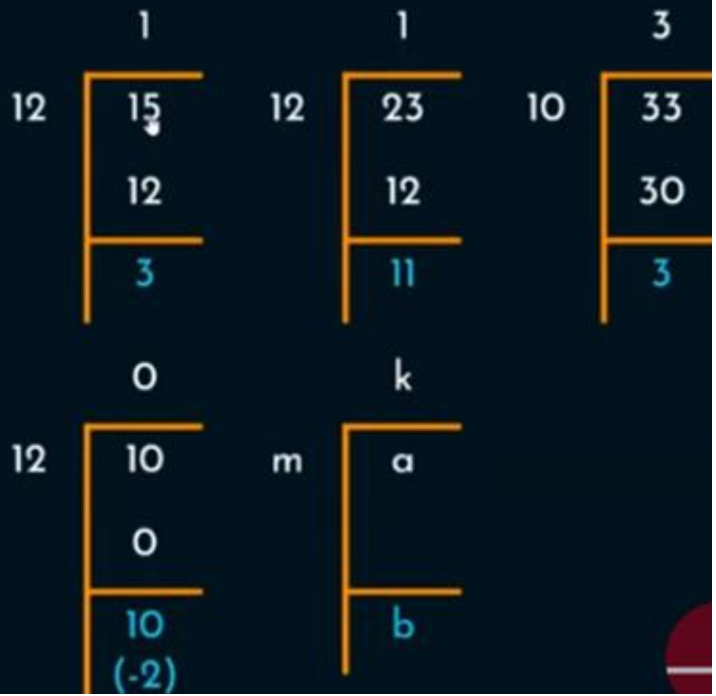
$23 \equiv 11 \pmod{12}$

$33 \equiv 3 \pmod{10}$

$10 \equiv -2 \pmod{12}$

$\therefore a \equiv b \pmod{m}$

i.e. $a = km + b$



Valid or Invalid

- ★ $38 \equiv 2 \pmod{12}$ ✓
- ★ $38 \equiv 14 \pmod{12}$ ✓
- ★ $5 \equiv 0 \pmod{5}$ ✓
- ★ $10 \equiv 2 \pmod{6}$ ✗
- ★ $13 \equiv 3 \pmod{13}$ ✗
- ★ $2 \equiv -3 \pmod{5}$ ✓

Properties of Modular Arithmetic

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

Example:

$$
\begin{aligned}
[(15 \bmod 8) + (11 \bmod 8)] \bmod 8 &= (15 + 11) \bmod 8 \\
&= 26 \bmod 8 \\
&= 2
\end{aligned}
$$

Example:

$$[(15 \bmod 8) - (11 \bmod 8)] \bmod 8 = (15 - 11) \bmod 8$$
$$= 4 \bmod 8$$
$$= 4$$

Example:

$$[(15 \bmod 8) \times (11 \bmod 8)] \bmod 8 = (15 \times 11) \bmod 8$$
$$= 165 \bmod 8$$
$$= 5$$

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	$(0 + a) \bmod n = a \bmod n$ $(1 \times a) \bmod n = a \bmod n$

Modular Exponentiation

- It is a type of exponentiation performed over a modulus.
- $a^b \bmod m$ or $a^b \pmod{m}$.

Example 1

Solve $23^3 \bmod 30$.

$23^3 \bmod 30 = -7^3 \bmod 30$ || 23 mod 30 can be 23 or -7.

$= -7^3 \bmod 30$

$= -7^2 \times -7 \bmod 30$

$= 49 \times -7 \bmod 30$

$= -133 \bmod 30$

$= -13 \bmod 30$

$= 17 \bmod 30$

$23^3 \bmod 30 = 17$

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 mod 13.

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

$11^7 \bmod 13 = 2$

Example 1

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 3

Solve 3^{100} mod 29.

3^1 mod 29	= 3 mod 29 = 3 or -26.			
3^2 mod 29	= 3^1 x 3^1 mod 29	= 3 x 3 mod 29	= 9 mod 29	= 9 or -20.
3^4 mod 29	= 3^2 x 3^2 mod 29	= 9 x 9 mod 29	= 81 mod 29	= 23 or -6.
3^8 mod 29	= 3^4 x 3^4 mod 29	= -6 x -6 mod 29	= 36 mod 29	= 7 or -22.
3^{16} mod 29	= 3^8 x 3^8 mod 29	= 7 x 7 mod 29	= 49 mod 29	= 20 or -9.
3^{32} mod 29	= 3^{16} x 3^{16} mod 29	= -9 x -9 mod 29	= 81 mod 29	= 23 or -6.
3^{64} mod 29	= 3^{32} x 3^{32} mod 29	= -6 x -6 mod 29	= 36 mod 29	= 7 or -22.
3^{100} mod 29	= 3^{64} x 3^{32} x 3^4 mod 29.			
	= 7 x -6 x -6 mod 29			
	= 252 mod 29			

Example 4

Solve $23^{16} \bmod 30$

$$
\begin{aligned}
23^{16} \bmod 30 &= (((23^2)^2)^2)^2 \bmod 30 \\
&= (((-7^2)^2)^2)^2 \bmod 30 \\
&= ((49^2)^2)^2 \bmod 30 \\
&= ((19^2)^2)^2 \bmod 30 \\
&= ((-11^2)^2)^2 \bmod 30 \\
&= (121^2)^2 \bmod 30 \\
&= (1^2)^2 \bmod 30 \\
&= 1 \bmod 30
\end{aligned}
$$

Euclidean Algorithm

- Euclidean Algorithm or Euclid's Algorithm.
- For computing the Greatest Common Divisor (GCD).
- aka Highest Common Factor (HCF).

Understanding GCD – Example 1

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

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

Understanding GCD – Example 2

	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	

∴ GCD(25, 150) = 25

Understanding GCD – Example 3

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

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

Euclid's Algorithm for finding GCD

GCD(12, 33) = 3.

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

Euclid's Algorithm for finding GCD

Find the GCD(750, 900).

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

Euclid's Algorithm for finding GCD

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

Euclid's Algorithm for finding GCD

Prerequisite: a > b

```
Euclid_GCD (a, b):
        if b = 0 then
                return a;
        else
                return Euclid_GCD (b, a mod b);
```

Euclid's Algorithm – Example 1

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

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

Two numbers are said to be relatively prime, if they have no prime factors in common, and their only common 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

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

Solution:

Here n=5.

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

GCD	Relatively Prime?
GCD (1, 5) = 1	✓
GCD (2, 5) = 1	✓
GCD (3, 5) = 1	✓
GCD (4, 5) = 1	✓

$\therefore \Phi(5) = 4.$

Euler's Totient Function

Example 2: Find $\Phi(11)$.

Solution:

Here n=11.

Numbers less than 11 are 1, 2, 3, 4, 5, 6, 7, 8, 9 and 10.

GCD	Relatively Prime?
GCD (1, 11) = 1	✓
GCD (2, 11) = 1	✓
GCD (3, 11) = 1	✓
GCD (4, 11) = 1	✓
GCD (5, 11) = 1	✓

GCD	Relatively Prime?
GCD (6, 11) = 1	✓
GCD (7, 11) = 1	✓
GCD (8, 11) = 1	✓
GCD (9, 11) = 1	✓
GCD (10, 11) = 1	✓

$\therefore \Phi(11) = 10.$

Euler's Totient Function

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 (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.

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

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

$\Phi(5) = 4$

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

Euler's Totient Function

Example 2: Find Φ(31).

Solution:

Here n=31.

'n' is a prime number.

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

$$\Phi(31) = (31-1)$$

$$\Phi(31) = 30$$

So, there are 30 numbers that are lesser than 31 and relatively prime to 31.

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

GCD	RP?
GCD(1,35)	✓
GCD(2,35)	✓
GCD(3,35)	✓
GCD(4,35)	✓
GCD(5,35)	✗
GCD(6,35)	✓
GCD(7,35)	✗
GCD(8,35)	✓
GCD(9,35)	✓

GCD	RP?
GCD(10,35)	✗
GCD(11,35)	✓
GCD(12,35)	✓
GCD(13,35)	✓
GCD(14,35)	✗
GCD(15,35)	✗
GCD(16,35)	✓
GCD(17,35)	✓
GCD(18,35)	✓

GCD	RP?
GCD(19,35)	✓
GCD(20,35)	✗
GCD(21,35)	✗
GCD(22,35)	✓
GCD(23,35)	✓
GCD(24,35)	✓
GCD(25,35)	✗
GCD(26,35)	✓
GCD(27,35)	✓

GCD	RP?
GCD(28,35)	✗
GCD(29,35)	✓
GCD(30,35)	✗
GCD(31,35)	✓
GCD(32,35)	✓
GCD(33,35)	✓
GCD(34,35)	✓

24

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.

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

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

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

$\Phi(1000) = 400$

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

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.

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' & 'n', which are said to be relatively prime, then $a^{\Phi(n)} \equiv 1 \bmod n$.

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.

<u>Definition made easy:</u>

'α' is said to be a primitive root of prime number 'p', if $\alpha^1 \bmod p$, $\alpha^2 \bmod p$, $\alpha^3 \bmod p$, . . . , $\alpha^{p-1} \bmod p$ are distinct.

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

Solution:

3^1 mod 7	3 mod 7	3	✓
3^2 mod 7	9 mod 7	2	✓
3^3 mod 7	6 mod 7	6	✓
3^4 mod 7	18 mod 7	4	✓
3^5 mod 7	12 mod 7	5	✓
3^6 mod 7	15 mod 7	1	✓

Yes, 3 is a primitive root of 7.

Primitive Root

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

Solution:

$2^1 \bmod 7$	$2 \bmod 7$	2	✓
$2^2 \bmod 7$	$4 \bmod 7$	4	✓
$2^3 \bmod 7$	$8 \bmod 7$	1	✓
$2^4 \bmod 7$	$16 \bmod 7$	2	✗
$2^5 \bmod 7$	$4 \bmod 7$	4	✗
$2^6 \bmod 7$	$8 \bmod 7$	1	✗

No, 2 is not a primitive root of 7.

Multiplicative Inverse

$$5 \times 5^{-1} = 1$$

$$5 \times \frac{1}{5} = 1$$

$$A \times \frac{1}{A} = 1$$

$$A \times A^{-1} = 1$$

Multiplicative Inverse

Under mod n

$A \times A^{-1} \equiv 1 \bmod n$

$3 \times ? \equiv 1 \bmod 5$

$3 \times 2 \equiv 1 \bmod 5$

$2 \times ? \equiv 1 \bmod 11$

$2 \times 6 \equiv 1 \bmod 11$

$4 \times ? \equiv 1 \bmod 5$

$4 \times 4 \equiv 1 \bmod 5$

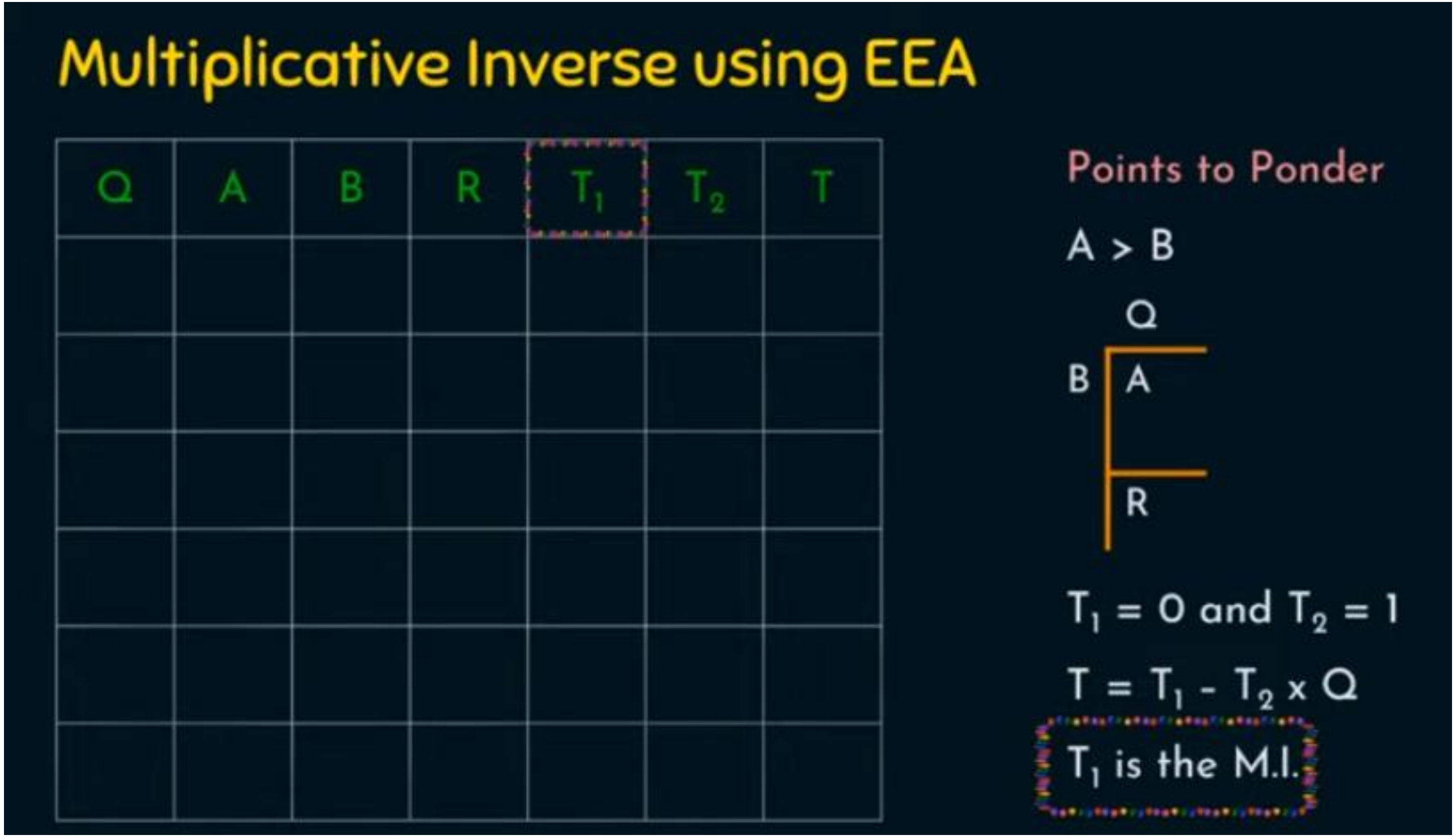
$5 \times ? \equiv 1 \bmod 10$

Multiplicative Inverse

The M.I. for 2 (mod 5) is 3.

The M.I. for 2 (mod 7) is 4.

Extended Euclidian Algorithm



Multiplicative Inverse using EEA

Example 1: What is the multiplicative inverse of 3 mod 5.

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	-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 EEA

Example 1: What is the multiplicative inverse of 3 mod 5.

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
X	1	0	X	$\boxed{2}$	-5	X

$\therefore$ 2 is the M.I of 3 mod 5.

Multiplicative Inverse using EEA

Example 2: What is the multiplicative inverse of 11 mod 13?

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	$\boxed{6}$	-13	X

∴ 6 is the M.I of 11 mod 13.

Multiplicative Inverse using EEA

Example 3: Find the M.I of 11 mod 26.

Q	A	B	R	T_1	T_2	T
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
X	1	0	X	$\boxed{19}$	26	X

$\therefore$ 19 is the M.I of 11 mod 26.

The 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.

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

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

Solution:

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

The Chinese Remainder Theorem

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

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}	

Solution:

$M = m_1 \times m_2 \times m_3$

$M = 3 \times 5 \times 7$

$M = 105$

The Chinese Remainder Theorem

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}	

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

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

$$M_1 = 35$$

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

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

$$M_2 = 21$$

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

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

$$M_3 = 15$$

The Chinese Remainder Theorem

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

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

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

$35 \times 2 = 1 \bmod 3$

$M_1^{-1} = 2$

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

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

$21 \times 1 = 1 \bmod 5$

$M_2^{-1} = 1$

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

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

$15 \times 1 = 1 \bmod 7$

$M_3^{-1} = 1$

m1,m2,m3 should be relatively prime to each other.

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

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

Solution:

$$X = (a_1M_1M_1^{-1} + a_2M_2M_2^{-1} + a_3M_3M_3^{-1}) \bmod M$$

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

$$= 233 \bmod 105$$

$$X = 23$$

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT:

$4X \equiv 5 \pmod 9$

$2X \equiv 6 \pmod{20}$

Rewrite the question as follows:

$4X \equiv 5 \pmod 9$

Multiply by 4^{-1} on both sides

$4^{-1} \times 4X \equiv 4^{-1} \times 5 \pmod 9$

$X \equiv 4^{-1} \pmod 9 \times 5 \pmod 9$

$X \equiv 7 \times 5 \pmod 9$

$X \equiv 35 \pmod 9$

$X \equiv 8 \pmod 9$

$2X \equiv 6 \pmod{20}$

$2X \equiv 2x3 \pmod{20}$

$X \equiv 3 \pmod{20}$

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT:

$X \equiv 8 \pmod{9}$

$X \equiv 3 \pmod{20}$

$X \equiv a_1 \pmod{m_1}$ $X \equiv a_2 \pmod{m_2}$	$X \equiv 8 \pmod{9}$ $X \equiv 3 \pmod{20}$

Solution:

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

Given		To Find		
$a_1 = 8$	$m_1 = 9$	M_1	M_1^{-1}	M
$a_2 = 3$	$m_2 = 20$	M_2	M_2^{-1}	

Solution:

$M = m_1 \times m_2$

$M = 9 \times 20$

$M = 180$

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

$$M_1 = \frac{180}{9}$$

$$M_1 = 20$$

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

$$M_2 = \frac{180}{20}$$

$$M_2 = 9$$

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

$$20 \times M_1^{-1} = 1 \bmod 9$$

$$20 \times 5 = 1 \bmod 9$$

$$M_1^{-1} = 5$$

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

$$9 \times M_2^{-1} = 1 \bmod 20$$

$$9 \times 9 = 1 \bmod 20$$

$$M_2^{-1} = 9$$

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT:

$X \equiv 8 \pmod{9}$

$X \equiv 3 \pmod{20}$

Given		To Find		
$a_1 = 8$	$m_1 = 9$	$M_1 = 20$	$M_1^{-1} = 5$	$M=180$
$a_2 = 3$	$m_2 = 20$	$M_2 = 9$	$M_2^{-1} = 9$	

Solution:

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

$$= (8 \times 20 \times 5 + 3 \times 9 \times 9) \bmod 180$$

$$= (800 + 243) \bmod 180$$

$$= 1043 \bmod 180$$

$$X = 143$$

Fermat's Primality Test

Is 'p' prime?

Test:

$a^p - a$ → 'p' is prime if this is a multiple of 'p' for all $1 \le a < p$.

- Not Accurate (561)

Example

Question 1: Is 5 prime?

Solution:

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

$1^5 - 1 = 1 - 1 = 0$

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

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

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

$\therefore$ 5 is prime

Example

Question 2: Is 3753 prime?

Solution:

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

$1^{3753} - 1$

$2^{3753} - 2$

$3^{3753} - 3$

$4^{3753} - 4$

...

$3752^{3753} - 3752$

Miller–Rabin Primality Test

Algorithm

Step 1: Find $n\text{-}1 = 2^k \times m$

Step 2: Choose 'a' such that $1<a<n\text{-}1$

Step 3: Compute $b_0 = a^m \pmod n, \ldots, b_i = b^2_{i-1} \pmod n$

$+1 \longrightarrow$ Composite

$-1 \longrightarrow$ Probably Prime

Example

Question: Is 561 prime?

Solution:

Given $n = 561$.

Step 1:

$n-1 = 2^k \times m$

$560 = 2^4 \times 35$

So $k = 4$, and $m = 35$

$\frac{560}{2^1} = 280$ | $\frac{560}{2^2} = 140$ | $\frac{560}{2^3} = 70$ | $\frac{560}{2^4} = 35$ | $\frac{560}{2^5} = 17.5$

Step 2:

Choosing $a = 2$; $1<2<560$

Example

Question: Is 561 prime?

Solution:

Given $n = 561$.

Step 3:

Compute $b_0 = a^m \pmod{n}$

$b_0 = a^m \pmod{n}$

$b_0 = 2^{35} \pmod{561} = 263$

Is $b_0 = \pm 1 \pmod{561}$? NO

So calculate b_1

$b_1 = b_0^2 \pmod{n}$

$b_1 = 263^2 \pmod{561}$

$b_1 = 166$

Is $b_1 = \pm 1 \pmod{561}$? NO

$b_2 = b_1^2 \pmod{n}$

$b_2 = 166^2 \pmod{561}$

$b_2 = 67$

Is $b_2 = \pm 1 \pmod{561}$? NO

$b_3 = b_2^2 \pmod{n}$

$b_3 = 67^2 \pmod{561}$

$b_3 = 1 \longrightarrow$ Composite

$\therefore$ 561 is composite.

Group

A group G denoted by $\{G, \bullet\}$, is a set under some operations $(\bullet)$ if it satisfies the CAIN properties.

- C - Closure
- A - Associative
- I - Identity
- N - iNverse.

Abelian Group

A group is said to be Abelian if it already a group and Commutative property is also satisfied i.e. $(a \bullet b) = (b \bullet a)$ for all a, b in G.

Group and Abelian Group

<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>

Example

Question: Is $(Z, +)$ a group?

Solution:

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

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 $\{G, \bullet\}$, 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

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

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

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

$\quad$ = Group generated by x

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

Cyclic Group

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

Solution:

Let us take an element y

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

$=$ 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) :

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

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

Note:

Subtraction $[a - b = a + (-b)]$

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

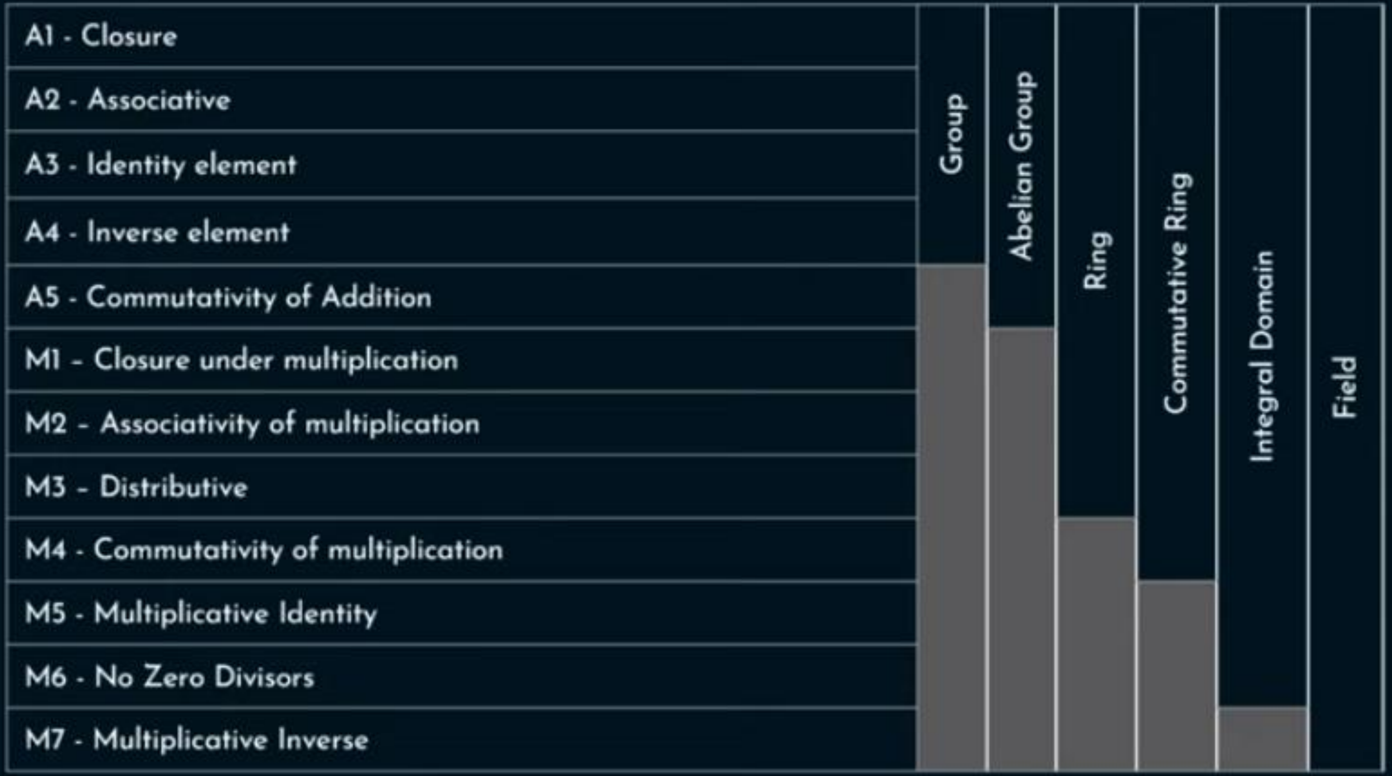
$$aa^{-1} = (a^{-1})a = 1$$

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.