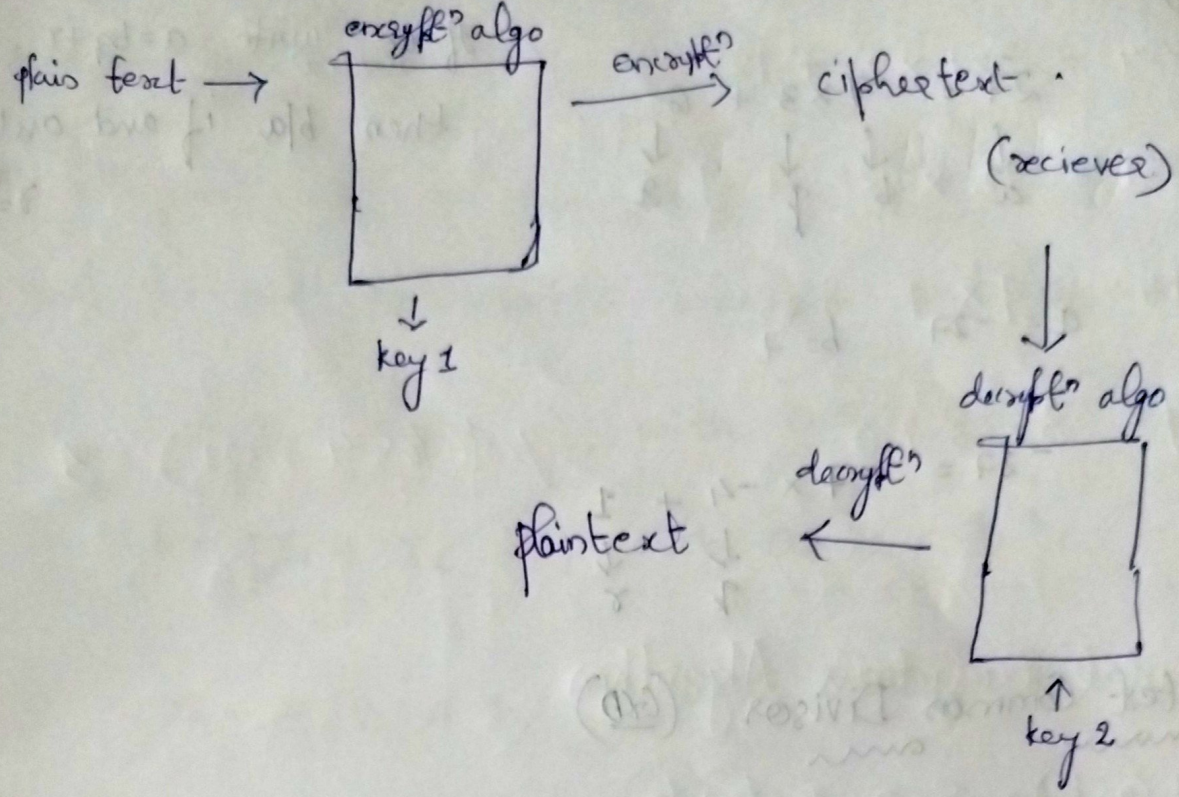
Number Theory & Cryptography MODULE 1 Number Theory



* Divisibility

- 'a' divides 'b', the remainder is zero then it is divisible.

represented ⇒ $a \mid b$ ($4 \mid 8$) eg: $8/4$, $r = 0$ (b/a)

- If not divisible, then it is represented as $a \nmid b$

eg: $2 \nmid 7 \Rightarrow 7/2, r \neq 0$

* Division Algorithm

Two integers a and b.

$$a = bq + r \quad ; \quad 0 \leq r \leq b$$

q → quotient, r → remainder

eg: $a = 27 \quad b = 7$

$27 = 7 \times 3 + 6$

(27 → a, 7 → b, 3 → q, 6 → r)

$a = -27 \quad b = 7$

$-27 = -7 \times -4 + 1$

(−4 → q, 1 → r)

*** Note**

If we write $a = bq + r$, $0 \le r < b$

then $b \mid a$ if and only if $r = 0$

* **Greatest Common Divisor (GCD)**

gcd (a, b)

$a = 12$

$b = 18$

Divisor of 12 { 1, 2, 3, 4, (6), 12 }

Divisor of 18 { 1, 2, 3, (6), 9, 18 }

$\therefore \gcd(12, 18) = 6$

• $\gcd(3, 7) = 1$

If gcd of (a, b) = 1, we can say that 'a' is relatively prime to 'b'.

Also called as coprime.

For higher number we use,

* **Euclidean Algorithms**

Used to find gcd of two no.s a & b.

'a' and 'b' are non negative integers and assume $b \neq 0$

$a = q_1 b + r_1$, with $0 \le r_1 < b$

$b = q_2 r_1 + r_2$, with $0 \le r_2 < r_1$

$r_1 = q_3 r_2 + r_3$, with $0 \le r_3 < r_2$

⋮

$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$, with $0 \le r_{n-1} \le r_{n-2}$

$r_{n-2} = q_n r_{n-1} + 0$

$\boxed{\gcd(a, b) = r_{n-1}}$

eg: Compute gcd (123, 456)

$456 = 123 \times 3 + 87$

$123 = 87 \times 1 + 36$

$87 = 36 \times 2 + 15$

$36 = 15 \times 2 + 6$

$15 = 6 \times 2 + 3$

$6 = 3 \times 2 + 0$

$\gcd(123, 456) = 3$

(side work: $123 \times 3 = 369$; $123 - 87 = 36$)

Q: gcd (654, 321)

$654 = 321 \times 2 + 12$

$321 = 12 \times 26 + 9$

$12 = 9 \times 1 + 3$

$9 = 3 \times 3 + 0$

gcd(654, 321) = 3

* gcd(a,b) = s·a + t·b
inverse and extended euclidean

* Extended Euclidean Algorithm

gcd(a,b) = s·a + t·b

Q: gcd (12, 34)

$34 = 12 \times 2 + 10$

$12 = 10 \times 1 + 2$

$10 = 2 \times 5 + 0$

∴ gcd (12, 34) = 2

$10 = 34 - 12 \times 2$ —①

$2 = 12 - 10 \times 1$ —②

(2 = 12 - 10 × 1) not 34(b)

∴ next eqt° —① contains 34

so, sub ① in ②

$2 = 12 - [34 - 12 \times 2] \times 1$

$2 = 12 - 34 + 2 \cdot 12$

$2 = 3 \cdot 12 - 34$ ∴ s = 3, t = -1

⇒ gcd(12, 34) = 3×12 − 1×34

Q: gcd (14, 5) and find s and t such that

s·a + t·b = gcd(a,b)

$14 = 5 \times 2 + 4$

$5 = 4 \times 1 + 1$

$4 = 1 \times 4 + 0$

gcd (14, 5) = 1

$4 = 14 - 5 \times 2$ —①

$1 = 5 - 4 \times 1$ —②

sub ② in ①

$1 = 5 - (14 - 5 \times 2) \times 1$

$1 = 5 - 14 + 5 \times 2$

$1 = -1 \cdot 14 + 5 \times 3$

∴ gcd (14, 5) = 1

s = -1

t = 3

Congruences

Two integers a and b are congruent mod m (written $a \equiv b \pmod{m}$) if $a - b$ is a multiple of m. The integer m is called the modulus of the congruence and is assumed to be +ve.

eg: $7 \equiv 1 \pmod 2$ $\quad -8 \equiv 12 \pmod 5$

$14 \equiv 0 \pmod 2$ $\quad 4 \equiv 4 \pmod{11}$

$19 \equiv 7 \pmod 6$ $\quad 6 \equiv 16 \pmod 5$

$34 \equiv 12 \pmod{11}$ $\quad 7 \equiv -2 \pmod 3$

$-11 \equiv 3 \pmod 7$

* n is even if and only if $n \equiv 0 \pmod 2$ and n is odd if and only if $n \equiv 1 \pmod 2$

* $2347 \equiv 7 \pmod{10}$, $65931 \equiv 1 \pmod{10}$, $2347 \equiv 47 \pmod{100}$ and $65931 \equiv 31 \pmod{100}$.

Generally, two +ve integers are congruent mod 10 if their last digits are the same, and they are congruent mod 100 if the last two digits of one are the same as the last two digits of the other.

* $4 \equiv 4 \pmod 8$, $12 \equiv 4 \pmod 8$, $20 \equiv 4 \pmod 8$ and $28 \equiv 4 \pmod 8$ and so on.

* $11 \equiv 1 \pmod 5$, $12 \equiv 2 \pmod 5$, $13 \equiv 3 \pmod 5$ and so on

$\therefore a \equiv b \pmod m$ if and only if $a = b + km$ for some integer 'k'.

Properties

Congruences have the following properties.

1. $a \equiv b \pmod m$ if $m \mid (a-b)$.
2. $a \equiv b \pmod m$ implies $b \equiv a \pmod m$.
3. $a \equiv b \pmod m$ and $b \equiv c \pmod m$ implies $a \equiv c \pmod m$.

- Congruence class mod m or Residue Class

One set consists of all the integers that are congruent to 0 mod m, another of the integers congruent to 1 mod m, then the integers congruent to 2 mod m until we get to the set which is made of the integers that are m-1 mod m. These m sets are called congruence classes mod m.

eg: m = 3

set of 0 mod 3 $\Rightarrow \{\dots -6, -3, 0, 3, 6 \dots\}$

set of 1 mod 3 $\Rightarrow \{\dots -5, -2, 1, 4, 7 \dots\}$

set of 2 mod 3 $\Rightarrow \{\dots -4, -1, 2, 5, 8 \dots\}$

Complete system of residues modulo m

Let m be a +ve integer. A set of integers $a_1, a_2 \cdots a_m$ is called a complete system of residues modulo m, if the set contains exactly on element from each residue class modulo m.

Let m = 5, then $\{-10, 11, 2, -7, 9\}$ is a complete system of residues modulo 5 since $-10 \in [0]$, $11 \in [1]$, $2 \in [2]$, $-7 \in [3]$ and $9 \in [4]$.

Reduced Residue systems.

Least Residue modulo m

The set of all of these least (non negative) residue is what we have shown as $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

In other words, the set $\mathbb{Z}_m$ is the set of all least residue modulo m.

Q. Find all congruent classes, 5 complete residue class and reduced residue classes mod m for m = 10. also find least residue.

m = 10

[1]

Operations in Z_n

* Perform the following operations:

- Add 7 to 14 in Z_{15}

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$= (7 + 14) \bmod 15$

$= 21 \bmod 15$

$= 6$

- Subtract 11 from 7 in Z_{13}
- Multiply 11 by 7 in Z_{20}

(i) $(7 - 11) \bmod 13$

$= -4 \bmod 13$

$= 9$

$-4 = 13 \times (-1) + 9$

13 | 4

(ii) $(11 \times 7) \bmod 20$

$= 77 \bmod 20$

$= 17$

a) Add 17 to 27 in Z_{14}

b) Subtract 43 from 12 in Z_{13}

c) Multiply 123 by -10 in Z_{19}

Properties

Three binary operations in the modular arithmetic can come from Z_n or Z_m

First property: $(a+b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m$

Second property: $(a-b) \bmod m = [(a \bmod m) - (b \bmod m)] \bmod m$

Third property: $(a \times b) \bmod m = [(a \bmod m) \times (b \bmod m)] \bmod m$

Eg: * $(1723345 + 2124945) \bmod 11$

$= (8 + 9) \bmod 11 = 17 \bmod 11$

$= 6$

* $(1723345 - 2124945) \bmod 11$

$= (8 - 9) \bmod 11 = -1 \bmod 11$

$= 10$

* $(1723345 \times 2124945) \bmod 11$

$= (8 \times 9) \bmod 11 = 72 \bmod 11$

$= 6$

- Exponentiation

$a^n \pmod m$ is performed by repeated multiplication, as in ordinary arithmetic.

Ex: To find $11^7 \bmod 13$

$11^2 = 121 = 4 \bmod 13$

$11^4 = (11^2)^2 = (4)^2 = 3 \bmod 13$

$11^7 = (11^2)^2 \times 11^2 \times 11$

$= 4^2 \times 3 \times 11 = 132$

$= 2 \bmod 13$

Q: $3^{385} \bmod (479)$

$3^6 = 729 = 250 \bmod 479$

$3^4 = 9^2 = 81 \bmod 479 = 81$

$3^8 = 81^2 = 6561 \bmod 479 = 534$

$3^{16} = 334^2 = 111556 \bmod 479 = 428$

$3^{32} = 428^2 = 183184 \bmod 479 = 206$

$3^{64} = 206^2 = 284$

$3^{128} = 284^2 = 184$

$3^{256} = 184^2 = 326$

$3^{385} = 3^{256} \times 3^{128} \times 3$

$= 326 \times 184 \times 3 = \_\_\_\_ \bmod 479$

$= 327$

Q: Compute $7^{256} \bmod 13$

Identity Element

Identity element e, for addition is

$e = 0$ ie, $a + e = e + a = a$

$a + 0 = 0 + a = a$

Identity element e, for scalar multi is

$e = 1$ ie, $a * e = e * a = a$

$a * 1 = 1 * a = a$

Additive modulo $m = 5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$(0+0) \bmod 5 = 0$

$(0+1) \bmod 5 = 1$

Multiplicative modulo $m = 5$

*	0	1	2	3	4
0	0	0	0	0	0
1	0	(1)	2	3	4
2	0	2	4	(1)	3
3	0	3	(1)	4	2
4	0	4	3	2	(1)

$(0*0) \bmod 5$

$(0*1) \bmod 5$

(1, 1)

(2, 3)

(3, 2)

(4, 4)

* Here multiplicative inverse of $2^{-1} = 3$ $\because a * e = a$ (↓ 1)

$2^{-1} = 3$

$\therefore 2^{-1} \bmod 5 = 3$

ie $2 \times 3 \bmod 5 = 1$

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

- $3^{-1} \bmod 5 = 2$

ie $3 \times 2 \bmod 5 = 1$

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

- $4^{-1} \bmod 5 = 4$

ie $4 \times 4 \bmod 5 = 1$

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

* Here additive inverse of $2 = 3$ $a + e = a$ (↓ 0)

ie $2^{-1} \bmod 5 = 3$

$2 + 3 \bmod 5 = 0$

$2 + 3 \equiv 0 \bmod 5$

- $3^{-1} \bmod 5 = 2$
- $4^{-1} \bmod 5 = 1$

ie $4 + 1 \bmod 5 = 0$

$4 + 1 \equiv 1 \bmod 5$

Modular additive identity ⇒ As in normal arithmetic

How

Q. Find all additive inverse pairs and multiplicative inverse pairs for modulo 10 operation.

Addi

Q. $5 \times x \equiv 1 \mod 14$ find x ?

or

$5^{-1} \mod 14$

$14 = 5 \times 2 + 4$

$5 = 4 \times 1 + 1$

$4 = 1 \times 4 + 0$

$4 = 14 - 5 \times 2$ — (1)

$1 = 5 - 4 \times 1$ — (2)

Sub (1) in (2)

$1 = 5 - (14 - 5 \times 2)$

$1 = 5 - 14 + 10$

$1 = 5 \times 3 - 14$

$s = 3$

$t = -1$

Multiplicative identity

$= 5 \times 3 - 14$

$= 1$

$\therefore s = 3$

$x = 3$

Q. $40x \equiv 1 \mod 7$

- Fermat's Theorum

If 'p' is prime and 'a' is positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

$\Rightarrow \gcd(a, p) = 1$

Eg: When 7^{200} by 23 what is the reminder.

$p = 23$
$a = 7$ $\qquad \gcd(23, 7) = 1$

$\therefore$ a is relatively prime to p

$\Rightarrow 7^{23-1} \equiv 1 \pmod{23}$

$\Rightarrow 7^{22} \equiv 1 \pmod{23}$

$\therefore 7^{22} \bmod 23 = 1$

$7^2 = 49 \bmod 23 = 3$

$7^4 = 7^2 \cdot 7^2 = 9 \bmod 23 = 9$

$7^{22} = 7^4 \cdot 7^4 \cdot 7^4 \cdot 7^4 \cdot 7^4 \cdot 7^2$

$= 9 \times 9 \times 9 \times 9 \times 3$

$= 19683 \bmod 23$

$= 18$

$22 \times 9 + r = 200$

$22 \times 9 + r = 200$

$r = 2.$

$(7^{22})^9 \times 7^2 \bmod 23$

$1^9 \times 7^2 \bmod 23$

$\Rightarrow 49 \bmod 23 = 3$

a: $2^{104} \bmod 101$

$p = 101$ $\qquad \gcd(101, 2) = 1$

$a = 2$

$\therefore$ a is relatively prime to p

$\Rightarrow 2^{101-1} \equiv 1 \pmod{101}$

$2^{100} \equiv 1 \bmod 101$

$100 \times 9 + 8 = 104$

$r = 4$

$(2^{100})^1 \times 2^4 \bmod 101$

$\Rightarrow 1 \times 2^4 \bmod 101$

$\Rightarrow 16 \bmod 101 = 16$

Euler's Theorem

Let n be a positive integer. Define the Euler-ϕ function $\phi(n)$ also called as Euler's totient function to be the number of integers j with $1 \le j \le n$ such that $\gcd(j, n) = 1$.

Examples:

* $\phi(3) = 2$ since $j = 1$ and $j = 2$ have $\gcd(j, 3) = 1$.
* $\phi(4) = 2$ $\because$ $j = 1$ and $j = 3$ have $\gcd(j, 4) = 1$.
* $\phi(12) = 4$ $\quad j = 1, 5, 7, 11 \quad \gcd(j, 12) = 1$

* If p is prime, then $\phi(p) = p - 1$.
* $\phi(1) = 1$

Proposition: Let m, n be +ve integers.

If $\gcd(m, n) = 1$ then, $\phi(mn) = \phi(m) \cdot \phi(n)$

$\gcd(3, 7) = 1$

$$\therefore \phi(21) = \phi(3) \cdot \phi(7)$$
$$= 2 \times 6$$
$$= 12$$

$$\phi(12) = \phi(3) \cdot \phi(4) \qquad \gcd(3, 4) = 1$$
$$= 2 \times 2$$
$$= 4$$

Proposition: If p is a prime and $k \ge 1$, then $\boxed{\phi(p^k) = p^k - (p^{k-1})}$

$$\text{eg- } \phi(100) = \phi(2^2) \cdot \phi(5^2)$$
$$= (2^2 - 2) \times (5^2 - 5)$$
$$= 4 - 2 \times 25 - 5$$
$$= 2 \times 20$$
$$= 40$$

Theorem - Let n be a positive integer and let b be an integer with $\gcd(b, n) = 1$. Then

$$b^{\phi(n)} \equiv 1 \pmod{n}$$

If n is prime then $\phi(n) = n - 1$

$$\therefore b^{n-1} \equiv 1 \pmod{n} \rightarrow \text{Fermat's Theorem}$$

$$\gcd(b, n) = 1$$

Q: Find the remainder when 3^{100} is divisible by 7

Q: Find the remainder when 7^{20} is divided by 21.

① By fermat's theorem.

$\Rightarrow 3^{7-1} \equiv 1 \pmod 7$

$\Rightarrow 3^6 \equiv 1 \pmod 7$

$\Rightarrow 3^6 \bmod 7 \equiv 1$

$\therefore (3^6)^{16} \times 3^4 \bmod 7$

$\Rightarrow 1 \times 3^4 \bmod 7$

$\Rightarrow 81 \bmod 7 = 4$

②

6/8/2024

Wilson's Theorem

Let p be prime, then $(p-1)! \equiv -1 \pmod p$

Eg: $p = 7$

$(p-1)! \equiv -1 \pmod p$

$(7-1)! \equiv -1 \bmod 7$

$720 \equiv -1 \pmod 7$

Proof $\Rightarrow 6! = 6 \cdot (5 \cdot 3) \cdot (4 \cdot 2) \cdot 1$

$= (-1)(1)(1)(1)$ (four congruence class)

$= -1$

Corollary: Let $n \geq 2$ be an integer. Then n is prime if $(n-1)! \equiv -1 \pmod n$

Eg: Let $n = 6$

$(n-1)! \equiv -1 \pmod n$

$(6-1)! \equiv -1 \pmod 6$

$5! \equiv -1 \bmod 6$

$120 \equiv -1 \bmod 6$

$5 \cdot 4 \cdot (3 \cdot 2)$

$\cdot 3 \times 0 = 0$

Then number $n = 6$ is not prime.

Q: $p = 13$

$(p-1)! \equiv -1 \mod 13$

- Chinese Remainder Theorem

The CRT is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime as shown below.

$$x \equiv a_1 \pmod{m_1}$$
$$x = a_2 \pmod{m_2}$$
$$\vdots$$
$$x = a_k \pmod{m_k}$$

1) Find $M = m_1 \times m_2 \times m_3 \cdots \times m_k$

2) Compute $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2} \cdots$, $M_k = \frac{M}{m_k}$

3) Find the multiplicative inverse of $M_1, M_2 \ldots, M_k$ using corresponding moduli $m_1, m_2 \cdots m_k$. called $M_1^{-1}, M_2^{-1} \cdots, M_k^{-1}$.

4) $x = \left[(a_1 \times M_1 \times M_1^{-1}) + (a_2 \times M_2 \times M_2^{-1}) \cdots + (a_k \times M_k \times M_k^{-1})\right] \mod M$.

Q: $x = 2 \mod 3$, $x = 3 \mod 5$, $x = 2 \mod 7$

$a_1 = 2$, $a_2 = 3$, $a_3 = 2$; $m_1 = 3$, $m_2 = 5$, $m_3 = 7$

* $M = 3 \times 5 \times 7 = 105$

* $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$

* $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$

$35^{-1} \mod 3 \Rightarrow 35 \times \textcircled{2} \mod 3 = 1$

* $x = \left[(2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1)\right] \mod 105$

$= \left[140 + 63 + 30\right] \mod 105$

$= 233 \mod 105$

$= 23$

Q: Find x such that $3x \equiv 7 \pmod{10}$

order (G) = no of elements in the group

order (element)

$a^i \bmod p = e$ $\quad \langle Z_7^*, * \rangle$

	i=1	i=2	i=3	i=4	i=5	i=6
n=1	1	1	1	1	1	1
n=2	2	4	1	2	4	1
n=3	3	2	6	4	5	1
n=4	4	2	1	4	2	1
n=5	5	4	6	2	3	1
n=6	6	1	6	1	6	1

order (1) = 1
order (2) = 3
order (3) = 6
order (4) = 3
order (5) = 6
order (6) = 2

order (G) = $\phi(n)$

$\phi(n) \Rightarrow$ no. of elements relatively prime to $n \Rightarrow n-1$

$\therefore \phi(7) =$ order (G) = 6

If order (G) = order (element) then it is the primitive root of group G.

Here order (G) = 6

and O(3) = O(5) = order (G) = 6

$\therefore$ 3 & 5 are the primitive roots.

* No. of primitive roots in a group $\Rightarrow \phi(\phi(n))$

$\because \phi(n) = 6$

$\phi(\phi(n)) \rightarrow \phi(6) = \phi(3) \times \phi(2)$

$= 2 \times 1$

$=$ 2 elements

* Each primitive root is a primitive generator (g)

- $g = 3$ $\quad Z_7^* = \{3^1 \bmod 7, 3^2 \bmod 7, 3^3 \bmod 7 \dots\}$
- $g = 5$ $\quad Z_7^* = \{5^1 \bmod 7, 5^2 \bmod 7, \dots, 5^6 \bmod 7\}$

The group $G = \langle Z_n^*, * \rangle$ has primitive roots only if n is $2, 4, p^t, 2p^t$ (p - prime no.)

Eg: Z_{17}^* ; i.e. p^t (17') & 17 is a prime no.

Q: (i) $(Z_{20}^*, *)$ no primitive root

(ii) $(Z_{38}^*, *)$ primitive root exists $\rightarrow 2 \cdot 19^1$

(iii) $(Z_{50}^*, *)$ primitive root exists $\rightarrow 2 \cdot 5^2$

Cyclic Group: If a group has a primitive root then it is also known as cyclic group.

Q: Group $(Z_{11}^*, \times)$

a) Find the order of the group
b) Find the order of each element in the group.
c) Find the no. of primitive roots in the group.
d) Find the primitive roots
e) Show that the group is cyclic.

- Quadratic Residues (QR)

* $x^2 \equiv a \pmod p$, 'a' is a quadratic residues if the eqn has two solutions.

* If 'a' is a quadratic non residue if the eqn has no solutions.

* If 'a' is 'a' square mod p, then it is quadratic residue mod p.

Eg: $Z_{11}^* \{0, 1 \dots 10\}$

$x^2 \equiv a \bmod p$

- $a = 1$

$x^2 \equiv 1 \pmod{11}$ $\quad 1^2 \bmod 11 = 1 \therefore 1$ is QR

- $a = 2$

$x^2 \equiv 2 \pmod{11}$ $\quad 2^2 \bmod 11 \neq 2 \therefore 2$ is QNR

- $a = 3$

$x^2 \equiv 3 \pmod{11}$

$6^2 \equiv 3 \pmod{11}$

$6^2 \bmod 11 = 3$
$5^2 \bmod 11 = 3$ $\longrightarrow$ 3 is QR

- $a = 4$

$x^2 \equiv 4 \pmod{11}$

$2^2 \equiv 4 \pmod{11}$

$2^2 \bmod 11 = 4 \neq 0 \Rightarrow 4$ is QR

- $a = 5$

$x^2 \equiv 5 \pmod{11}$

$4^2 \rightarrow 7^2 \equiv 5 \pmod{11}$

$7^2 \bmod 11 = 5 \longrightarrow 5$ is QR

- $a = 6$ $\quad x^2 = 6 \pmod{11}$

QR = $\{1, 3, 4, 5, 9\}$

QNR = $\{2, 6, 7, 8, 10\}$

Proposition -

Let p be an odd prime and let a not congruence [0 mod p] then

$a^{(p-1)/2} \equiv \pm 1 \pmod p$

Moreover 'a' is 'a' square mod p if and only if

$a^{(p-1)/2} \equiv 1 \pmod p$

proof

Let $b \equiv a^{(p-1)/2} \pmod p$

Taking Squ. $b^2 \equiv a^{(p-1)} \pmod p$

By Fermat's Theorem

$b^2 \equiv a^{p-1} \equiv 1 \pmod p$ $\quad (\because a^{p-1} \equiv 1 \pmod p)$

$b^2 \equiv 1 \pmod p$

$b \equiv \pm 1 \pmod p$

$a^{(p-1)/2} \equiv \pm 1 \pmod p$

If 'a' is 'a' square mod p

$x^2 \equiv a \pmod p$ for some x.

So $a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \pmod p \equiv 1 \pmod p$

By Fermat's Theorem $x^{p-1} \equiv 1 \pmod p$

$a^{(p-1)/2} \equiv 1 \pmod p$ $\Longrightarrow$

Legendre Symbol

Let p be an odd prime and let a be an integer $a \not\equiv 0 \pmod p$ defines the legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } x^2 \equiv a \pmod p \text{ has a solution} \\ -1 & \text{if } x^2 \equiv a \pmod p \text{ has no solution} \end{cases}$$

* $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$

$\therefore \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{(p-1)/2} \pmod p \times b^{(p-1)/2} \pmod p$

$= a^{(p-1)/2} \times b^{(p-1)/2} \mod p$

$= (ab)^{(p-1)/2} \pmod p$

$\rightarrow \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

* If $a \equiv b \pmod p$,

then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

$x^2 \equiv a \pmod p$ has a solution only when $x^2 \equiv b \pmod p$ has a solution.

* $\left(\frac{-1}{p}\right) = \begin{cases} +1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$

$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$, $a = -1$

- Case 1 :- $(p-1)/2$ is even

$\frac{(p-1)}{2} = 2k$, k is some even integer

$(p-1) = 4k$

$p = 4k+1 \Longrightarrow p \equiv 1 \pmod 4$

- Case 2 : $(p-1)/2$ is odd

$$\frac{(p-1)}{2} = 2k+1$$

$$p-1 = 4k+2$$

$$p = 4k+3 \longrightarrow p \equiv 3 \pmod 4$$

* Quadratic Reciprocity –

- Let p and q be distinct odd primes. Then,

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right)$$

In other words,

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if at least one of } p, q \text{ is } 1 \pmod 4 \\ \left(\frac{-p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

- Let p be an odd prime. Then,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{, if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{, if } p \equiv 3, 5 \pmod 8 \end{cases}$$

Q: Evaluate the $\left(\frac{8}{13}\right)$

$$\left(\frac{8}{13}\right) = \left(\frac{2 \times 2 \times 2}{13}\right)$$

$$= \left(\frac{2^2}{13}\right) \cdot \left(\frac{2}{13}\right)$$

$x^2 \equiv a^2 \pmod p$

- $\frac{2^2}{13} \longrightarrow x^2 \equiv 2^2 \pmod{13}$

$2^2 \equiv 2^2 \pmod{13}$

∴ the eqtn has a solution $\Rightarrow +1$

- $\frac{2}{13} \Rightarrow p \equiv 3, 5 \pmod 8$

∵ $13 \equiv 5 \pmod 8$

So the value $= -1$

∴ $\left(\frac{8}{13}\right) = +1 \times -1$

$= -1 \Rightarrow$ no solution for $\left(\frac{8}{13}\right)$

Q: Evaluate $\left(\frac{10}{13}\right)$

$$\left(\frac{10}{13}\right) = \left(\frac{5}{13}\right)\left(\frac{2}{13}\right)$$

$$= \left(\frac{5}{13}\right) \cdot -1 \longrightarrow \left(\frac{2}{p} \text{ ppfy}\right)$$

$\left(\frac{5}{13}\right) \Rightarrow x^2 \equiv 5 \pmod{13}$ $a^{(p-1)/2} \pmod p$

$= 5^6 \pmod{13}$

$= 12 \pmod{13}$

$= -1$

$\left(\frac{10}{13}\right) = -1 \cdot -1$

$= +1 \longrightarrow$ Soln exists for $\left(\frac{10}{13}\right)$

Q: Does $x^2 \equiv 19 \pmod{101}$ has any solution

Q: Evaluate $\left(\frac{12+2}{43}\right)$

Q: Evaluate $\left(\frac{319}{9}\right)$

- Jacobi symbol

Let m be a +ve odd integer. Write the prime factorization of m as

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_s^{a_s}$$

Let $\gcd(b, m) = 1$. Define the jacobi symbol

$$\left(\frac{b}{m}\right) = \left(\frac{b}{p_1}\right)^{a_1} \left(\frac{b}{p_2}\right)^{a_2} \cdots \left(\frac{b}{p_s}\right)^{a_s}$$

where $\left(\frac{b}{p_i}\right)$ is the Legendre symbol.

Eg: $\left(\frac{2}{15}\right) = \frac{2}{5^1 \times 3^1}$ $\quad 15 = 5 \times 3^1$

$$= \left(\frac{2}{5}\right)^1 \times \left(\frac{2}{3}\right)^1$$

$$= -1 \times -1$$

$$= +1$$

$\therefore \frac{2}{15}$ has solution

$\left(\frac{2}{75}\right) = \frac{2}{5^2 \times 3^1}$ $\quad 75 = 5^2 \times 3^1$

$$= \left(\frac{2}{5}\right)^2 \times \left(\frac{2}{3}\right)^1$$

$$= (-1)^2 \times -1 = -1$$

no solution

19/9/2024

Gauss's Lemma

Let 'p' be an odd prime and 'a' $\not\equiv 0 \pmod 3$

Let 'n' be the no of integers in the set $\{a, 2a, 3a \cdots \frac{(p-1)}{2}a\}$ that are congruent to an integer between $\frac{p}{2}$ and p.

Then, $\left(\frac{a}{p}\right) = (-1)^n$

Eg: $p = 11$ $\quad a = 7$ $\quad \{7, 14, 21 \cdots, \frac{10}{2} \times 7\}$

$\{7, 14, 21, \cdots 35\}$

↓ mod p

$\{7, 3, 10, 6, 2\}$

$\frac{p}{2}$ to $p \Rightarrow (5, \cdots 11)$

$\therefore (7, 10, 6)$ and $n = 3$

$\Rightarrow \left(\frac{7}{11}\right) = (-1)^3 = -1$

Proof

Let $a \not\equiv 0 \pmod p$, $\quad \gcd(a, p) = 1$

$S = \{0, 2a, 3a \cdots, \frac{(p-1)}{2}a\}$

none of the integers in S congruent to zero

$j = a \pmod p$ or $a = 0 \pmod p$ $\quad 1 \le j \le \frac{(p-1)}{2}$

not possible $\quad$ not possible.

$1 \le j \le \frac{p-1}{2}$

None of elements in S are congruent to each other

$r \cdot a \equiv s \pmod p$ $\quad 1 \le r$

$r \equiv s \pmod p$ $\quad s \le \frac{p-1}{2}$

$\gcd(a,p) = 1$

Eg: $a = 5$

$p = 13$

$S = \{5, 10, 15, 20, 25, 30\} \bmod p$

$S = \{5, 10, 2, 7, 12, 4\}$

Let $r_1, r_2, \cdots r_m$ be the those remainders upon divisible by p $\quad 0 < r_i < p/2$

Let $s_1, s_2, \cdots s_n$ be those remainder such that

$\frac{p}{2} < s_i < p \quad \left(m+n = \frac{p-1}{2}\right)$

Consider $(r_1, r_2 \cdots r_m), (p-s_1, p-s_2 \cdots p-s_n)$ these are +ve and less than $p/2$ and none of them are congruent to each other.

$r = \{2, 4, 5\}$

$p = \{10, 7, 12\}$

$p - s_i = \{3, 6, 1\}$

$\left[r \cdot p - s_i\right] = \left(\frac{p-1}{2}\right)!$

$\left(\frac{p-1}{2}\right)! = (r_1, r_2 \cdots r_m)(p-s_1, p-s_2 \cdots p-s_n)$

taking mod p

$\equiv (r_1, r_2 \cdots r_m)(-s_1), (+s_2), (-s_3) \cdots (-s_n))$

$\equiv (-1)^n r_m \cdot s_n$

$\equiv (-1)^n \{a, 2a, 3a \cdots \left(\frac{p-1}{2}\right)a\} \bmod p$

taking 'a' outside

$\equiv (-1)^n a^{\frac{p-1}{2}} \{1, 2 \cdots \frac{p-1}{2}\} \bmod p$

$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a^{\left(\frac{p-1}{2}\right)} \left(\frac{p-1}{2}\right)! \bmod p$

$1 \equiv (-1)^n a^{\left(\frac{p-1}{2}\right)} \bmod p$

$\left(\frac{a}{p}\right) \bmod p$

$(-1)^n \equiv \left(\frac{a}{p}\right) \bmod p$

$\left(\frac{a}{p}\right) = (-1)^n$

Primality Test : given a number, check if it is prime or not.

Pseudo prime : A composite number that satisfies the primality test, which fails the primality test

Let n greater than 1 be an odd number, choose an integer 'b' with $1 < b < n$. If $b^{n-1} \not\equiv 1 \pmod{n}$ then n is composite number. This is known as Fermat's Primality Test.

Q. Check whether 209 is prime or composite

* Usually $b = 2$

$1 = 2 \times 104 + 1$

$2^{208} \equiv 1 \bmod 209$

$2^{10} \cdot 2^{10} \cdot 2^{2}$

b-pseudo prime → A composite integer $n > 1$ is called a b-pseudo prime if $b^{n-1} \equiv 1 \pmod{n}$

Fermat's pseudo prime

Carmichael Number

A composite number $n > 1$ is called a Carmichael number if $b^{n-1} \equiv 1 \pmod{n}$ for all integers b with $\gcd(b, n) = 1$

eg: 561

$561 = 3 \cdot 11 \cdot 17$

Suppose $b \in \mathbb{Z}$ $\quad \gcd(b, 561) = 1$

then $3 \nmid b$, $11 \nmid b$, $17 \nmid b$

∴ By Fermat's Theorem

- $b^2 \equiv 1 \pmod 3$ — (1)
- $b^{10} \equiv 1 \pmod{11}$ — (2)
- $b^{16} \equiv 1 \pmod{17}$ — (3)

$560 \equiv 1 \pmod{81}$

(1) ⇒ $(b^2)^{280} \equiv 1 \pmod 3$ — (4)

(2) ⇒ $(b^{10})^{56} \equiv 1 \pmod{11}$ — (5)

(3) ⇒ $(b^{16})^{35} \equiv 1 \pmod{17}$ — (6)

Note: CRT

If $a \equiv b \pmod{m_1}$
$a \equiv b \pmod{m_2}$
$a \equiv b \pmod{m_3}$

then $a \equiv b \pmod{\text{LCM}(m_1, m_2, m_3)}$

here $m_1 = 3$, $m_2 = 11$, $m_3 = 17$ are relatively prime ⇒ $\text{LCM}(3, 11, 17) = 3 \times 11 \times 17$

$= 561$

∴ $b^{560} \equiv 1 \pmod{561}$

∴ It satisfies the eqn $b^{n-1} \equiv 1 \pmod n$, it is a carmichael number.

Euler pseudoprimes

A composite number 'p' is called an Euler pseudoprime to base 'a' if it satisfies:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$$

They "fool" the Euler criterion primality test, making them appear to be prime under this test.

eg: 561 base = 2

LHS $\left(\frac{a}{p}\right) = \left(\frac{2}{561}\right) = \frac{2}{3 \cdot 11 \cdot 17}$

$= \left(\frac{2}{3}\right) \cdot \left(\frac{2}{11}\right) \cdot \left(\frac{2}{17}\right)$

$= (-1) \cdot (-1) \cdot (1)$

$= 1$

RHS

$a^{(p-1)/2} \bmod p$

$= 2^{(561-1)/2} \bmod 561$

$= 2^{280} \bmod 561$

$\Rightarrow$ (illegible) $\bmod 561$

$561 = 3 \cdot 11 \cdot 17$

Fermat's: $2^2 \equiv 1 \pmod 3$

$\rightarrow (2^2)^{140} \equiv 1 \pmod 3$

$\rightarrow (2^{10})^{28} \equiv 1 \pmod{11}$

$\rightarrow (2^{16})^{17} \equiv 1 \pmod{17}$

$(2^{16})^{17} \quad 2^8 \equiv 1 \pmod{17}$

$1 \quad 1$

$2^{280} \equiv 1 \pmod{3 \times 11 \times 17}$

$\therefore 2^{280} \equiv 1 \pmod{561}$

$\Rightarrow$ LHS = RHS = 1

RHS $a^{(p-1)/2} \bmod p$

$= 2^{\left(\frac{561-1}{2}\right)} \bmod 561$

$= 2^{280} \bmod 561$

$\Rightarrow$ [illegible] $\bmod 561$

$561 = 3 \cdot 11 \cdot 17$

Fermat's : $2^2 \equiv 1 \pmod 3$

$\rightarrow (2^2)^{140} \equiv 1 \pmod 3$

$\rightarrow (2^{10})^{28} \equiv 1 \pmod{11}$

$\rightarrow$ [illegible]

$(2^{16})^{17} \cdot 2^8 \equiv 1 \pmod{17}$

$1 \quad 1$

$2^{560} \equiv 1 \pmod{3 \times 11 \times 17}$

$\therefore 2^{560} \equiv 1 \pmod{561}$

$\Rightarrow$ LHS = RHS = 1