UNIT- V

ELEMENTERY NUMBER THEORY AND CRYPTOGRAPHY

DIVISIBILITY

If a and b are any two integers such that $b \neq 0$ then we say that "b divides a" if there exists an integer k such that $a = kb$. And it is written as $b|a$

Note

If "b divides a", then we say that "b is factor of a" or "a is multiple of b".

DIVISION ALGORITHM

If a and b are any two integers such that $b > 0$ then there exist unique integer q and r such that,

$$a = bq + r$$

where q is called quotient.
r is called remainder.

CONGRUENCE RELATION

Let m be a positive integer. Then an integer 'a' is said to be congruent to an integer 'b' under modulo m, if "m divides (a-b)". $(m | (a-b))$ symbolically it is written as $a \equiv b \pmod{m}$ or $a \equiv b \pmod{m}$

It is read as "a is congruent to b modulo m".

Note

b is called remainder or residue of $a \pmod{m}$
OR b is remainder when m divides a

Properties of Congruence Relation

(i) If $a \equiv b \pmod m$, then $m \mid (a-b)$

(ii) If $a \equiv b \pmod m$ then $b \equiv a \pmod m$

(iii) If $a \equiv b \pmod m$ & $b \equiv c \pmod m$ then $a \equiv c \pmod m$

MODULAR ARITHEMATIC OPERATION

If $a \equiv b \pmod m$, then for $k \neq 0 \in Z$

(i) $a + k \equiv b + k \pmod m$

(ii) $a - k \equiv b - k \pmod m$

(iii) $a \cdot k \equiv b \cdot k \pmod m$

(iv) $a^k \equiv b^k \pmod m$

Properties of Modular Arithematic

- Residue sysbem Modulo m

Define the set Z_m as a set of non-negative integers less than m,

$Z_m = \{0, 1, 2, \ldots\ldots (m-1)\}$

It is called residue sysbem modulo m.

- Residue classes

Each integer in Z_m represents a residue class and it is divided by $[a]$ and defined by

$[r] = \{x : x \equiv r \pmod m\}$

For Example:

(1) Residue sysbem modulo 3 is,

$Z_3 = \{0, 1, 2\}$

∴ Residue classes of elements of Z_3 are

$[0] = \{x : x \equiv 0 \pmod 3\}$

$[0] = \{\ldots\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\ldots\}$

$[1] = \{\ldots\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\ldots\}$

$[2] = \{\ldots\ldots -7, -4, -1, 2, 5, 8, 11, \ldots\ldots\}$

Theorem

Let m be a positive integer and $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Then prove that $a+c \equiv b+d \pmod m$ and $ac \equiv bd \pmod m$.

Proof: Given $a \equiv b \pmod m$ and $c \equiv d \pmod m$

$m \mid (a-b)$ and $m \mid (c-d)$ ——— (1)

$\Rightarrow m \mid (a-b)+(c-d)$

$\rightarrow m \mid (a-b+c-d)$

$\Rightarrow m \mid (a+c)-(b+d)$

$\Rightarrow \boxed{a+c \equiv b+d \pmod m}$

By (1) we get

$a-b = k_1 m$ and $c-d = k_2 m$

$c(a-b) = ck_1 m$ and $b(c-d) = bk_2 m$

$ac-bc = (k_1 c)m$ and $bc-bd = (k_2 b)m$

$ac-bc+bc-bd = (k_1 c)m + (k_2 b)m$

$ac-bd = k'm + k''m$ where $k' = k_1 c$, $k'' = k_2 b$

$ac-bd = (k'+k'')m$

$ac-bd = k_1 m$ where $k_1 = k' + k'' \in \mathbb{Z}$

$\Rightarrow m \mid (ac-bd)$

$\Rightarrow \boxed{ac \equiv bd \pmod m}$

PRIME NUMBER

An integer $p \geq 2$ is called prime number if it is divisible by 1 and itself. Otherwise a number is called composite number.

Ex: (1) Prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

(2) Composite numbers are 4, 6, 8, 9, 10, ...

Note

Every composite number can be expressed as product of prime integers:

Ex: ① $10 = 2 \times 5$ ② $20 = 2 \times 10 = 2 \times 2 \times 5$ ③ $35 = 5 \times 7$

RELATIVELY PRIME NUMBER (CO-PRIME NUMBERS)

Two number a and b are said to be relatively prime if they have no common divisors other than 1.
$(GCD(a, b) = 1)$

Ex: ① 10 and 21 are relatively prime as $GCD(10, 21) = 1$

~~EULER'S ϕ - FUNCTION / EULER'S Tobient Fu~~

REDUCED RESIDUE SYSTEM MODULO m

The reduced residue system modulo m is the set of all elements from residue system modulo m. $Z_m = \{0, 1, 2 \ldots m-1\}$ which are relatively prime to m.

i.e $S = \{x : GCD(x, m) = 1\}$

EULER'S ϕ - FUNCTION / EULER'S TOTIENT FUNCTION.

The Euler's ϕ Function of an integer $n \geq 1$ is denoted by $\phi(n)$ and defined by the number of non-zero positive integers less than n that are relatively prime n

Ex: $\phi(1) = 0$, $\phi(2) = n(\{1\}) = 1$, $\phi(3) = n(\{1, 2\}) = 2$
$\phi(4) = n(\{1, 3\}) = 2$, $\phi(5) = n(\{1, 2, 3, 4\}) = 4$
$\phi(6) = n(\{1, 3\}) = 2$, $\phi(7) = 6$

Note

1. If $n = p$ is a prime number then Euler ϕ function of p is $\phi(p) = p - 1$
2. If n is number that can be expressed as a product of relatively prime number (a, b) Euler's ϕ function of n is.

Ex:- ① $\phi(20) = \phi(4 \cdot 5) = \phi(4) \cdot \phi(5) = 2 \times 4 = 8$

② $\phi(35) = \phi(5 \cdot 7) = \phi(5) \cdot \phi(7) = 4 \times 6 = 24$

③ $\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(5) = 1 \times 4 = 4$

Euler's Theorem.

Statement: Let n and a be positive integer which are relatively prime. (GCD(n, a) = 1). Then.

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

where $\phi(n)$ - is Euler ϕ - Function.

Proof:

Given that $n, a > \mathbb{Z}$, such that GCD(n, a) = 1.

Euler ϕ- function of n is,

$\phi(n) = k$

~~Let us take~~

Consider a reduced system modulo n.

$S = \{a_1, a_2, a_3, \ldots, a_{\phi(n)}\}$

OR $S = \{a_1, a_2, a_3, \ldots, a_k\}$

Take $a \neq 0 \in \mathbb{Z}$ such that GCD(n, a) = 1

$aS = \{aa_1, aa_2, aa_3, \ldots, aa_k\}$

$aa_1 \equiv a_1 \pmod{n}$; $aa_2 = a_2 \pmod{n}$ .... $aa_k \equiv a_k \pmod{n}$

Next, we know that,

$aa_1 \cdot aa_2 \cdot aa_3 \ldots aa_k \equiv a_1 \cdot a_2 \cdot a_3 \ldots a_k \pmod{n}$

$a^k (a_1 \cdot a_2 \cdot a_3 \ldots a_k) \equiv (a_1 \cdot a_2 \cdot a_3 \ldots a_k) \pmod{n}$

$\Rightarrow a^k \equiv 1 \pmod{n}$

$\Rightarrow \boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$

FERMAT'S THEOREM / FERMAT'S LITTLE THEOREM

Statement: Let P be a prime number and $P \nmid a$. Then,

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

OR $a^P \equiv a \pmod{P}$

Proof

Given that, P is a prime number and $P \nmid a$.

$\Rightarrow GCD(P, a) = 1$

Euler ϕ-function of prime no ϕ is.

$\phi(P) = P-1$

Consider a residue system modulo P.

$S = \{a_1, a_2, a_3, \ldots a_{P-1}\}$

Take $a \neq 0 \in \mathbb{Z}$ such that $P \nmid a$

$aS = \{aa_1, aa_2, aa_3, \ldots aa_{P-1}\}$

$aa_1 \equiv a_1 \pmod{P}$; $aa_2 \equiv a_2 \pmod{P}$ ..... $aa_{P-1} \equiv a_{P-1} \pmod{P}$

Next we know that,

$aa_1 \cdot aa_2 \cdot aa_3 \cdot \ldots aa_{P-1} \equiv a_1 \cdot a_2 \cdot a_3 \ldots a_{P-1} \pmod{P}$

$\Rightarrow a^{P-1}(a_1 \cdot a_2 \cdot a_3 \cdot \ldots a_{P-1}) \equiv (a_1 \cdot a_2 \cdot a_3 \ldots a_{P-1}) \pmod{P}$

$\Rightarrow a^{P-1} \equiv 1 \pmod{P}$

$\Rightarrow a^P \equiv a \pmod{P}$

For example

① $4^{\phi(7)} \equiv 1 \pmod 7$.

$\phi(7) = 6$

$4^6 \equiv 1 \pmod 7$

$4^2\ 4^2\ 4^2 \equiv 1 \pmod 7$

$2 \cdot 2 \cdot 2 \equiv 1 \pmod 7$

$8 \equiv 1 \pmod 7$

$4^2/7$ rem = 2

② $5^{\phi(6)} \equiv 1 \pmod 6$

$\phi(6) = n\{\{1,3\}\} = 2$

$5^2 = 1 \pmod 6$

CHINESE REMAINDER THEOREM

Statement: If $m_1, m_2, m_3, \ldots, m_k$ are pairwise relatively prime numbers and $a_1, a_2, a_3, \ldots, a_k$ are any integers then; the simultaneous congruences relations,

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

$\vdots \qquad \vdots$

$x \equiv a_k \pmod{m_k}$

has a unique solution under modulo M,

where $M = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_k$.

STEPS TO SOLVE SIMULTANEOUS CONGURENCE RELATION BY CHINESE THEOREM.

Step 1: Check $GCD(m_i, m_j) \equiv 1$; for $i \neq j$

Step 2: $x \equiv (M_1 X_1 a_1 + M_2 X_2 a_2 + \ldots\ldots + M_k X_k a_k) \pmod M$

where $M = m_1, m_2, \ldots\ldots m_k$

and $M_i = \frac{M}{m_i} = m_1 \cdot m_2 \ldots m_{i-1} \cdot m_{i+1} \ldots m_k$

Next, to calculate x_i. x_i is a multiplicative inverse of M_i under modulo m_i

i.e. $M_i x_i \equiv 1 \pmod{m_i}$

Step 3: Using values of M_i and x_i in (1) we can find the value of x

Examples

(1) Solve the following system of congruences by using chinese remainder theorem.

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

→ Given,

$x \equiv 2 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 3 \pmod 5$.

$a_1 = 2$, $a_2 = 1$, $a_3 = 3$

$m_1 = 3$, $m_2 = 4$, $m_3 = 5$

$GCD(3, 4) = GCD(4, 5) = GCD(3, 5) = 1$

∴ 3, 4, 5 are pair wise relatively prime

Next, $x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod M$ —(1)

where $M = m_1 m_2 m_3 = 3 \cdot 4 \cdot 5 = 60$

$M = 60$.

$M_1 = \frac{M}{m_1} = m_2 m_3 = 4 \cdot 5 = 20$

$M_2 = \frac{M}{m_2} = m_1 m_3 = 3 \cdot 5 = 15$

$M_3 = \frac{M}{m_3} = m_1 m_2 = 3 \cdot 4 = 12$

Calculate x_i

$M_i x_i \equiv 1 \pmod{m_i}$

$M_1 x_1 \equiv 1 \pmod{m_1}$

$\Rightarrow 20x_1 \equiv 1 \pmod 3$

$\rightarrow 2x_1 \equiv 1 \pmod 3$

$\therefore x_1 = 2$ as $3 \times 2 - 1$

$M_2 x_2 \equiv 1 \pmod{m_2}$

$15x_2 \equiv 1 \pmod 4$

$3x_2 \equiv 1 \pmod 4$

$x_2 = 3$ as $4 \times 3 - 1$

$M_3 x_3 \equiv 1 \pmod{m_3}$

$12 x_3 \equiv 1 \pmod 5$

$2x_3 \equiv 1 \pmod 5$

$x_3 = 3$ as $5 \times 2 - 1$

$\therefore$ Relation (1) becomes,

$x \equiv [20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 3] \pmod{60}$

$x \equiv [80 + 45 + 108] \pmod{60}$

$x \equiv 233 \pmod{60}$

$x \equiv 53 \pmod{60}$

$60 \overline{)233}$ (3, 180, 53)

$\boxed{x = 53}$

(2) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

$\rightarrow a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$m_1 = 3$, $m_2 = 5$, $m_3 = 7$

GCD(3,5) = GCD(5,7) = GCD(3,7) = 1.

3, 5, 7 are pair wise relative prime.

Next,

$x \equiv (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod M$ — (1)

where $M = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$

$M = 105$

$M_1 = \frac{M}{m_1} = 5 \cdot 7 = 35$

$M_2 = \frac{M}{m_2} = 3 \cdot 7 = 21$

$M_3 = \frac{M}{m_3} = 3 \cdot 5 = 15$

Calculate x_i

$M_1x_1 = 1 \pmod{m_1}$	$M_2x_2 = 1 \pmod{m_2}$	$M_3x_3 = 1 \pmod{m_3}$
$35x_1 = 1 \pmod 3$	$21x_2 = 1 \pmod 5$	$15x_3 = 1 \pmod 7$
$2x_1 = 1 \pmod 3$	$1x_2 = 1 \pmod 5$	$1x_3 = 1 \pmod 7$
$x_1 = 2$ $3(2(2)-1$	$x_2 = 1$ $5(1(1)-1$	$x_3 = 1$ $7(1(1)-1$

∴ Relation ① becomes

$x = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \pmod{105}$

$x \equiv 140 + 63 + 30$

$x \equiv 233 \pmod{105}$

$x \equiv 23 \pmod{105}$.

$\boxed{x = 23.}$

GREATEST COMMON DIVISION BETWEEN THE POSITIVE INTEGER

Find GCD between following pair of integer.

(ii) 100, 37

→ GCD (37, 100) = GCD (37, 300 (mod 37))

= GCD (37, 26)

= GCD (26, 37 (mod 26))

= GCD (26, 11)

= GCD (11, 26 (mod 11))

= GCD (11, 4)

= GCD (4, 11 (mod 4))

= GCD (4, 3)

= GCD (3, 4 (mod 3))

= GCD (3, 1)

= GCD (1, 3 (mod 1))

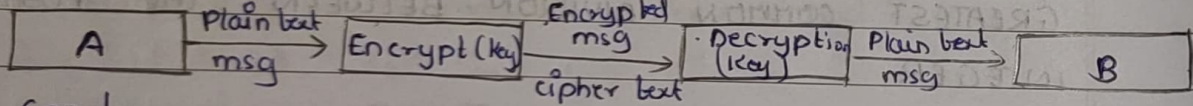
= 1

(ii) 52, 52

→ GCD(52, 252) = GCD(52, 252 (mod 52))
= GCD(52, 44)
= GCD(44, 52 (mod 44))
= GCD(44, 8)
= GCD(8, 44 (mod 8))
= GCD(8, 4)
= GCD(4, 8 (mod 4))
= 4

CRYPTOGRAPHY AND NETWORK SECURITY

Cryptography: A method of protecting information by transforming it into a unreadable format is called cryptography



Sender

Receiver

case

1) If Key are same then it is symmetric cryptography
2) If Key are different then it is asymmetric cryptograph

Encryption: The process of transforming information from readable format to unreadable format

Decryption: The process of transforming information from unreadable format to readable format.

Key: String of bits used by cryptography algorithm convert plain text to cipher text and vise-versa.

RSA ALGORITHM (Rivest, Shamir

RSA Algorithm is asymmetric cryptographic algorithm it means that 2 keys public key and private key are different.

Public Key: It is known to all users in the network

Private Key: It is kept secret and not shareable to all.

If a public key of a user A is used for encryption then we have to use the private key of the same user A for decryption.

RSA is a block cipher in which the plain text and cipher text are integers between zero to n-1 for some value n.

Algorithm

STEP 1: Key Generation.

[i] Select two large prime numbers p and q If p and q are more and more large then security is higher.

[ii] Calculate $n = p * q$.

[iii] Calculate Euler's ϕ function.

$$\phi(n) = \phi(pq) = \phi(p)\,\phi(q) = (p-1)(q-1)$$

[iv] Choose the value e such that

$$1 < e < \phi(n) \quad \text{and} \quad GCD(\phi(n), e) = 1$$

[v] Calculate $ed \equiv 1 \pmod{\phi(n)}$

OR $d \equiv e^{-} \pmod{\phi(n)}$

It means that e is multiplicate inverse of d under modulo $\phi(n)$

[vi] Public Key : $\{e, n\}$

[vii] Private Key : $\{d, n\}$

STEP 2: RSA Encryption

$C \equiv M^e \pmod{n}$

STEP 3: RSA Decryption

$M \equiv C^d \pmod{n}$

Where M is a plain text.
C is a cipher text.

① Perform encryption and decryption using RSA algorithm for $p=7$, $q=11$ and $M=6$

→ Given that $p=7$, $q=11$

(ii) $n = pq = 7 \cdot 11 = 77$

$\boxed{n=77}$

(iii) Euler's ϕ function is

$\phi(n) = \phi(pq)$

$= (p-1)(q-1)$

$= 6 \times 10$

$\boxed{\phi(n) = 60}$

(iv) Choose $e=7$ such that $1<7<60$ and GCD $(60,7)=1$

(v) $ed \equiv 1 \pmod{\phi(n)}$

$7d \equiv 1 \pmod{60}$

$d = 43$ as $60 / 7(43-1)$

$60 / 7d-1$

$60k = 7d-1$

$7d = 60k+1$

$d = \frac{60k+1}{7}$

$d=43$ for $k=5$

$\frac{3633}{77)67}$

Public key : $\{e, n\} = \{7, 77\}$

Private key : $\{d, e\} = \{43, 77\}$

STEP : 2 RSA Encryption

$C \equiv M^e \pmod{n}$

$C \equiv 6^7 \pmod{77}$

$C \equiv 41 \pmod{77}$

Cipher text $C = 41$

STEP 3 :

$M \equiv C^d \pmod{n}$

$M \equiv 41^{43} \pmod{77}$

$M \equiv 6 \pmod{77}$

Plain text is $M = 6$.

② Perform encryption and decryption using RSA algorithm for $P = 13$ $q = 17$ and $M = 18$

→ Given that $p = 13$ $q = 17$

$n = p \cdot q$

$= 13 \cdot 17$

$n = 221$

Euler's ϕ function

$\phi(n) = \phi(p-q)$

$= (p-1)(q-1)$

$= 12 \cdot 16$

$= 192$

Choose $e = 7$ such that $1 < 7 < 192$ and $GCD(192, 5) = 1$

$ed \equiv 1 \pmod{\phi(n)}$

$7d \equiv 1 \pmod{192}$

$d = 55$ for $k = 2$

$d = \frac{192}{7d-1}$ $\quad d = \frac{192k+1}{7}$

$d = \frac{192 \times 2 + 1}{7}$

$d = 77$

Public key $= \{e, n\} = \{5, 221\}$

Private key $= \{d, n\} = \{55, 221\}$

RSA encryption

$C \equiv M^e \pmod{n}$

$= 18^7 \pmod{221}$

$= 18^7 \pmod{221}$

$= 86 \pmod{221}$

Cipher text is $C = 86$

RSA decryption.

$M = C^d \pmod{n}$

$= 86^{55} \pmod{221}$

$M = 18 \pmod{221}$

Plain text is $M = 18$

GROUPS

A non-empty set G with binary operation $*$ denoted by $(G, *)$ is said to be group if satisfies following axiome (Laws)

(1) Closure Laws : $\forall a, b \in G \; . \; a * b \in G$

(2) Associative law : $a * (b * c) = (a * b) * c$

(3) Existance of identity Element : $\forall e \in G \ni e * a = a * e = a \; \forall a \in G$

(4) Existance of inverse element : $\forall a \in G \; \exists a^{-1} \in G \ni a * a^{-1} = a^{-1} * a = e$

If $(G, *)$ is said to be abelian group if it satisfies

(5) Commutative law : $a * b = b * a \quad \forall\ a, b \in G$.

RINGS

A set R with two binary operations + and × is denoted by $(R, +, \times)$ is said to be ring if it satisfies following axiomes

1 Closure under addition: $\forall\ a, b \in R,\ a+b \in R$

2 Associative under addition: $a+(b+c) = (a+b)+c$

3 Additive identity element : $\exists\ a \in R, \ni a+0 = 0+a = a\ \forall\ a \in$

4 Additive inverse element : $\forall\ a \in R,\ \exists -a \in R$.
$\exists\ a+(-a) = (-a)+a = 0$.

5 Commutative under addition: $a+b = b+a;\ \forall\ a, b \in R$.

6 Closure under multiplication: $\forall\ a, b \in R,\ ab \in R$.

7 Associative under multiplication: $a(bc) = (ab)c$.

8 Distributive Law : $a(b+c) = ab+ac \quad \forall\ a, b, c \in R$.

A ring $(R, +, \times)$ is said to be commutative ring if it satisfies.

9 Commutative under multiplication : $ab = ba \quad \forall\ a, b \in R$

A commutative ring $(R, +, \times)$ is called integral domain if it satisfies

10 Multiplicative identity $\exists\ 1 \in R, \ni 1 \cdot a = a \cdot 1 = a, \forall a \in$

11 No zero Divisions: $\forall\ a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$.

FIELDS

A set F under the operation + and × is denoted by

$(F, +, \times)$ and said to be field if $(F; +; \times)$ is integral domain and satisfies

12) Multiplicative inverse: $\forall a \in F, \exists a^{-1} \in F$
$\ni a a^{-1} = a^{-1} a = 1$

Finite Field.

For a given prime number P we define the finite field of order P denoted by GF(P) as the set $\mathbb{Z}_p$ of all integers $\{0, 1, 2, \ldots\ldots (p-1)\}$ together with arithmetic operation modulo P.

Finite field of the form GF(P)

GF stands for Galois Field in honor of great math ... Evariste Galois (25^{th} October 1811 – 31^{st} 1832) who first studied finite fields..... We have finite field of GF. This finite field is studied for prime number P.

Example

(1) Show that GF(3) is a finite field

→ Given that $P = 3$ is a prime number.

$\mathbb{Z}_3 = \{0, 1, 2\}$

Addition under modulo 3

⊕	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Multiplication under modulo 3.

⊗	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Additive inverse under modulo 3

a	0	1	2
-a	0	2	1

Multiplicative inverse under modulo 3

a	0	1	2
a^{-1}	-	1	2

∴ GF(3) is a finite field.

(2) Show that GF(5) is a finite field.

→ Given that P = 5 is a prime number

$Z_5 = \{0, 1, 2, 3, 4\}$

Addition under modulo 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

Multiplication under modulo 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

Additive inverse under modulo 5

a	0	1	2	3	4
-a	0	4	3	2	1

Multiplicative inverse under modulo 5.

a	0	1	2	3	4
-a	-	1	3	2	4

∴ GF(5) is a finite field.