



National Institute of Technology, Warangal

(*Department of Computer Science Engineering*)

Number Theory

Lecture By:-
Dr R Padmavathy
Dept of CSE, NIT Warangal

Content

- 1. Standard Notations
- 2. Basic Facts
- 3. Primes and Positive Divisions
- 4. Fundamental Theorem of
Arithmatic
- 5. Euclid's Theorem
- 6. GCD and LCM
- 7. Division Algorithm
- 8. Euclid and Extended Euclidean
- 9. Groups, Rings and Integral
Domain
- 10. Fields
- 11. Modular Arithmetic
- 12. Residue Classes
- 13. Galios Field



Standard Notations

- \mathbb{N} : Set of positive Integers $\{1, 2, 3, \dots\}$
- \mathbb{Z} : Set of all integers $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- \mathbb{Q} : Set of all rational numbers $\{p/q : p, q \in \mathbb{Z}, q \neq 0\}$
- \mathbb{R} : Set of all real numbers
- \mathbb{C} : Set of all Complex numbers



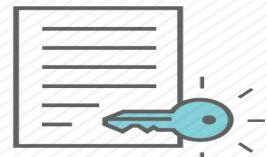
Basic Facts

- Every even integer is of the form $2m$ with $m \in \mathbb{Z}$
- Every odd integer is of the form $2m + 1$ or $2m-1$ with $m \in \mathbb{Z}$
- We say a divides b or $a \mid b$ if $b = ac$ with $c \in \mathbb{Z}$.
- When $a \mid b$, we say a is factor or a divisor of b .
- 1 and -1 are divisor of any integer.
- $a \mid 0$ for any $a \in \mathbb{Z}$
- $a \nmid b$ means a does not divide b .



Primes and positive divisors

- A positive integer $p > 1$ is prime if 1 and p are the only positive divisors of p .
- $2, 3, 5, 7, 11, 13, \dots$ are primes.
- A positive integer $n > 1$ is composite if it is not a prime.
- $4, 6, 8, 9, 10, \dots$ are composites.
- 1 is neither a prime nor a composite.



Fundamental Theorem of Arithmetic

- Every positive integer $n > 1$ can be written as product of primes and it is unique upto order of primes.
- Hence every $n \in \mathbb{N}$ can be written uniquely in the form

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

- where $p_1 < p_2 < \dots < p_r$ are primes and a_1, a_2, \dots, a_r are non negative integers. e.g. $100 = 2^2 \cdot 5^2$.
- 1 is neither a prime nor a composite else this Theorem is violated.
- Every $n > 1$ has a prime divisor.



Euclid's Theorem

Theorem 1:

The set of primes is finite.

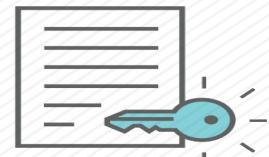
We denote the primes by $p_1 = 2, p_2 = 3, p_3 = 5, \dots$

However finding large primes is a challenge. Currently the largest known prime number is $2^{43112609} - 1$ which is about 12.9 million digits and before that $2^{37156667} - 1$ (only 11.1 million digits).



GCD and LCM

- a is a common divisor of b and c if $a \mid b$ and $a \mid c$.
- *Greatest Common Divisor (GCD)* of a and b , denoted by (a, b) is the largest positive common divisor of a and b . Also called as *HCF* of a and b .
- $(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.
- a and b are *relatively prime* or *coprime* if $(a, b) = 1$.
- *Lowest Common Multiple* or *LCM* of a and b , denoted by $[a, b]$ is the least positive integer l such that $a \mid l$ and $b \mid l$.



GCD and LCM

- If $a = p_1^{a_1} p_2^{a_2} \dots P_r^{a_r}$ and $b = p_1^{b_1} p_2^{b_2} \dots P_r^{b_r}$, then $(a, b) = p_1^{c_1} p_2^{c_2} \dots P_r^{c_r}$ and $[a, b] = p_1^{d_1} p_2^{d_2} \dots P_r^{d_r}$ where $c_i = \min\{q_i, b_i\}$ and $d_i = \max\{a_i, b_i\}$.
- Hence $ab = (a, b) \cdot [a, b]$.



Division Algorithm

- Let $a, b \in \mathbb{Z}$ with $a > 0$. Then there exist unique integers q and r such that $b = aq + r$ with $0 \leq r < a$.
- If $b = 0$, then $q = r = 0$, i.e., $0 = a \cdot 0 + 0$.
- $r = 0$ iff $a|b$
- Given a positive integer m , every other integer n is of the form Km or $km + 1$ or \dots $Km + m - 1$.



Modular Symbol

- We say a is congruent to b modulo m if $m \mid (a - b)$ and write $a \equiv b(m)$.
- $3 \equiv 25(11); 5 \equiv -7(12)$
- $a(m)$ is the “remainder” of a when divided by m .
- $b = aq + r$ is same as $b \equiv r(a)$.
- If $a \equiv b(m)$, then $b \equiv a(m)$ and $a \equiv bx(m)$ for any $x \in \mathbb{Z}$.
- If $a \equiv b(m)$ and $c \equiv d(m)$, then $ax + cy \equiv bx + dy$



Euclid's GCD Algorithm

Algorithm EuclidGCD(a, b):

Input: non negative integers a and b

Output: $\text{gcd}(a, b)$

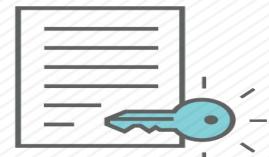
If $b = 0$ **then**

return a

return EuclidGCD($a, b(a)$)

$$\text{gcd}(412, 260)$$

	1	2	3	4	5	6	7
b	412	260	152	108	44	20	4
a	260	152	108	44	20	4	0



Stein's GCD Algorithm

Depends on following 3 observations, each of which allows one to reduce the size of at least one of the input by half:

- (a) If a & b are both even and not both zero, then

$$\gcd(a, b) = 2 \cdot \gcd(a/2, b/2)$$

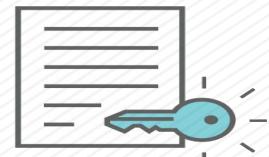
- (b) If a is even & b is odd, then

$$\gcd(a, b) = \gcd(a/2, b)$$

- (c) If a and b are both odd, then

$$\gcd(a, b) = \gcd((a-b)/2, b)$$

An “extended” version of Stein’s algorithm is available.



Extended Euclid Algorithm

Extended Euclidean algorithm also finds integer coefficients x and y such that: $ax + by = \gcd(a, b)$

$$r_0 = a$$

$$s_0 = 1$$

$$t_0 = 0$$

$$\vdots$$

$$r_1 = b$$

$$s_1 = 0$$

$$t_1 = 1$$

$$\vdots$$

$$r_{i+1} = r_{i-1} - q_i r_i \quad \text{and } 0 \leq r_{i+1} < |r_i| \quad (\text{this defines } q_i)$$

$$s_{i+1} = s_{i-1} - q_i s_i$$

$$t_{i+1} = t_{i-1} - q_i t_i$$

$$\vdots$$

ar to Euclidean ,

Where s and t are called as Bezout's co-efficients.



Extended Euclid Algorithm

The computation also stops when $r_{k+1} = 0$ and gives

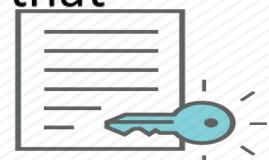
- r_k is the greatest common divisor of the input $a = r_0$ and $b = r_1$.
- The Bézout coefficients are s_k and t_k , that is $\gcd(a, b) = r_k = a*s_k + b*t_k$
- The quotients of a and b by their greatest common divisor are given by $s_{k+1} = \pm b / \gcd(a, b)$ and $t_{k+1} = \pm a / \gcd(a, b)$



Groups

A **group** G , denoted by $\{G, \cdot\}$ is a set of elements with a binary operation (\cdot) , that associates to each ordered pair (a, b) of elements in G an element $(a \cdot b)$ in G , such that the following axioms are obeyed:

- **(A1) Closure:** If $a & b \in G$, then $a \cdot b \in G$.
- **(A2) Associative:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c , \forall a, b, c \in G$.
- **(A3) Identity element:** $\exists e \in G$, such that
$$a \cdot e = e \cdot a = a, \quad \forall a \in G.$$
- **(A4) Inverse element:** $\forall a \in G$ there is an element $a' \in G$ such that
$$a \cdot a' = a' \cdot a = e.$$



Abelian Groups

A group is said to be **abelian** if it satisfies the following additional condition:

- **(A5) Commutative:** $a \cdot b = b \cdot a$ for all a, b in G .

Example :

- \mathbb{Z} under addition ,
- \mathbb{R} (except 0) under multiplication, are abelian groups.

NOTE :

- If G has a finite no. of elements, it is referred to as a **finite group**, otherwise, **infinite group**.
- The **order** of the group is equal to the no. of elements in the group.



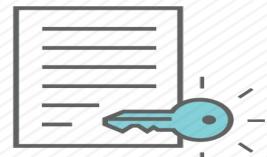
Cyclic Groups

A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$.

- The element a is said to **generate** the group G , or to be a **generator** of G .
- A cyclic group is always abelian, and may be finite or infinite.

Example :

- \mathbb{Z} under addition is an infinite cyclic group with 1 as generator.



Rings

A **ring** R , sometimes denoted by $\{R, +, \times\}$, 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:

- **(A1-A5)** i.e. R is an abelian group with respect to addition.
- **(M1) Closure under multiplication:** If $a & b \in R$, then $ab \in R$.
- **(M2) Associativity of multiplication:** $a(bc) = (ab)c \forall a, b, c \in R$.
- **(M3) Distributive laws:** $a(b + c) = ab + ac \forall a, b, c \in R$.
 $(a + b)c = ac + bc \forall a, b, c \in R$.

Example :

- The set of all n -square matrices over the real numbers is a ring.



Commutative Rings

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

- **(M4) Commutativity of multiplication:** $ab = ba \quad \forall a, b \in R$.

Example :

- Let S be the set of even integers. S is a commutative ring.



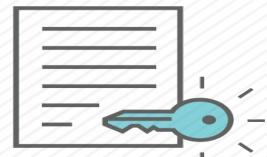
Integral Domain

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

- **(M5) Multiplicative identity:** There is an element 1 in R such that $a1 = 1a = a, \forall a \in R.$
- **(M6) No zero divisors:** If $a, b \in R$ & $ab = 0$, then either $a = 0$ or $b = 0$

Example :

- \mathbb{Z} is an integral domain.



Fields

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

- **(A1-M6)** i.e. F is an integral domain.
- **(M7) Multiplicative inverse:** $\forall a \in F$ (except 0), $\exists a^{-1} \in F$ such that $aa^{-1} = (a^{-1})a = 1$.

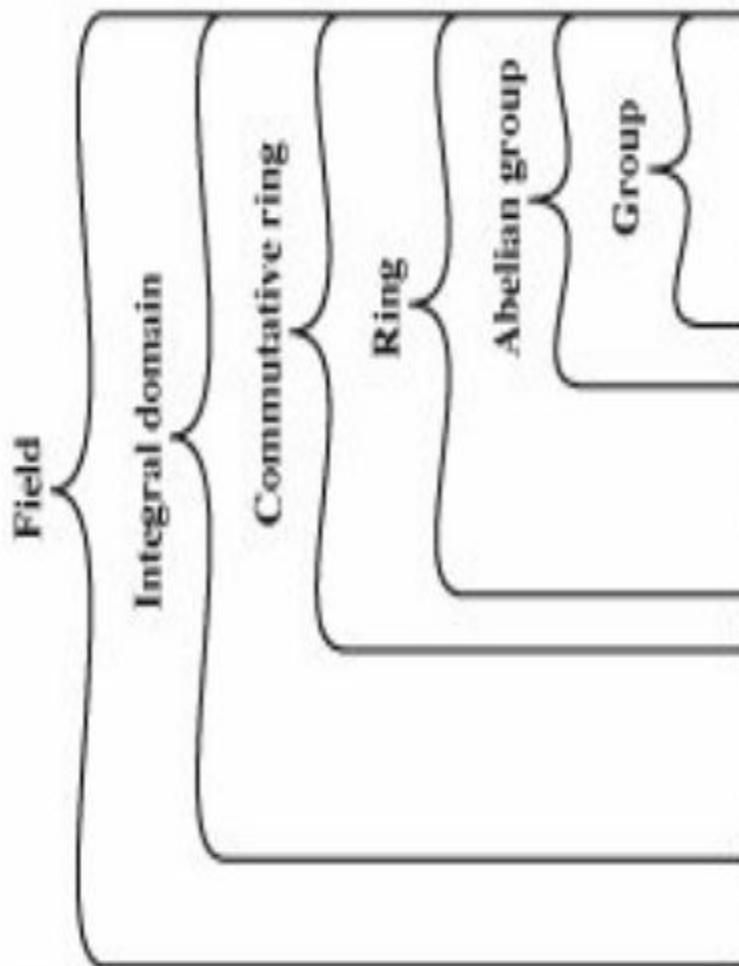
Example :

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are Fields.

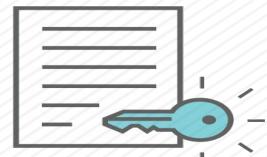
Note : \mathbb{Z} is not a field, because not every integer has a multiplicative inverse.



Group, Ring and Field



- (A1) Closure Under Addition
- (A2) Associativity Under Addition
- (A3) Additive Identity
- (A4) Additive Inverse
- (A5) Commutative under Addition
- (M1) Closure Under Multiplication
- (M2) Associativity Under Multiplication
- (M3) Distributive Laws
- (M4) Commutativity of Multiplication
- (M5) Multiplicative Identity
- (M6) No Zero Division
- (M7) Multiplicative Inverse



Modular Arithmetic

Given any positive integer n and any non-negative integer a , if we divide a by n , we get integers q and r be quotient and remainder respectively that obey the following relationship:

$$a = qn + r \quad 0 \leq r < n; q = \lfloor a/n \rfloor$$

Example:

$a = 11;$	$n = 7;$	$11 = 1 \times 7 + 4;$	$r = 4$	$q = 1$
$a = -11;$	$n = 7;$	$-11 = (-2) \times 7 + 3;$	$r = 3$	$q = -2$

If a is an integer and n is a positive integer, we define $a \bmod n$ to be the remainder when a is divided by n . The integer n is called the **modulus**. Thus, for any integer a , we can always write:

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

$$11 \bmod 7 = 4;$$

$$-11 \bmod 7 = 3$$



Modular Arithmetic

Two integers a and b are said to be **congruent modulo n** ,
if $(a \bmod n) = (b \bmod n)$.

This is written as

$$a \equiv b \pmod{n}.$$

Example :

- $73 \equiv 4 \pmod{23}$
- $21 \equiv -9 \pmod{10}$



Modular Arithmetic

Divisors

We say that a nonzero b divides a if $a = mb$ for some m , where a, b , and m are integers. And denoted as $a \mid b$.

The following relations hold:

- If $a \mid 1$, then $a = \pm 1$.
- If $a \mid b$ and $b \mid a$, then $a = \pm b$.
- Any $b \neq 0$ divides 0.
- If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n .



Modular Arithmetic

Congruences have the following properties:

1. $a \equiv b \pmod{n}$, if $n \mid (a-b)$
2. $a \equiv b \pmod{n}$, implies $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$



Modular Arithmetic in \mathbb{Z}_n

Property	Expression
Commutative laws	$(w + x) \text{ mod } n = (x + w) \text{ mod } n$ $(w \times x) \text{ mod } n = (x \times w) \text{ mod } n$
Associative laws	$[(w + x) + y] \text{ mod } n = [w + (x + y)] \text{ mod } n$ $[(w \times x) \times y] \text{ mod } n = [w \times (x \times y)] \text{ mod } n$
Distributive laws	$[w + (x + y)] \text{ mod } n = [(w \times x) + (w \times y)] \text{ mod } n$ $[w + (x \times y)] \text{ mod } n = [(w + x) \times (w + y)] \text{ mod } n$
Identities	$(0 + w) \text{ mod } n = w \text{ mod } n$ $(1 + w) \text{ mod } n = w \text{ mod } n$
Additive inverse $(-w)$	For each $w \in \mathbb{Z}_n$, there exists a z such that $w + z \equiv 0 \pmod{n}$



Residue Class

- The congruence relation $a \equiv b \pmod{n}$ on the set of integers I separates the integers into n equivalence classes, $[0]_n$, $[1]_n$, $[2]_n$, ..., $[n-1]_n$, called ***residue classes modulo n***.
- Each equivalence class $[r]_n$ consists of all integers congruent to r where r is one of the integers $0, 1, 2, \dots, n-1$.
- These n integers $0, 1, 2, \dots, n-1$ are called the class representatives.
- Thus equivalence class $[3]_n$ consists of all integers congruent to 3 mod n where the integer 3 is the class representative.



Residue Class

Example. The residue classes of integers mod 4 are:

$$[0]_4 = \{ \dots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \dots \}$$

$$[1]_4 = \{ \dots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \dots \}$$

$$[2]_4 = \{ \dots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \dots \}$$

$$[3]_4 = \{ \dots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \dots \}$$



Residue Class

Complete Residue system

Any set of integers $\{a_1, a_2, \dots, a_n\}$ representing all the residue classes $(\text{mod } n)$ is called a *complete residue system (mod n)*. The simplest complete residue system is $0, 1, 2, \dots, n-1$.

Reduced residue system

Any set of $\varphi(n)$ integers that are relatively prime to n and that are mutually incongruent modulo n , where $\varphi(n)$ denotes *Euler's Totient Function*, is called a **reduced residue system modulo n** .



Two Types of Fields

- Prime Field , Which can be represented as , $GF(P) = F_p = Z_p$
- Polynomial Fields : represented as $GF(P^n)$



Galios Field GF(p^n)

Polynomials in which the coefficients are elements of some field F and of the degree less than “n” are said to form a polynomial ring in $GF(P)^n$, Where P is a prime number. It can be referred as **Galios field** as well.

Normally we work on field where $p = 2$, which is given a $GF(2)^n$ Arithmatic over the polynomial field is similar to modular arithmetic in Z_p , Where Prime number p is being replaced by an **irreducible polynomial**.

Modular operation happens with the Irreducible Polynomial that defines the field.

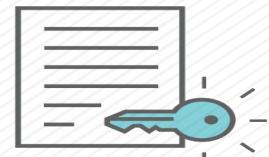


Modular Arithmetic in $GF(2)^n$

A polynomial $f(x)$ over a field F is called irreducible if and only if $f(x)$ cannot be expressed as a product of two polynomials, both over F , and both of degree lower than that of $f(x)$. By analogy to integers, an **irreducible polynomial** is also called a **prime polynomial**.

Modular Arithmatic : $m(x)$ is the irreducible polynomial

1. $f(x) \text{ mod } m(x) + g(x) \text{ mod } m(x) = (f(x) + g(x)) \text{ mod } m(x)$
2. $f(x) \text{ mod } m(x) * g(x) \text{ mod } m(x) = (f(x) * g(x)) \text{ mod } m(x)$
3. $f(x) \text{ mod } m(x) / g(x) \text{ mod } m(x) = (f(x) * g'(x)) \text{ mod } m(x)$



Construction of Field F_p

- Construction of Field F_p involves just selecting a Prime “P”. Elements in the Field will be $[0 \dots P-1]$.
- Ex : $F_{11} = [0,1,2,3,4,5,6,7,8,9,10]$
- We can enumerate all the elements of the field with generator g.
- F_{11} can be enumerated with generator 2 as, $2^0, 2^1, \dots, 2^9$.



Construction of Field $GF(P^n)$

Construction of $GF(P^n)$ can be done in two ways :

- 1 . Select a Prime P and degree n , Construct the field with all the polynomials of degree less than n, with co-efficients in the field F_p .
2. Select a Prime P and irreducible polynomial of degree n , Construct the field with all the polynomials of degree less than n, with co-efficients in the field F_p . The polynomial $f(x) = "x"$ can be used as generator.



Construction of Field GF(Pⁿ)

Eg : Construction of GF(2³)

Constant polynomials :

000 : 0

001 : 1

Other Polynomials :

010 : x

011 : x+1

100 : x²

101 : x² + 1

110: x² + x

111 : x² + x + 1

Enumeration of GF(2³) with irreducible polynomial x³+x+1

Generator = x , x³+x+1 = 0, So we have x³ = x+1.

now we can enumerate all the polynomials as x⁰, x, x², x³.....x⁷

eg : x⁴ = x³ . x = (x+1)x= x²+x



References

- 1 . Cryptograpgy and Network Secuirty , by Wiliam Stallings
2. Handbook of Applied Cryptography , by Alfred J. Menezes Paul C. van Oorschot Scott A. Vanstone
3. Wikipedia



Any Queries ?



Thank You...

