UNIT-1
Number Theory

Prime Numbers

- Prime numbers are central to number theory
- Prime numbers only have divisors of 1 and self
  - They cannot be written as a product of other numbers
  - e.g. 2,3,5,7 are prime, 4,6,8,9,10 are not

Relatively Prime Numbers

- Determining the GCD of two positive integers is easy
  - if they are expressed each - as the product of primes
  - e.g. if $300 = 2^2 \times 3^1 \times 5^2$ and $18 = 2^1 \times 3^2$ then the gcd(300, 18) is given as $2^1 \times 3^1 \times 5^0 = 6$
- Two numbers a and b are relatively prime if they have no common divisors apart from 1
  - e.g. 8 & 15 are relatively prime (even though none of them is prime) since factors of 8 are 1,2,4,8 and of 15 are 1,3,5,15 and 1 is the only common factor
  - e.g. check whether 6 and 8 are relative prime or not?
  - e.g. check whether 14 and 9 are relative prime or not?

Euclidean Algorithm (EA)

- Efficient way to find the GCD(a,b)
- Euclidean Algorithm to compute GCD(a,b) is:

```
EUCLID(a,b)
1. A = a; B = b
2. if B = 0 return  A (where A = gcd(a, b) )
3. R = A mod B
4. A = B
5. B = R
6. goto 2
```

  - e.g. check whether 6 and 8 are relative prime or not?
  - e.g. check whether 14 and 9 are relative prime or not?

Applications: Key Generation, Extended Euclidean Algorithm, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography and more

Example GCD(1970,1066) with EA

A = 1970; B = 1066

1970 = 1 x 1066 + 904(R=904)	gcd(1066, 904) (A=B; B=R)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x **2** + **0**	**gcd(2, 0)** **(Return A if B=0)**

Therefore, GCD(1970, 1066) = **2**

GCD(270,192) ??

Modular Arithmetic

- Two integers "a" and "b" are said to be congruent modulo "n" if their difference "a - b" is divisible by "n."
- This is denoted as "a ≡ b (mod n)." In other words, "a" and "b" leave the same remainder when divided by "n." e.g. 100 ≡ 34 mod 11 (where 100 and 34 leave same remainder when divided by 11)
- Modular addition rule
  - `e.g. (a+b)mod n = (a mod n + b mod n) mod n`
- Process of **modulo reduction:**
  - `E.g. -12 mod 7 ≡ -5 mod 7 ≡ 2 mod 7`
  - `E.g. 17 mod 5 ≡ 2 mod 5`

Abstract Algebra

- Number theory has increasing importance in cryptography
  - AES, Elliptic Curve, IDEA, Public Key
- Abstract algebra is a branch of mathematics that deals with algebraic structures, such as groups, rings, and fields, in a more abstract and general way than elementary algebra. It is called "abstract" because it focuses on the study of algebraic systems and their properties without necessarily specifying the nature of the elements involved.

Group

- A set of elements or “numbers”
- With some operation whose result is also in the set
- Obeys:
  - Closure: For any two elements "a" and "b" in the group, the result of the operation "a * b" is also in the group.
  - Associative law: $(a.b).c = a.(b.c)$
  - Has identity e: $e.a = a.e = a$
  - Has inverses a^{-1}: $a.a^{-1} = e$
- E.g. the set of integers "Z" under addition "+" forms a group.
- If commutative $a.b = b.a$
  - Then forms an **Abelian Group**

Cyclic Group

- A group is cyclic if every element is a addition/multiple/power of some fixed element
- It is a group that can be generated by a single element, which is often referred to as the generator of the group.
- In a cyclic group, repeated applications of the group operation to the generator produce all the elements of the group.
- E.g. Cyclic Group of Integers Modulo 5: The set of integers modulo 5 is {0, 1, 2, 3, 4}, and the group operation is addition modulo 5
- $0+1 \equiv 1 \bmod 5$ (Add 1 once) **1**
  $1+1 \equiv 2 \bmod 5$ (Add 1 twice) **2**
  $2+1 \equiv 3 \bmod 5$ (Add 1 thrice) **3**
  $3+1 \equiv 4 \bmod 5$ (Add 1 four times) **4**
  $4+1 \equiv 0 \bmod 5$ (Add 1 five times) **0**

Therefore, 1 is a generator of the cyclic group of integers modulo 5 because it can produce every element in the set through the operation of addition modulo 5.

...Cyclic Group

Here are the key properties of this cyclic group:

- **Generator:** The integer 1 is a generator for this group. This means that by repeatedly adding 1 (modulo 5), we can generate all the elements of the group (as discussed on the previous slide)
- **Closure:** When we add two integers modulo 5, the result remains within the set {0, 1, 2, 3, 4}, so the group is closed under addition modulo 5.
- **Associativity:** Addition modulo 5 is associative, as the order in which we add elements doesn't affect the result.

  Let a=2, b=3 and c=4

  (a+b)+c mod 5 = **4** and also, a+(b+c) mod 5=**4**
- **Identity Element:** The identity element in this group is 0 because adding 0 to any element doesn't change it.
- **Inverse Element:** Each element has an inverse within the group:
  - The inverse of 1 is 4 because $1 + 4 \equiv 0 \pmod 5$.
  - The inverse of 2 is 3 because $2 + 3 \equiv 0 \pmod 5$.
  - The inverse of 3 is 2 because $3 + 2 \equiv 0 \pmod 5$.
  - The inverse of 4 is 1 because $4 + 1 \equiv 0 \pmod 5$.
  - The inverse of 0 is itself ($0 + 0 \equiv 0 \pmod 5$).

Ring

- A set of “numbers”
- With two binary operations (addition and multiplication) which form
  - An Abelian Group with addition operation
- And multiplication:
  - Has closure
  - Is associative
  - Distributive over addition: `a(b+c) = ab + ac`
- If multiplication operation is commutative, it forms a **commutative ring**

Field

- A set of numbers with two operations which form:
  - Abelian Group for addition
  - Abelian Group for multiplication (ignoring 0)
  - Ring
- E.g. The field of real numbers (denoted as "R") with ordinary addition and multiplication.
- Hierarchy
  - Group -> Ring -> Field

Summary: Group, Ring and Field

- A group focuses on a single binary operation and is characterized by closure, associativity, identity, and inverses.
- A ring adds the concept of two operations (addition and multiplication) and maintains closure, associativity, and additional properties specific to rings. It may or may not have a multiplicative inverses for all elements.
- A field builds upon the ring structure but adds multiplicative inverses and a multiplicative identity, making it the most versatile and fundamental of the three structures.
  - Fields are particularly important because they encompass both addition and multiplication, and they play a crucial role in various mathematical and scientific applications, including number theory, linear algebra, and cryptography.

Galois Fields

- Galois Fields (Finite fields) play a key role in cryptography
- It 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 number of elements of a finite field is called its order or, sometimes, its size.
- A Galois field consists of a finite number of elements, denoted as "GF(p)," where “p" is a prime number (forms a Prime Field) or a power of a prime number (forms an Extension Field).
- Extension fields are constructed by defining irreducible polynomials over the prime field
- An irreducible polynomial is a polynomial that cannot be factored into two lower-degree polynomials with coefficients in the base field

Galois Fields GF(p)

- In particular often use the fields
  - GF(p)
  - GF(2^n)
- GF(p) is the set of integers Z_p ={0,1, … , p-1} with arithmetic operations modulo prime p
  - E.g. GF(7)={0,1,2,3,4,5,6}
- The arithmetic in GF is “well-behaved”
  - i.e. can do addition, subtraction, multiplication, and division without leaving the field GF(p)

GF(7) Addition/Multiplication Example

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

(a) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(c) Additive and multiplicative inverses modulo 7

Polynomial Arithmetic

- can compute using polynomials

  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum a_i x^i$

  - We are not interested in any specific value of x (known as the indeterminate)

- Different types of polynomial arithmetic that can be performed under various modular conditions

  1. ordinary polynomial arithmetic
  2. Polynomial Arithmetic with Coefficients Modulo p
  3. Polynomial Arithmetic with Coefficients Modulo p and Polynomials Modulo m (x)

Ordinary Polynomial Arithmetic

- add or subtract corresponding coefficients
- multiply all terms by each other
- E.g.

  let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

  $f(x) + g(x) = x^3 + 2x^2 - x + 3$

  $f(x) - g(x) = x^3 + x + 1$

  $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$

Polynomial Arithmetic with Modulo Coefficients

- Coefficients of the polynomial are reduced modulo a prime number p
- We are most interested in mod 2
  - i.e. all coefficients are 0 or 1
  - E.g. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

$$f(x) + g(x) = x^3 + x + 1$$

$$f(x) \times g(x) = x^5 + x^2$$

Polynomial Division

- If $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- Arithmetic modulo an irreducible polynomial forms a field (As discussed earlier)
- Consider the example of polynomial division, specifically polynomial division modulo another polynomial
    - x13+x11+x9+x8+x6+x5+x4+x3+1 **modulo** x8+x4+x3+x+1 (11B)
    - x7+x6+1=C1

Modular Polynomial Arithmetic

- In field GF(2^n)
  - working with polynomials that have coefficients modulo 2 and a degree less than n.
  - To perform multiplication, these polynomials must be reduced modulo an irreducible polynomial of degree n.
  - This process forms a finite field, where it is always possible to find an inverse for any non-zero element.
  - Additionally, Euclid's Inverse Algorithm can be extended to find these inverses.

Example GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

Computational Example

- In GF(2^3) have (x^2+1) is 101_2 & (x^2+x+1) is 111_2
- So addition is
  - (x^2+1) + (x^2+x+1) = x
  - 101 XOR 111 = 010_2
- And multiplication is
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$ (which is 1111)
- Polynomial modulo reduction (get q(x) & r(x)) is
  - (x^3+x^2+x+1) mod $(x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$ (which is 0100)

Euler Totient Function ø(n)

- When doing arithmetic modulo n
- **complete set of residues** is: `0..n-1`
- **Reduced set of residues** is; those numbers (residues) which are relatively prime to n (GCD should be 1)
  - e.g. for n=10,
  - Complete set of residues is {0,1,2,3,4,5,6,7,8,9}
  - Reduced set of residues is $Z_n^* = Z_{10}^* = \{1,3,7,9\}$
- **Number of elements** in reduced set of residues is called the **Euler Totient Function ø(n)**
- $\phi(1) = 1$ since for n = 1 the only integer in the range from 1 to n is 1 itself, and gcd(1, 1) = 1

Euler Totient Function ø(n) (Cont.)

- To compute ø(n) need to count number of residues to be excluded
- In general need prime factorization, but
  - For p (p prime) ø(p) = p-1
  - For p*q (p,q prime) ø(p*q) =(p-1)x(q-1)
- Multiplicative group Z**n** is denoted by Z**n***
- Examples

$|Z_{10}^*| = \phi(10)=\phi(2)*\phi(5)=(2-1)*(5-1)=4$

$|Z_{37}^*| = \phi(37) = 36$

$|Z_{21}^*| = \phi(21) = \phi(3)*\phi(7)=(3-1)x(7-1) = 2x6 = 12$

$|Z_{27}^*| = \phi(27) = \phi(3^3)= 3^2*\phi(3)= 9*2 = 18$

(for a prime p, ϕ(p^n) = (p^(n-1))*ϕ(p)

Find ø(135) and ø(115)

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_z}\right)$$

Euler's Theorem

- Also known as the **Fermat–Euler Theorem** or **Euler's Totient Theorem**
- States that if *n* is a positive integer and *a* is a positive integer relatively prime to *n* (i.e. gcd (a,n)=1), then $a^{\phi(n)} \equiv 1 \pmod{n}$
- e.g.

  a=3;*n*=10 (3 is relative prime to 10)

  ø(10)=ø(2) x ø(5)=4;

  hence $3^4 = 81 \equiv 1 \bmod 10$

  a=2;*n*=11;

  ø(11)=10 (2 is relative prime to 11)

  hence $2^{10} = 1024 \equiv 1 \bmod 11$

Modular Multiplicative Inverse

- The modular multiplicative inverse of A mod C is the B value that makes A * B mod C = 1
- **Example: A=3, C=7** **Calculate A * B mod C for B values 0 through C-1**

  3 * 0 ≡ 0 (mod 7)

  3 * 1 ≡ 3 (mod 7)

  3 * 2 ≡ 6 (mod 7)

  3 * 3 ≡ 9 ≡ 2 (mod 7)

  3 * 4 ≡ 12 ≡ 5 (mod 7)

  3 * 5 ≡ 15 (mod 7) ≡ 1 (mod 7) <------ FOUND INVERSE!

  3 * 6 ≡ 18 (mod 7) ≡ 4 (mod 7)
- **Example: A=2 C=6** **Calculate A * B mod C for B values 0 through C-1**

  2 * 0 ≡ 0 (mod 6)

  2 * 1 ≡ 2 (mod 6)

  2 * 2 ≡ 4 (mod 6)

  2 * 3 ≡ 6 ≡ 0 (mod 6)

  2 * 4 ≡ 8 ≡ 2 (mod 6)

  2 * 5 ≡ 10 ≡ 4 (mod 6)

  No value of B makes A * B mod C = 1. Therefore, A has no modular inverse (mod 6). This is because 2 is not coprime to 6 (they share the prime factor 2).

Extended Euclidean Algorithm

- It is easy to find multiplicative inverse for small value of n by just constructing multiplication table.
- But this method is not practical for large value of n. so for that we need Extended Euclidean algorithm.
- Euclidean Algorithm can be extended so that in addition to finding gcd(m,b), if gcd is 1, the algorithm returns the multiplicative inverse of b.

Finding Inverses – Extended Euclidean algorithm

```
EXTENDED_EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 -
   Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Inverse of 49 in GF(37)

i.e. calling Extended_Euclid(37, 49)

Q	A1	A2	A3	B1	B2	B3
—	1	0	37	0	1	49
0	0	1	49	1	0	37
1	1	0	37	-1	1	12
3	-1	1	12	4	-3	1

- Hence $49^{-1} \equiv (-3) \bmod 37$
- But, $-3 \pmod{37} \equiv 34 \pmod{37}$. Hence,

multiplicative inverse of 49 modulo 37 is 34.

Inverse of 550 in GF(1759)

i.e. calling Extended_Euclid(1759, 550)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	355	1

Primitive Roots

- A primitive root is any number g in multiplicative group that generates whole group of integers
- e.g. $Z_{14}^*=\{1,3,5,9,11,13\}$

  Calculate n^k mod 14 for k=1 to ø(n) (i.e. k=1 to 6)

  1 : 1

  3 : 3, 9, 13, 11, 5, 1

  5 : 5, 11, 13, 9, 3, 1

  9 : 9, 11, 1

  11 : 11, 9, 1

  13 : 13, 1

  Thus, **3 and 5 are primitive roots** modulo 14

Discrete Logarithms

- Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the digital signature algorithm (DSA).
- The inverse problem to exponentiation is to find the **discrete logarithm** of a number modulo p
- That is to find x such that $y = g^x \pmod p$
  - This is written as $x = \log_g y \pmod p$
- If **g is a primitive root then it always exists**, otherwise it may not,
  - e.g.
    $x = \log_3 4 \bmod 13$ has no answer !
    $x = \log_2 3 \bmod 13 = 4$ (i.e. $3=2^x \bmod 13$ $3=2^4 \bmod 13$)
- Exponentiation is relatively easy, but finding discrete logarithms is generally a **hard** problem
- Problems with this type of asymmetry are very rare, but are of critical usefulness in modern cryptography.

n	n - 1	b^{n-1}	$b^{n-1} \bmod p$
1	0	$2^0 = 1$	$2^0 \bmod 13 = \mathbf{1}$
2	1	$2^1 = 2$	$2^1 \bmod 13 = \mathbf{2}$
3	2	$2^2 = 4$	$2^2 \bmod 13 = \mathbf{4}$
4	3	$2^3 = 8$	$2^3 \bmod 13 = \mathbf{8}$
5	4	$2^4 = 16$	$2^4 \bmod 13 = \mathbf{3}$
6	5	$2^5 = 32$	$2^5 \bmod 13 = \mathbf{6}$
7	6	$2^6 = 64$	$2^6 \bmod 13 = \mathbf{12}$
8	7	$2^7 = 128$	$2^7 \bmod 13 = \mathbf{11}$
9	8	$2^8 = 256$	$2^8 \bmod 13 = \mathbf{9}$
10	9	$2^9 = 512$	$2^9 \bmod 13 = \mathbf{5}$
11	10	$2^{10} = 1024$	$2^{10} \bmod 13 = \mathbf{10}$
12	11	$2^{11} = 2048$	$2^{11} \bmod 13 = \mathbf{7}$