CHAPTER 6

UNIT 4

Basic Number Theory

Syllabus :

Modular arithmetic, Solving ax + by = d, Congruences, Chinese Remainder Theorem, Modular Exponentiation, Fermat's Little and Euler Theorem, Prime Number Generation, Random Number Generation, Primitive Roots, Legendre and Jacobi Symbols, Discrete Probability, Discrete Logarithms.

6.1 Basic Notations :

The encryption process, makes use of mathematical operations to convert input numerical values into output numerical values. First we will discuss some basic notations used in number theory.

6.1.1 Divisibility :

Let 'a' and 'b' are integers and $a \neq 0$. Then 'a' divides 'b' is denoted by a/b.

Definition : 'a' divides 'b' if integer k exists such that b = ak. Alternatively, 'a' divides 'b' such that 'b' is multiple of 'a'.

Example :

1. 8/72

   Here a = 8, b = 72.

   'a' divides 'b' because k = 9 exists such that b (72) = ak (8×9)

2. 5/30

   Here a = 5, b = 30.

   a/b, because k = 6 and b = ak that means $30 = 5 \times 6$.

3. 5/19

   Here a/b is not valid because there is no integer k such that b = ak.

Properties of divisibility :

1. For every $a \neq 0$, a/0 and a/a. Similarly 1/b for every b.
2. If a/b and b/c then a/c.
3. If a/b and a/c then a/ (sb + tc) for all integers s and t
4. For every $c \neq 0$, a/b if and only if ca/cb.

5. Bigger number cannot divide the smaller positive number.
6. Only zero is divisible by zero.

6.1.2 Prime Numbers :

- Any integer p such that $p > 1$ is called as prime number if p is divisible by 1 and itself.
- An integer, which is not prime number is called as composite.

Prime number theorem :

Let $\pi(x)$ denotes the number of primes less than x then

$$\pi(x) \approx \frac{x}{\ln x}$$

And the ratio $\pi(x) \mid (x \mid \ln x) \to 1$ as $x \to \infty$.

- Every positive integer can be expressed as the product of prime numbers raised to different powers.

  Example $9720 = 2^3 3^5 5$, $504 = 3^2 \times 2^3 \times 7$
- This factorization into primes is unique and reordering of factors can be done.
- If a prme p, divides a product ab.....z then p must divide one of the factors a, b ....z.
- If the product of two integers is even then one of the integers must be even.

6.1.3 Greatest Common Divisor (gcd) :

- The greatest common division of 'a' and 'b' is denoted by gcd (a, b) or (a, b). It is the largest positive integer that divides both 'a' and 'b'.
- If gcd (a, b) = 1 then integers 'a' and 'b' are called as **relative prime numbers.**
- To find gcd of integers 'a' and 'b' ; factorize 'a' and 'b' into primes. Then take a common prime divisor having smallest exponent. It is gcd.

Example : gcd (9720, 504) = gcd $(2^3 3^5 5, 3^2 2^3 7)$

Here gcd is 2^3.

- If it is not easy to factorize, then **Euclidean algorithm** is used.

Ex. 6.1.1 : Suppose we want gcd (385, 1270)

Soln. :

Divide 1270 by 3 and 5

$$\therefore \quad 385 \overline{)\,1270\,(3} \qquad \text{(E-1281)}$$
$$\underline{1155}$$
$$115$$

Here quotient is 3 and remainder is 115

$$\therefore \quad 1270 = 3.385 + 115$$

Then divide 385 by 115

$$115 \overline{)\,385\,(3} \qquad \text{(E-1282)}$$
$$\underline{345}$$
$$40$$

Quotient is 3 and remainder is 40

$$\therefore \quad 385 = 3.115 + 40$$

Now divide 115 by 40

$$\begin{array}{r|l} 40 & 115 \quad (2 \\ & \underline{80} \\ & 35 \end{array}$$ (E-1283)

The quotient is 2 and remainder is 35

$$\therefore \quad 115 = 2.40 + 35$$

Divide 40 by 35

$$\begin{array}{r|l} 35 & 40 \quad (1 \\ & \underline{35} \\ & 5 \end{array}$$ (E-1284)

← Last nonzero remainder

Here quotient is 1 and remainder is 5

$$\therefore \quad 40 = 1.35 + 5$$

Divide 35 by 5

$$\begin{array}{r|l} 5 & 35 \quad (7 \\ & \underline{35} \\ & 0 \end{array}$$ (E-1285)

← zero remainder

Now we have got zero remainder

$$\therefore \quad 35 = 7.5 + 0$$

The last non zero remainder is gcd. It is 5.

Thus gcd (385, 1270) = 5

- The generalized form can be expressed as follows :
- Suppose we want to calculate gcd (a, b) and a > b. If a is not greater than 'b' then simply change the positions of 'a' and 'b'.
- Initially express 'a' as

$$a = q_1 b + r_1$$

- Here q_1 is the quotient and r_1 is remainder. If r_1 is zero then gcd is b. But if $r_1 \neq 0$ then b as,

$$b = q_2 r_1 + r_2$$

- This procedure is continued, till zero remainder is obtained.

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \quad \vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$ (E-1286)

The gcd is r_k.

- The following fundamental theorems are based an Euclidean algorithm.
  1. If 'a' and 'b' are relatively prime numbers then there exists an integer x and y such that ax + by = 1.
  2. If 'p' is a prime and 'p' divides the product of two integers ab then either 'p' divides 'a' or 'p' divides 'b'.

6.2 Modular Arithmetic or Congruences :

New Syll. : MU : May 14

- Modulation arithmetic is one of the basic notations used in the number theory.
- Consider 'n' is any positive integer. Consider also that 'a' is some other integer. Then a mod n is defined as the remainder when 'a' is divided by 'n'.
- The symbol is a (MODn)

  Example : 6 = 16 (MOD10)
- a (mod n) denotes the smallest positive number x such that,

  $x \equiv a \pmod{n}$
- $x \equiv b \bmod m$ is an equivalence relation with many solutions. For x, while $x = b \bmod m$ is an equality.
- If n is positive integer then for other two integers a and b ; a is congruent to b mod n is denoted by,

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

- If is said that a is congruent to b mod n if a-b is either positive or negative multiple of n.

$$\text{Example } 42 \equiv 7 \pmod{5}$$

$$\text{Here } a = 42,\ b = 7 \text{ and } n = 5$$

$$a-b = 35 \text{ and it is multiple of } 5.$$

  Thus 42 is congruent to 7 mod 5.
- Alternately we can say that a is congruent to b mod n if a and b differ by a multiple of n.
- Thus $a \equiv b \pmod{n}$ can also be expressed as,

  $a = b + nk$; where k is an integer.

  Example : $-19 \equiv 37 \pmod{7}$

  Here $a = -19,\ b = 37,\ n = 7$

  Now $a = b + nk$

$$\therefore -19 = 37 + 7k$$

$$\therefore -56 = 7k$$

$$\therefore k = -8$$

  Since k is an integer ; – 19 is congruent to 37 mod 7.
- The set of all integers congruent to a (mod n) is called as residue class [a].
- The residue classes mod 5 are,

$$[0] = \{\ldots,-10,-5,0,5,10,\ldots\}$$

$$[1] = \{\ldots,-11,-6,1,6,11,\ldots\}$$

$$[2] = \{\ldots,-12,-7,2,7,12,\ldots\}$$

6.2.1 Properties of Congruences :

Consider integers a, b, c, n and $n \neq 0$. Then

1. $a \equiv 0 \pmod{n}$ if and only if n/a

   Here $a = a - 0$ is a multiple of n. This answer is same as n/a.

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

   Here $a - a = 0 = 0 \cdot n$

3. $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$

   Here $a \equiv b \pmod{n}$ can be expressed as,

   $$a - b = nk$$

   $$\therefore b - a = (-k)n$$

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

4. If $a \equiv b$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$

   Here $a \equiv b$ can be written as,

   $$a = b + nk$$

   Similarly, $b \equiv c$ can be written as

   $$c = b + nm$$

   Then $a - c = n(k - m)$

   Thus $a \equiv \pmod{n}$

6.2.2 Properties of Modular Arithmetic :

- The set $Z_n = \{0, 1, 2 \ldots\ldots n\text{-}1\}$ is called as integers mod n.
- Consider 'a' and 'n' are integers then, after dividing a by n, suppose the quotient is q and remainder is r.

  $$\therefore a = nq + r \text{ with } 0 \leq r \leq n$$

- Here every number 'a' is congruent mod n to some integer 'r' such that $0 \leq r < n$.
- Consider integers a, b, c, d, n and $n \neq 0$ then,
  1. $a + c \equiv b + d$
  2. $a - c \equiv b - d$
  3. $ac \equiv bd$
- Suppose we have two numbers (a and b) and we want to perform addition mod n ; then start adding two numbers as integers.
- If addition (a + b) is equal to n then answer is zero.
- If addition (a + b) is greater than (n – 1) then answer is n – 1.

- The following table shows addition mod 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

- Consider two numbers and let us perform multiplication of these two numbers mod n.
- Starts multiplying these numbers as integers. If the product is equal to 'n' then answer is zero. If the product is larger than n – 1 then divide by n and take the remainder.
- A table for multiplication mod-8 is as follows :

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	3	3
6	0	6	4	2	0	6	4	0
7	0	7	6	5	4	5	2	7

- For performing the division ; it is possible to divide by a (mod n) if gcd (a, n) = 1.
- If 'a' and 'n' are relatively prime then we can divide both sides of the congruence by a.
- A fraction b/a mod n can be performed if gcd (a, n) = 1. Here b/a mod n can be written as b^{-1} a (mod n) and a^{-1} indicates integer mod n which satisfies the condition a^{-1} a $\equiv$ 1 (mod n).

6.3 Solving ax + by = d :

- To solve the equations ax + by = d ; an extended Euclidean algorithm is used.
- In earlier Euclidean algorithm ; we have not used the quotients.
- In Euclidean algorithm we have used following steps.

$$a = q_1 b + r_1 \quad , \quad 0 < r < b$$

$$b = q_2 r_1 + r_2 \quad , \quad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \quad , \quad 0 < r_3 < r_2$$

$$r_2 = q_4 r_3 + r_4 \quad , \quad 0 < r_4 < r_3$$

$$\vdots \qquad \text{(E-1288)}$$

$$r_i = q_{i+2} r_{i+1} + r_{i+2} \quad , \quad 0 < r_{i+2} < r_{i+1}$$

- In the Euclidean algorithm ; if we have two integers 'a' and 'b' ; there exists integers x and y such that,

$$ax + by = \gcd(a, b) \quad \ldots(6.3.1)$$

- We have calculated gcd (385, 1270). It is as follows

$$1270 = 3.385 + 115$$
$$385 = 3.115 + 40$$
$$115 = 2.40 + 35$$
$$40 = 1.35 + 5$$
$$35 = 7.5 + 0$$

- Here the last non-zero remainder is 5 ; so gcd of (385, 1270) is 5.
- The different quotients are, $q_1 = 3$, $q_2 = 3$, $q_3 = 2$, $q_4 = 1$, $q_5 = 7$.
- Now consider the following equations,

$$x_0 = 0, \quad x_1 = 1, \quad x_j = -q_{j-1} x_{j-1} + x_{j-2} \quad \ldots(6.3.2)$$

and $$y_0 = 1, \quad y_1 = 0, \quad y_j = -q_{j-1} y_{j-1} + y_{j-2} \quad \ldots(6.3.3)$$

- Using Equation (6.3.1) we can write,

$$a x_n + b y_n = \gcd(a, b) \quad \ldots(6.3.4)$$

- Using Equation (6.3.2) we get,

$$x_0 = 0, \quad x_1 = 1$$

For $j = 2 \Rightarrow$

$$x_2 = -q_{2-1} x_{2-1} + x_{2-2}$$
$$\therefore x_2 = -q_1 x_1 + x_0$$
$$\therefore x_2 = -(3 \times 1) + 0 = -3$$

For $j = 3 \Rightarrow$

$$x_3 = -q_{3-1} x_{3-1} + x_{3-2}$$
$$\therefore x_3 = -q_2 x_2 + x_1$$
$$\therefore x_3 = -3(-3) + 1 = 10$$

For $j = 4 \Rightarrow$

$$x_4 = -q_{4-1} x_{4-1} + x_{4-2}$$
$$\therefore x_4 = -q_3 x_3 + x_2$$
$$\therefore x_4 = -2 \times (10) + (-3) = -23$$

For $j = 5 \Rightarrow$

$$x_5 = -q_{5-1} x_{5-1} + x_{5-2}$$
$$\therefore x_5 = -q_4 x_4 + x_3$$
$$\therefore x_5 = -1(-23) + 10 = 33$$

- Similarly using Equation (6.3.3), we get,

$$y_0 = 1, \quad y_1 = 0$$

For $j = 2 \Rightarrow$

$$y_2 = -q_{2-1} y_{2-1} + y_{2-2}$$
$$\therefore y_2 = -q_1 y_1 + y_0$$
$$\therefore y_2 = -3 \times (0) + 1 = 1$$

For $j = 3 \Rightarrow$

$$y_3 = -q_{3-1} y_{3-1} + y_{3-2}$$
$$\therefore y_3 = -q_2 y_2 + y_1$$
$$\therefore y_3 = -3 \times 1 + 0 = -3$$

For j = 4 ⇒

$$y_4 = -q_{4-1}\, y_{4-1} + y_{4-2}$$

$$\therefore\ y_4 = -q_3\, y_3 + y_2$$

$$\therefore\ y_4 = -2(-3) + 1 = 7$$

For j = 5 ⇒

$$y_5 = -q_{5-1}\, y_{5-1} + y_{5-2}$$

$$\therefore\ y_5 = -q_4\, y_4 + y_3$$

$$\therefore\ y_5 = -1 \times 7 + (-3) = -10$$

- Now we have a = 385 and b = 1270.

  Using Equation (6.3.4), for n = 5 we get,

  $$ax_5 + by_5 = (385 \times 33) + [1270 \times (-10)] = 5$$

- It is gcd of (385, 1270).

  Thus, $ax + by = \gcd(a, b)$

- This method is also called as extended extended Euclidean algorithm.

6.4 Chinese Remainder Theorem :

- Sometimes it is convenient to break a congruence mod n into subsystems of congurances mod factor of n.
- Consider that the number x satisfies the relation,

  $$x \equiv 15 \pmod{44}$$

- Thus we can write the equation as,

  $$x = 15 + 44k$$

  Here k is some integer.
- Now we can write 44 as 11×4 or 4×11
- The equation, $x = 15 + 11(4k)$ can be expressed as,

  $$x \equiv 15 \equiv 4 \pmod{11}$$

- Similarly the equation, $x = 15 + 4(11k)$ can be expressed as,

  $$x \equiv 15 \equiv 3 \pmod{4}$$

  $$\text{Thus, } x \equiv 15 \pmod{44} = \begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{4} \end{cases}$$

- In this case, we have divided single congruence into number of congruences.
- The Chinese remainder theorem shows that, the number of congruences can be replaced by single congruence, under certain conditions.
- That means for Chinese remainder theorem, reverse procedure is applied.

Statement :

Suppose gcd (m, n) = 1. Given integers 'a' and 'b', there exists exactly one solution x (mod mn) for the simultaneous congruence's, $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$

Proof :

- Consider that, there exists two integers s, t such that ms + nt = 1