NARSIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS INSTITUTION
Maisammaguda (V), Kompally - 500100, Secunderabad, Telangana State, India
UGC - Autonomous Institute
Accredited by NBA & NAAC with 'A' Grade
Approved by AICTE
Permanently affiliated to JNTUH

UNIT- I
Basics of Number Theory

Greatest Common Divisors, Prime Factorization and Congruences

Greatest Common Divisor (GCD):

The Greatest Common Divisor is used to determine the **largest common factor shared by two or more numbers**. It plays an important role in number theory, algebra, cryptography, and computer science. The GCD helps simplify fractions, solve Diophantine equations, and determine whether two numbers are relatively prime.
There are several methods for finding the GCD, including:

- **Listing common factors**
- **Prime factorization**
- **Euclidean Algorithm** (the fastest and most efficient method)

The **Greatest Common Divisor (GCD)** of two integers is the largest positive integer that divides both numbers.

Notation: GCD(a , b)

Finding GCD by Listing Factors:

Ex1 : Find GCD of 18 and 30.

Factors of 18 : 1,2,3,6,9,18

Factors of 30 : 1,2,3,5,6,10,15,30

Common factors: 1,2,3,6

Hence, gcd(18,30)=6

Problem 2: Find the GCD of **60 and 84**.

Solution: Prime factorization: $60 = 2^2 \times 3 \times 5$

$84 = 2^2 \times 3 \times 7$

Common prime factors: $2^2 \times 3$

Therefore $\boxed{\gcd(60,84) = 12}$

Example 3: Find the GCD of 24, 36, and 60.

Solution **:**First, $\gcd(24,36) = 12$

Then, $\gcd(12,60) = 12$

Therefore $\boxed{\gcd(24,36,60) = 12}$

Example 4: Find Whether Two Numbers are Co-prime 35 and 64

Solution Prime factorization:

$$35 = 5 \times 7$$
$$64 = 2^6$$

There are no common prime factors.

Hence,

$$\boxed{\gcd(35,64) = 1}$$

Since the GCD is 1, **35 and 64 are co-prime numbers**.

Example 5: A shopkeeper has 72 chocolates and 48 biscuits. He wants to pack them into identical gift boxes without any leftovers. Find the greates t number of gift boxes he can make.

Solution :

Find the GCD of 72 and 48.

Using the Euclidean Algorithm:

$$72 = 48 \times 1 + 24$$
$$48 = 24 \times 2 + 0$$

Thus,

$$\boxed{\gcd(72,48) = 24}$$

So, the greatest number of gift boxes is $\boxed{24}$
Each box contains:

- Chocolates: $\frac{72}{24} = 3$

- Biscuits: $\frac{48}{24} = 2$

Answer: 24 gift boxes, each with **3 chocolates and 2 biscuits**.

Example 6: Find the GCD of Large Numbers 840 and 360

Solution : Using the Euclidean Algorithm:

$$840 = 360 \times 2 + 120$$
$$360 = 120 \times 3 + 0$$

Therefore, $\boxed{\gcd(840,360) = 120}$

Example 7: Find the GCD 126 and 210 Using Prime Factorization .

Solution:

Prime factorization:

$$126 = 2 \times 3^2 \times 7$$
$$210 = 2 \times 3 \times 5 \times 7$$

Common prime factors:

$$2 \times 3 \times 7$$

Therefore, $\boxed{\gcd(126,210) = 42}$

Properties of GCD :

1. GCD is always positive.
2. GCD(a,0) = a
3. GCD (a , b) = GCD (b, a)
4. If GCD(a, b)=1, then a and b are relatively prime.

Euclidean Algorithm:

Definition: The Euclidean Algorithm is an efficient method for finding the Greatest Common Divisor (GCD) of two positive integers. It is based on the principle that the GCD of two numbers does not change if the larger number is replaced by its remainder when divided by the smaller number.

The algorithm repeatedly divides the larger number by the smaller number and replaces the larger number with the remainder until the remainder becomes zero. The last non-zero remainder is the GCD of the given numbers.

Mathematical Statement

For two positive integers $\boldsymbol{a}$and $\boldsymbol{b}(\boldsymbol{a} > \boldsymbol{b})$,

$$\boldsymbol{a} = \boldsymbol{bq} + \boldsymbol{r}, \boldsymbol{0} \leq \boldsymbol{r} < \boldsymbol{b}$$

where:

- $\boldsymbol{q}$= Quotient
- $\boldsymbol{r}$= Remainder

Then , $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b}) = \mathbf{gcd}(\boldsymbol{b}, \boldsymbol{r})$
This pocess is repeated until $\boldsymbol{r} = \boldsymbol{0}$. The last non-zero remainder is the GCD.

Example :

1. Find GCD(252,105)

Sol: 252 = 105×2 +42

105 = 42×2 +21

42 =21×2 +0

Therefore, GC D (252,105) = 21

Example :2 Find GCD(391,299)

Sol: 391 =299×1+92

299 =92×3+23

92 =23×4+0

Hence GCD(391,299) = 23

Fundamental Theorem of Arithmetic

Definition :

The Fundamental Theorem of Arithmetic states that:

Every integer greater than 1 is either a prime number or can be expressed as a product of prime numbers in a unique way, except for the order of the prime factors.

In other words, every composite number can be written as a product of prime numbers, and this prime factorization is unique.

For every integer $\boldsymbol{n > 1}$, $\boldsymbol{n = p_1 p_2 p_3 \cdots p_k}$ where $\boldsymbol{p_1, p_2, \ldots, p_k}$ are prime numbers.

If $\boldsymbol{n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m}$, then both factorizations contain the same prime numbers with the same exponents, differing only in the order of the factors.

Example 1:

Find GCD of 60 by using Fundamental theorem of Arithmetic.

Prime factorization: $60=2\times2\times3\times5$

or

$60=2^2\times3\times5$.

Example 2 : Find the prime factorization of 450.
Solution:

$$450 = 2 \times 225$$
$$225 = 3 \times 75$$
$$75 = 3 \times 25$$
$$25 = 5 \times 5$$

Hence,

$$450 = 2 \times 3 \times 3 \times 5 \times 5$$
$$\boxed{450 = 2 \times 3^2 \times 5^2}$$

Prime Factorization Method :

Divide repeatedly by the smallest prime.

Ex: **Find GCD of 180 by using Prime Factorization Method**

$180\div2=90$

$90 \div 2 = 45$

$45 \div 3 = 15$

$15 \div 3 = 5$

$5 \div 5 = 1$

Hence $180 = 2^2 \times 3^2 \times 5$.

Ex : Find Using Prime Factorization to Find GCD (48 , 72).

$48 = 2^4 \times 3$

$72 = 2^3 \times 3^2$

Take common minimum powers $2^3 \times 3 = 24$

Hence GCD (48 , 72) = 24 .

Fermat Numbers

Definition :

A Fermat number is a positive integer of the form

$$F_n = 2^{2^n} + 1, n = 0, 1, 2, \ldots$$

where $n$is a non-negative integer.

These numbers were introduced by the French mathematician Pierre de Fermat, who conjectured that all numbers of this form are prime. However, this conjecture was later disprove

First Few Fermat Numbers :

N	Fermat Number
0	$2^{2^0} + 1 = 3$
1	$2^{2^1} + 1 = 5$
2	$2^{2^2} + 1 = 17$
3	$2^{2^3} + 1 = 257$
4	$2^{2^4} + 1 = 65537$

Congruences :

Definition

Congruence is a relation between two integers that have the same remainder when divided by a positive integer (called the modulus).

Two integers $\boldsymbol{a}$and $\boldsymbol{b}$are said to be congruent modulo $\boldsymbol{m}$if their difference is exactly divisible by $\boldsymbol{m}$.

Mathematical Definition

Let $\boldsymbol{a}$, $\boldsymbol{b}$ be integers and $\boldsymbol{m}$ be a positive integer ($\boldsymbol{m > 1}$).

Then, $\boxed{\boldsymbol{a \equiv b (\mathrm{mod} m)}}$

if and only if $\boxed{\boldsymbol{m \mid (a - b)}}$

That is, $\boldsymbol{m}$divides the difference $(\boldsymbol{a-b})$.

The symbol for congruence is $\boxed{\equiv}$

and it is read as: "$\boldsymbol{a}$ is congruent to $\boldsymbol{b}$modulo $\boldsymbol{m}$."

Ex 1: Find $17 \equiv 5 (\mathrm{mod}\ 12)$

Because $17-5=12$

and 12 is divisible by 12.

Ex 2 : Find $25 \equiv 1 (\mathrm{mod}\ 8)$

Because $25-1=24$

and

24 is divisible by 8.

Properties of Congruence :

If $a \equiv b (\mathrm{mod}\ n)$

Then Addition $a+c \equiv b+c (\mathrm{mod}\ n)$

Subtraction $a-c \equiv b-c (\mathrm{mod}\ n)$

Multiplication $ac \equiv bc (\mathrm{mod}\ n)$

Linear Congruence :

A linear congruence is a congruence of the form

$$\boxed{ax \equiv b(\mathrm{mod} m)}$$

where:

- a, b, and $m$are integers,
- $m > 1$is called the modulus,
- $x$is the unknown integer to be determined.

A linear congruence asks us to find all integers $x$that satisfy the congruence relation.

General Form $\boxed{ax \equiv b(\mathrm{mod} m)}$

where:

- a= coefficient of x
- b= constant term
- m= modulus

Solution exists only if GCD(a , n)|b

Ex 1: Solve 3x ≡ 6(mod 9)

Since GCD(3,9) = 3

and

3 divides 6

Solution exists.

Divide by 3

X ≡ 2(mod 3)

Henc e x=2,5,8,…

Ex 2 : Solve 5x≡3(mod 7)

Inverse of 5 modulo 7 is 3.

Multiply both sides by 3.

X ≡ 9 ≡ 2(mod7)

Answer x≡2(mod 7).

Example1:Show that $29 \equiv 5(\mathbf{mod} 12)$
Solution :

Find the difference: $29 - 5 = 24$

Since $24 = 12 \times 2,$

12 divides 24 exactly.

Therefore, $\boxed{29 \equiv 5(\text{mod}12)}$

Example 2: Show that $43 \equiv 8(\text{mod}7)$

Solution $43 - 8 = 35$

Since $35 = 7 \times 5,$

7 divides 35.

Hence, $\boxed{43 \equiv 8(\text{mod}7)}$

Example 3: Check whether $35 \equiv 6(\text{mod}10)$

Solution : $35 - 6 = 29$

Since $10 \nmid 29,$

the congruence is **false**.

Answer *is* $\boxed{35 \equiv /6(\text{mod}10)}$

Example 4: Find the remainder when 125 is divided by 8.

Solution: $125 = 8 \times 15 + 5$

Hence, $125 \equiv 5(\text{mod}8)$

Answer **is** 5

Example 5: Solve Linear Congruence $3x \equiv 12(\text{mod}9)$

Solution :

Since $12 \equiv 3(\text{mod}9)$

the congruence becomes $3x \equiv 3(\text{mod}9).$

Divide both sides by 3 (since $\gcd(3,9) = 3$divides 3):

$$x \equiv 1(\text{mod}3).$$

Therefore,

$$\boxed{x = 1, 4, 7(\text{mod}9)}$$

Example 6: Find the solution of -15≡ -84(mod 7)

Sol : Reduce both sides modulo 7

Reduce the coefficients:

$$-15 \equiv -1 \equiv 6(\text{mod}7)$$

since $-15 + 21 = 6$.

Also,

$$-84 \equiv 0(\text{mod}7)$$

because $-84$is divisible by 7.
Thus, the congruence becomes

$$6x \equiv 0(\text{mod}7).$$

Find the multiplicative inverse of 6 modulo 7
Since

$$6 \times 6 = 36 \equiv 1(\text{mod}7),$$

the inverse of 6 modulo 7 is 6.
Multiply both sides by 6:

$$x \equiv 0(\text{mod}7).$$

Final Answer

$$\boxed{x \equiv 0(\text{mod}7)}$$

Example 7 : Find all possible solutions of the linear congruence 14x≡12(mod 18)

Sol: Given

$$a = 14, b = 12, m = 18$$

Calculate

$$\gcd(14,18) = 2$$

Since

$$2 \mid 12,$$

the congruence has **2 incongruent solutions modulo 18**.

Step 2: Divide the congruence by the GCD
Divide by 2:

$$7x \equiv 6(\text{mod}9)$$

Step 3: Find the inverse of 7 modulo 9
We need a number $k$such that

$$7k \equiv 1(\text{mod}9).$$

Since

$$7 \times 4 = 28 \equiv 1(\text{mod}9),$$

the inverse of 7 modulo 9 is **4**.
Multiply both sides by 4:

$$x \equiv 4 \times 6$$
$$x \equiv 24$$
$$x \equiv 6(\text{mod}9).$$

Step 4: Write all solutions modulo 18
Since $d = 2$, there are two solutions:

$$x = 6,\ 6 + 9 = 15.$$

Hence,

$$\boxed{x \equiv 6,\ 15(\text{mod}18)}$$

Example 9 : Solve the system of linear congruences

$$\mathbf{2x + 4y \equiv 5(mod13)}$$
$$\mathbf{2x + 5y \equiv 7(mod13)}$$

Sol : **Eliminate x**
Subtract the first equation from the second:

$$(2x + 5y) - (2x + 4y) \equiv 7 - 5(\text{mod}13)$$
$$y \equiv 2(\text{mod}13)$$

Thus, $\boxed{y = 2}$

Step 2: Find x
Substitute $y = 2$into the first equation:

$$2x + 4(2) \equiv 5(\text{mod}13)$$
$$2x + 8 \equiv 5(\text{mod}13)$$
$$2x \equiv -3(\text{mod}13)$$

Since

$$-3 \equiv 10(\text{mod}13),$$

we get

$$2x \equiv 10(\text{mod}13).$$

Step 3: Find the inverse of 2 modulo 13
Since

$$2 \times 7 = 14 \equiv 1(\text{mod}13),$$

the inverse of 2 is **7**.
Multiply both sides by 7:

$$x \equiv 7 \times 10$$
$$x \equiv 70$$
$$70 \equiv 5(\text{mod}13).$$

Therefore, $\boxed{x = 5}$

Verification

First equation:

$$2(5) + 4(2) = 10 + 8 = 18 \equiv 5(\text{mod}13)$$

Second equation:

$$2(5) + 5(2) = 10 + 10 = 20 \equiv 7(\text{mod}13)$$

Example 10: Find the value of x if possible, such that

x≡4(mod 6)

x≡2(mod 8)

x≡1(mod 7).

Sol :

Solve the first two congruences

Given

$$x \equiv 4(\text{mod}6)$$
$$x \equiv 2(\text{mod}8)$$

Let

$$x = 6k + 4.$$

Substitute into the second congruence:

$$6k + 4 \equiv 2(\text{mod}8)$$
$$6k \equiv -2 \equiv 6(\text{mod}8).$$

Divide both sides by 2:

$$3k \equiv 3(\text{mod}4).$$

Since the inverse of 3 modulo 4 is 3,

$$k \equiv 1(\text{mod}4).$$

Hence,

$$k = 4t + 1.$$

Therefore,

$$x = 6(4t + 1) + 4$$
$$x = 24t + 10.$$

Thus,

$$\boxed{x \equiv 10(\text{mod}24)}.$$

Step 2: Use the third congruence

Now solve

$$x \equiv 10(\text{mod}24)$$

and

$$x \equiv 1(\text{mod}7).$$

Let

$$x = 24t + 10.$$

Substitute into the third congruence:

$$24t + 10 \equiv 1(\text{mod}7).$$

Since

$$24 \equiv 3(\text{mod}7), 10 \equiv 3(\text{mod}7),$$

we get

$$3t + 3 \equiv 1(\text{mod}7).$$
$$3t \equiv -2 \equiv 5(\text{mod}7).$$

The inverse of 3 modulo 7 is 5 because

$$3 \times 5 = 15 \equiv 1(\text{mod}7).$$

Multiply both sides by 5:

$$t \equiv 25 \equiv 4(\text{mod}7).$$

Hence, $t = 7m + 4.$

Substitute into $x = 24t + 10$:

$$x = 24(7m + 4) + 10$$
$$= 168m + 96 + 10$$
$$= 168m + 106.$$

Therefore, $\boxed{x \equiv 106(\text{mod}168)}$