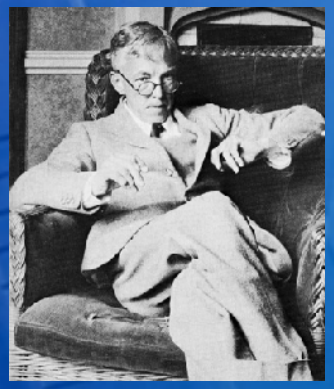
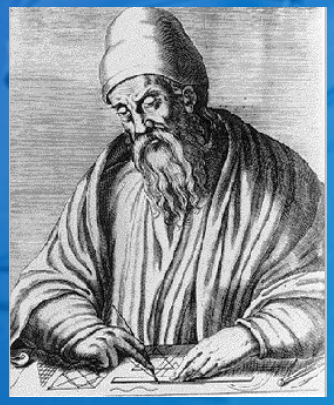
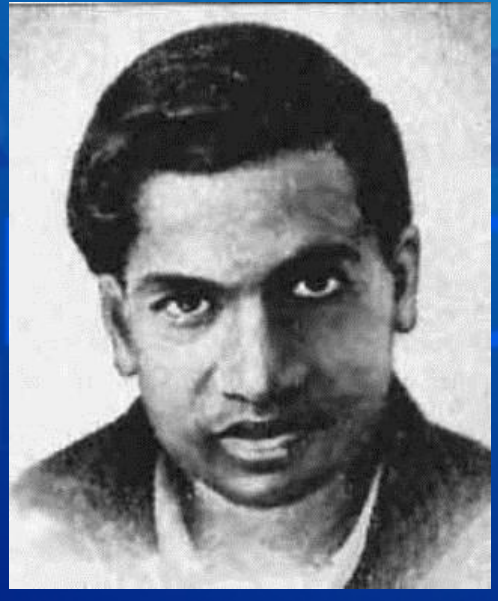
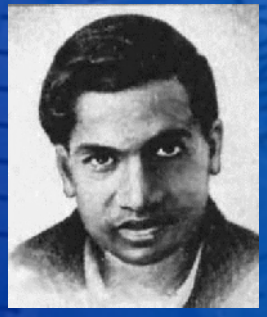



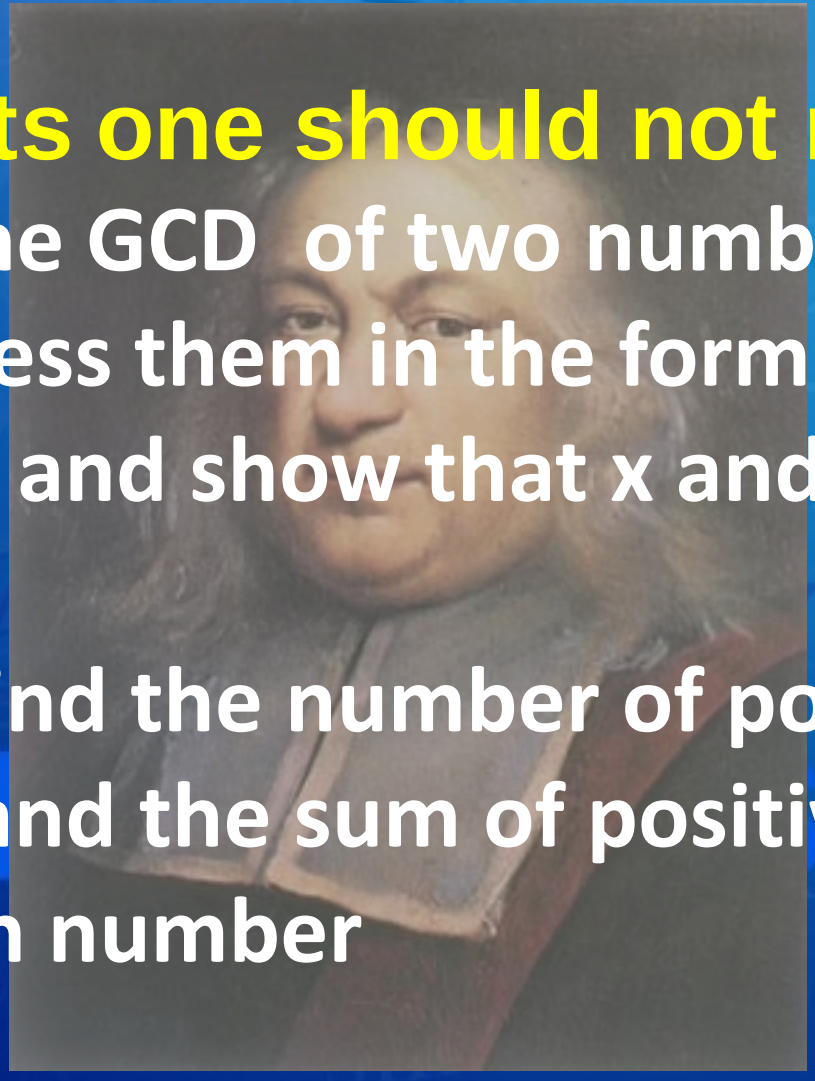

ELEMENTS OF NUMBER THEORY

Examination corner…

1 – one mark question in part A
1 - two mark question in part B
1 – five mark OR 3mark+2 mark question in part C
1 – two or four mark question in part E



concepts one should not neglect:

To find the GCD of two numbers a and b and express them in the form d=ax+by and show that x and y are not unique

- To find the number of positive divisors and the sum of positive divisors of a given number

Important area

Finding the remainder when 3^{50} is divided by 7&related problems

Properties of Divisibility and congruences

Use of properties of congruence to find the unit digit and the remainder &

solving linear congruences

PART E- Questions of following type

To find the least +ve remainder and the digit in the unit place of a given a number using congruence,

To find the incongruent solutions of a linear congruence.

Divisibility

Define Divisibility.

An integer ‘ $a \neq 0$ is said to divide an integer b if there is an integer k such that $b=ak$.

we then write $a|b$

The symbol ‘|’denotes “divides”

We write $a \nmid b$ when a does not divide b

DIVISIBILITY: Usage

a|b 

- b is equal to product of a by an integer i.e b=ka for some integer k
- “a divides b” ,
- a is a divisor of b
- a is a factor of b
- b is divisible by a
- b is a multiple of a.

If a|b and a|c then a|b±c

- $a|b \Rightarrow b=ak_1 \quad k_1 \in Z$ .....(1)
- $a|c \Rightarrow c=ak_2 \quad k_2 \in Z$.....(2)
- Adding (1) and (2)
- $b+c=a(k_1+k_2)=ak$;
- where $k=k_1+k_2 \in Z$
- $\Rightarrow a|(b+c)$
- similarly a|(b-c) can be proved
- by subtracting (1) and (2)

Divisibility Theorems

- For integers a , b and c it is true that
  If a|b and a|c then a|bc

if a | b, then a | bx for all integers x
Example: 5 | 10, so 5 | 20, 5 | 30, 5 | 40,

if a | b and b | c, then a | c
(transitive property)
Example: 4 | 8 and 8 | 24, so 4 | 24.

Properties of divisibility:

- If a|b and a|c then i) a|(bx+cy) (linearity property)

- If a|b and b|a then a=±b if a, b ∈ Z

Greatest Common Divisor

A positive integer d is said to be the greatest common divisor of a and b if the following conditions are satisfied:

- d|a and d|b

- If c|a and c|b then c|d

The greatest common divisor of a and b is denoted by (a, b)
i.e. (a, b)=d

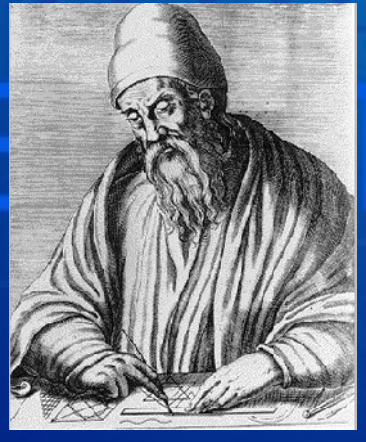
Greatest Common Divisors

Example : What is gcd(48, 72) ?
The positive common divisors of 48 and 72 are 1, 2, 3, 4, 6, 8, 12, 16, and 24,

so gcd(48, 72) = 24.

EUCLIDEAN ALGORITHM

- **Euclidean algorithm is based on the principle that the greatest common divisor of two numbers does not change if the smaller number is subtracted from the larger number.**



- For example, 21 is the GCD of 252 and 105 (252 = 21 × 12;105 = 21 × 5);
- since 252 − 105 = 147, the GCD of 147 and 105 is also 21.
- Repeat this process by subtracting the smaller number from the larger number every time until one of them is zero. When that occurs, the GCD is the remaining nonzero number

gcd(252, 105)

= gcd (252, 252 - 105)

= gcd (252, 147)

= gcd (252 - 147, 147)

= gcd (105, 147)

= gcd (105, 147 - 105)

= gcd (105, 42)

= gcd (105-42, 42)

= gcd (63, 42)

= gcd (63-42, 42)

= gcd (21, 42) = 21

By subtracting the smaller number from the larger number every time until one of them is zero. When that occurs, the GCD is the remaining nonzero number

GCD OF TWO NUMBERS

- **Find the GCD of 252 and 105 and represent as linear combination of 252 and 105. Show that the expression is not unique.**

105)252(2 252=105x2+42……..(1)

210 42=252-105x2

42

42)105(2 105= 42x2+21……..(2)

84 21=42x2-105

21

21)42(2 42=21x2+0

42

00

(252, 105) = (42, 105)= (42, 21) =21(?)

Therefore, gcd(252, 105) = 21.

105)252(2 42)105(2 21)42(2

210 84 42

42 21 00

252=105x2+42 $\Rightarrow$ 42=252-105x2.....(1)

105=42x 2+21 $\Rightarrow$ 21=105-42x2.....(2)

Expressing GCD as linear combination :

21=105-42x2=105-(252-105x2)x2

=105-252x2+105x4

=105x5+252x(-2)

=105x+252y

x=5 and y=-2

(Bezout's identity)

$21=105-42x2=105-(252-105x2)x2$

$=105-252x2+105x4$

$=105x5+252x(-2)$

$=105x+252y$

$x=5$ and $y=-2$

To show that this expression is not unique add and subtract 105x252

$21= =105x5+252x(-2) +105x252-105x252$

$=105(-247)+252(103)$

Here $x=-247$ $y=103$

- If (252, 105)=252x+105y , Find two sets of values of x and y
- Express (252, 105) as 252x+105y where x, y $\in$ Z in two different ways
- If (252, 105)=252(-2)+105(x), Find x

Number and sum of divisors of a number

Every composite number can be expressed as a product of power of primes uniquely.(Unique factorisation theorem)

e.g: $252=4 \times 63 = 4 \times 7 \times 9 = 2^2 3^2 7^1$

In general a composite number ' a' can be expresse d uniquely as a=

$$p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times p_4^{\alpha_4} \ldots\ldots \times p_n^{\alpha_n}$$

Where p_1, p_2, … are primes and α's are integers

Number and sum of divisors of a number

If $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times p_4^{\alpha_4} \ldots\ldots\ldots \times p_n^{\alpha_n}$

$T(a)=(1+\alpha_1)(1+\alpha_2)(1+\alpha_3)..(1+\alpha_n)$

$S(a)=$

$$\frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \frac{p_3^{\alpha_3+1}-1}{p_3-1} \ldots\ldots\ldots \frac{p_n^{\alpha_n+1}-1}{p_n-1}$$

Find the number of all +ve divisors of sumz of all divisors of 252

$252=4 \times 63 = 4 \times 7 \times 9 = 2^2 3^2 7^1$

$T(252)=(1+2)(1+2)(1+1)=18$

$S(252)=$

$$\frac{2^{2+1}-1}{2-1}\cdot\frac{3^{2+1}-1}{3-1}\cdot\frac{7^{1+1}-1}{7-1}=7\times13\times8=728$$

Properties of Primes and Composite numbers

1. If p is any prime and a is any integer, either (p, a)=1 or (p, a)=p
2. The smallest divisor > 1 of any integer > 1 is a prime number*
3. Number of primes is infinite

Proof :of number of primes is infinite

Let if possible the number of primes be finite say $p_1\ p_2\ p_3\ \ldots.p_n$ and let p_n be the largest prime.Consider $N= p_1\ p_2\ p_3\ \ldots.p_n + 1$.

When we divide N by any p_i remainder is 1 and hence N is not divisible by any of the primes $p_1\ p_2\ p_3\ \ldots.p_n$.

N cannot be composite. N should be new prime and $N>p_n$ the greatest prime, which contradicts assumption.

Properties of Prime and Composite numbers

- 4. If (c, a)=1 and c|ab, then c|b.*

- 5. If p is a prime and p|ab,
- then p|a or p|b.*
- 6. The smallest +ve divisor of a
- composite number 'a' does not
- exceed $\sqrt{a}$

Congruences

Let a and b be integers and m be a positive integer. We say that a is congruent to b modulo m if m divides (a – b) i.e. m|(a-b)

- **We write $a \equiv b \pmod{m}$**

$615 \equiv 805 \pmod{10}$ ∵ 10|(615-805)=-190

$79 \equiv 7 \pmod{8}$ ∵ 8|79-7=72

Congruence:

$a \equiv b \pmod{m} \Leftrightarrow m \mid a-b$

$\Leftrightarrow a-b=mk \Leftrightarrow a=b+mk,\ k \in Z$

$a \equiv b \pmod{m} \Rightarrow a=km+b \quad k \in Z$

$\Rightarrow a \equiv b+km \pmod{m}$ for any $k \in Z$

$\Rightarrow$ b is the remainder when a is divided by m

$\Rightarrow$ a and b leave the same remainder when divided by m

CONGRUENCES

- The remainders when any integer is divided by 5 is 0,1,2,3,4. We say that two integers a and b are ‘ congruent to modulo 5’ if they leave same remainders on division by 5.
- Thus 2,7,12,22…….-3,-8,-13,-18….. are all congruent modulo 5, since they leave remainder 2.

Properties of Congruence:

- The relation " congruence modulo m" is an equivalence relation on Z
- If $a \equiv b \pmod{m}$ and x is an integer,*

  i)$(a \pm x) \equiv (b \pm x) \pmod{m}$

  ii)$ax \equiv bx \pmod{m}$

  iii)$a^n \equiv b^n \pmod{m}$

Properties of Congruence:

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then*

1. $(a \pm c) \equiv (b \pm d) \pmod{m}$
2. $ac \equiv bd \pmod{m}$

(congruence with same modulus may be added, subtracted and multiplied)

Properties of Congruence:

- If $ca \equiv cb \pmod{m}$ and $(c, m) = 1$
  then $a \equiv b \pmod{m}$ * [Cancellation Law]

If $a \equiv b \pmod{m}$ and $n>1$ is a positive divisor of m, then $a \equiv b \pmod{n}$*

Linear Congruence:

A congruence of the form $ax \equiv b \pmod{m}$ is called a linear congruence.

A value of x satisfying the linear congruence is called a solution or root of the congruence.

LINEAR CONGRUENCE

$ax \equiv b \pmod m$

If $x=\alpha$ is a solution , then $\beta \equiv \alpha \pmod m$ is also a solution. i.e.

i.e If α is a solution of linear congruence

$ax \equiv b \pmod m$,

then all integers congruent to $\alpha \pmod m$ are also solutions.

- In general , if $x=\alpha$ is a solution of the congruence $ax \equiv b \pmod m$ then

  $\alpha + km$ where k is any integer , is also a solution.

- i.e , $\beta = \alpha , \alpha \pm m, \alpha \pm 2m, \alpha \pm 3m, \ldots\ldots\ldots$ are all solutions.

consider the linear congruence $3x \equiv 4 \pmod 5$,

Among the integers 0,1,2,3,4 the integer 3 satisfies the congruence.

$\alpha = 3$ is a solution of linearcongruence.

But the numbers 3, 3 ± 5, 3 ± 10, 3 ± 15,..... are also solutions. i.e all integers of the form $3+5k$, $k \in Z$, are also solution of $3x \equiv 4 \pmod 5$.i.e. .... -12,-7,-2,3,8..... are solutions or simply ={....-12, -7, -2, 3,8,13,18.....}

=Integers which leave remainder 3 when divided by 5 (Which is an AP)

Linear Congruence: Rules

Linear congruence $ax \equiv b \pmod{m}$

will-have a solution only if $(a, m) / b$

have no solution if (a, m) does not divide b

have unique solution if $(a, m)=1$

have ‘d’ incongruent solutions if

$(a, m)=d$ and d/b

Solve the congruence $6x+3 \equiv 1 \pmod{10}$

- $6x \equiv -2 \pmod{10}$ (why?) $\quad a \equiv b \pmod{m}$

  $-2 \equiv 8 \pmod{10} \quad \Rightarrow a-x \equiv b-x \pmod{m}$

  $6x \equiv 8 \pmod{10}$ (by transitive property)

Now $(6, 10)=2$ and $2 \mid 8$; 2 incongruent solutions

Solve the congruence $6x+3 \equiv 1 \pmod{10}$

$6x \equiv 8 \pmod{10} \Rightarrow 6x = 10k+8 \Rightarrow x = \frac{10k+8}{6}$

For k=1, x=3; k=4, x=8

$x \equiv 3 \pmod{10}$ & $x \equiv 8 \pmod{10}$ are incongruent solutions of given linear congruence.

Solution set =10k+3={..... -7, 3,13,23.....}

& 10k+8={.....-12, -2,8,18.....}

Solve the congruence $6x+3 \equiv 4 \pmod{10}$

It reduces to $6x \equiv 1 \pmod{10}$

$(6,10)=2$ and $2 \nmid 1$

Linear congruence $ax \equiv b \pmod{m}$

have no solution if (a, m) does not divide b

Hence given congruence has no solution

Solve the congruence $51x \equiv 32 \pmod 7$

Here $(51, 7)=1$; Unique solution

since $51 \equiv 2 \pmod 7$ $\quad 32 \equiv 4 \pmod 7$

$51x \equiv 32 \pmod 7 \Rightarrow 2x \equiv 4 \pmod 7$ (How?)

Solve the congruence $51x \equiv 32 \pmod 7$

since $51 \equiv 2 \pmod 7 \Rightarrow 51x \equiv 2x \pmod 7$

$\Rightarrow 2x \equiv 51x \pmod 7$ (?)

&$51x \equiv 32 \pmod 7 \Rightarrow 2x \equiv 32 \pmod 7$(?)

But $32 \equiv 4 \pmod 7$

$\therefore 2x = 4 \pmod 7 \Rightarrow x \equiv 2 \pmod 7$(?)

since (2,7)=1

Find the unit digit(last digit) of 17^{221}

If $a \equiv r \pmod{10}$, $0 < r < 10$, then the last digit (unit's digit) of a is r

Here $17 \equiv 7 \pmod{10}$

$\Rightarrow (17)^{221} \equiv 7^{221} \pmod{10}$(?)

$7^2 = 49 \equiv -1 \pmod{10} \Rightarrow$

$7^{221} = 7^{2 \times 110+1} = (7^2)^{11}\, 7$

$\equiv (-1)^{110}\, 7 \pmod{10} \equiv 7 \pmod{10}$

$\therefore$ 7 is the last digit.

Find the least non negetive remainder when 2^{12} is divided by 41

OR

Find x, if $2^{12} \equiv x \pmod{41}$

Find x, if $2^{12} \equiv x \pmod{41}$

$2 \equiv 2 \pmod{41}$ (by reflexive property)

$2^6 \equiv 23 \pmod{41}$ (23 is the remainder when 64 ÷41)

$(2^6)^2 \equiv (23)^2 \pmod{41}$ (squaring on both sides)

$(23)^2 \equiv 529 \pmod{41} \equiv 37 \pmod{41}$ [37 is the remainder when 529÷41]

Thus 37 is the remainder

Find the remainder when 79x101x125 is divided by 11

Or If 79x101x125=x(mod11) , Find x

$79 \equiv 2 \pmod{11}$

$101 \equiv 2 \pmod{11}$

$125 \equiv 4 \pmod{11}$

$79 \times 101 \times 125 \equiv 2 \times 2 \times 4 \pmod{11} \equiv 16 \pmod{11}$

$\equiv 5 \pmod{11}$

5 is the remainder or x=5

OTHER IMPORTANT FACTS:

- If $a \equiv r \pmod{m}$, $0 < r < m$, then r is the least non negative remainder when a is divided by m.
- n! always ends with 0 when $n \geq 5$. n! is a multiple of 10 when $n \geq 5$

Thank you ...