NUMBER THEORY NOTES

AKSHANSH CHAUDHARY

Number Theory Notes, First Edition

Presented by: Akshansh Chaudhary
Graduate of BITS Pilani, Dubai Campus
Batch of 2011

Course content by: Dr. Priti Bajpai
Then Faculty, BITS Pilani, Dubai Campus

Layout design by: AC Creations © 2013

The course content was prepared during Spring, 2014.
More content available at: www.Akshansh.weebly.com

Number Theory

* Branch of Number Theory :

1) ELEMENTARY NUMBER THEORY
   ↳ Branch deals with INTEGERS only.

2) Analytical Number Theory
   ↳ Deals with complex no.

3) Geometrical Number Theory
   ↳ Deals with concepts of geometry

4) Computational Number Theory
   ↳ all algorithms are developed in this branch.

5) Algebraic Number Theory
   ↳ when roots of polynomials are used (rational no.)

* Geometrical no. theory :
  no.s were defined on the basis of no. of vertices of a polygon.

* Pythagorean Triplets.

eg	x	y	z
	3	4	5
	5	12	13
	7	24	25
	9	40	41
	-	-	-

x	y	z
8	15	17
	35	37
12		
16	63	65
20	99	101
-	-	-

Quiz Question

$z = y + 1$

$x = n$ (odd)

$y = \frac{1}{2}(n^2 - 1)$

$z = \frac{1}{2}(n^2 + 1)$

$z = y + 2$

$x = n$ (even) ; $n \geq 2$

$y = \frac{1}{4}(n^2 - 4)$

$z = \frac{1}{4}(n^2 + 4)$

Q. Find n, s.t $61n^2 + 1$ is a square.

Ans - $n = 226153980$

↳ studied by Bhaskaracharya

Quiz Question

* Perfect no.

eg: consider no. 6

divisors (except 6 itself) = 1, 2, 3

$1 + 2 + 3 = 6$ So, 6 is perfect no.

Some perfect nos. 28, 496, 8128, 33503336 - - -

* Euclid's Algo/Theorem: An even no. is perfect if it has the form $2^{p-1}(2^p - 1)$ where both p and $2^p - 1$ are prime

Page No

* Different types of eqns.

① Diophantine eqns

$$ax + by = c.$$

↳ solving only for $\mathbb{Z}$ sol^n of x & y

② Fermat's theorem

$$x^n + y^n = z^n.$$

↳ for $n \in \mathbb{Z}$, only $n = 2$ is satisfied.

↳ Pythagorean theorem

③ Pell's eqn

$$x^2 - ny^2 = \pm 1$$

④ Erdos Straus Conjective

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

Chapter - 2

✱ Basic represent^{n} theorem :

Let k be any integer > 1, then, for each +ve integer n, $\exists$ a represent^{n}

$$n = a_s k^s + a_{s-1} k^{s-1} + \dots + a_1 k + a_0$$

- $a_s \neq 0$
- each a_i is non-ve and less than k.
- This represent^{n} is unique.
- Its called the represent^{n} of n to the base k.

eg : $333 = n_0$ say.

then, $333 = 3 \times 10^2 + 3 \times 10^1 + 3 \times 10^0$

- base, $k = 10$
- $a_s = 3 (\neq 0)$
- $a_i < k$ $(3 < 10$ ✓$)$

✱ Note :

Integers can be expressed to ANY base, $k > 1$.

eg ② : $(23)_2 = 10111 = 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 10^0$

- base, $k = 2$
- $a_s = 1 (\neq 0)$
- $a_i < k$

Page No

eg (3) $320 = 3\times10^2 + 2\times10^1 + 0\times10^0$

* Euclid's Division Lemma :

For any integer, $k>0$ & j ($\to>0$ or <0 → no restriction), $\exists$ unique ~~representation~~ integers q & r, s.t.,

$$0 \le r < k$$

& $j = qk + r$.

(= Dividend = Divisor × Quotient + Remainder)

$$\begin{array}{r} -6 \\ 3\overline{)-20} \\ -18 \\ \hline -2 \end{array}$$

$$-\frac{20}{3}$$

$-20 = (-7)3 + 1$ ✓

Proof :

Using Principle of Mathematical Induction

Case ① : $k = 1$

to show :- j has the form, $j = qk + r$

$j = j = j\cdot 1 + 0$ ✓ ; $k = 1$, $r = 0$

Case ② : $k > 1$ ($j>0$, $j=0$, $j<0$)

ⓐ Let $k>1$ & $j>0$

j can be written as

$$j = a_s k^s + a_{s-1} k^{s-1} + \dots + a_1 k + a_0 \to (A)$$

$$\Rightarrow j = k(\underbrace{a_s k^{s-1} + a_{s-1} k^{s-2} + \dots + a_1}_{q}) + a_0$$

q (can be written, if

$$q = a_s k^{s-1} + a_{s-1} k^{s-2} + \dots + a_1) \to (1)$$

then, $j = kq + a_0$

$j = kq + r$ ✓, $(0 \le r = a_0 < k)$

Page No

To prove uniqueness :

Let $\exists$ q', r' s.t

$$j = kq' + r' \longrightarrow (2).$$

From basic representation theorem,

q' can be written as, $q' = b_t k^t + b_{t-1} k^{t-1} + \ldots + b_1 k + b_0$

So, from (2),

$$j = k(b_t k^t + b_{t-1} k^{t-1} + \ldots + b_1 k + b_0) + r'$$

$$\Rightarrow j = b_t k^{t+1} + b_{t-1} k^t + \ldots + b_1 k^2 + b_0 k + r' \longrightarrow (3)$$

From (1) & (3), as j is same, we compare powers of k

$\Rightarrow$ $a_0 = r'$

$a_1 = b_0$

$a_2 = b_1$

....

From the trend, we have

$$b_i = a_{i+1}$$

& b_t, $s = t+1$

for $b_t = a_{t+1} = a_s$. So, $b_t = a_s$.

Now, q' becomes

$$q' = a_s k^{s-1} + a_{s-1} k^{s-2} + \ldots + a_2 k + a_1$$

$$= q \quad \text{(from (1))}$$

So, the representation is unique.

(b) $j = 0$

$\Rightarrow 0 = 0 \cdot 0 + 0$

(trivial case)

(c) $k>1$, $j<0$.

Now,

$$j<0 \Rightarrow -j>0$$

Now $j = qk + r$

let $\exists\ q'', r''$, s.t

$$-j = q''k + r''$$

$$\Rightarrow j = -q''k - r''$$

$$= -qk - r'' + k - k$$

↳ making remainder +ve.

$$= (-q-1)k + (k - r'')$$

q ''' r '''

$$\Rightarrow j = qk + r.$$

again in that form

Proved

eg: $55 \div 7$ ⁰₀—

$$55 = 7 \cdot 7 + 6$$

eg (2): $-101 = -9 \cdot 11 - 2$ ✗

↳ remainder becomes -ve.

So, $+k - k$ (base)

$$= -101 = -9 \cdot 11 - 2 + 9 - 9$$

$$\Rightarrow -101 = -9 \cdot 12 + 7$$ ✓

↳ $r>0$

Q. Prove that if a is an odd integer, then,

$\{a^2 + (a+2)^2 + (a+4)^2 + 1\}$ is divisible by 12.

Idea: To be divisible completely, remainder should be 0
So, in the form $f = kq + 0$, we should have
$f = kq$.

For a to be an odd integer, let $a = 2m+1$

$\Rightarrow = (2m+1)^2 + (2m+3)^2 + (2m+5)^2 + 1$

$= 4m^2 + 1 + 4m + 4m^2 + 9 + 12m + 4m^2 + 25 + 20m + 1$

$= 12m^2 + 36m + 36$

$= 12(m^2 + 3m + 3)$

$= k(q \quad) + 0$

Hence, divisible

Q. Prove that if a & b are odd $\in_s$. then,
$(a^2 - b^2)$ is divisible by 8.

Both odd

$\Rightarrow$ let $a = 2m+1$, $b = 2n+1$

$\Rightarrow (2m+1)^2 - (2n+1)^2$

$= 4m^2 + 1 + 4m - [4n^2 + 1 - 4n]$

$= 4[m^2 - n^2] + 1 - 1 + 4m - 4n$

$= 4[m^2 - n^2] + 4[m - n]$

$= 4[m-n][m+n] + 4[m-n]$

$= 4[m-n][m+n+1]$

here, $\exists$ 3 cases:

(1) m, n → even (both)

(2) m, n → odd (both)

(3) m, n → one even one odd.

Page No

① when both are even.

Say, $m = 2k$, $n = 2s$.

$\Rightarrow 4(m+n+1)(m-n) = 4(2k+2s+1)(2k-2s)$

$= 8(2k+2s+1)(k-s)$

✓ divisible by 8.

② If both are odd.

Say, $m = 2k+1$, $n = 2s+1$

$\Rightarrow 4(m+n+1)(m-n) = 4(2k+2s+3)(2k+1-2s-1)$

$= 8(2k+2s+3)(k-s)$

✓.

③ If one odd one even

Say, $m = 2k+1$, $n = 2s$.

$\Rightarrow 4(m+n+1)(m-n) = 4(2k+2s+2)(2k+1-2s)$

$= 8(k+s+1)(2k+1-2s)$

✓.

Proved

★ PIGEON HOLE PRINCIPLE:

If m pigeons are assigned to n pigeon holes where $m > n$, then atleast 2 pigeons will occupy the same hole.

Q. Let k be an integer ≥ 2. Suppose $k+1$ integers are randomly selected. Prove that $\exists$ atleast 2 Z's, s.t the diff. b/w them is divisible by k.

Sol:- Let there be k integers and $k+1$ have to be selected. Here, $k+1$ integers are the pigeons and k pigeon holes. So, by pigeon hole principle, 2 numbers (integers) will be there s.t. their remainders are same. Let these integers be x & y.

Then, by basic representation theorem,

$x = kq_1 + r$

$y = kq_2 + r$.

(∵ their diff. have to be divisible by k)

$x - y = k(q_1 - q_2)$

⇒ diff is divisible by k

eg Consider a no. 2000. say. Find no. of Z_5 before 2000, that are divisible by 3. say.

how to do? →

* Method of finding no. of +ve integers less than or equal to a given integer "a", s.t. they are divisible by one or more integers.

Theorem 2.5: Let 'a' & 'b' be any +ve Z_s. Then, no. of +ve integers less than or equal to 'a' & divisible by 'b' is $\left[\frac{a}{b}\right]$

So, in above example, $a = 2000$, $b = 3$.

So, no. of $Z_s = \left[\frac{2000}{3}\right] = 666$.

Formulas: ① If $|A \cap B| = n$

$|A| = n + k$

$|B| = n + s$

↳ $n, k, s \geq 0$.

A: no. of Z_s divisible by k

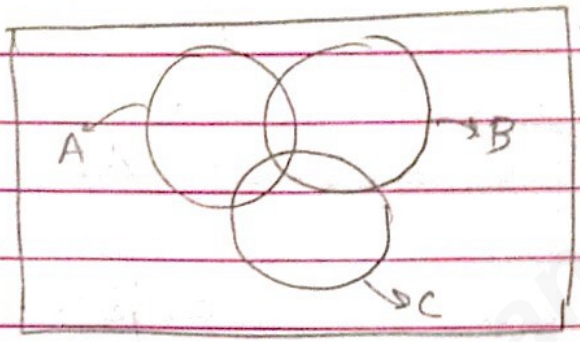
B: no. of Z_s divisible by s.

Then, $|A \cup B| = n + k + s = (n+k) + (n+s) - n$.

⇒ $|A \cup B| = |A| + |B| - |A \cap B|$. *

Page No

② $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$



eg. 2.6 Find the no. of +ve $Z_s \leq 2076$ & divisible by neither 4 nor 5

Let A = set of +ve integers, x s.t $x \leq 2076$ and divisible by 4

i.e $A = \{x \in N \mid x \leq 2076 \text{ and divisible by } 4\}$

$B = \{x \in N \mid x \leq 2076 \text{ and divisible by } 5\}$

Idea: find $|A \cup B|$ i.e nos divisible by both 4 & 5 then, subtract from 2076 for answer.

$|A \cup B| = |A| + |B| - |A \cap B|$

$\left[\frac{2076}{4}\right]$ $\left[\frac{2076}{5}\right]$ $\left[\frac{2076}{LCM(4,5)}\right]$

By theorem 2.5

$\Rightarrow |A \cup B| = 519 + 415 - 103$

$\Rightarrow |A \cup B| = 831$

Now, nos. neither divisible by 4 nor 5 = 2076 - 831 = 1245

eg ② Find no. of +ve integers ≤ 3000 & divisible by 3, 5 or 7.

$A = \{ x \in N \mid x \leq 3000 \text{ \& divisible by } 3 \}$

$B = \{ \quad " \quad \mid \quad " \quad " \quad 5 \}$

$C = \{ \quad " \quad \mid \quad " \quad " \quad 7 \}$

$\therefore |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$

$= \left[\frac{3000}{3}\right] + \left[\frac{3000}{5}\right] + \left[\frac{3000}{7}\right] - \left[\frac{3000}{15}\right] - \left[\frac{3000}{35}\right] - \left[\frac{3000}{21}\right] + \left[\frac{3000}{105}\right]$

$= 1000 + 600 + 428 - 200 - 85 - 142 + 28$

$\Rightarrow |A \cup B \cup C| = 1629.$ Ans

~

∵ Gregorian calendar started from 1600

☆ Method for finding no. of leap years beyond 1600 and not exceeding a given year y

Note :- It is a leap year if it's a century & divisible by 400 or it's a non-century & divisible by 4

eg :- find no. of leap years b/w 1600 and 2014.

Idea :- find no. of centuries, divisible by 4, divisible by 400

Formula :- Let l be no. of leap years.

Then, $l = \left[\frac{y}{4}\right] + \left[\frac{y}{400}\right] - \left[\frac{y}{100}\right] - 388$

So, here, $y = 2014$

$\therefore l = \left[\frac{2014}{4}\right] + \left[\frac{2014}{400}\right] - \left[\frac{2014}{100}\right] - 388$

$\Rightarrow l = 503 + 5 - 20 - 388$

$= 508 - 408$

$\Rightarrow l = 100$. Ans

eg ② Find how many leap years are there from 1700 to 2014.

We know,

formula for finding how many leap years leap years are there from 1600 to y :

$$\left[\frac{y}{4}\right] + \left[\frac{y}{400}\right] - \left[\frac{y}{100}\right] - 388$$

Idea : (b/w 1700 & 2014) = (b/w 1600 & 2014) − (b/w 1600 & 1700)

let $y = 2014$

$\Rightarrow$ leap years $= \left[\frac{2014}{4}\right] + \left[\frac{2014}{400}\right] - \left[\frac{2014}{100}\right] - 388 = 100$ → ①

let $y = 1700$.

$\left[\frac{1700}{4}\right] + \left[\frac{1700}{400}\right] - \left[\frac{1700}{100}\right] - 388 = 24$ → ②

Subtracting ① & ② gives leap years b/w 1700 & 2014

$= 76$ leap yeass

✱ Divisibility:

Defin^n: If a & b are integers and b divides a or b is a divisor of a if $\frac{a}{b}$ is an integer.

Notation: $b|a \equiv$ b divides a; if $\frac{a}{b}$ is integer.

$b \nmid a \equiv$ b doesn't divide a, if $\frac{a}{b}$ is not an integers.

eg: $2|4$ ✓

$3 \nmid 4$ ✓

✱ Note: (known facts)

$1|a$

$-1|a$

$a|0$

$a|a$

$-a|a$

ex: let a, b, c and d be integers. Given e divides both a & c, then show that

$e|ab+cd$, where e is an integer

Sol^n Given: $e|a$ & $e|c$

$\Rightarrow \frac{a}{e} = x, x \in Z \Rightarrow a = ex$ (integer)

$\frac{c}{e} = y, y \in Z \Rightarrow c = ey$. (integer)

Now, $ab+cd = ex(b) + ey(d) = e[xb+yd]$

$=$ (integer)(integer)

$\Rightarrow \frac{ab+cd}{e} =$ integer.

So, $e|ab+cd \rightarrow$ Satisfied.

Page No

CLASSMATE

* Defin^{n}:

A +ve integer, p, other than 1 is said to be prime if its only +ve divisors are 1 and p.
(i.e, a prime no. is divisible by itself and 1)

* Theorem:

If a, b, c, d are integers, then, the following hold:

(i) If $a|b$ & $c|d$, then, $ac|bd$

(ii) If $a|b$ & $b|c$, then, $a|c$

(iii) If $a|b$ & $a|c$, then, $a|(bx+cy)$
↳ linear combin^{n} of b & c
↳ arbitrary integers x & y

(iv) If $a|b$ & $a|c$, then $a|(b \pm c)$

(v) If $a|b$ & $b|a \Rightarrow a = \pm b$

Proof:

(i) Given $a|b$ & $c|d$ To show: $ac|bd$.

$\frac{b}{a} = x$ & $\frac{d}{c} = y$, say

$\Rightarrow b = ax$ & $d = cy$.

Now,

$bd = (ax)(cy)$

$\Rightarrow bd = (ac)(xy)$

$\Rightarrow \frac{bd}{ac} = xy = \text{integer}$.

$\Rightarrow ac|bd$., proved.

(ii) Given $a|b$ & $b|c$

Show: $a|c$

$a|b \Rightarrow \frac{b}{a} = x$, $b|c \Rightarrow \frac{c}{b} = y$.

$\Rightarrow b = ax$, $c = by$

$\Rightarrow c = (ax)y$

$\Rightarrow c = a(xy)$

$\Rightarrow \frac{c}{a} = xy = \text{integer}$

$\Rightarrow a|c$, proved

(iii) Given $a|b$ & $a|c$,

Show: $a|(bx+cy)$

$a|b \Rightarrow \frac{b}{a} = p$, $a|c \Rightarrow \frac{c}{a} = q$.

$\Rightarrow b = ap$, $c = aq$

$\Rightarrow bx = a(px)$ & $cy = a(qy)$.

$\rightarrow$ (1) $\rightarrow$ (2)

(1) + (2).

$\Rightarrow bx+cy = a(px) + a(qy)$

$= a[px+qy]$

$= a[\text{integer}]$

(∵ Sum of integer = integer)

$\Rightarrow \frac{bx+cy}{a} = \text{integer}$.

$\Rightarrow a|bx+cy$, proved.

(iv) Given: $a|b$ & $a|c$.

Prove: $a|b \pm c$.

let $\frac{b}{a} = x$ & $\frac{c}{a} = y$

Page No

$\Rightarrow b = ax$ & $c = ay$

We know sum or difference of integers is integer.

$\Rightarrow b \pm c \in Z$.

$\Rightarrow ax + ay \in Z$

$\Rightarrow a(x+y) \in Z$. $\rightarrow (1)$.

Now, $b \pm c = a(x+y)$

$\Rightarrow \frac{b \pm c}{a} = x+y \in Z$

$\Rightarrow a \mid b \pm c$, Proved

Alter: In previous proof,

put $x = 1$, $y = \pm 1$

(v) Given: $a \mid b$ & $b \mid a$.

Prove: $a = \pm b$.

let $\frac{b}{a} = x$ and $\frac{a}{b} = y$.

$\Rightarrow b = ax$ & $a = by$.

$\Rightarrow b = (by)(x)$

$\Rightarrow b = b(xy) \rightarrow (1)$

For (1) to be true,

$xy = 1$

$\Rightarrow x = 1, y = 1 \rightarrow (a)$

or $x = -1, y = -1 \rightarrow (b)$.

for (a), $a = b$.

(b), $a = -b$.

Hence, $a = \pm b$., proved

CLASSMATE

* Theorem:
If $a|b$ & $c|d$, then
$$(a+c) \nmid (b+d)$$

Proof: $a|b \Rightarrow \frac{b}{a} = x \Rightarrow b = ax$.

$c|d \Rightarrow \frac{d}{c} = y \Rightarrow d = cy$.

Now, suppose $(a+c)|(b+d)$

$$\Rightarrow \frac{b+d}{a+c} = p, \text{ say}$$

$$\Rightarrow \frac{ax+cy}{a+c} = p, \text{ say}$$

This is true iff $x = y = k$ (constant $\in \mathbb{Z}$) p (for $x, y \in \mathbb{Z}$)
In other cases, $(a+c) \nmid (b+d)$
So, in general, its not satisfied, proved

* Corollary :-
If $p | a_1 a_2 a_3 \cdots a_n$,
then, $\exists$ some a_i, s.t, $p|a_i$

* Corollary ②:
If $c | a_1, a_2, \cdots, a_n$
then, $c | a_1x_1 + a_2x_2 + \cdots + a_nx_n$

↳ $x_1, x_2, \cdots, x_n \in \mathbb{Z}$.

Self :- Exercise 2.1

Chapter - 3

GREATEST COMMON DIVISOR

* Defin^{n}: If a & b are integers, not both equal to zero, then, an integer d is called the greatest common divisor of a, b, if:
  1. d > 0
  2. d is common divisor of a & b
  3. Each integer f, that is a common divisor of both a & b is also a divisor of d.

Notation: g.c.d (a, b) : used in this course.
(a, b) : not followed here.

* The Method of finding g.c.d (a, b)
  ↳ Method using Euclidean Algorithm.

eg: find g.c.d (69, 59)

Idea: take bigger no. out of the two & use basic representation theorem.

So, $69 = 59 \times (1) + 10$
(1) → multiple.

59 ⟌ 69 | 1
−59
10

Now, do Remainder ÷ 59

$\Rightarrow 59 = 10 \times (5) + 9$
(5) → multiple.

$10 = 9 \times 1 + 1$

$9 = 1 \times (9) + (0)$
(9) → multiple
(0) → Process ends when remainder = 0

Page No

Note: g.c.d is the no. with which we are dividing.
In ~~me~~ * g.c.d. is the divisor, when remainder = 0.
So, here,
$$g.c.d(59, 69) = 1$$

eg (2) gcd (341, 527)

$$527 = 341 \times 1 + 186$$
$$341 = 186 \times 1 + 155$$
$$186 = 155 \times 1 + 31$$
$$155 = 31 \times 5 + 0$$

remainder = 0

So, g.c.d (341, 527) = 31 Ans

2 13 341
− 186
155

Note: If a & b are integers, not both zero, then g.c.d (a, b) exists & is unique.

* Theorem:
If d = g.c.d (a, b), then, ∃ integers x & y s.t. $ax + by = d$.
i.e, from previous example, we can write
$$341x + 527y = 31$$
So, finding integers x & y for above eqⁿ, where 31 = g.c.d (341, 527)
Idea: Start from Euclidian algorithm & move backward
So, $31 = 186 - 155 \times 1$ (from above)
$\Rightarrow 31 = 186 - (341 - 186 \times 1) \times 1$
$= 186 - 341 + 186 \times 1$
$= 186 \times 2 - 341$

* Replace smaller no. while solving.

$$\Rightarrow 31 = (527 - 341 \times 1) \times 2 - 341$$
$$= (527) \times 2 - (341) 2 - 341$$
$$= (527) \times 2 + (341) \times (-3)$$
$$\Rightarrow x = -3, \; y = 2$$

* **Corollary:** In order that $\exists$ integers x & y, satisfying the eqn $ax + by = c$
iff $d \mid c$ where $d = g.c.d(a, b)$

* **Note:**
a & b are relatively prime,
if $g.c.d(a, b) = 1$.
eg: $g.c.d(59, 69) = 1$
So, they are relatively prime

eg find $g.c.d(12321, 8658)$ using Euclidean Algorithm

$12321 = 8658 \times 1 + 3663$
$8658 = 3663 \times 2 + 1332$
$3663 = 1332 \times 2 + 999$
$1332 = 999 \times 1 + 333$
$999 = 333 \times 3 + 0$
$\Rightarrow g.c.d(12321, 8658) = 333$

12321
- 8658
3663
- 7326
8658
- 7326
1332
× 2
2664
3663
- 2664
999

Q. Use Euclidean algorithm to find gcd (299, 481)
Then find integers x & y s.t $299x + 481y = d$

$481 = 299 \times 1 + 182$
$299 = 182 \times 1 + 117$
$182 = 117 \times 1 + 65$
$117 = 65 \times 1 + 52$
$65 = 52 \times 1 + 13$
$52 = 13 \times 4 + 0$
$\Rightarrow g.c.d = 13 = d$

Now,

$13 = 65 - 52 \times 1$ — 52 < 65, so, replacing 52
$= 65 - (117 - 65 \times 1) \times 1$
$= 65 - 117 + 65 \times 1$
$= 65 \times 2 - 117$
$= (182 - 117 \times 1) \times 2 - 117$
$= 182 \times 2 - (117) \times 3$ — 117 < 182, so, replacing 117
$= 182 \times 2 - (299 - 182 \times 1) \times 3$
$= 182 \times 5 - 299 \times 3$
$= (481 - 299 \times 1) \times 5 - 299 \times 3$
$= (481) \times 5 - (299) \times 8.$

$\Rightarrow 299x + 481y = d. \equiv 299(-8) + 481(5) = 13$

$\Rightarrow x = -8, y = 5$

eg Find the g.c.d. of (39, 102, 75) using Euclidean algorithm

Soln: Idea: Take any 2 nos. Find their g.c.d. Then, use that no. & the third no. & find its g.c.d. That is overall g.c.d.

Page No

Let take 39 & 102.

Now,

$102 = 39 \times 2 + 24$

$39 = 24 \times 1 + 15$

$24 = 15 \times 1 + 9$

$15 = 9 \times 1 + 6$

$9 = 6 \times 1 + 3$

$6 = 3 \times 2 + 0$

$g.c.d(39, 102) = 3$.

Now, find $g.c.d(3, 75)$

$75 = (3) \times 25 + 0$.

$\Rightarrow g.c.d(3, 75) = 3$

So, $g.c.d(39, 102, 75) = 3$. Ans

* Finding LEAST COMMON MULTIPLE (l.c.m)

↳ Formula : $l.c.m(a, b) = \frac{a \times b}{g.c.d(a, b)}$

eg. Find the $g.c.d(n, n+1)$

By Euclidean algorithm.

$n+1 = n \times 1 + 1$

$\Rightarrow n = 1 \times n + 0$

$g.c.d(n, n+1) = 1$

Note : Consecutive no's are relatively prime.

Q. Find l.c.m(n, n+1)

$$l.c.m(n, n+1) = \frac{n(n+1)}{g.c.d(n, n+1)} = \frac{n^2+n}{1}$$

Q. Find g.c.d (2n-1, 2n+1) & l.c.m (2n-1, 2n+1)

$2n+1 = (2n-1) \times 1 + 2$.

$2n-1 = (2) \times (n-1) + 1$.

$2 = 1 \times 2 + 0$.

$\Rightarrow g.c.d = 1$.

$$l.c.m = \frac{(2n-1)(2n+1)}{1} = 4n^2 - 1$$

Q. If d is the g.c.d (a, b). Show that $\frac{a}{d}$ & $\frac{b}{d}$ are relatively prime.

Given :- $d = g.c.d(a, b)$.

$\Rightarrow \exists\ x, y$ (integers), s.t

$ax + by = d$

$\Rightarrow \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1$.

$\Rightarrow \frac{a}{d}$ & $\frac{b}{d}$ are relatively prime.

Corollary * If p is a prime and 'a' is an integer s.t $p \nmid a$, then, p & a are relatively prime.

Proof :-

$\because p \nmid a \Rightarrow g.c.d(p, a) = 1$.

Hence, they are relatively prime.

Alter: Proof by contradiction:

Say p & a are not relatively prime

$\Rightarrow \exists$ some integer x, s.t $x = g.c.d(p, a)$

Now, by defn of a prime no., it is only divisible by 1 or itself. But, here we have $x | p$, which cannot be true.

Hence, our supposition is false.

So, p & a are relatively prime.

Hence, proved

Q. If a, b & c are integers, where a & c are relatively prime, & $c | ab$ then show c divides b.

∵ a & c are relatively prime $\Rightarrow g.c.d(a, c) = 1$

$\Rightarrow \exists$ integers x & y s.t $ax + cy = 1$

Multiply by b.

$\Rightarrow (ab)x + (cb)y = b.$

Now, we know $c | ab$.

$\Rightarrow \frac{ab}{c} = z$, say, for $z \in$ integer

$\Rightarrow ab = cz$

$\Rightarrow (cz)x + (cb)y = b$

$\Rightarrow c(zx) + cb(y) = b.$

$\Rightarrow c[zx + by] = b.$

$\Rightarrow c[\text{integer}] = b$

$\Rightarrow \frac{b}{c} = \text{Integer}$

$\Rightarrow c | b.$ Hence, Proved.

Q. If a & b are integers, p is a prime no., s.t., $p \mid ab$. Given: $p \nmid a$.

Show: $p \mid b$.

Now, we have $p \mid ab$.

$\Rightarrow \frac{ab}{p} = z$ say.

$\Rightarrow ab = pz$, $z \in$ integer

$\because p \nmid a \Rightarrow g.c.d(p, a) = 1$

$\Rightarrow px + ay = 1$

$(\times b)$ both sides.

$\Rightarrow pbx + aby = b$

$\Rightarrow pbx + (pz)y = b$

$\Rightarrow p(bx + zy) = b$

$\Rightarrow p(\text{integer}) = b$

$\Rightarrow \frac{b}{p} = \text{integer} \Rightarrow p \mid b$

Hence, proved

Q. Show: $g.c.d(ab, ad) = a[g.c.d(b, d)]$

Proof:- Let a, b, d be integers assuming $b > d$.

So, by Euclid's division algorithm, doing $b \div d$.

Following g.c.d steps:

$$b = dq_1 + r_1$$
$$d = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\vdots$$
$$r_{n-1} = r_n q_{n+1} + 0.$$

q_1 : quotient, r_1 = remainder. (A)

$\Rightarrow g.c.d(b, d) = r_n \rightarrow (1)$

Multiply 'a' on both sides of eq^n (A)

$\Rightarrow ab = adq_1 + ar_1$

$ad = ar_1 q_2 + ar_2$

$ar_1 = ar_2 q_3 + ar_3$

$\vdots$

$ar_{n+1} = ar_n q_{n+1} + 0$

$\Rightarrow g.c.d(ab, ad) = ar_n \rightarrow (2)$

Multiplying eq^n (1) by 'a'

$\Rightarrow a[g.c.d(b, d)] = ar_n \rightarrow (3)$

From (2) & (3).

$g.c.d(ab, ad) = a[g.c.d(b, d)]$

Proved

Q. Prove : $l.c.m(ab, ad) = a[l.c.m(b, d)]$

LHS

We know $lcm(ab, ad) = \frac{(ab)(ad)}{g.c.d(ab, ad)}$

$= \frac{(ab)(ad)}{a[g.c.d(b, d)]}$ (from previous question)

$= \frac{a(bd)}{g.c.d(b, d)}$

$$= a\left[\text{l.cm}(b,d)\right]$$

$$= \text{RHS}.$$

Hence, proved

8. Prove : $g.c.d(a+b, a-b) \geq g.c.d(a,b)$

Let $d = g.c.d(a,b)$

$\Rightarrow d|a$ & $d|b$.

$\Rightarrow d|a+b$ & $d|a-b$. (previous theorems)

$\Rightarrow d \mid g.c.d(a+b, a-b)$

$\Rightarrow d \leq g.c.d(a+b, a-b)$

$\Rightarrow g.c.d(a,b) \leq g.c.d(a+b, a-b)$

---

* Method of Blankinship for finding $d = g.c.d(a,b)$ & x, y, s.t $ax+by=d$

Steps : (S1) If $d = g.c.d(a,b)$, then, we first write :

$$A = \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$$

only using integers

(S2) Transform A using elementary (row transformations) s.t A reduces to :

$$\begin{pmatrix} d & x & y \\ 0 & x' & y' \end{pmatrix} \text{ or } \begin{pmatrix} 0 & x' & y' \\ d & x & y \end{pmatrix}$$

$\hookrightarrow x', y'$: any integer.

Page No

eg Find g.c.d (12, 30)

sol) $A = \begin{pmatrix} 12 & 1 & 0 \\ 30 & 0 & 1 \end{pmatrix}$

$R_2 \to R_2 - 2R_1$

$\begin{pmatrix} 12 & 1 & 0 \\ 6 & -2 & 1 \end{pmatrix}$

$R_1 \to R_1 - 2R_2$

$\begin{pmatrix} 0 & 5 & -2 \\ 6 & -2 & 1 \end{pmatrix}$

g.c.d x y

$\Rightarrow d = 6, \quad x = -2, \quad y = 1$

Now, $ax + by = d$

$\Rightarrow 12(-2) + 30(1) = 6$

Hence, verified.

Idea : Get 0 on R_1 or R_2.
Keep solving until that is done.
The row not having 0 is answer.

Q. Find g.c.d (621, 414)

Let d = g.c.d (621, 414)

So, $ax + by = d$.

↳ $a = 621, \; b = 414$

$\Rightarrow$ we can write

$A = \begin{pmatrix} 621 & 1 & 0 \\ 414 & 0 & 1 \end{pmatrix}$

$R_1 \to R_1 - R_2$.

$$\Rightarrow A = \begin{bmatrix} 207 & 1 & -1 \\ 414 & 0 & 1 \end{bmatrix}$$

$$R_2 \to R_2 - 2(R_1)$$

$$A = \begin{bmatrix} 207 & 1 & -1 \\ 0 & -2 & 3 \end{bmatrix}$$

$$\equiv \begin{bmatrix} d & x & y \\ 0 & x' & y' \end{bmatrix}$$

$\Rightarrow d = 207 = g.c.d(621, 414)$ Ans

⚠ Ensure d (g.c.d.) > 0 always.

Q. g.c.d (1876, 365)

$$A = \begin{pmatrix} 1876 & 1 & 0 \\ 365 & 0 & 1 \end{pmatrix}$$

$$R_1 \to R_1 - 5(R_2)$$

$$= \begin{bmatrix} 51 & 1 & -5 \\ 365 & 0 & 1 \end{bmatrix}$$

$$R_2 \to R_2 - 7(R_1)$$

$$= \begin{pmatrix} 51 & 1 & -5 \\ 8 & -7 & 36 \end{pmatrix}$$

$$R_1 \to R_1 - 6(R_2)$$

$$= \begin{pmatrix} 3 & 43 & -221 \\ 8 & -7 & 36 \end{pmatrix}$$

$$R_2 \to R_2 - 2R_1$$

$$= \begin{pmatrix} 3 & 43 & -221 \\ 2 & -93 & 478 \end{pmatrix}$$

$$R_1 \to R_1 - R_2$$

$$= \begin{pmatrix} 1 & 136 & -699 \\ 2 & -93 & 478 \end{pmatrix}$$

365 × 5 = 1825 ; 1876 − 1825 = 51

51 × 7 = 357 ; 365 − 357 = 8

8 × 6 = 48 ; 51 − 48 = 3

3 × 2 = 6 ; 8 − 6 = 2

221 × 2 = 442 ; 136 + 93 = 229 ; 478 − 221 = 257 ; 699 − 257 = 442

$R_2 \to R_2 - 2R_1$

$$= \begin{pmatrix} 1 & 136 & -899 \\ 0 & -365 & 920 \end{pmatrix}$$

So, $d = 1 = g.c.d(1876, 365)$

So, 1876 & 365 are relatively prime.

Verification :- $1876(136) + 365(-699)$

Should be equal to 1.

272
385
389
82
778
266
104
699
82
526
478
920

* Note :-

Operation :

$R_1 \to R_1 - (\,)R_2$ ✓

$R_1 \to (\,)R_1 - (\,)R_2$ ✗ don't do

* Fundamental Theorem of Arithmetic.

Theorem : For each integer $n > 1$, $\exists$ primes, $p_1 \leq p_2 \leq \dots \leq p_k$ s.t, $n = p_1 \cdot p_2 \cdot p_3 \dots p_k$.

This factorization is unique

i.e, any integer can be expressed in product of powers of prime nos.

eg : $48 = 2^4 \cdot 3$; 2, 3 : prime nos.

* Finding g.c.d using Prime Factors"

eg : g.c.d (12, 30)

$12 = 2^2 \cdot 3 \cdot 5^0$

$30 = 2 \cdot 3 \cdot 5$.

Idea: For g.c.d take all the factors (primes). Now, see lower powers of those primes from both the nos.

$g.c.d = 2^1 \cdot 3^1 \cdot 5^0 = 6.$

Idea: for l.c.m. take Higher powers of primes

$l.c.m = 2^2 \cdot 3^1 \cdot 5^1 = 60.$

Note: ① To find g.c.d, we first write the nos as product of prime powers. We then write the smaller power for each prime and take the product.

② for finding l.c.m. we take highest power of each prime & take product.

* Prime factoriz^n method can be used for finding l.c.m & g.c.d of any no. of nos integers.

eg. Find g.c.d & l.c.m (1876, 365)

$1876 = 2^2 \cdot 7 \cdot 67$

$365 = 5 \cdot 73$

So, $g.c.d = 2^{(0)} \cdot 5^{(1)} \cdot 7^{(0)} \cdot 67^{(0)} \cdot 73^{(0)}$

$= 2^0 \cdot 5^0 \cdot 7^0 \cdot 67^0 \cdot 73^0 = 1$

$l.c.m = 2^2 \cdot 5^1 \cdot 7^1 \cdot 67^1 \cdot 73^1 = 684,740$

eg. Find g.c.d (39, 102, 75)

$39 = 3 \cdot 13 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 13^1 \cdot 17^0$

$102 = 2 \cdot 3 \cdot 17 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 13^0 \cdot 17^1$

$75 = 5^2 \cdot 3 = 2^0 \cdot 3^1 \cdot 5^2 \cdot 13^0 \cdot 17^0$

$g.c.d = 2^{(\ )} \cdot 3^{(\ )} \cdot 5^{(\ )} \cdot 13^{(\ )} \cdot 17^{(\ )}$

$= 2^0 \cdot 3^1 \cdot 5^0 \cdot 13^0 \cdot 17^0$

$\Rightarrow g.c.d = 3$ ans

$l.c.m = 2 \cdot 3 \cdot 5^2 \cdot 13 \cdot 17 = 33,150$

8 Find g.c.d & l.c.m (p^2q, pqr) where p, q, r are primes.

$p^2q = p^2 \cdot q^1$

$pqr = p^1 \cdot q^1 \cdot r^1$

$g.c.d = p^{(\ )} q^{(\ )} \cdot r^{(\ )}$

$= p^1 \cdot q^1 \cdot r^0 = pq$

$l.c.m = p^{(\ )} q^{(\ )} \cdot r^{(\ )}$

$= p^2 \cdot q^1 \cdot r^1 = p^2qr$

DIOPHANTINE EQ^{ns} :

↳ Linear Diophantine Eq^{ns} (LDE)

Defin^{n}: Let a, b & c be integers ($a \neq 0$, $b \neq 0$), then, $ax + by = c$ is called Diophantine eq^{n}. The pair (x, y) of integers which satisfies the above eq^{n} is called a sol^{n}.

* **Theorem:**
Linear diophantine eq^{n} $ax + by = c$ has a sol^{n} if $d \mid c$, where d is the g.c.d (a, b).
Furthermore, if (x_0, y_0) is a sol^{n} of this eq^{n}, then, the set of sol^{ns} consists of all integer pair (x, y), where

General sol^{n}:
$$x = x_0 + \frac{b}{d}t$$
$$y = y_0 - \frac{a}{d}t \; ; t = 0, \pm 1, \pm 2, \ldots$$

* **Note:-** If eq^{n} is
$$ax - by = c$$
General sol^{n}:
$$x = x_0 + \frac{b}{d}t$$
$$y = y_0 + \frac{a}{d}t \; ; t = 0, \pm 1, \pm 2, \ldots$$

eg Find if $15x + 27y = 1$ has a sol^{n} or not.
Find g.c.d $(15, 27) = 3 = d$
Now, $c = 1$
$3 \nmid 1$. So, solution doesn't exist
(no integer solution (x, y))

i.e.

eg Does $5x+6y=1$ have a solution?

$g.c.d(5,6) = 1 = d$.

$1 \mid 1$. So sol^n exists

Solution $(x,y) = (-1,1)$ (By observation)

So, $x_0 = -1, y_0 = 1$

So, general sol^n:-

$$x = -1 + \frac{6}{1}t \Rightarrow x = 6t - 1$$

$$y = 1 - 5t \Rightarrow y = -5t + 1$$

Different values of t gives diff sol^n.

$t = 0, \quad x = x_0 = -1$

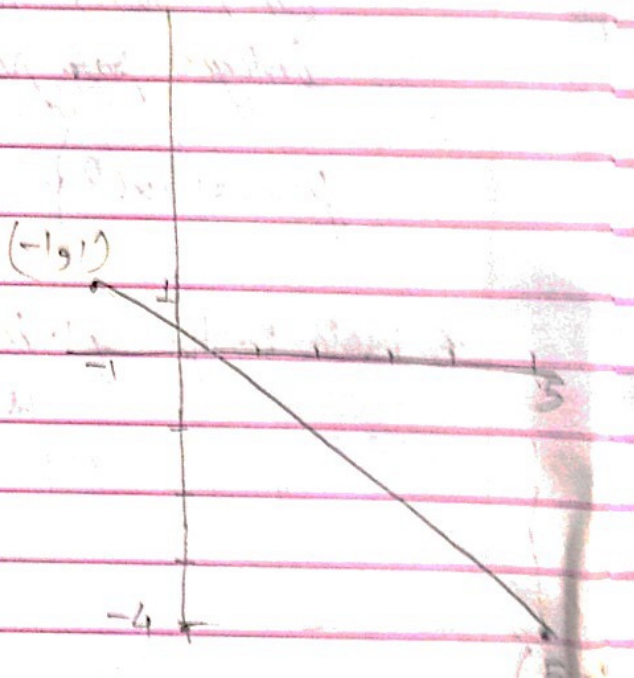
$y = y_0 = 1$

$t = 1, \quad x = 5$

$y = -4$

$t = -1, \quad x = -7$

$y = 6$



All these sol^{ns} lie on the line & will be EQUALLY SPACED.

eg find sol^n of $7x + 18y = 208$, if it exists.

$g.c.d(7,18) = 1$

& $1 \mid 208$. So, sol^n exists.

For finding sol^n: Use Euclidean algorithm.

$18 = 7\times2 + 4$

$7 = 4\times1 + 3$

$4 = 3\times1 + 1$

$3 = 1\times3 + 0.$

So, $g.c.d(18, 7) = 1$

Writing backwards:

$1 = 4 - 3\times1$

$= 4 - (7 - 4\times1)\times1$

$= 4 - (7\times1) + 4\times1$

$= 4\times2 - 7\times1$

$= (18 - 7\times2)\times2 - 7\times1$

$= 18\times2 - 7\times5 \Rightarrow 7(-5) + 18(2) = 1$

$\Rightarrow$ We got eqn:-

$\Rightarrow$ $7(-5) + 18(2) = 1$

$\times 208$, both sides

$\Rightarrow$ $7(-1040) + 18(416) = 208$

So, general soln:

$x = -1040 + 18t$

$y = 416 - 7t$

Suppose we want +ve value of x.

So, take $t \geq 58$

↳ for $t = 58$

$x = -1040 + 1044 = 4$

$y = 416 - 406 = 10.$

Verific^n: $7\times4 + 18(10) = 208.$

eg A man pays $1.43 for some apples & oranges. If oranges cost 17c each & apples, 15c each, how many of each did he buy?

So, $x \rightarrow$ no. of oranges
$y \rightarrow$ no. of apples

So, $17x + 15y = 143$

$g.c.d(15, 17) = 1$

$1 \mid 143$. So, sol^n exists.

Now,

$17 = 15 \times 1 + 2$

$15 = 2 \times 7 + 1$,

$2 = 1 \times 2 + 0$.

Now, $g.c.d = 1$

$1 = 15 - 2 \times 7$

$= 15 - (17 - 15 \times 1) \times 7$

$= 15 + 15(7) - 17(7)$

$1 = 15(8) - 17(7)$

$\Rightarrow 17(-7) + 15(8) = 1$

$\times 143$, both sides

$\Rightarrow 17(-1001) + 15(1144) = 143$

$x_0 = -1001$

$y_0 = 1144$.

$\Rightarrow$ General sol^n:- $x = -1001 + 15t$

$y = 1144 - 17t$

let $t = 67$, for making $x > 0$

So, $x = -1001 + 15(67) = 4$

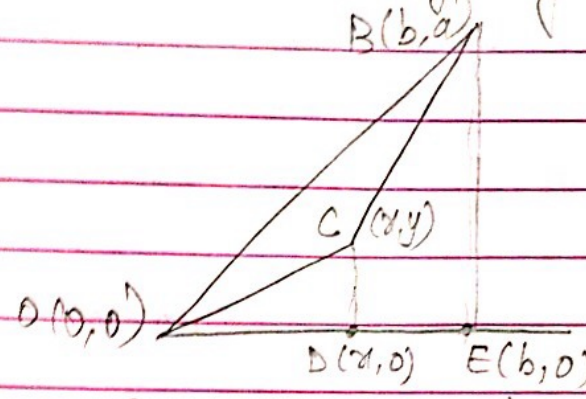
$y = 1144 - 17(67) = 5$.

$\Rightarrow x = 4, y = 3$ Ans

eg: Let the vertices of a triangle be O : (0,0), B : (b,a) & C : (x,y)

Show that area is given by $\left|\frac{bx-ay}{2}\right|$

Idea :- Make any angled Δ from given pts.



Make it a right angled Δ, as shown.

$\therefore$ Area (OBE) − Area (OCD) − Area (CDEB)
(Δ) (Δ) (Trap.)

= Area (OBC)

$\Rightarrow$ Area $(\Delta OBC) = \frac{1}{2}(ab) - \frac{1}{2}(xy) - \frac{1}{2}(b-x)[y+a]$

$\frac{1}{2} \times h(b_1+b_2)$

$= \frac{ab}{2} - \frac{xy}{2} - \frac{by}{2} - \frac{ab}{2} + \frac{xy}{2} + \frac{ax}{2}$

$\Rightarrow$ Area $(\Delta OBC) = \left|\frac{ax-by}{2}\right| = \left|\frac{bx-ay}{2}\right|$

eg: Show that if (x_0, y_0) is a sol^n of linear diophantine eq^n (l.d.e), $ax - by = 1$, then area of triangle, whose vertices are (0,0), (b,a) & (x_0, y_0) is $\frac{1}{2}$.

From previous question:
area of Δ with vertices $(0,0), (b,a), (x,y)$

$$= \left| \frac{by - ax}{2} \right|$$

& We are given :- (x_0, y_0) is a sol^n of

$$ax - by = 1$$

$$\Rightarrow ax_0 - by_0 = 1$$

$$\text{or} \quad |by_0 - ax_0| = |1|$$

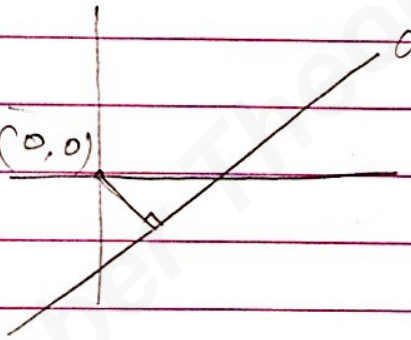
Using this in area

$$\Rightarrow \left| \frac{by_0 - ax_0}{2} \right| = \text{area}$$

$$\Rightarrow \text{area} = \frac{1}{2} \text{ sq. units}$$

---

eg Find the perpendicular distance to the origin $(0,0)$, from the line defined by $ax - by = 1$.



Using distance formula :-
Instead of $(0,0)$, say $(x', y') = (x', y')$

$$d = \left| \frac{ax' + by' + c}{\sqrt{a^2 + b^2}} \right|$$

↳ $x' = 0, \; y' = 0, \; c = -1$

$$\Rightarrow d = \left| \frac{-1}{\sqrt{a^2 + b^2}} \right| = \frac{1}{\sqrt{a^2 + b^2}}$$

Q. Show that the g.c.d $(2a+1, 9a+4) = 1$

Sol^n :- Idea : If we can find x & y s.t

$$x(2a+1) + y(9a+4) = 1$$

By observation : $x = 9, \; y = -2$ (can have other solutions)

Page No

Q. For any integer n, show:
$\frac{21n+4}{14n+3}$ is irreducible.

$\Rightarrow GCD = 1$.

$(21n+4)x + (14n+3)y = 1$

↳ If ∃ some x, y for this to be true, we get ans.

Using $x = -2, y = 3$ (observation)

$-42n - 8 + 42n + 9 = 1$.

So, its satisfied

Can be true for other values also HP

(Idea: find l.c.m (14, 21) = 42.
So, the factors are 3, 2.)

After

$21n+4 = (14n+3) + (7n+1)$

$14n+3 = (7n+1) \times 2 + 1$

$7n+1 = 1 \times (7n+1) + 0$

$\Rightarrow GCD = 1$. HP

Q. What is the shortest possible distance b/w 2 lattice pts. on the line defined by linear diophantine eqⁿ. $ax - by = c$

↓ Integer pts. satisfying the line.

Ans:- $\frac{(a^2+b^2)^{1/2}}{g.c.d(a,b)}$

* Lattice pt :- A pt. whose coordinates are integers.

If eqn is $ax - by = c$.

So, sol^n $\Rightarrow x = x_0 + \frac{b}{d}t$.

& $y = y_0 + \frac{a}{d}t$.

$\hookrightarrow t = 0, \pm 1, \pm 2, \ldots$

For subsequent points, take $t = 0, t = 1$.

$\Rightarrow$ (pt. 1) $x = x_0 + 0 = x_0$

$y = y_0 + 0 = y_0$

(pt. 2)

$x = x_0 + \frac{b}{d}$

$y = y_0 + \frac{a}{t}$.

Now, distance b/w them

$$\text{Distance} = \sqrt{\left[\left(x_0 + \frac{b}{d}\right) - x_0\right]^2 + \left[\left(y_0 + \frac{a}{t}\right) - y_0\right]^2}$$

$$= \sqrt{\frac{b^2}{d^2} + \frac{a^2}{d^2}}\, d^2$$

$$= \frac{\sqrt{a^2 + b^2}}{d}$$

$$\text{Distance} = \frac{\sqrt{a^2 + b^2}}{g.c.d(a,b)} \quad \text{Ans}$$

General Theorem: The linear diophantine eqⁿ

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c$$

is solvable iff $g.c.d.(a_1, a_2, \dots, a_n) \mid c$.

eg Find whether $6x + 8y + 12z = 10$ is solvable or not?

Idea: find g.c.d (6, 8, 12)

$6 = 2 \cdot 3$

$8 = 2^3$

$12 = 2^2 \cdot 3$.

So, g.c.d = 2.

Also $2 \mid 10$ ∴ So, eqⁿ is solvable.

eg (2) Find whether eqⁿ $6x + 12y + 15z = 10$ is solvable

g.c.d (6, 12, 15) = 3.

$3 \nmid 10$, so, its not solvable for integer solution

Notation: $g.c.d(a, b, c \dots) \equiv (a, b, c, \dots)$

$l.c.m(a, b, c \dots) \equiv [a, b, c \dots]$

Q. If a cock is worth 5 coins, a hen - 3 coins & 3 chicks together - 1 coin.

How many cocks, hens & chicks totalling 100 can be bought from 100 coins

Let no. of cocks = x

no. of hens = y

no. of chicks = z

So, $5x + 3y + \frac{z}{3} = 100 \rightarrow (1)$

$x + y + z = 100 \rightarrow (2)$

2 eqns, 3 variables.

Now, find sol^n:

Idea: Get rid of any one variable, say z

$\Rightarrow$ from (2),

$$z = 100 - x - y$$

$\Rightarrow$ (1) becomes

$$5x + 3y + \frac{(100 - x - y)}{3} = 100$$

$$\Rightarrow \frac{14}{3}x + \frac{8}{3}y + \frac{100}{3} = 100$$

$$\Rightarrow 7x + 4y = 100.$$

Finding sol^n of this l.d.e.

finding g.c.d (7, 4)

$= 1$.

Now, $7 = 4 \times 1 + 3.$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$

Now,

$1 = 4 - 3 \times 1$

$= 4 - (7 - 4 \times 1) \times 1$

$\Rightarrow 1 = 4 \times 2 - 7 \times 1$

$\Rightarrow 7(-1) + 4(2) = 1$

$\Rightarrow 7(-100) + 4(200) = 100$

So, general sol^n:-

$$x = -100 + 4t$$

$$y = 200 - 7t$$

Make $x > 0 \Rightarrow t = 26$

$\Rightarrow x = 4$

$y = 18.$ (3)

Using (3) in (2)

$\Rightarrow 4 + 18 + z = 100$

$\Rightarrow z = 100 - 22$

$\Rightarrow z = 78$

So, one solution :-

$x = 4,\ y = 18,\ z = 78.$

& we can get also get other values.

(1) $6x + 8y + 12z = 10$ → (1)

Q. was found to be solvable.

Now, find soln of it

Soln: Here, ∃ 1 eqn, 3 unknowns.

Idea : Start by taking/considering only 2 terms.

Say, we take :-

$8y + 12z$

↳ g.c.d = 4.

So, we can have :

$8y + 12z = 4u$ → (2)

$12 = 8 \times 1 + 4$

$8 = 4 \times 2 + 0$

$\Rightarrow 4 = 12 - 8 \times 1$

$\Rightarrow 4 = 8(-1) + 12(1)$ → (A)

Now, using (2) in (1)

$\Rightarrow 6x + 4u = 10$

↳ g.c.d = 2

$6 = 4\times1 + 2$

$4 = 2\times2 + 0$

$\Rightarrow 2 = 6 - 4\times1$

$\Rightarrow 2 = 6(1) + 4(-1)$

$\times 5$ both sides

$\Rightarrow 6(5) + 4(-5) = 10$

So, $x_0 = 5$, $u_0 = -5$.

So, general:- $\left.\begin{aligned} x &= 5 + 2t \\ u &= -5 - 3t \end{aligned}\right\} \rightarrow (3)$

From (2),

$8y + 12z = 4u$

$\Rightarrow 8y + 12z = 4(-5 - 3t)$

From (A)

$8(-1) + 12(1) = 4.$

$\times (-5 - 3t)$

$\Rightarrow 8(5 + 3t) + 12(-5 - 3t) = 4(-5 - 3t)$

So, $y_0 = 5 + 3t$, $z_0 = -5 - 3t$

$\Rightarrow y = (5 + 3t) + 3t'$

$\Rightarrow y = 5 + 3t + 3t' \longrightarrow (4)$

& $z = (-5 - 3t) - 2t'$

$\Rightarrow z = -5 - 3t - 2t' \longrightarrow (5)$

From (3), (4) & (5), we get

$x = 5 + 2t$

$y = 5 + 3t + 3t'$

$z = -5 - 3t - 2t'$

Say, $t = t' = 1$

$\Rightarrow x = 7$

$y = 11$

$z = -10$

---- we can find other values for t & t'.

Page No

Q. 29 Does $2x+3y+4z=5$ ① have a solution? If yes, find it

Here, g.c.d (2, 3, 4) = 1. So, solution ∃.

Consider:

$2x+3y=u \rightarrow ②$

Using ② in ①

$\Rightarrow u+4z=5$

↳ g.c.d = 1

$\Rightarrow u_0=1, z_0=1$

$\Rightarrow u = 1+4t$
$z = 1-t.$ } → ③.

From ②.

$2x+3y=(1+4t)$.

& $2(-1)+3(1)=1$

$\times (1+4t)$

$\Rightarrow 2(-1-4t)+3(1+4t)=1+4t$.

$\Rightarrow x_0 = -1-4t$

$y_0 = 1+4t$.

$\Rightarrow x = -1-4t+3t'$
$y = 1+4t-2t'$ } → ④

& $z = 1-t$ (from ③)

Now, different values of t & t' gives solution.

↳ let $t=t'=0$.

$\Rightarrow x=-1, y=1, z=1$

$\Rightarrow -2+3+4=5$. So, satisfies.

≡ : Symbol for congruency

CLASSMATE

CHAPTER- CONGRUENCES

eg: What time is 22 hours.

idea :- $\frac{22-?}{12}$ ⇒ ? = 10.

∴ 22 hrs = 10 o'clock

This is the idea of congruences — Gauss.

Similar is seen in car odometers & finding day of any year, date.

* Defin^{n}: If $c \neq 0$, we say

$a \equiv b \pmod{c}$; provided $c \mid a-b$

eg :- $\frac{22-10}{12} = 1$ (integer)

↳ ∴ we write $22 \equiv 10 \pmod{12}$

eg :- $5 \equiv 3 \pmod{2}$ ✓

∵ $\frac{5-3}{2} = 1$

eg: $7 \not\equiv 2 \pmod{3}$

∵ $\frac{7-2}{3} \not\in$ integer.

* Theorem: For arbitrary integers a and b,

$a \equiv b \pmod{c}$

iff a & b leave the same non-ve remainder.

eg: we had $5 \equiv 3 \pmod{2}$

∴ $\frac{5}{2}$ leaves remainder = 1 ($5 = 2 \times 2 + 1$) → same non-ve remainder

$\frac{3}{2}$ leaves remainder = 1 ($3 = 2 \times 1 + 1$)

Page No

* Format's Little Theorem:
If p is prime and n is a +ve integer, then,
$p \mid n^p - n$

eg :- $n = 5$, $p = 3$
Then, $3 \mid 5^3 - 5$.

* $n^p \equiv n \pmod{p}$

* Wilsons Theorem :
If p is a prime, then, $p \mid [(p-1)! + 1]$

we can also write :-
$$(p-1)! \equiv -1 \pmod{p}$$

eg : consider $p = 7$
$\Rightarrow 6! = 720$.
$6! + 1 = 721$
& $7 \mid 721$ So, true.

* Properties :

P1) $a \equiv a \pmod{c}$

P2)
If $a \equiv b \pmod{c}$
$\Rightarrow a \equiv b \pmod{-c}$

* Theorem: If a, b, c & d are integers ($c \neq 0$), then, the following assertions hold.
1. $a \equiv a \pmod{c}$ → Reflexive property
2. $a \equiv b \pmod{c}$ then $b \equiv a \pmod{c}$ → Symmetric property

3. If $a \equiv b \pmod c$ and $b \equiv d \pmod c$, then, $a \equiv d \pmod c$ → Transitive property.

Proof :-

- Reflexive property :
  Show $a \equiv a \pmod c$
  As. $\frac{a-a}{c} = 0$. So, congruent. True $\forall$ c ($\in$ Integer)

- Symmetric property :
  Let $a \equiv b \pmod c$
  $\Rightarrow \frac{a-b}{c}$ = integer = k, say.
  $\Rightarrow -\left(\frac{b-a}{c}\right) = k$
  $\Rightarrow \frac{b-a}{c} = -k$ = Integer
  $\Rightarrow b \equiv a \pmod c$

- Transitive property :
  let $\frac{a-b}{c} = k_1$ and $\frac{b-d}{c} = k_2$.
  Adding $k_1 + k_2$
  $\Rightarrow \frac{a-b}{c} + \frac{b-d}{c} = k_1 + k_2$
  $\Rightarrow \frac{a-d}{c} = k_1 + k_2$ = integer
  $\Rightarrow a \equiv d \pmod c$ H.P

eg : $a = 5, b = 3, c = 2, d = 1$.
clearly, $5 \equiv 3 \pmod 2$ and $3 \equiv 1 \pmod 2$
So, $5 \equiv 1 \pmod 2$ ($\because \frac{5-1}{2} \in Z$)

★ Theorem :-

Suppose $a \equiv a' \pmod{c}$ & $b \equiv b' \pmod{c}$

Then, $a \pm b \equiv a' \pm b' \pmod{c}$

& $ab \equiv a'b' \pmod{c}$

eg :- $a = 5,\ a' = 3,\ b = 3,\ b' = 1,\ c = 2$

$5 \equiv 3 \pmod 2$ & $3 \equiv 1 \pmod 2$

So, $5 + 3 \equiv 3 + 1 \pmod 2$

$5 \cdot 3 \equiv 3 \cdot 1 \pmod 2$

Proof :-

$\frac{a - a'}{c} = k_1$, say ; $\frac{b - b'}{c} = k_2$, say

Adding :- $\frac{(a+b) - (a'+b')}{c} = k_1 + k_2$

$= \text{Integer}.$

$\Rightarrow a + b \equiv a' + b' \pmod c$

Ily for $a - b \equiv a' - b' \pmod c$

Now, proving

$ab \equiv a'b' \pmod c$

Lets say we take difference of ab & $a'b'$ divided by c (given $a \equiv a' \pmod c$ & $b \equiv b' \pmod c$)

i.e $\frac{ab - a'b'}{c}$.

Add and subtract by ab'

$\Rightarrow \frac{ab - ab' + ab' - a'b'}{c}$

$= \frac{a(b-b') + b'(a-a')}{c} = \frac{a(b-b')}{c} + \frac{b'(a-a')}{c}$

$= a(k_1) + b'(k_2) = \text{Integer}.$

$\Rightarrow \frac{ab - a'b'}{c} = \text{Integer}.$ So, $ab \equiv a'b' \pmod c$

* Theorem : Cancellation Law.

If $bd \equiv bd' \pmod{c}$,

then, $d \equiv d' \pmod{c}$ iff $g.c.d(b,c) = 1$

Proof :-

Given :- $bd \equiv bd' \pmod{c}$

$\Rightarrow \frac{bd - bd'}{c} = k.$

$\Rightarrow \frac{b(d-d')}{c} = k.$

$\because g.c.d(b,c) = 1$, So, $c \nmid b$.

Hence, $c \mid (d-d')$ So that $\frac{b(d-d')}{c} = k$ = integer

$\Rightarrow d \equiv d' \pmod{c}$

eg :- $6 \equiv 12 \pmod{2}$ i.e $2 \times 3 \equiv 2^2 \cdot 3 \pmod{2}$

If we divide by 2

$\Rightarrow 3 \equiv 6 \pmod{2}$

doesn't hold.

($\because$ 2 is not relatively prime to 2 $\because$ g.c.d(2,2) = 2)

If we divide by 3

$\Rightarrow 2 \equiv 4 \pmod{2}$

So, holds.

So, it held true $\because$ 2 & 3 are not relatively prime.

eg :- $5x \equiv 4 \pmod{3}$

$\Rightarrow \frac{5x-4}{3} = k$, integer.

Let $x = 2$ It satisfies

$\exists$ infinitely many sol^{n}.

Q. Prove that if $x \equiv y \pmod m$ & $a_0, a_1, a_2, \ldots, a_k$ are integers. Then,

$$a_0 x^k + a_1 x^{k-1} + \ldots + a_k \equiv a_0 y^k + a_1 y^{k-1} \ldots + a_k \pmod m$$

So, we have to show

$$\frac{(a_0 x^k + a_1 x^{k-1} + \ldots + a_k) - (a_0 y^k + a_1 y^{k-1} + \ldots + a_k)}{m}$$

will give integer

$$\Rightarrow \frac{a_0 (x^k - y^k) + a_1 (x^{k-1} - y^{k-1}) + \ldots + a_{k-1}(x - y)}{m}$$

$$\Rightarrow (x-y)\left[\frac{\text{integer}}{m}\right] \rightarrow (1)$$

Now, $x \equiv y \pmod m$, given

$$\Rightarrow \frac{x-y}{m} = \text{integer} \rightarrow (2)$$

Using (2) in (1)

$\Rightarrow$ integer (integer)

So, it gives integer

eg If $bd \equiv bd' \pmod p$; p : prime no.

Show :- $d \equiv d' \pmod p$

Also, given $p \nmid b$.

Given :- $p \nmid b$ & $\frac{bd - bd'}{p} = k = \text{Integer}$.

$$\Rightarrow \frac{b(d-d')}{p} = k.$$

As $p \nmid b$. So, $p \mid (d-d') \Rightarrow d \equiv d' \pmod p$

Page No

✱ RESIDUES & RESIDUE SYSTEM

Defin^n: If $a \equiv r \pmod m$, where $0 \leq r < m$.
Then, r is called the residue.

way to see:

$$6\overline{)20}\,3 \qquad 20 = 6 \times 3 + 2$$

$$-18$$

remainder $\rightarrow$ (2) So, $20 \equiv (2) \pmod 6$

✱ Complete Residue System: (CRS)

Defin^n: The set of integers $\{r_1, r_2, \ldots, r_s\}$ is called a complete residue system mod m, if

(i) $r_i \not\equiv r_j$ whenever $i \neq j$

(ii) for each integer n, there corresponds an r_i s.t.

$$n \equiv r_i \pmod m$$

eg :- Set : $\{1, 2, 3\}$.
Show this set is a complete residue sys. mod 3.

Seeing cond^{ns} :-

(i) $1 \not\equiv 2 \pmod 3$
$1 \not\equiv 3 \pmod 3$
$2 \not\equiv 3 \pmod 3$

(ii) eg : $n = 3$
$\Rightarrow 3 \equiv 3 \pmod 3$
$5 \equiv 2 \pmod 3$
$6009 \equiv 3 \pmod 3$

* Note: No. of elements in a CRS should be equal to value of mod.

CLASSMATE

* Theorem :-

If s different integers $r_1, r_2, r_3, \ldots, r_s$ form a complete residue sys mod m, then,

$$s = m.$$

* Note: let m be a +ve integer.

Then, $\{0, 1, 2, \ldots, m-1\}$ is a CRS.

▶ Alternate defin^n of CRS.

The set $\{r_1, r_2, \ldots, r_s\}$ is said to be a CRS mod m, if each r_i is congruent to some element in $0, 1, 2, \ldots, m-1$.

Q Show $\{1, 5, 9\}$ is CRS mod (3)

$\{r_1, r_2, r_3\}$ — 3 elements

Sol^n: Here, we have $m = 3$.

So, $\{0, 1, 2\}$ will be a CRS

Now, we have to show that each element of $\{1, 5, 9\}$ is congruent to some element of $\{1, 2, 3\}$

(1) $1 \equiv 1 \pmod 3$

(2) $5 \equiv 2 \pmod 3$

(3) $9 \equiv 0 \pmod 3$

So, each residue has a pair in 0 to $m-1$.

Use of residues

eg Find an integer n s.t $325n \equiv 11 \pmod 3$ is satisfied.

Idea: Replace $325 \in \mathbb{N}$ by its residues (mod 3)

So, we can write

$$325 \equiv 1 \pmod 3$$

$$\& \; 11 \equiv 2 \pmod 3$$

So, we get

$$1(n) \equiv 2 \pmod 3$$

$\Rightarrow$ This will be satisfied with $n = 2$

So, Ans. = $n = 2$ (smallest value. Other values also exist)

✱ Reduced Residue System (R.R.S)

Defⁿ: The set of integers $\{r_1, r_2, \dots, r_s\}$ is called a reduced residue system mod m, iff

(1) $g.c.d(r_i, m) = 1 \quad \forall \; i$

(2) $r_i \not\equiv r_j \pmod m$ whenever $i \neq j$

(3) for each integer n, relatively prime to m, there corresponds an r_i, s.t

$$n \equiv r_i \pmod m$$

eg:- we have mod 6.

So, a CRS = $\{0, 1, 2, 3, 4, 5\}$ mod 6.

Idea: leave the no's which dont have a common factor with 6.

So, leave $0, 2, 3, 4$.

× × × ×

Page No

hence, $\{1, 5\}$ form a reduced residue system

- Special case; if $m = p$, a prime no, then,

$$C.R.S = \{0, 1, 2, \ldots, p-1\}$$
$$\& \quad R.R.S = \{1, 2, \ldots, p-1\}$$
(Remove zero)

* Defⁿ:

The fⁿ $\phi(m)$ gives the no. of elements in a RRS., where $\phi(m)$: Euler's fⁿ.

eg: for RRS $= \{1, 2, \ldots, p-1\}$

$\phi(p) = p-1$.

element, mod

eg: Find whether $\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21\}$ is a CRS (mod 11) or not

→ It's not an RRS (∵ g.c.d (11, 11) = 11)

Note: here, no. of elements in set = value of mod = 11.

So, we can write a CRS

CRS = $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Now, we have to pair our set with this set

So, $1 \equiv 1 \pmod{11}$

$3 \equiv 3 \pmod{11}$

$5 \equiv 5 \pmod{11}$

$7 \equiv 7 \pmod{11}$

$9 \equiv 9 \pmod{11}$

$11 \equiv 0 \pmod{11}$

$13 \equiv 2 \pmod{11}$

$15 \equiv 4 \pmod{11}$

$17 \equiv 6 \pmod{11}$

$19 \equiv 8 \pmod{11}$

$21 \equiv 10 \pmod{11}$

So, every no. has a match.

(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)

eg Find whether $\{1, 5, 7, 11, 13, 17\}$ is an RRS mod 18 or not.

(1) i.e. show none of the elements are congruent to each other (they are relatively prime).
here, we can see directly
g.c.d of $1, 5, 7, 11, 13, 17$ with 18 is 1

(2) Now, clearly, $\because$ none of the elements are (-ve) or (> 18), so, we have

$1 \not\equiv 5 \pmod{18}$	$5 \not\equiv 7$	$7 \not\equiv 13$
$1 \not\equiv 7$ "	$5 \not\equiv 11$	$7 \not\equiv 17$
$1 \not\equiv 11$ "	$5 \not\equiv 13$	$11 \not\equiv 13$
$1 \not\equiv 13$ "	$5 \not\equiv 17$	$11 \not\equiv 17$
$1 \not\equiv 17$ "	$7 \not\equiv 11$	$13 \not\equiv 17$

(3) Take $n = 31$, say → Chosen s.t g.c.d $(18, 31) = 1$
So, we have to find some no. from our set, s.t $31 \equiv 13 \pmod{18}$
So, we can find some integer to make it possible.
So, our set is an RRS.

☆ SOLVING CONGRUENCES.

eg $15x \equiv 9 \pmod{12}$
Solve the above congruence. i.e find x.

(1) Note: Check if solution exists.
$15x \equiv 9 \pmod{12}$
$\Rightarrow ax \equiv b \pmod{c}$ & g.c.d $(a, c) = d$.
If $d \mid b$, then, soln exists.

Here,

$g.c.d(15, 12) = 3$ & $3 \mid 9$.

$\therefore$ soln exists.

✱ Theorem:

If $d = g.c.d(a, b, c)$. Then, congruence $ax \equiv b \pmod{c}$ has no solution if $d \nmid b$ & has d mutually incongruent sol^{ns} if $d \mid b$.

eg Solving above eq.

$$15x \equiv 9 \pmod{12}$$

$$\Rightarrow \frac{15x - 9}{12} = \text{integer} = y, \text{ say}$$

$$\Rightarrow 15x - 9 = 12y$$

$$\Rightarrow 15x - 12y = 9 \quad \text{(A diophantine eq}^{n}\text{)}$$

$\div$ eq^{n} by 3

$$\Rightarrow 5x - 4y = 3 \longrightarrow (1)$$

$$5 = 4 \times 1 + 1.$$

$$4 = 1 \times 4 + 0. \quad ; g.c.d = 1.$$

$$\Rightarrow 1 = 5 - 4 \times 1.$$

$$1 = 5(\ ) - 4(1)$$

$$\Rightarrow 3 = 5(3) - 4(3) \longrightarrow (2).$$

Comparing (1) & (2).

$$\Rightarrow x_0 = 3$$

General solution: $x = 3 + 4t$; $t = 0, \pm 1, \pm 2, \pm 3, \ldots$

Now, note that our g.c.d was 3 ⇒ 3 incongruent sol^n
Also, we take value of t that gives smallest positive value of x.

Now, for $t=0$, $x=3$
$t=1$, $x=7$.

So, x can vary ∈ {... −9, −5, −1, 3, 7, 11, 15, 19, ...}

Seeing the value of x & smallest value of x ∈ the set {3, 7, 11} form a mutually incongruent sol^n. [If any other +ve 3 values are taken, it not smallest & its congruent (mod 12)]

eg (a) $7x \equiv 5 \pmod{11}$

g.c.d (7, 11) = 1

So, 1 | 5. So, solution exists.

Now, $\frac{7x-5}{11} = y$, say

$\Rightarrow 7x - 11y = 5.$

Solving :-

$11 = 7 \times 1 + 4$

$7 = 4 \times 1 + 3$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$

g.c.d = 1

$\Rightarrow 1 = 4 - 3 \times 1$

$= 4 - [7 - 4 \times 1] \times 1$

$= 4 \times 2 - 7 \times 1$

$= (11 - 7 \times 1) \times 2 - 7 \times 1$

$\Rightarrow 1 = 11 \times 2 - 7 \times 3$

$\Rightarrow 7(-3) - 11(-2) = 1$

$\times 5$

$\Rightarrow 7(-15) - 11(-10) = 5$

$\Rightarrow x_0 = -15$

So, general solution : $x = -15 + 11t$

$t = 0, \; x = -15$

$t = 1, \; x = -4$

$t = 2, \; x = 7$

$t = 3, \; x = 18$

$t = 4, \; x = 29$

$3 \cdot 4 \cdot 4$
$- \; 15$
$\overline{29}$

$\therefore$ g.c.d = 1. So, $\exists$ no incongruent sol^n.

Now, value of t s.t x has smallest +ve value is $t = 2$

So, unique sol^n : $x = 7$

(b) $8x \equiv 10 \pmod{30}$

g.c.d$(8, 30) = 2$.

$2 \mid 10$. So, solution exists.

Now, we have to find 2 incongruent solutions.

$\frac{8x - 10}{30} = y$

$\Rightarrow 8x - 30y = 10.$

$\Rightarrow 4x - 15y = 5. \rightarrow (1)$

Now, $15 = 4 \times 3 + 3$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$

$\Rightarrow$ g.c.d $= 1$.

$\Rightarrow 1 = 4 - 3 \times 1$

$= 4 - (15 - 4 \times 3) \times 1$

$\Rightarrow 1 = 4(4) - 15(1)$

Page No

$\Rightarrow 4(4) - 15(1) = 1$

$\times 5$

$\Rightarrow 4(20) - 15(5) = 5.$

So, $x_0 = 20$

& x = General sol^n $= 20 + 15t$.

$t = -1$, $x = 5$.

$t = 0$, $x = 20$

$t = 1$, $x = 35$.

⋮

So, $\{5, 20\}$ is the set of mutually incongruent solutions.

Note: Our original problem had $(8, 10)$, having g.c.d $= 2$.

We reduced it to $(4, 5)$ having g.c.d $= 1$

∵ originally, g.c.d $= 2$, So, ∃ 2 mutually incongruent sol^{ns} (not 1)

☆ Euler's Theorem:

If g.c.d$(a, m) = 1$

then, $a^{\phi(m)} \equiv 1 \pmod{m}$

eg: If $m = 7$

RRS $= \{1, 2, 3, 4, 5, 6\}$.

$\phi(m) = 6$. (6 elements in RRS)

Now, take any prime no. (a: relatively prime to m)

s.t g.c.d(prime no, 7) $= 1$.

So, let $= 2$.

So, $2^6 \equiv 1 \pmod{7}$ holds.

Proof :-

Let $k_1, k_2, \dots, k_{\phi(m)}$ be no. of elements of RRS.

Then, $ak_1, ak_2, \dots, ak_{\phi(m)}$ will be relatively prime to m

So, each ak_i can be paired with some k_j s.t. $a_{k_i} \equiv k_j \pmod m$

Now, we saw, if $a \equiv b \pmod m$

$c \equiv d \pmod m$

Then, $ac \equiv bd \pmod m$

Hy. $ak_1, ak_2, \dots, a_{k_{\phi(m)}} \equiv k_1, k_2, \dots k_{\phi(m)} \pmod m$

$\Rightarrow a^{\phi(m)} (k_1, k_2 \dots k_{\phi(m)}) \equiv (k_1, k_2 \dots k_{\phi(m)}) \pmod m$

→ Cancellation was done ∵ k_i are relatively prime to m (Otherwise, cancellation in mod cannot be done)

$\Rightarrow a^{\phi(m)} \equiv 1 \pmod m$

Proved

23.3.2014

APPLICATIONS OF CONGRUENCES.

(1) ☆ RIFFLING

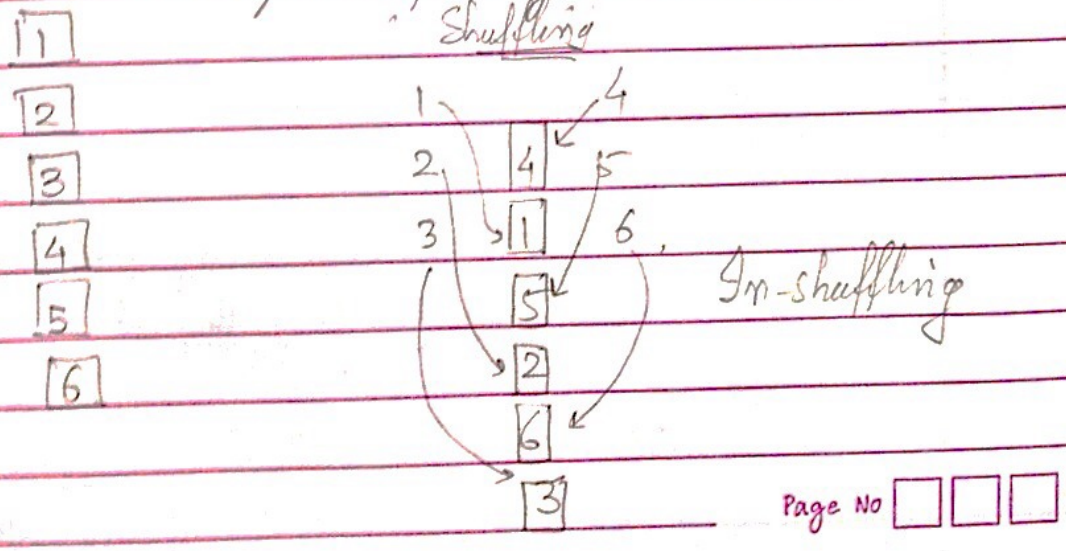
↳ related to playing cards

↳ Faro Shuffling : ordered shuffling to give interleaved space

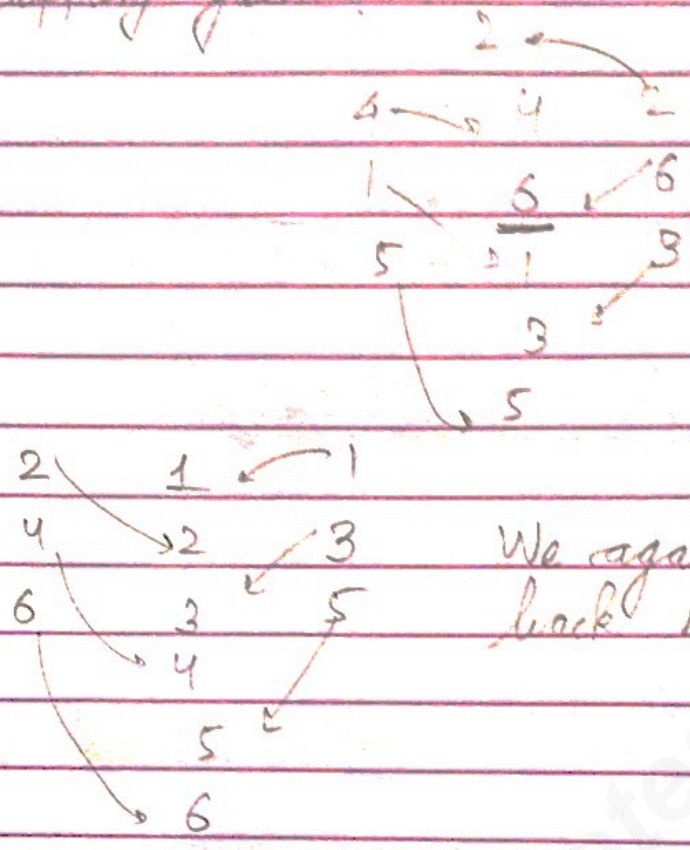
Defn :- Modified Faro Shuffle :

- It happens when a deck is cut into two equal parts & the cards are interleaved alternately.
  - If we start from left hand, its called IN. SHUFFLE & if we start from right its called OUT SHUFFLE.
- In n-In Shuffles of 'n' even no. of cards, brings back the pack to original order if $n+1$ is prime & $n-2$ → Out shuffles are reqd if $n-1$ is prime.
  - It was shown by Aldous that $(1.5)\log_2 n$ shuffles are sufficient to randomise the pack.

eg: consider a pack of only 6 cards :

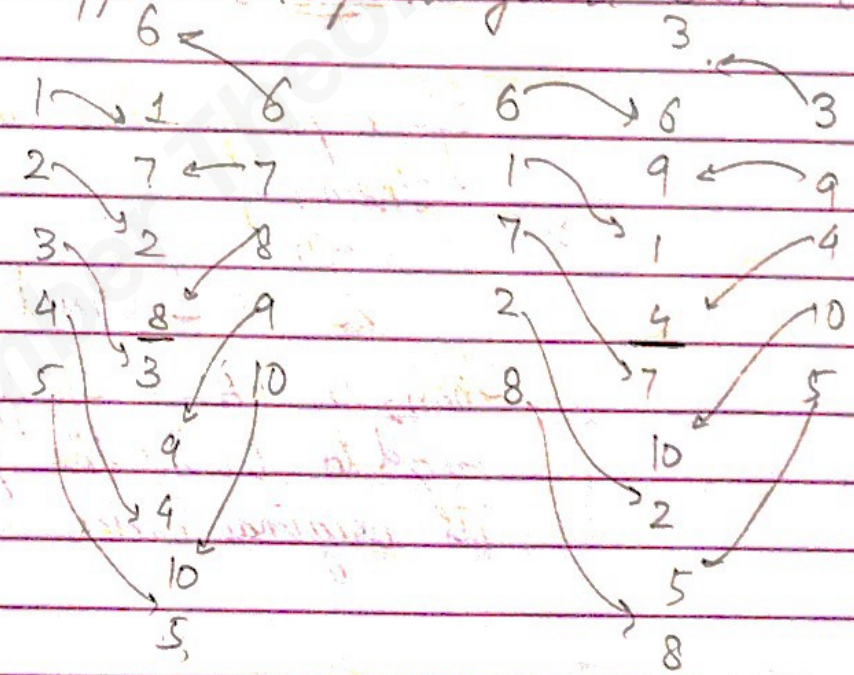


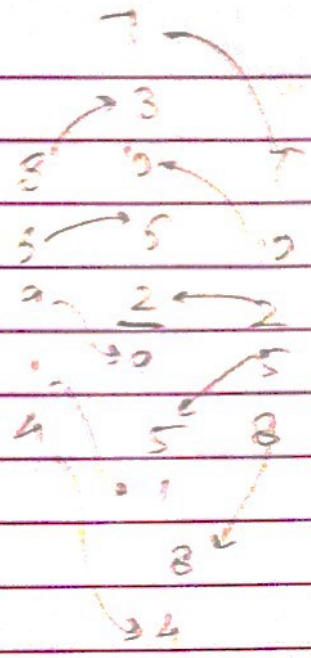
Shuffling again

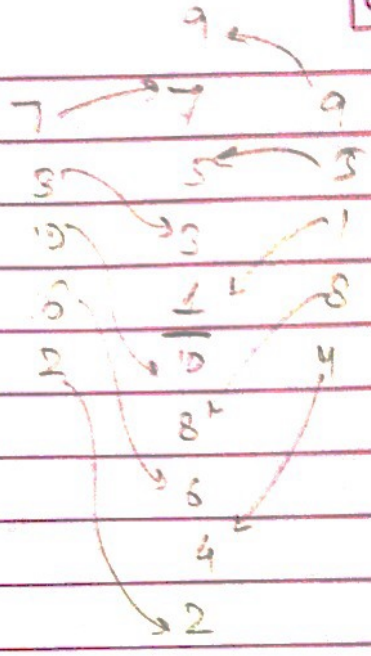


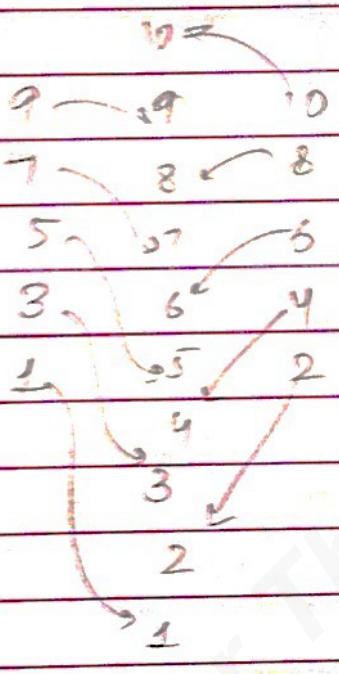
We again get the order back in 3 shuffles.

eg ② Consider a pack of 10 cards & seeing how many shuffles are req'd to get it back (n=10)









So, 5 Shuffles bring by order back

Formula :

If a pack has m cards. Then, if

$$2^n \equiv 1 \pmod{m+1}$$

Then, n FANO Shuffles are req^d to bring the pack to its original order.

eg :- If $m = 2$

$\Rightarrow 2^2 \equiv 1 \pmod 3$

So, 2 shuffles bring back.

$6+1$

eg (2) $2^3 \equiv 1 \pmod 7$

$\Rightarrow$ 3 shuffles bring a pack of 6 back

eg (3) $2^5 \equiv 1 \pmod 3$

So, 5 shuffles req'd for a pack of 30.

eg (4): Using Euler's Theorem:

We know:- $a^{\phi(m)} \equiv 1 \pmod m$

If $m = p$, a prime no.,

$$\phi(p) = p-1$$

$\Rightarrow$

$$a^{p-1} \equiv 1 \pmod p$$

eg: For a pack of 62 cards, find no. of shuffles.

$$2^n \equiv 1 \pmod{63}$$

$n = 6$ will solve it

$$\Rightarrow \frac{64-1}{63} \in \mathbb{Z}$$

eg: How many modified perfect Faro shuffles are needed to return the cards to their original posn in a deck of

(i) 8 cards

(ii) 12 cards

$2^n \equiv 1 \pmod 9$ & $2^n \equiv 1 \pmod{13}$

↳ $n = 6$ ↳ $m+1$ = prime (= 13)

$2^6 \equiv 1 \pmod 9$

So, 6 shuffles... So, m cards are reqd to bring back

(2) ✱ DIVISIBILITY (FINDING REMAINDER)

eg: What is the remainder when 41^{75} is divided by 3

Idea:- If we have

$a \equiv b \pmod m$

we will also have

$a^n \equiv b^n \pmod m$

So, with this idea:

$41 \equiv ? \pmod 3$

↳ 2

$\Rightarrow 41 \equiv 2 \pmod 3$

So, $(41)^{75} \equiv 2^{75} \pmod 3$

Now, $2^2 \equiv 1 \pmod 3$

$2^{75} = 2^{37 \times 2 + 1}$

$= (2^2)^{37} \times 2$

Now, $(2^2)^{37} \times 2 \equiv (1)^{37} \times 2 \pmod 3$

$\Rightarrow 41^{75} \equiv 2^{75} \equiv (2) \pmod 3$

↳ Residue, ans ✓

Page No

Other residue = (-1)

$2 \equiv -1 \pmod 3$

Q. Find remainder when 473^{38} is divided by 5

$473 \equiv 3 \pmod 5$

$\Rightarrow (473)^{38} \equiv 3^{38} \pmod 5$

Also, $(473)^2 \equiv 4 \pmod 5$

$\Rightarrow (473)^{19} \equiv 4^{19} \pmod 5$

$4^2 \equiv 1 \pmod 5$

$\Rightarrow (4^2)^9 \cdot 4 \equiv 4$

So, remainder = 4 (residue)

M2

$(473)^{38} \equiv (3)^{38} \pmod 5$

$3^{37} \equiv 2 \pmod 5$

$\Rightarrow (3^3)^{12} \cdot 3 \equiv 2$

---

eg Find the remainder when 34×17 is divided by 29

A big no. can be broken up into factors & replaced by its residues.

$34 \equiv ? \pmod{29}$

Now, $34 \equiv 5 \pmod{29}$

So, $34 \times 17 \equiv 5 \times 17 \pmod{29}$

$= 85 \pmod{29}$

$\Rightarrow 34 \times 17 \equiv 27 \pmod{29}$

$29 \overline{)85(2}$
-58
27

Q. Find the remainder when 19×14 is divided by 23.

(M1) $19 \times 14 = 38 \times 7$.

$38 \equiv ? \pmod{23}$

$\Rightarrow 38 \equiv 15 \pmod{23}$

So, $19 \times 14 \equiv 15 \times 7 \pmod{23}$

$= 105 \pmod{23}$

$\equiv 13 \pmod{23}$

(M2) $19 \times 14 \equiv (-4)(-9) \pmod{23}$

$\equiv 36 \pmod{23}$

$\equiv 13 \pmod{23}$

Q. Show that $47 \mid 5^{23} + 1$

Idea - If $a \equiv b \pmod{m}$
then, $a^n \equiv b^n \pmod{m}$: use this.

We know → we want to make $(5)^{?4}$

$5^4 = 625 \equiv ? \pmod{47}$

So, $5^4 \equiv 14 \pmod{47}$

$\Rightarrow (5^4)^2 \equiv 14^2 \pmod{47}$

$\Rightarrow 5^8 \equiv 196 \pmod{47}$

$\Rightarrow 5^8 \equiv 8 \pmod{47}$ → ①

$47 \overline{)196(4}$
188
8

Page No

So, $5^{8 \cdot 2} \equiv 2^2 \pmod{47}$

$\Rightarrow 5^{16} \equiv 17 \pmod{47} \rightarrow (2)$

(M1) From (1)

$(5^8)^3 \equiv 8^3 \pmod{47} \equiv 42$

or $5^{24} \equiv -5 \pmod{47}$

Using Cancellation law:

As g.c.d $(5, 47) = 1$

So, we can divide by 5 from both sides

$\Rightarrow 5^{23} \equiv -1 \pmod{47}$

$\Rightarrow 5^{23} + 1 \equiv 0 \pmod{47}$

$\Rightarrow 5^{23} + 1$ is divisible by 47

(M2) Multiply (1) & (2) and solve.

$5^8 \cdot 5^{16} \equiv 8 \times 17 \pmod{47}$

- - -

Q. Find if 41 divides $(7 \times 3^{20}) + 6$

Idea: Start with a no. which has some power

We know, $3^4 \equiv ? \pmod{41}$

$\Rightarrow 3^4 \equiv (-1) \pmod{41}$

Raise to power 5

$\Rightarrow (3^4)^5 \equiv (-1)^5 \pmod{41}$

$\Rightarrow 3^{20} \equiv -1 \pmod{41}$

$\Rightarrow 3^{20} \equiv -1 \pmod{41}$

$\Rightarrow 7 \times 3^{20} \equiv -7 \pmod{41}$

$\Rightarrow 7 \times 3^{20} + 6 \equiv -1 \pmod{41}$

So, remainder $= 40$

So, $41 \nmid 7 \times 3^{20} + 6$

✡ (3) Finding the day of the week.

If date, month and year is known, the day of the week can be found.

∃ some codes that have to be found.

Codes for days :-		Codes for months		
Saturday	0	Jan	1	
Sunday	1	Feb	4	12^2
Mon	2	Mar	4	
Tue	3	Apr.	0	
Wed	4	May	2	5^2
Thu	5	Jun	5	
Fri	6	July	0	
		Aug	3	6^2
		Sep.	6	
		Oct.	1	
		Nov.	4	12^2+2
		Dec.	6	

eg: 22 May 1992.

Idea: Start with year.

Code for year: (y)

Do: $y + \left[\frac{y}{4}\right]$

Take last 2 digits of year: = y

$\Rightarrow y = 92$

$\Rightarrow 92 + \left[\frac{92}{4}\right] = 92 + 23 \equiv ?\ (\text{mod } 7)$

For day of week, use (mod 7)

So, $115 \equiv 3 \pmod 7$

So, code = 3.

So, Start with date + month + year

$22 + 2 + 3 = 27$

Now,

$27 \equiv 6 \pmod 7$

$\Rightarrow$ 6 is the day's code.

So its FRIDAY

Note: The formula requires correction, ∵ we have to account for leap years

~

Correction :

If the years are as follows, some corrections are made :-

For

① 2000 Subtract 1 (from date + month + year)

② 1900 no correction

③ 1800 add 2

④ 1700 add 4

⑤ 1600 add 6

⑥ 1500 If date is Oct. 15, 1582 to Dec 31, 1599

↓

no correction (or, add 0)

⑦ Before Oct 15, 1582 The first 2 digits of the year is subtracted from 18.

Q. Battle of Hastings was fought on 14th October, 1066. What day of the week was it?

1066

→ 66 = y

$y + \left[\frac{y}{4}\right] = 66 + 16 \equiv 5 \pmod 7$

→ Code for year

date + month + year.

$\Rightarrow (14 + 1 + 5) + (18 - 10) \equiv ? \pmod 7$

→ Code for October

$\Rightarrow 20 + 8 \equiv ? \pmod 7$

$\Rightarrow 28 \equiv 0 \pmod 7$

$\Rightarrow$ Code $= 0 \Rightarrow$ Saturday

(4) (2) 25th May year 1993

Which day?

$y = 93$

$y + \left[\frac{y}{4}\right] = 93 + 23 = 116$

So, $116 \equiv ? \pmod 7$

$\Rightarrow 116 \equiv (9) \pmod 7$

→ code for year

So,

$25 + 2 + 1 \equiv ? \pmod 7$

$31 \equiv ? \pmod 7$

$\Rightarrow$ code $= 3 \Rightarrow$ Tuesday ✓

(4)

Q. (1) Show the remainder is 5 when $(17)^7$ is divided by 7.

(2) Show 2^{37} is a multiple of 223

(1) $17 \equiv 3 \pmod 7$

$\Rightarrow 17^2 \equiv 9 \pmod$

Q. (TPT): Any date in the 20th Century beginning with March 1, 1900, falls on the same day of the week, 28 yrs later to 1900.

→ To Prove that

Soln: Let y' be the year that comes after every 28 years s.t

$$y' = y + 28k$$

As we deal with years, so, only year code is reqd. We show: year code is same every 28 years.

i.e. Show: $y' + \left[\frac{y'}{4}\right] \equiv y + \left[\frac{y}{4}\right] \pmod 7$

$$\Rightarrow (y+28k) + \left[\frac{y+28k}{4}\right]$$

$$= y + \left[\frac{y}{4}\right] + 28k + 7k$$

$$= y + \left[\frac{y}{4}\right] + 7(5k) \equiv y + \left[\frac{y}{4}\right] \pmod 7$$

H.P

Q. Find the non-ve residue (remainder) when 2^{68} is divided by 19.

So, → notice: m = prime

$$2^{68} \equiv ? \pmod{19}$$

Using Euler's Theorem:

we know, $a^{\phi(m)} \equiv 1 \pmod m$

If $m = p$, $\phi(m) = p-1$

as $m = 19$,

$$\Rightarrow a^{18} \equiv 1 \pmod{19}$$

→ 2

Page No

$\Rightarrow 2^{18} \equiv 1 \pmod{19} \rightarrow (1)$

Now:

$2^{68} = (2^{18})^3 \cdot 2^{14} \equiv (1)^3 (2)^{14} \pmod{19}$

Now,

$2^4 = 16 \equiv (-3) \pmod{19}$

$\Rightarrow 2^{14} = (2^4)^3 \cdot 2^2$

$\equiv (-3)^3 \cdot 4$

$\equiv (-108)$

$\therefore -108 \equiv ? \pmod{19}$

$-108 \equiv 6 \pmod{19}$

→ residue ✓

Aliter: $2^{14} \equiv (2^4)^3 \cdot 2^2$

$\equiv (-3)^3 \cdot 2^2$

$= (-27)4$

$\equiv (-8)4 = 32 \equiv 6.$

Alternative method for Solving Congruences

eg Q. $179x \equiv 283 \pmod{313}$

M1) done before : $\frac{179x - 283}{313} = y$

↳ solve diophantine eq"

M2) S1) Divide 313 by LHS (179) & take the rounded off value.

$$\text{Round off}\left(\frac{313}{179}\right) = 2$$

S2) Multiply by 2, the congruence.

$\Rightarrow 358x \equiv 566 \pmod{313}$

↳ Note : If ∃ some common no. b/w 358 & 566, divide by that, provided its relatively prime with 313

S3) Now, replace 358 & 566 by its residues

$\Rightarrow 45x \equiv 253 \pmod{313}$

S4) Divide 313 by 45 & round off value.

$$\text{round}\left(\frac{313}{45}\right) = 7$$

S5) Multiply by 7, the congruence :

$315x \equiv 1771 \pmod{313}$

6) If can't cancel, replace by residue.

$\Rightarrow 2x \equiv 206 \pmod{313}$

↳ 2 & 313 are relatively prime

So, divide by 2

$\Rightarrow x \equiv 103 \pmod{313}$

$\Rightarrow$ ans : $x = 103$

eg ⇒ $42x \equiv 90 \pmod{156}$

Remove all common factors

We see 2, 3 are common

$\div 2$ & $\div 3$

$\Rightarrow 21x \equiv 45 \pmod{78}$ ↝ $7x \equiv 15 \pmod{26}$

Don't do like this ⇒

Now

S1) $\text{round}\left(\frac{26}{7}\right) = 4$

S2) $\times 4$

$\Rightarrow 28x \equiv 60 \pmod{26}$

S3) Replace with residues

$\Rightarrow 2x \equiv 8 \pmod{26}$

$\Rightarrow x \equiv 4 \pmod{13}$

eg ⇒ $42x \equiv 90 \pmod{156}$

$\frac{156}{42} = 4$

$\times 4$, both sides of congruence

$\Rightarrow 168x \equiv 360 \pmod{156}$

$\Rightarrow 12x \equiv 48 \pmod{156}$

$\frac{156}{12} = 13$.

$\times 13$

$\Rightarrow 156x \equiv 624 \pmod{156}$

$\Rightarrow 0x \equiv 624 \pmod{156}$

→ So, method doesn't work

Alter :- $42x \equiv 90 \pmod{156}$

$\Rightarrow 7x \equiv 15 \pmod{26}$

$33x \equiv 15 \pmod{26}$

$11x \equiv 5 \pmod{26}$ $\div 3$ ($\because \gcd(3,26)=1$)

$\Rightarrow -15x \equiv 5 \pmod{26}$

$\Rightarrow -3x \equiv 1 \pmod{26}$

$\Rightarrow -3x \equiv 27 \pmod{26}$

$\Rightarrow x \equiv -9 \pmod{26}$

$\Rightarrow x \equiv 17 \pmod{26}$

So, $x = 17$

INVERSE

Defin^n: We say a sol^n 'x' of a congruence
$ax \equiv b \pmod c$
is unique (mod c) if any solution, 'x'' of it is congruent to 'x' (mod c)

eg: $15n \equiv 9 \pmod{12}$
↳ $n = 3, 7$ satisfies
as $7 \not\equiv 3 \pmod{12}$
↳ may not be unique.

($n = 63$ satisfies) ↳ & $63 \equiv 3 \pmod{12} \Rightarrow$ unique

$15x - 9 = 12y$
$\Rightarrow 5x - 4y = 3$
$x_0 = y_0 = 3$
$x = 3 + 4t$
$y = 3 + 5t$

Defin^n.: If $a\bar{a} \equiv 1 \pmod c$ then $\bar{a}$ is inverse of a (mod c)
eg: $15x \overset{?}{\equiv} 1 \pmod{12}$
? is our inverse.

Corollary:
If g.c.d$(a, c) = 1$, where $ax \equiv b \pmod c$
then a has an inverse and its unique.
eg:
$5 \cdot 5^* \equiv 1 \pmod 8$
5^* is inverse of 5
All numbers congruent to $5^* \pmod 8$ are also inverses.
✓ As $-3 \equiv 5^* \pmod 8$
$\Rightarrow -3$ is also an inverse
$\therefore 5(-3) \equiv 1 \pmod 8$
✓ As $13 \equiv 5 \pmod 8$
$\Rightarrow$ even 13 is an inverse

Now, $-3, 13$, all are congruent to 5. So, 5^* is unique

Page No

Q For the congruence $ax \equiv b \pmod{c}$:

(a) $a = 2$ & $c = 5$.

Find inverse (mod c)

So, we have

$$2 \cdot \bar{a} \equiv 1 \pmod 5$$

$\hookrightarrow \bar{a} = -2$ satisfies.

Now, $-2 \equiv 8 \pmod 5$

$-2 \equiv 13 \pmod 5$

So, $-2, 3, 8, 13$ are inverses.

(b) Let $a = 7, c = 9$.

$$7 \cdot \bar{a} \equiv 1 \pmod 9$$

$\hookrightarrow \bar{a} = 4, -5$. - satisfies.

So, they are inverses.

Q If $m = 13$, then RRS (mod 13) is

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ ⟶ (A)

Let $a = 13$. Then, exhibit the pairing of each of the nos. from (A) with the nos. in RRS

$3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36$.

We find

$3 \equiv 3 \pmod{13}$

$6 \equiv 6 \pmod{13}$

$9 \equiv 9 \pmod{13}$

$12 \equiv 12 \pmod{13}$

$15 \equiv 2 \pmod{13}$

$18 \equiv 5 \pmod{13}$

$21 \equiv 8 \pmod{13}$

$24 \equiv 11 \pmod{13}$

$27 \equiv 1 \pmod{13}$

$30 \equiv 4 \pmod{13}$

$33 \equiv 7 \pmod{13}$

$36 \equiv 10 \pmod{13}$

We see : everyone has a pair.

What we did :-
If we multiply any no. by (A), where (A) is the set of all RRS, then, we will always find a pair of elements (congruency)

Q. If m = 11 then RRS :-
1, 2, 3, 4, 5, 6, 7, 8, 9, 10
Leave 1 and m-1 aside, we get
2, 3, 4, 5, 6, 7, 8, 9
Each of these elements will find its inverse here itself :-

✓ $2 \times ? \equiv 1 \pmod{11}$
$? = 6$

✓ $3 \times ? \equiv 1 \pmod{11}$
$? = 4$

✓ $5 \times ? \equiv 1 \pmod{11}$
$? = 9$

✓ $7 \times ? \equiv 1 \pmod{11}$
$? = 8$.

So, all used.

Note :- If m is the modulus (i.e, (mod m)). Then 1 to m-1 forms the RRS. If we leave 1 & (m-1), then 2 to (m-2) has elements. These elements can be paired s.t they find their own inverse.

$$a \cdot \bar{a} \equiv 1 \pmod{m}$$

Q. Prove that

$$1 + a + a^2 + \dots + a^{\phi(m)-1} \equiv 0 \pmod{m}$$

if g.c.d $(a, m) = 1$ and g.c.d. $(a-1, m) = 1$.

i.e. To show:-

$$\frac{1 + a + a^2 + \dots + a^{\phi(m)-1} - 0}{m} = k$$

↳ some integer.

Idea: We know $a^{\phi(m)} \equiv 1 \pmod{m}$ (Euler's theorem)

So, we have $\frac{a^{\phi(m)} - 1}{m}$ = integer $= \delta$, say $\rightarrow$ ①

Expand $a^{\phi(m)} - 1 = (a-1)(1 + a + a^2 + \dots + a^{\phi(m)-1})$ ↳ ②.

From ① & ②.

$\Rightarrow$ LHS of ② is divisible by m.

So, RHS of ② has to be divisible.

Now, on RHS of ②,

$$m \nmid (a-1)$$

↳ ∵ g.c.d $(a-1, m) = 1$

$$\Rightarrow m \mid 1 + a + a^2 + \dots + a^{\phi(m)-1} \equiv \delta \pmod{m}$$

Q. Prove: if $k_1, k_2, \dots, k_{\phi(m)}$ is an RRS $\pmod{m}$ & m is odd.

Then, $k_1 + k_2 + \dots + k_{\phi(m)} \equiv 0 \pmod{m} \rightarrow$ (A)

Proof: As $k_1, k_2, \dots, k_{\phi(m)}$ will be congruent to some integer in $1, 2, \dots, m-1$.

We know

$$1 + 2 + 3 + \dots + (m-1) = \frac{(m)(m-1)}{2} \rightarrow$$ ①

Clearly (1) is divisible by m.

So, (1) ≡ (A)

$$k_1 + k_2 + \dots + k_{\phi(m)} \equiv 1 + 2 + \dots + m-1 \equiv \frac{m(m-1)}{2}$$

$$\Rightarrow k_1 + k_2 + \dots + k_{\phi(m)} \equiv 0 \pmod m$$

Q. Prove that if $A = a_0 10^n + a_1 10^{n-1} + \dots + a_n$

& $S = a_0 + a_1 + \dots + a_n$.

Then, $A \equiv S \pmod 9$

To show $A - S$ is div. by 9.

Now, $A - S = a_0 10^n + a_1 10^{n-1} + \dots + a_n - (a_0 + a_1 + \dots + a_n)$

$\Rightarrow a_0[10^n - 1] + a_1[10^{n-1} - 1] + \dots + a_{n-1}(10 - 1)$

Now,

Note :- $10 \equiv 1 \pmod 9$

$\Rightarrow 10^n \equiv 1 \pmod 9$

$10^{n-1} \equiv 1 \pmod 9$

So, each term is divisible by 9.

$\Rightarrow A - S$ is divisible by 9

§ Chinese Remainder Theorem.

↳ was started when we wanted a mathematical model for questions like :-

What no. yields remainders 2, 3, 2 when divided by 3, 5, 7.

Let no. be x : $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

We need an x that satisfies all congruences

Statement :

Suppose $m_1, m_2, \ldots, m_s$ are integers, no two of which have a common factor, other than 1. (relatively prime)

Let $M = m_1 \times m_2 \times \ldots \times m_s$ and suppose that $a_1, a_2, \ldots, a_s$ are integers, s.t, g.c.d. $(a_i, m_i) = 1$ for each i.

Then, the s-congruences

$a_1 x \equiv b_1 \pmod{m_1}$

$a_2 x \equiv b_2 \pmod{m_2}$

$\vdots$

$a_s x \equiv b_s \pmod{m_s}$

have a simultaneous solution, that is unique (mod M).

Process of solving :-

Find these :

$$n_i = \frac{M}{m_i}$$

- c_i : initial solutions for each congruence.
- We find $\overline{n_i}$.

Then,

$$x_0 = c_1 n_1 \overline{n_1} + c_2 n_2 \overline{n_2} + \dots + c_s n_s \overline{n_s}.$$

Soln to ← question

Here, $M = 3 \times 5 \times 7 = 105$.

Now, $n_1 = \frac{M}{m_1} \Rightarrow n_1 = \frac{105}{3} = 5 \times 7 = 35$

$$n_2 = \frac{3 \times 5 \times 7}{5} = 21$$

$$n_3 = \frac{3 \times 5 \times 7}{7} = 15.$$

Finding c_i's :- take initial trivial soln (others can also be taken)

i.e., for $x \equiv 2 \pmod 3$

$c_1 = 2$, making $2 \equiv 2 \pmod 3$

Ily, $c_2 = 3$

$c_3 = 2$.

Finding $\overline{n_i}$.

Now, $n_1 \overline{n_1} \equiv 1 \pmod 3$

$\Rightarrow 35(\overline{n_1}) \equiv 1 \pmod 3$

Solve / seeing by observation,

$\overline{n_1} = 2$.

Also, $n_2 \overline{n_2} \equiv 1 \pmod 5$

$\Rightarrow 21\,\overline{n_2} \equiv 1 \pmod 5$

$\overline{n_2} = 1$ Ily, $\overline{n_3} = 1$.

Solution is

$$x_0 = c_1 n_1 \bar{n_1} + c_2 n_2 \bar{n_2} + c_3 n_3 \bar{n_3}$$

$$\Rightarrow x_0 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 11 + 2 \cdot 15 \cdot 1$$

$$= 233$$

Now, $233 \equiv ? \pmod{105}$

$$? = 23$$

So, Ans $= x = \underline{\underline{23}}$

Q. Solve : $3x \equiv 11 \pmod{2275} \rightarrow (A)$

M1) Diophantine eqn solving — lengthy.

M2) Chinese remainder theorem

Factorise $2275 = 25 \cdot 7 \cdot 13$

(A) can be written as a system of congruences:

$$3x \equiv 11 \pmod{25}$$

$$3x \equiv 11 \pmod{7}$$

$$3x \equiv 11 \pmod{13}$$

We have

$$M = 2275 = 25 \cdot 7 \cdot 13$$

$$n_1 = \frac{25 \cdot 7 \cdot 13}{25} = 91$$

$$n_2 = \frac{25 \cdot 7 \cdot 13}{7} = 325$$

$$n_3 = \frac{25 \cdot 7 \cdot 13}{13} = 175$$

$$c_1 = 12, \; c_2 = 6, \; c_3 = 8$$

$n_1 \bar{n_1} \equiv 1 \pmod{25}$

$\Rightarrow a(\bar{n_1}) \equiv 1 \pmod{25}$

$\bar{n_1} = 11$

$n_2 \bar{n_2} \equiv 1 \pmod{7}$

$\Rightarrow 325(\bar{n_2}) \equiv 1 \pmod{7}$

$\bar{n_2} = 5, 22, \ldots$

$n_3 \bar{n_3} \equiv 1 \pmod{13}$

$\Rightarrow 175(\bar{n_3}) \equiv 1 \pmod{13}$

$\bar{n_3} = 11$

Soln:

$x_0 = 91 \cdot 12 \cdot 11 + 325 \cdot 6 \cdot 5 + 175 \cdot 8 \cdot 11$

$\Rightarrow x_0 = 37162 \equiv ? \pmod{2275}$

$? = 762 = x$

Ans

Q. Find all soln of

$3x \equiv 1 \pmod{5}$

$4x \equiv 6 \pmod{14}$

$5x \equiv 11 \pmod{3}$

Soln: Find M.

So, $M = 5 \times 14 \times 3 = 210$.

$C_1 = 2, C_2 = 5, C_3 = 4$

$n_1 = \frac{5 \times 14 \times 3}{5} = 42$.

$n_2 = 15, n_3 = 70$.

$n_1 \bar{n_1} \equiv 1 \pmod 5$

$\Rightarrow 42\, \bar{n_1} \equiv 1 \pmod 5$

$\bar{n_1} = 3$

$n_2 \bar{n_2} \equiv 1 \pmod{14}$

$\Rightarrow 15(\bar{n_2}) \equiv 1 \pmod{14}$

$\bar{n_2} = 1$

$n_3 \bar{n_3} \equiv 1 \pmod 3$

$\Rightarrow 70(\bar{n_3}) \equiv 1 \pmod 3$

$\Rightarrow \bar{n_3} = 1$

So,

$x_0 = c_1 n_1 \bar{n_1} + c_2 n_2 \bar{n_2} + c_3 n_3 \bar{n_3}$

$= 2 \cdot 42 \cdot 3 + 5 \cdot 15 \cdot 1 + 7 \cdot 70 \cdot 1$

$= 817 \pmod{210}$

Now

$817 \equiv ? \pmod{210}$

$? = 187$

So, $x = \underline{187}$

Q. Find the residue when $12!$ is divided by 13.

Note : 13 is prime. So, it forms an RRS!

Hence, each element will have its pair (leaving 1st & last)

$12! = 1) 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot (12$

Pairs :- $2 \times 7 \equiv 1 \pmod{13}$

$3 \times 9 \equiv 1 \pmod{13}$

$4 \times 10 \equiv 1 \pmod{13}$

$5 \times 8 \equiv 1 \pmod{13}$

$6 \times 11 \equiv 1 \pmod{13}$

Page No

As each element $\equiv 1$, leaving behind 12.
So, we see 12 is the residue

Hence, $\frac{12! - 12}{13} =$ integer.

* Fermat's Little Theorem (revisited)
If p is a prime no.
Then,
$$n^p \equiv n \pmod{p}$$

Proof :

Case (1) :- Let $p \mid n \Rightarrow p \mid n^p \Rightarrow p \mid n^p - n$

$$\Rightarrow n^p \equiv n \pmod{p}$$

Case (2) :- If $p \nmid n \Rightarrow gcd(p, n) = 1$.
So, from Euler's theorem, (for m = prime no., $m = p-1$)
$$n^{p-1} \equiv 1 \pmod{p} \quad \left(a^{\phi(m)} \equiv 1 \pmod{m}\right)$$
$\times n$.
$$\Rightarrow n^p \equiv n \pmod{p}$$

Chapter: PRIME NUMBERS.

FACTS
- ✓ 2: Only even prime no.
- ✓ 1: Not a prime no.
- ✓ 2 & 3 are the only consecutive primes.
- ✓ Twin primes: Odd consecutive primes which differ by two.

• To find a no. is prime or not
↳ SEIVE OF ERATOTHENESE

eg Find all primes before 50 → taken as n

list the numbers till n (50)

(2)	(3)	4	(5)	6	(7)	8	9	10	(11)
12	(13)	14	15	16	(17)	18	(19)	20	21
22	(23)	24	25	26	27	28	(29)	30	(31)
32	33	34	35	36	(37)	38	39	40	(41)
42	(43)	44	45	46	(47)	48	49	50	

S1) Leaving 2, cancel all multiples of 2
S2) Next, leaving 3, cancel all multiples of 3
Do that for the coming nos.

Keep doing till you reach $\sqrt{n}$
Here $\sqrt{50} = 7$.... So, Stop at 7.

The circled nos are the primes.
No. of primes = 15
This method is not suitable for large n

* No. of primes are infinite.
* Avg. distribution of primes is very irregular.
* Density shows steady but slow decrease.
* ∃ many prime triplets of the type $(p, p+2, p+6)$ and $(p, p+4, p+6)$
* ∃ no formula to find the n^{th} prime p_n.
  → eg. we can't find the 100^{th} prime no., say.
* ∃ no simple general formula for a prime which follows a given prime no.
* Every integer $n, \geq 2$, has a prime factor.
* Every composite no. n has a prime factor $\leq \sqrt{n}$.

☆ Theorem:-
For every +ve integer n, ∃ n consecutive integers that are composite numbers:

$$(n+1)!+2,\ (n+1)!+3,\ \text{----}\ (n+1)!+(n+1)$$

eg:
If $n=6$,
$7!+2,\ 7!+3,\ 7!+4,\ \text{---}\ ,\ 7!+7$
$\Rightarrow$ 5042, 5043, - - - , 5047

★ ~~CUM~~ Cunningham Chains

Chains having elements of the form "$2p+1$"

eg: Smallest Cunningham chain:
2, 5, 11, 23, 47.

★ To find whether a no. 'n' is prime or not?

① Find whether the no. is divisible by any of the primes occuring before $\sqrt{n}$.
If its divisible, its composite, otherwise prime.

eg:- See if 2011 is prime or not?
here $n = 2011$
So, $\sqrt{n} \simeq 44$.
So, divide 2011 by all prime nos below 44
(2, 3, 5, 7, 11, ... 43)

eg ② :- 203 is prime or not?
$\sqrt{n} = \sqrt{203} = 14$.
primes before 14 are 2, 3, 5, 7, 11, 13.
$\nmid$ 203. So, its not a prime.

eg ③ :- 191 is prime or not?
$\sqrt{191} \simeq 14$.
So, primes before 14 are 2, 3, 5, 7, 11, 13.
No prime divides 191. So, its composite

CLASSMATE

* No. of primes which do not exceed a given no. "x"
  - denoted by $\pi(x)$
  - given by: $\pi(x) \simeq \frac{x}{\log_e x}$
    - $\pi(1) = 0$
    - $\pi(2) = 1$

eg $\pi(20) = 8$

Note: This is just an approxim". Doesn't give exact results

eg: for $x = 10^3$
$\pi(x) = 168$, by formula, $\pi(x) = 144$

* Tchebycher Approximation:-
For all positive numbers C_1 and C_2,

$$C_1 \frac{x}{\ln x} < \pi(x) < C_2 \frac{x}{\ln x}$$

- gives a range.
- C_1, C_2: +ve integers.

* Theorem:-
There are infinite number of primes.

Proof: Let ∃ finite no. of primes, say
$p_1, p_2, \dots, p_n$
Lets take some no.
$m = (p_1 p_2 p_3 \dots p_n) + 1$

Page No

Now, m can be prime or composite.

Case ①:- m is prime

If m is prime, we have found another prime

$\Rightarrow$ Our assumption is wrong. So, in similar lines $\exists$ many other primes also.

Case ②:- m is composite

From fundamental theorem of arithmetic, m can be represented as a product of prime powers.

That is, m has to be divisible by some prime p, from $p_1, p_2, \ldots, p_n$

$\Rightarrow p \mid m$. Also, $p \mid (p_1 p_2 p_3 \ldots p_n)$

We know $m - (p_1 p_2 \ldots p_n) = 1$

As $p \mid m - (p_1 p_2 \ldots p_n)$

$\Rightarrow p \mid 1 \longrightarrow$ a contradiction.

Hence, $\exists$ infinite prime nos.

* Note:- Every odd integer is either of the form $4n+1$ or $4n+3$.

* Lemma:- If a & b are integers, both of the form $4n+1$. Then, ab is also of the form $4n+1$.

* Theorem: $\exists$ infinitely many primes of the form $4n+3$

Proof: Let $\exists$ finite no. of primes of the form $4n+3$, say $p_1, p_2, \ldots, p_n$.

Let $m = (4p_1p_2\ldots p_n)^2 - 1 \longrightarrow (1)$

So, m has a form $4q+3$, where

$q = (p_1p_2\ldots p_n) - 1$

(can be seen if we put $p_1p_2\ldots p_n = q+1$ in eq^n (1))

Case (1): m is prime.

$\Rightarrow$ we got one more prime.

So, no. of primes is NOT finite

Hence, infinitely many primes.

Case (2): m is composite

$\Rightarrow$ as m is odd, so, it'll have odd factors.

Now, odd factors are of the form $4n+1$ or $4n+3$. We cannot have all factors of the form $4n+1$, $\because$ then, their product will be of the form $4n+1$ (from Lemma) whereas, we have $m = 4q+3$ form

$\Rightarrow$ $\exists$ atleast one odd no. (prime factor) of the form $4n+3$. let the no. be p.

Now, $p \mid p_1p_2\ldots p_n$ & $p \mid m$

$\Rightarrow p \mid 4(p_1p_2\ldots p_n) - m$.

$\Rightarrow p \mid 1$

$\hookrightarrow$ Contradiction.

So, $\exists$ infinite no. of primes.

Page No

✡ FIBONACCI Numbers.

↳ 1, 1, 2, 3, 5, 8, 13, 21, - - - -

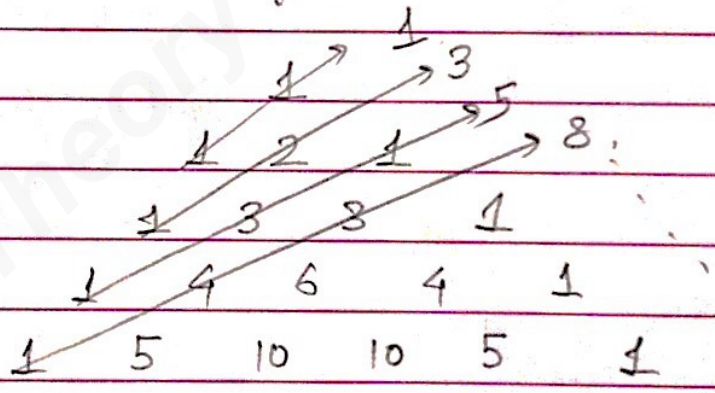
Defn: If $F_1 = 1 = F_2$.

Then,

$$F_n = F_{n+} + F_{n-2}, \quad n \geq 3.$$

✡ It has a no. of practical applic^{ns}.
↳ Read: Golden Ratio

We also get this sequence from diagonals of Pascal's triangle:



✡ Lucas Numbers:

$L_1 = 1, L_2 = 3$.

$L_n = L_{n-1} + L_{n-2}$; $n \geq 3$

↳ 1, 3, 4, 7, 11, 18, - - -

CLASSMATE

(Fn) (Ln)

✱ Relationship b/w Fibonacci No's and Lucas Nos.

Take n = 1 to 10 & observe

n	1	2	3	4	5	6	7	8	9	10
F_n	1	1	2	3	5	8	13	21	34	55
L_n	1	3	4	7	11	18	29	47	76	123

↳ Observation: Adding alternate nos in Fibonacci series gives the sequence of Lucas

i.e., $L_n = F_{n-1} + F_{n+1}$; $n \geq 2$

↳ $L_2 = F_1 + F_3$

$= 1 + 2 = 3$

Other patterns:

- $2F_{n+1} - F_n = L_n$
- $F_n \cdot L_n = F_{2n}$
- $5F_n = L_{n-1} + L_{n+1}$
- $2F_{n-1} + F_n = L_n$
- $L_{n-3} + L_{n+3} = 10F_n$

* - $L_{n-4} + L_{n+4} = 30F_n$

- $L_{n-5} + L_{n+5} = 50F_n$.

✱ Fermat Numbers. (denoted by f_n)

Numbers of the form $2^{2^n} + 1$.

If $2^{2^n} + 1$ is prime, it called a Fermat prime.

$f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$

$f_5 = 4294967297$

f_0, f_1, f_2, f_3, f_4 are primes

Now, when $f_5 = 641 \times 6700417$.

So, f_5 is not prime.

* Fermat's Conjecture :-

All nos. of the form 2^{2^n} $\forall$ n are prime

↳ Disproved by Euler.

✡ MERSENNE NUMBERS. (M_p)

↳ no.s of the form $2^p - 1$.

↳ p : prime. (2, 3, 5, 7, - - - -)

eg: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ → prime

$M_{11} = 2047$ → not a prime ($2047 = 23 \times 89$)

* M_{756839} is the largest Mersenne Prime.

Or Find all +ve integers n for which $3n-4$, $4n-5$, $5n-3$ are all prime numbers.

Soln : As $3n-4$ and $5n-3$ can be even numbers.

∵ when we add all 3 nos., sum = even, which means atleast one no. is even.

As $3n-4$ & $5n-3$ are prime, so, equating them to 2 as 2 is the only even prime.

$3n-4 = 2 \Rightarrow n = 2$

Putting it ($n=2$) in $3n-4, 4n-5, 5n-3$, we get $2, 7, 3$ ∴ So, they are primes.

Now, equating $5n-3 = 2$

$\Rightarrow n = 1$.

This gives $-1, -1, 2$

→ -ve So, $n=1$ ignored

So, value of n is 2 Ans

eg If p & q are primes. And, $x^2 - px + q = 0$ has distinct positive integral roots. Find p & q.

Soln: Let the roots be x_1 & x_2

So, we have $x_1 + x_2 = -(-p)$

$\Rightarrow x_1 + x_2 = p$

& $x_1 x_2 = q$

↳ As q = prime. ⇒ either x_1 or $x_2 = 1$

Let $x_2 = 1$

$\Rightarrow x_1 + 1 = p$.

Also, $x_1 = q$ ($\because x_2 = 1$) } → (1)

From (1), p & q are consecutive primes

We know that only consecutive primes are 2 & 3.

So, $p = 2$

$q = 3$.

eg Find all primes p, s.t. $17p + 1$ is a square

Let $17p + 1 = x^2$

$\Rightarrow 17p = x^2 - 1$

$\Rightarrow 17p = (x-1)(x+1)$

Page No

As both 17 & p are primes

$\Rightarrow$ either $x-1 = 17$ or $x+1 = 17$

$\Rightarrow x = 18$ $\quad$ $\Rightarrow x = 15$

$\Rightarrow x+1 = 19$ $\quad$ ↳ Not a prime no. $(p \neq 15)$

So, other factor, $p = 19$

$p = 19$: $17 \times 19 + 1 = 324 = (18)^2$

Hence, $p = 19$ is answer.

eg If p & $p+2$ are both primes. Prove with $p > 3$, show :- $2p+2$ is divisible by 12.

$p + p+2 = 2p+2 = 2(p+1)$

we have to show: $12 \mid 2(p+1)$

or $6 \mid (p+1)$ → (1)

✡ Any odd prime is of the form $3k+1$ or $3k+2$.

So, $p = 3k+1$ or $3k+2$ → (2)

We have to see divisibility by 6

$\Rightarrow$ It has to be divisible by 2 & 3

Now, let $p = 3k+1$.

$\Rightarrow p+1 = 3k+2$: Not divisible by 3

let $p = 3k+2$

$\Rightarrow p+1 = 3k+3 = 3(k+1)$: Divisible by 3

Now, If k = even $\Rightarrow 3k$ = even $\Rightarrow 3k+2$ = even

So, k can only be odd (∵ $3k+2$ is odd prime)

$\Rightarrow k+1$ = even = $2m$, say.

So, $p+1 = 3(k+1) = 3(2m) = 6m$

So, $6 \mid 6m \Rightarrow 6 \mid (p+1)$ (or p = prime → odd $\Rightarrow p+1$ = even ✓)

Page No

Self eg If g.c.d $(a, b) = p$.
What are the possible values of g.c.d (a^2, b^2)

We know, g.c.d $(a, b) = p$

$\Rightarrow p \mid a$ & $p \mid b$.

$\Rightarrow p \mid a^2$ & $p \mid b^2$

$\Rightarrow$ g.c.d. $(a^2, b^2) = p$.

Now, checking if its true for p^2

Suppose a has factors $a = p, \alpha$.

b has factors $b = p, \beta$

So, g.c.d $(a, b) = p$, clearly

Now, $a^2 = p^2, \alpha^2$

$b^2 = p^2, \beta^2$.

So, Clearly, g.c.d $(a^2, b^2) = p^2$.

Hence p^2 is the greatest common divisor.

ARITHMETIC FUNCTIONS

Any fn, whose domain is a set of integers is called arithmetic function.

(1) ✡ $\phi(n)$: Euler's ϕ fn
(2) ✡ $\mu(n)$: Mobius μ fn
(3) ✡ $\sigma(n)$: Sum fn
(4) ✡ $d(n)$: Sum of divisors

(1) ✡ $\phi(n)$:

If n is prime, p.

* $\phi(p) = p-1$

Let us have $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots$
(writing a no. as powers of prime)

Now, instead of $n = p$, we see

If $n = p^\alpha$

* $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Note: The positive integers $\leq p^n$ that are not relatively prime to p^n, are the p^{n-1} multiples of p, i.e., $p, 2p, 3p, \ldots, p^{n-1}p$.
These multiples have a common factor with p^n

Note (2): If $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_n^{\alpha_n}$

* $\phi(n) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \ldots \phi(p_n^{\alpha_n})$

eg find $\phi(243)$

$243 = 3^5$

$\Rightarrow \phi(243) = \phi(3^5)$

We know,

$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$

$= 3^5 - 3^4 = 162$

So, 3 162 numbers in RPS, all of them, relatively prime to 243.

eg (2): $24 = 2^3 \cdot 3$

We know:- If $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$

$\Rightarrow \phi(n) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2})$

$\Rightarrow \phi(2^3 \cdot 3^1) = \phi(2^3) \cdot \phi(3^1)$

$= (2^3 - 2^2) \cdot 2$

for $n = p$, $\phi(p) = p-1$

$\Rightarrow \phi(2^3 \cdot 3) = 4 \cdot 2 = 8$

— x —

List: Note $\phi(n)$: no. of elements in RPS

$\phi(1) = 1$	$\phi(11) = 10$
$\phi(2) = 1$	$\phi(12) = 4$
$\phi(3) = 2$	$\phi(13) = 12$
$\phi(4) = 2$	$\phi(14) = 6$
$\phi(5) = 4$	$\phi(15) = 8$
$\phi(6) = 2$	$\phi(16) = 8$
$\phi(7) = 6$	$\phi(17) = 16$
$\phi(8) = 4$	$\phi(18) = 6$
$\phi(9) = 6$	$\phi(19) = 18$
$\phi(10) = 4$	$\phi(20) = 8$

* Note: $\phi(n)$ values are always EVEN!

eg Show: $1 + \phi(p) + \phi(p^2) + \cdots + \phi(p^n) = p^n$.

LHS

$$= 1 + p - 1 + p^2 - p + p^3 - p^2 + \cdots + p^n - p^{n-1}$$

$$= p^n$$

$= RHS$ Hence, proved.

(2) ✱ Mobius Function $\mu(n)$

$$\mu(n) = \begin{cases} 1 & , n = 1 \\ 0 & , p^2 \mid n \\ -1 & , n = p_1 p_2 \cdots p_k, \ p_i \text{ are distinct primes.} \end{cases}$$

↳ $\mu(n)$ is always 1 or 0 or -1

↳ Just like $\phi(n)$, $\mu(n)$ is also following multiplicative property.

eg: $\mu(1) = 1$
$\mu(2) = -1$
$\mu(3) = -1$
$\mu(4) = 0$
$\mu(5) = -1$
$\mu(6) = 1$
$\mu(7) = -1$
$\mu(8) = 0$
$\mu(9) = 0$
$\mu(10) = 1$

✱ $\mu(2^4) = \mu(2^3 \cdot 3)$
$= \mu(2^3)\mu(3)$
$= 0 \cdot (-1)$
$= 0.$

✱ Theorem :

$$\phi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d} = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

⇒ Let $n = 6$

d = Divisors of 6 = $1, 2, 3, 6$

$\phi(6) = \phi(2)\,\phi(3) = 1 \cdot 2 = 2$

LHS $\sum_{d \mid n} \mu(d) \frac{n}{d} = \mu(1)\left(\frac{6}{1}\right) + \mu(2)\left(\frac{6}{2}\right) + \mu(3)\left(\frac{6}{3}\right) + \mu(6)\left(\frac{6}{6}\right)$

$= (1)(6) + (-1)(3) + (-1)(2) + 1(1)$

$\Rightarrow \phi(6) = 2$

RHS : $n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = 6\left[\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\right]$

taking only primes

$= 6\left[\frac{1}{2} \cdot \frac{2}{3}\right] = 2$

$\Rightarrow \phi(6) = 2$

Ex. Theorem Based

Ex. Find all integers n s.t. $\phi(n) = 12$

Idea - put LHS (= $\phi(n)$) as powers of prime nos

Ex. $\phi(p_1^{\alpha} \cdot p_2^{\alpha-1} \cdot p_3^{\alpha-2}) = 12$

or $6 \cdot 2$

or $3 \cdot 4$

or $2 \cdot 2 \cdot 3$

Page no. □□□

Comparing LHS & RHS

① (1·12) $\Rightarrow \phi(p_1^{\alpha_1} p_2^{\alpha_2}) = 1 \cdot 12 = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2})$

$\therefore \phi(p_1^{\alpha_1}) = 1$ & $\phi(p_2^{\alpha_2}) = 12$

$\Rightarrow \phi(1) = 1$ & $\phi(13) = 12$

$\Rightarrow \phi(1 \cdot 13) = \phi(1)\phi(13) = 12$

② (6·2) $\Rightarrow \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2}) = 6 \cdot 2 = \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2})$

$\Rightarrow \phi(p_1^{\alpha_1}) = 6$ & $\phi(p_2^{\alpha_2}) = 2$

$\Rightarrow \phi(7) = 6$ & $\phi(3) = 2$

(we can also use $\phi(9), \phi(14)$ or $\phi(18)$...) (or $\phi(4)$ or $\phi(6)$)

$\Rightarrow$ we have $p_1^{\alpha_1} = 7$ or 9 or 14 or 18...

& $p_2^{\alpha_2} = 2$ or 4 or 6 ....

So, $n = 7 \times 2 = 14$ satisfies

(others also possible)

CONJECTURES

Q C Goldbach conjectured that every even no. > 2 is a sum of two primes. P Erdos conjectured that for any even no. $2n$, $\exists$ integers q & r, s.t $\phi(q) + \phi(r) = 2n$.

Does the conjecture of Goldbach imply that of Erdos?

Let Goldbach conjecture be true

$\Rightarrow$ every even no, say $2n+2$

$\therefore 2n+2 = q+r \longrightarrow (1)$

From $\phi(q) = q-1$ & $\phi(r) = r-1$

($\because q$ & r have to be primes)

$\Rightarrow \phi(q)+1 = q$ & $\phi(r)+1 = r \longrightarrow (2)$

Substituting (2) in (1)

$\Rightarrow 2n+2 = \phi(q)+1+\phi(r)+1$

$\Rightarrow 2n = \phi(q)+\phi(r)$

= P Erdos' Conjecture

Hence Satisfied

Q D. Carmichael Conjectured that for each integer n, $\exists$ an m, different from n, s.t. $\phi(n) = \phi(m)$. Prove Carmichael's Conjecture for each n → congruent to 2 (mod 4)

$n \equiv 2 \pmod 4$

$\Rightarrow \frac{n-2}{4} = \text{integer} = k$, say

$\Rightarrow n = 4k+2$

n, k : integers

Now, $\phi(n) = \phi(4k+2) = \phi(2.(2k+1))$

$= \phi(2)\,\phi(2k+1)$

$= 1 \cdot \phi(2k+1)$

$\Rightarrow \phi(n) = \phi(2k+1)$

↳ for for 2 diff values, we get same values of ϕ.

Q Find infinitely many integers n, for which $10 \mid \phi(n)$

We know, $\phi(11) = 10$.

So, $10 \mid \phi(11)$

(one of the integer $n = 11$)

Finding infinitely many integers

$$\phi(11^n) = 11^n - 11^{n-1} = 11^{n-1}(11-1)$$
$$= 11^{n-1}(10)$$

$\Rightarrow 10 \mid \phi(11^n)$

For different values of n, above will be true.

Q Find $\phi(19)$, $\phi(49)$, $\phi(243)$, $\phi(1024)$

$\phi(19) = 18$ (i.e $19-1$)

$\phi(49) = \phi(7^2) = 7^2 - 7 = 49 - 7 = 42$

$\phi(243) = \phi(3^5) = 3^5 - 3^4 = 243 - 81 = 162$

$\phi(1024) = \phi(2^{10}) = 2^{10} - 2^9 = 512$

(Basically, using $\because \phi(p^n) = p^n - p^{n-1}$)

Q Prove that $\exists$ infinitely many integers, n, for which $\phi(n)$ is a perfect square.

Proof: Let the no. be 2^{2n+1}

$$\phi(2^{2n+1}) = 2^{2n+1} - 2^{2n} = 2^{2n}(2-1)$$
$$= 2^{2n} = (2^n)^2$$

So, its of the form of perfect square.

eg. $n = 2$

$\Rightarrow \phi(2^5) = 2^5 - 2^4 = 16 = 4^2$.

So, its a form of whole square

(3) ✱ $\sigma(n)$: The Summation Function.

* $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$

↳ $\sigma(n)$ denotes the sum of all positive divisors of n.

↳ $\sigma(p) = p+1$

(Comes from : divisors of p^n are $1, 2, 3, \ldots, p^n$.

Add $\Rightarrow 1+2+3+\ldots+p^n$

$= \frac{p^{n+1}-1}{p-1}$ (sum of n terms of GP))

* σ is multiplicative function.

i.e, $\sigma(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_n^{\alpha_n}) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2}) \ldots \sigma(p_n^{\alpha_n})$

$= \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \ldots$

eg : Find $\sigma(100) = \sigma(2^2 \cdot 5^2) = \sigma(2^2)\sigma(5^2)$

$= \left(\frac{2^3-1}{2-1}\right)\left(\frac{5^3-1}{5-1}\right)$

$= \left(\frac{7}{1}\right)\left(\frac{124}{4}\right) = 7(31)$

$\Rightarrow \sigma(100) = 217$

eg ($\sigma(6) = \sigma(2 \cdot 3) = \sigma(2)\sigma(3)$

$= \left(\frac{2^2-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right) = 3(4) = 12$

Verifying : divisors of 6 are 1, 2, 3 & 6

So, $1+2+3+6 = 12$

Page No

eg find $\tau(210)$ and $\tau(999)$

$\tau(210) = \tau(2 \cdot 3 \cdot 5 \cdot 7) = \tau(2)\tau(3)\tau(5)\tau(7)$

$= \left(\frac{2^2-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)\left(\frac{7^2-1}{7-1}\right)$

$= (3)(4)(6)(8)$

$\Rightarrow \tau(210) = 576$

$\tau(999) = \tau(3^3 \cdot 37) = \tau(3^3)\tau(37)$

$= \left(\frac{3^4-1}{3-1}\right)\left(\frac{37^2-1}{37-1}\right)$

$\Rightarrow \tau(999) = (40)\left(\frac{1368}{36}\right) = 1520$

(4) $d(n)$: The number of divisors.

- for n = prime = p,
  $d(p) = 2$
- If $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n}$
  then, $d(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$
- $d(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}) = d(p_1^{\alpha_1})\, d(p_2^{\alpha_2}) \cdots d(p_n^{\alpha_n})$

eg $d(120) = d(2^3 \cdot 3 \cdot 5)$

$= d(2^3)\, d(3)\, d(5)$

$= (3+1)(2)(2) = 16$

$\Rightarrow$ 120 has 16 divisors

$\tau(120) = \tau(2^3)\tau(3)\tau(5) = \left(\frac{2^4-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)$

$= (15)(4)(6) = 360$

Page No

Q Find $d(47)$, $d(63)$, $d(150)$

$d(47) = 2$

$d(63) = 3(2) = 6$

$d(150) = (2)(2)(3) = 12$

Q Find $d(9!)$ & $\sigma(9!)$

$9! = 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2$

$= 2^7 \cdot 3^4 \cdot 5 \cdot 7$

$d(9!) = (7+1)(4+1)(1+1)(1+1)$

$d(9!) = 160.$

$\sigma(9!) = \sigma(2^7 \cdot 3^4 \cdot 5 \cdot 7)$

$= \left(\frac{2^8-1}{2-1}\right)\left(\frac{3^5-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)\left(\frac{7^2-1}{7-1}\right)$

$= (255)(121)(6)(8)$

$\Rightarrow \sigma(9!) = 1481040$

2560
256
2304
42
4255
48
2040
1020
12240
134640
1481040

Q. Prove $d(n)$ is odd iff n is a perfect square.
Or, for which integer n, $d(n)$ is odd?

Sol^n:- Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$d(n) = d(p_1^{\alpha_1})\, d(p_2^{\alpha_2}) \cdots d(p_k^{\alpha_k})$

$d(n) = (\alpha_1+1)(\alpha_2+1) \cdots (\alpha_k+1)$

For $d(n)$ to be odd, all factors $(\alpha_1+1), (\alpha_2+1), \ldots, (\alpha_k+1)$ should be odd

(∵ odd × odd = odd)

Now, as $\alpha_i + 1 = \text{odd} \Rightarrow \alpha_i = \text{even}$.

$\Rightarrow \alpha_1 = 2m_1, \alpha_2 = 2m_2, \ldots$

Page No

$\Rightarrow n = p_1^{2m_1} p_2^{2m_2} \dots p_k^{2m_k}$

$\Rightarrow n = \left(p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}\right)^2$

So, n should be a perfect square

Table

n	$d(n)$	n	$d(n)$
1	1	11	2
2	2	12	6
3	2	13	2
4	3	14	4
5	2	15	4
6	4	16	5
7	2	17	2
8	4	18	6
9	3	19	2
10	4	20	6

↳ when $d(n)$ = odd, n is a whole square

Q. For which n will $\sigma(n)$ be odd.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$$\sigma(n) = \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2}) \dots \sigma(p_k^{\alpha_k})$$

$$= \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}\right) \dots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)$$

$$= \left(1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1}\right)\left(1 + p_2 + p_2^2 \dots + p_2^{\alpha_2}\right) \dots$$

For $\sigma(n)$ to be odd, all the above terms are odd.

Note :-

$1 + p_i + p_i^2 + \dots + p_i^{\alpha_i} = \text{odd}$

$\Rightarrow p_i + p_i^2 + \dots + p_i^{\alpha_i} = \text{even}$

↳ when $p = \text{even}$

$\Rightarrow p^2 = \text{even}$

or $p^{\alpha_i} = \text{even}$

So, satisfied.

↳ when $p = \text{odd}$

$p^2 = \text{odd} \dots p^{\alpha_i} = \text{odd}$

Now, odd + odd = even

$\Rightarrow$ we need to have even no. of terms. $\Rightarrow \alpha_i = \text{even}$.

$\Rightarrow \alpha_1 = 2m_1$

$\alpha_2 = 2m_2$

$\dots \alpha_i = 2m_i$, say

So, we have $n = [p_1^{m_1} p_2^{m_2} \dots p_k^{\alpha_k}]^2$

Again, perfect square.

Q. Show integers which have only 3 +ve divisors are squares of prime numbers.

So, we have $d(n) = 3$

$RHS = 3 = 3 \times 1$

$LHS = d(p_1^{\alpha_1} \cdot p_2^{\alpha_2})$

$\Rightarrow (\alpha_1 + 1)(\alpha_2 + 1) = 3 \times 1.$

$\Rightarrow \alpha_1 = 2, \alpha_2 = 0.$

$\Rightarrow d(p_1^2 \cdot p_2^0) = d(n) = 3 \times 1$

$\Rightarrow n = p_1^2 \Rightarrow$ Its square of a prime number.

Page No

Q. Integers which have 4 +ve divisors are cube / product of primes

So, here, $d(n) = 4$

$\Rightarrow d(p_1^{\alpha_1} p_2^{\alpha_2}) = 4 \times 1$ or 2×2.

Let: $(\alpha_1+1)(\alpha_2+1) = 4 \times 1$

$\Rightarrow \alpha_1 = 3, \alpha_2 = 0$

$\Rightarrow n = p_1^3 p_2^0 = p_1^3$

$\Rightarrow$ Its cube of prime no.

Let: $(\alpha_1+1)(\alpha_2+1) = 2 \times 2$

$\Rightarrow \alpha_1 = 1, \alpha_2 = 1$

$\Rightarrow n = p_1^1 \cdot p_2^1 = p_1 p_2 \Rightarrow$ Its product of primes.

Q. Prove that n is prime iff $\nabla(n) = n+1$

Case (1):

If n is prime, then, only 2 divisors are there: 1 & n.

Then, $\nabla(n) = n+1$ (Sum of divisors)

Case (2): If n is not prime $\Rightarrow \exists$ atleast one more divisor besides 1 and n. Say, its d.

So, $\nabla(n) = 1 + n + d$.

This $\neq n+1$

So, $\nabla(n) = n+1$ iff n is prime.

Q. Find an integer n, s.t. $\nabla(n) = 36$.

Considering only 2 (for simplicity) factors of 36.

CLASSMATE

Removed factors

So, $36 = 2 \times 18$ ✗

4×9 ✗

6×6 ✓

12×3 ✓

36×1 ✗

Say, $n = p_1^{\alpha_1} p_2^{\alpha_2}$.

So, $\sigma(n) = \sigma(p_1^{\alpha_1} p_2^{\alpha_2}) = \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2})$

$$= \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}\right)$$

$$= (1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1}) \times (1 + p_2 + p_2^2 + \ldots + p_2^{\alpha_2})$$

Note: $p_1, p_2, \ldots$ are primes

As 1 is not prime. So, p_1 or $p_2 \neq 1$

So, we can never get 2. $(1 + (1))$

So, remove the factor 2×18. -1

Illy, 1 can also not be got in factors

So, remove 1×36

Seeing if we can write other factors. -1

So, 4×9 cancelled

$4 = 1 + 3$

9 can't be written

$3 = 1 + 2$

$12 = 1 + 11$

trying to write in the form of $1 + p_1 + p_1^2 + \ldots$

So, 12×3 satisfies.

So, $12 \times 3 = (1+11)(1+2)$

$p_1 = 11, \quad p_2 = 2$

$\alpha_1 = 1 \quad \alpha_2 = 1$

$n = p_1^{\alpha_1} p_2^{\alpha_2} = 11 \times 2 = 22$

(Note: 6×6 also satisfies. So, we can have other values of n)

Page No

TPT : To prove that

CLASSMATE

Q. If $\tau(n) = 51$, find n

$51 = 3 \times 17$

$3 = 1+2$

$17 =$ can never be expressed in the form $(1 + p + p^2 \dots)$

So, we can't find

LIST :

$3 = 1+2$

$4 = 1+3$

$6 = 1+5$

$12 = 1+11$

$18 = 1+17$

$14 = 1+13$

HW Q. Find $\tau(n) = 72$

$= 4 \times 18$

$= (1+3) \times (1+17)$

$P_1 = 3, \alpha_1 = 1$; $P_2 = 17, \alpha_2 = 1$

$\Rightarrow n = P_1^{\alpha_1} P_2^{\alpha_2} = 3 \times 17 = 51$

Q. TPT : If $n = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k}$

Show : (1) $\tau(n)\,\phi(n) = n^2 \left(1 - P_1^{-\alpha_1 - 1}\right)\left(1 - P_2^{-\alpha_2 - 1}\right) \dots \left(1 - P_k^{-\alpha_k - 1}\right)$

(2) $\phi(n)\,\tau(n) > n^2 \left(1 - \frac{1}{P_1^2}\right)\left(1 - \frac{1}{P_2^2}\right) \dots \left(1 - \frac{1}{P_k^2}\right)$

Page No

$\phi(n) = \phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$

& $\sigma(n) = \sigma(p_1^{\alpha_1})\,\sigma(p_2^{\alpha_2}) \cdots \sigma(p_k^{\alpha_k})$

$\therefore \phi(n)\sigma(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) \times \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right)$

Taking out common $p_1^{\alpha_1}$ from first bracket
$p_2^{\alpha_2}$ from second bracket....

$\therefore p_1^{\alpha_1-1}(p_1-1)\,p_2^{\alpha_2-1}(p_2-1) \cdots p_k^{\alpha_k-1}(p_k-1) \times \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right)$

$= \left(\frac{p_1^{\alpha_1}}{p_1} \cdot \frac{p_2^{\alpha_2}}{p_2} \cdots \frac{p_k^{\alpha_k}}{p_k}\right) \times \left(p_1^{\alpha_1+1}-1\right)\left(p_2^{\alpha_2+1}-1\right) \cdots \left(p_k^{\alpha_k+1}-1\right)$

$= \underbrace{\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right)}_{n}\left(\frac{p_1^{\alpha_1+1}-1}{p_1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k}\right)$

$= n \times \left[p_1^{\alpha_1}\left(1-p_1^{-1-\alpha_1}\right) p_2^{\alpha_2}\left(1-p_2^{-1-\alpha_2}\right) \cdots\right]$

$= n \times \left[\underbrace{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}_{n}\right]\left[\left(1-p_1^{-1-\alpha_1}\right)\left(1-p_2^{-1-\alpha_2}\right) \cdots\right]$

$\Rightarrow \phi(n)\sigma(n) = n^2\left(1-p_1^{-1-\alpha_1}\right)\left(1-p_2^{-1-\alpha_2}\right) \cdots \left(1-p_k^{-1-\alpha_k}\right)$ $\rightarrow (1)$

In (1), calculate,

$\alpha_1 = \alpha_2 \ldots = \alpha_k = 1$

$\Rightarrow \sigma(n)\phi(n) > n^2\left(1-p_1^{-2}\right)\left(1-p_2^{-2}\right)\ldots$

true for larger values of α — only $\alpha = 1$

Q TPT: $\frac{\phi(n)\tau(n)+1}{n}$ is an integer if n is prime & not if not an integer if n is divisible by square of a prime

If n = prime

$\Rightarrow \phi(n) = n-1$

$\tau(n) = n+1$

$\Rightarrow \frac{\phi(n)\tau(n)+1}{n} = \frac{n^2-1+1}{n} \in \mathbb{Z}$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots$

$\because$ given n is a square number

then, $\left[\phi(p_1^2)\phi(p_2^{\alpha_2})\phi(p_3^{\alpha_3})\ldots\right]\left[\tau(p_1^2)\tau(p_2^{\alpha_2})\ldots\right]$

$p_1^2 p_2^{\alpha_2} p_3^{\alpha_3} \ldots$

$= \left[(p_1^2-p_1)(p_2^{\alpha_2}-p_2^{\alpha_2-1})\ldots\right]\left[\frac{p_1^3-1}{p_1-1} \times \frac{p_2^{\alpha_2+1}-1}{p_2-1}\ldots\right]$

$p^2 p_2^{\alpha_2} p_3^{\alpha_3} \ldots$

$\ldots$ Simplifying it, we find it is not integer.

Hence proved

* Theorem : $\phi(n), d(n), \sigma(n), \mu(n)$ are multiplicative functions.

Proof : $\phi(n)$

To show : $\phi(mn) = \phi(m)\,\phi(n)$

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$

So, $m \times n = (p_1^{\alpha_1} p_2^{\alpha_2} \cdots) (q_1^{\beta_1} q_2^{\beta_2} \cdots)$

$$\phi(mn) = \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \cdots [\phi(q_1^{\beta_1}) \phi(q_2^{\beta_2}) \cdots]$$

$$= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \phi(q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s})$$

$$= \phi(m)\,\phi(n)$$

Similar proof for others.

Ch: Primitive Roots

Defin^n: Order of a positive integer:
If a is some +ve integer. Then, if
$a^e \equiv 1 \pmod m$,
e is called order of $a \pmod m$ if
e is the smallest power s.t. $g.c.d(a, m) = 1$

eg: Let $m = 7$

observ^n: as m is prime
So, $a^e \equiv 1 \pmod m \equiv a^{\phi(p)} \equiv 1 \pmod p$
$\Rightarrow e = m-1$ or $p-1$
$\Rightarrow e = 6.$

Eg, $a = 3$.

$3 \equiv 3 \pmod 7$
$3^2 \equiv 2 \pmod 7$
$3^3 \equiv 6 \pmod 7$
$3^4 \equiv 4 \pmod 7$
$3^5 \equiv 5 \pmod 7$
$3^6 \equiv 1 \pmod 7$

we have got all the RRS elements of elements 7 $\{1, 2, 3, 4, 5, 6\}$
Smallest power giving 1, is 6. So, $e = 6$.

Notation of order is $ord_m a$.

eg: find $Ord_6 5$ & $ord_{13} 7$.

$\Rightarrow 5^e \equiv 1 \pmod{13}$

Page No

- Start putting all powers of RRS

$5 \equiv 5 \pmod{13}$

$5^2 \equiv 12 \pmod{13}$

$5^3 \equiv 8 \pmod{13}$

$5^4 \equiv 1 \pmod{13}$

$\therefore e = 4$.

Now,

$7^e \equiv 1 \pmod{13}$

$7 \equiv 7 \pmod{13}$

$7^2 \equiv 10 \pmod{13}$

$7^3 \equiv$

$7^{12} \equiv 1 \pmod{13}$

$\Rightarrow e = 12$

$\therefore$ order $= 12$

Theorem: Let a be a +ve integer, s.t. $g.c.d(a, m) = 1$ & ~~order~~ $\text{ord}_m a = e$. Then, $a^n \equiv 1 \pmod{m}$ iff $e \mid n$.

Corollary: Let a be a +ve integer s.t. $g.c.d(a, m) = 1$. Then, $\text{ord}_m a \mid \phi(m)$

In particular, if p is prime & $p \nmid a$, then, $\text{ord}_p a \mid (p-1)$.

eg: Compute $\text{ord}_{21} 5$.

We have mod 21.

Complete residue system (CRS) =

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}$

3 has common factor with 21. Hence remove all

Now, RRS = {1, 2, ~~3~~, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}

Note: Take all the divisors of $\phi(m)$ i.e, $\phi(21)$

i.e $\phi(3)\phi(7) = 2 \cdot 6 = 12$.

Divisors of 12 are: 1, 2, 3, 4, 6, 12

Now, raise no. only to these powers and check.

So, $5^1 \equiv 5 \pmod{21}$

$5^2 \equiv 4 \pmod{21}$

$5^3 \equiv 20 \pmod{21}$

$5^4 \equiv 16 \pmod{21}$

$5^6 \equiv 1 \pmod{21}$

So, we got $e = 6$.

eg: $ord_{10} 3$

$\Rightarrow \mod 10$.

$\therefore \phi(10) = \phi(2)\phi(5) = 4$

divisors of 4 are 1, 2, 4

$3^1 \equiv 3 \pmod{10}$

$3^2 \equiv 9 \pmod{10}$

$3^4 \equiv 1 \pmod{10}$

So, $e = 4$

* Corollary 10.2: Let $ord_m a = e$. Then $a^i \equiv a^j \pmod m$ iff $i \equiv j \pmod e$

eg: given $ord_{21} 5 = 6$. Verify $5^{14} \equiv 5^2 \pmod{21}$

by corollary, as $14 \equiv 2 \pmod 6$ is holding true

$\Rightarrow 5^{14} \equiv 5^2 \pmod{21}$

CLASSMATE

* Theorem 10.2: Let $\text{ord}_m a = e$ & k is any +ve integer. Then, $\text{ord}_m(a^k) = \frac{e}{g.c.d(e,k)}$

eg If $\text{ord}_{21} 5 = 6$. Then, $\text{ord}_{21}(5^{14}) = \frac{6}{gcd(6,14)}$

$\Rightarrow \text{order} = \frac{6}{2} = (3)$

eg: find $\text{ord}_{21} 5^9$

We know, $\text{ord}_{21} 5 = 6$

now, $\text{ord}_{21} 5^9 = \frac{6}{g.c.d(6,9)} = \frac{6}{3} = (2)$

* Corollary 10.3: Let $\text{ord}_m a = e$ & k is any +ve integer. Then, $\text{ord}_m(a^k) = e$ iff $g.c.d(e,k) = 1$

* PRIMITIVE ROOTS

• Defin^n: Let a be a +ve integer s.t. $g.c.d(a,m) = 1$. Then, a is a primitive root (mod m) if $\text{ord}_m a = \phi(m)$

(≡ Euler's theorem)

eg mod (10)

If $a = 3$ Then, $3^4 \equiv 1 \pmod{10}$

So, $a = 3$ = primitive root

(note: $g.c.d(3,10) = 1$)

eg(2): $5^6 \equiv 1 \pmod 7$

So, 5 is a primitive root

Page No

eg: $\text{ord}_7 3 = ?$

$3^{(\quad)} \equiv 1 \pmod 7$

So, by Euler's, $\text{ord} = 6$ $(m=7,\ \phi(m) = 7-1)$

Also, $\text{ord}_7 5 = 6$ (similarly)

$\Rightarrow$ 3 & 5 are primitive roots $\pmod 7$ of Euler

Also, $\text{ord}_{13} 7 = 12$ $(\text{mod } m = \text{mod } 13 \Rightarrow \phi(m) = 13-1)$

eg: Verify 2 is primitive root $(\text{mod } 9)$

$2^{(\quad)} \equiv 1 \pmod 9$

(M1) So, by previous ideas,

$2^6 \equiv 1 \pmod 9$

$\Rightarrow$ 2 is a primitive root.

(M2) Find $\phi(m)$

$\phi(9) = \phi(3^2) = 3^2 - 3 = 6$

So, divisors of 6 = 1, 2, 3, 6

So, only take powers 1, 2, 3 & 6 & try

$2^1 \equiv 2 \pmod 9$

$2^2 \equiv 4 \pmod 9$

$2^3 \equiv 8 \pmod 9$

$2^6 \equiv 1 \pmod 9$

Note: 3 & 5 are the only Fermat primes for which, 2 is a primitive root.

* Corollary: If m has a primitive root, then, it has $\phi(\phi(m))$ primitive roots.

In particular, if n is prime, say p.
Then, it has $\phi(p-1)$ primitive roots.

✡ PRIMALITY TEST

Theorem 10.4 (by Lucas)

Let n be a +ve integer. If $\exists$ a +ve integer x s.t. $x^{n-1} \equiv 1 \pmod{n}$

& $x^{\frac{(n-1)}{q}} \not\equiv 1 \pmod{n}$ ∀ prime factors q of $n-1$.

Then, n is prime.

eg: Find whether 1117 is prime or not

Choose any x

① Let $x = 2$. So, $2^{1117-1} \equiv 1 \pmod{1117}$

So $2^{1116} \equiv 1 \pmod{1117}$

$1116 = 2^2 \cdot 3^2 \cdot 31$

$2^{1116} = (2^{100})^{11} 2^{16} \equiv (2^{93})^{11} \cdot 750$

$\equiv 70 \cdot 750$

$\equiv 1$

② $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$

here, $q = 2, 3, 31$

So, $\frac{1116}{2}$

$2^{2} \not\equiv 1 \pmod{1117}$

$2^{558} \equiv ? \pmod{1117}$

Seeing $2^{558} = (2^{30})^{18} \cdot 2^{18}$

$\equiv (1000)^{18} \cdot 766$

$= (2^3 5^3)^{18} \cdot 766$

$= 2^{54} \cdot 5^{54} \cdot 766$

$(2^{100})^5 \cdot 2^{58} \cdot 2^5$

2^{558} $\quad 279$

3^2

or, $2^{558} = (2^{50})^{11} \cdot 2^8$

$\equiv (69)^{11} \cdot 256$

$\equiv -1 \not\equiv 1$

Show for this.

Page No

Ily, show for $q = 3$ & 31 & show

$2^{1116} \equiv 2^{372} \equiv 996 \neq 1$

$2^{1116/31} \equiv 2^{36} \equiv 331 \neq 1$

So, 1117 is prime.

* **Corollary:** Let n be an odd +ve integer. If $\exists$ a +ve integer x, s.t. $x^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ & $x^{\frac{n-1}{q}} \neq 1 \pmod{n}$ $\forall$ odd prime factors q of $n-1$. Then, n is prime.

In previous question I used $q = 2, 3, 31$

Now, don't use $q = 2$ (even). Use others

eg Verify 1213 is prime

Let $n = 5$

$5^{\frac{1213-1}{2}} \equiv (-1) \pmod{1213}$

$\Rightarrow 5^{\frac{1212}{2}} \equiv -1 \pmod{1213}$

$\Rightarrow 5^{606} \equiv (-1) \pmod{1213}$

Try: $5^{51} \equiv -528 \pmod{1213}$

$(5^{51})^8 \equiv (-528)^8 \pmod{1213}$

$\Rightarrow 5^{53} \equiv 256 \pmod{1213}$

$\Rightarrow 5^{256} \equiv 117$

$\Rightarrow 5^{512} \cdot 5^{94} \equiv -1 \pmod{1213}$

Now, factors of $n-1 = 1212 = 2^2 \cdot 3 \cdot 101$

$5^{\frac{1212}{2}} \equiv ? \pmod{1213}$

$\Rightarrow 5^{1212/2} \equiv 909 \pmod{1213} \not\equiv 1 \pmod{1213}$

& $5^{1212/101} \equiv 115 \pmod{1213} \not\equiv 1 \pmod{1213}$

Defin^{n}: Let $f(x)$ be a poly. with integral coeffs. An integer α is a sol^{n} of $f(x) \equiv 0 \pmod m$ if $f(\alpha) \equiv 0 \pmod m$.

If $\beta \equiv \alpha \pmod m$, β is also a sol^{n}.

eg: Given: $f(x) = x^2 - x + 1 \equiv 0 \pmod{13}$

Find sol^{n}.

Sol) Factoring $x^2 - x + 1$

Idea: One of the methods can be, factoring "1" by its residue $\pmod{13}$

So, $x^2 - x + 1 \equiv x^2 - x - 12 \pmod{13}$

$= (x-4)(x+3) \pmod{13}$

Now, equate $\not\equiv 0 \Rightarrow x - 4 = 0 \Rightarrow x = 4$

$x + 3 = 0 \Rightarrow x = -3$

Checking $4^2 - 4 + 1 = 13 \equiv 0 \pmod{13}$

Checking $(-3)^2 + 3 + 1 = 13 \equiv 0 \pmod{13}$

So, both satisfy Hence, both are sol^{ns}.

Now, as -3 is sol^{n} $\Rightarrow -3 \equiv 10 \pmod{13}$

$\Rightarrow$ even 10 is a sol^{n}

So, incongruent solutions are 4 & 10 (don't take $-ve$)

* Lagrange's Theorem:

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ be a polynomial of degree $n \geq 1$ with integral coefficients, where $p \nmid a_n$.

Then, the congruence $f(x) \equiv 0 \pmod p$ has atmost n incongruent solutions $\pmod p$

eg: find the incongruent solutions of

$(x^3-1) \equiv 0 \pmod{13}$

$\Rightarrow (x-1)(x^2+x+1) \equiv 0 \pmod{13}$

$x^2+x+1 \equiv x^2+x-12 \pmod{13}$

$= (x+4)(x-3) \pmod{13}$

$\Rightarrow (x-1)(x+4)(x-3) \equiv 0 \pmod{13}$

$\Rightarrow (x-1)(x-9)(x-3) \equiv 0 \pmod{13}$

$x+4=0$ gives $x=-4$.

Don't take -ve.

$\Rightarrow (x-9)$ gives the factor $x=9$

That is +ve.

So, roots are 1, 9 & 3

incongruent

$1 \not\equiv 3 \pmod{13}$

$1 \not\equiv 9 \pmod{13}$

$3 \not\equiv 9 \pmod{13}$

* Corollary:

Every prime p has $\phi(p-1)$ incongruent primitive roots.

eg: $p=7$ $\Rightarrow$ we are doing $\pmod 7$

we know $\phi(7)=6$

& RRS = {1, 2, 3, 4, 5, 6}

Now, $\phi(7-1)=\phi(6)=2$.

$\Rightarrow \exists$ 2 incongruent primitive roots.

$\Rightarrow a^6 \equiv 1 \pmod 7$

$\rightarrow$ has 2 values from RRS.

Quadratic Residues (Q.R.)

Already done : $29 \equiv ? \pmod 5$

Now do : $\begin{cases} x^2 \equiv a \pmod m \\ x^2 + bx + c \equiv l \pmod m \end{cases}$

↳ here, a, l are quadratic residues

We will mainly do : $x^2 \equiv a \pmod p$

↳ p = prime ∀ cases

Defin^n : If p is a prime no. & g.c.d $(a, p) = 1$, then, we say a is a quadratic residue of the congruence $x^2 \equiv a \pmod p$.

eg : $x^2 \equiv 4 \pmod 7$

↳ as 4 is quadratic residue, $x = 2$ is a sol^n

$x^2 \equiv 9 \pmod 7$

↳ as 9 is quadratic residue, $x = 3$ is a sol^n

g.c.d $(7, 9) = 1$

$x^2 \equiv 49 \pmod 7$

↳ as g.c.d $(49, 7) \neq 1 \Rightarrow$ 49 is not a quadratic residue

* Note : (ALL) whole squares are (NOT) quadratic residues.

* Theorem : The no. a is a quadratic residue $\pmod p$, iff

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Ex If $a=2$, $p=5$

$$2^{\frac{5-1}{2}} = 2^2 \not\equiv 1 \pmod 5$$

So, 2 not a quadratic residue

If $a=3$, $p=11$

$$3^{\frac{11-1}{2}} = 3^5 = 243 \equiv 1 \pmod{11}$$

So, 3 is a QR.

★ Legendre Symbol:

↳ used to say if any quadratic congruence has sol^n

Notation: $\left(\frac{a}{p}\right)$: p : ODD PRIME

(Reduce $\frac{a}{p}$ to standard form)

Now,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & ; \text{if } a \text{ is Q.R.} \\ 0 & ; \text{if } p \mid a \\ -1 & \text{otherwise} \end{cases}$$

★ Theorem:

If p is odd prime, & a & b are relatively prime to p. Then,

P① $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod p$

P② $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

P③ $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$

(P1)

proof: to show: $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod p$

Let $a \equiv b \pmod p$

- Then, a & b are either QR or not, for $x^2 \equiv a \pmod p$

If a & b are QR, then, $\left(\frac{a}{p}\right) = 1$ & $\left(\frac{b}{p}\right) = 1$

$\Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

If a & b are not QR, then,

$\left(\frac{a}{p}\right) = -1$ & $\left(\frac{b}{p}\right) = -1$

$\Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(P2) L.H.S $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod p$

(using P3)

$\Rightarrow \left(\frac{ab}{p}\right) = (a^{\frac{p-1}{2}})(b^{\frac{p-1}{2}}) \pmod p$

$= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

$\Rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

↳ from P1, $\left(\frac{a}{p}\right)$ & $\left(\frac{b}{p}\right)$ should have same value.

(P3) From Euler's criterion,

$a^{\frac{p-1}{2}} \equiv 1 \pmod p$ if a is a Q.R.

Also, if a is a Q.R,

$$\left(\frac{a}{p}\right) = 1$$

Put $1 = \left(\frac{a}{p}\right)$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

If a is not a QR.

↳ either $p \mid a \Rightarrow p \mid a^{\frac{p-1}{2}} \Rightarrow a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$

& $\left(\frac{a}{p}\right) = 0. \Rightarrow a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$

↳ $p \nmid a$.

$\Rightarrow \left(\frac{a}{p}\right) = -1$

↳ Also, $\left(\frac{a}{p}\right) \begin{cases} = 0, & p \mid a \\ = \pm 1, & p \nmid a \end{cases}$

Now, $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

$\Rightarrow a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

✡ JACOBI SYMBOLS

If $n = p_1, p_2, \ldots, p_r$

↳ p_i are ~~distinct~~ odd primes, not necessarily distinct, then,

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right) \cdots \left(\frac{n}{p_r}\right)$$

eg: $\left(\frac{4}{25}\right) = \left(\frac{4}{5}\right)\left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{5}\right)\left(\frac{2}{5}\right)\left(\frac{2}{5}\right)$

Ques : Show $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$

Let $c = p_1 p_2 \cdots p_k$

then, $\left(\frac{ab}{c}\right) = \left(\frac{ab}{p_1 p_2 \cdots p_k}\right) = \left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right) \cdots \left(\frac{ab}{p_k}\right)$

From P2, as done before

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$\Rightarrow \left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right)\cdots\left(\frac{ab}{p_k}\right) = \left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)\left(\frac{b}{p_k}\right)$$

$$= \left[\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)\right]\left[\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\right]$$

$$\Rightarrow \left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$$

H.P

Q. Show : $\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$

let $b = p_1 \cdot p_2 \cdots p_k$

$c = q_1 \cdot q_2 \cdots q_s$

$$\Rightarrow \left(\frac{a}{bc}\right) = \frac{a}{(p_1 p_2 \cdots p_k)(q_1 q_2 \cdots q_s)} = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right) \times \left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\cdots\left(\frac{a}{q_s}\right)$$

$$\Rightarrow \left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$$

eg. take any two nos. : 21 & 25

Find $\left(\frac{21}{25}\right) = \left(\frac{3\times7}{5\times5}\right) = \left(\frac{3}{5\times5}\right)\left(\frac{7}{5\times5}\right) = \left(\frac{3}{5}\right)\left(\frac{7}{5}\right)\left(\frac{3}{5}\right)\left(\frac{7}{5}\right)$

eg Find $\left(\frac{-2}{5}\right)$

$$\left(\frac{-2}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right)$$

done by formula (from the list) →

eg :- Find $\left(\frac{-1}{3\times3}\right)$

$$\left(\frac{-1}{3\times3}\right) = \left(\frac{-1}{3}\right)\left(\frac{1}{3}\right) = (-1)(1) = -1$$

✡ Quadratic Reciprocity Law

If p and q are distinct odd primes, then
$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv 3 \pmod 4$

↳ In this case,
$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

- Theorem : If p is an odd prime integer & g.c.d $(a,p)=1$, then, $x^2 \equiv a \pmod{p^n}$ has a sol^n if $\left(\frac{a}{p}\right) = 1$ and has no sol^n if $\left(\frac{a}{p}\right) = -1$.

- Note : If one sol^n of $x^2 \equiv a \pmod p$ is x_0. Then, other sol^n is given by $p - x_0$.

✱ Formulas / Results / Rules

① $\left(\frac{a^2}{p}\right) = 1$, if a & p are integers; p → prime.

eg: $\left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$

eg(2): $\left(\frac{4}{17}\right) = 1$

② $\left(\frac{1}{p}\right) = 1$; p : prime

③ $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$; for p = prime > 2

eg: $\left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$

④ $\left(\frac{-1}{p}\right) = \begin{cases} -1, & \text{if } p \equiv 1 \pmod 4 \\ 1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$

⑤ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

⑥ $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8 \\ -1, & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$

⑦ $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

⑧ $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$

⑨ $\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12} \\ -1, & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$

eg Find whether $x^2 \equiv 15 \pmod{89}$ has a soln.

Soln exists if $\left(\frac{15}{89}\right) = 1$

$$\left(\frac{15}{89}\right) = \left(\frac{3}{89}\right)\left(\frac{5}{89}\right) = (-1) \times \left(\frac{5}{89}\right)$$

Finding $\left(\frac{3}{89}\right)$: M1 $\left(\frac{3}{89}\right) = -1$ ($\because 89 \equiv 5 \pmod{12}$)

M2 $\left(\frac{3}{89}\right) = \left(\frac{p}{q}\right)$, say

If $3 \equiv 3 \pmod 4$ → holds

& $89 \equiv 3 \pmod 4$ → ✗ hold

$\Rightarrow \left(\frac{3}{89}\right) = \left(\frac{89}{3}\right)$ (can be reversed as one of them doesn't hold)

Now,

$\left(\frac{89}{3}\right) = \left(\frac{2}{3}\right)$ (replacing 89 by its residue)

$\left(\frac{2}{3}\right) = (-1)^{\frac{9-1}{8}} = -1$

Finding $\left(\frac{5}{89}\right)$: $5 \to x$, $89 \to y$.

$\Rightarrow x \equiv 3 \pmod 4$ i.e. $5 \equiv 3 \pmod 4$ ✗

$\Rightarrow \left(\frac{5}{89}\right) = \left(\frac{89}{5}\right)$ (Reciprocity law)

Replace 89 by its residue $\pmod 5$

$= \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$

So, finally, $\left(\frac{3}{89}\right)\left(\frac{5}{89}\right) = (-1)(1) = -1$

$\Rightarrow$ NO SOLUTION.

Page No

eg Find $\left(\frac{83}{103}\right)$

Note: Find (if not known) that 83 & 103 are primes.

(M1) Using Reciprocity:

$\frac{83}{103} = \frac{p}{q}$, say. Is $83 \equiv 3 \pmod 4$? Yes

Is $103 \equiv 3 \pmod 4$? Yes.

} both yes.

$$\Rightarrow \left(\frac{83}{103}\right) = -\left(\frac{103}{83}\right)$$

$$= -\left(\frac{20}{83}\right) = -\left(\frac{4}{83}\right)\left(\frac{5}{83}\right)$$

$$= -(1)\left(\frac{5}{83}\right)$$

$\left(\frac{5}{83}\right)$ $\quad 5 \equiv 3 \pmod 4$ ✗

$83 \equiv 3 \pmod 4$ ✓

$$\Rightarrow \left(\frac{5}{83}\right) = \left(\frac{83}{5}\right) = \left(\frac{3}{5}\right)$$

Now, Is $5 \equiv \pm 1 \pmod{12}$ ✗

Is $5 \equiv \pm 5 \pmod{12}$ ✓

$$\Rightarrow \left(\frac{3}{5}\right) = -1$$

$$\Rightarrow \left(\frac{83}{103}\right) = -(1)(-1) = 1$$

Ans

eg $\left(\frac{3}{29}\right) = -1 \quad (\because 29 \equiv 5 \pmod{12})$

eg $\left(\frac{5}{29}\right) \rightarrow 5 \not\equiv 3 \pmod 4 \Rightarrow \left(\frac{5}{29}\right) = \left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = 1$ ✓

Page No

ex Find whether $x^2 \equiv -46 \pmod{17}$ has a sol^n or not?

Sol^n: Idea: find $\left(\frac{a}{p}\right)$. If $\left(\frac{a}{p}\right) = 1$, $\exists$ sol^n

$a = -46$, $p = 17$

$$\Rightarrow \left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{2 \times 23}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right)\left(\frac{23}{17}\right)$$

$$= (-1)^{\frac{17-1}{2}} (-1)^{\frac{289-1}{2}} \left(\frac{6}{17}\right)$$

replacing 23 by its residue.

$$\Rightarrow \left(\frac{-46}{17}\right) = 1 \cdot 1 \cdot \frac{2}{17} \cdot \frac{3}{17}$$

$$= 1 \cdot (-1) = -1$$

$$\neq 1.$$

So, $x^2 \equiv -46 \pmod{7}$ doesn't have a sol^n.

Alter :- $\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right)$

replacing 46 by its residue (mod 17)

$$= \left(\frac{-1}{17}\right)\left(\frac{12}{17}\right)$$

$$= 1 \cdot \left(\frac{4}{17}\right)\left(\frac{3}{17}\right)$$

$$= 1 \cdot \left(\frac{2^2}{17}\right)\left(\frac{3}{17}\right) = 1 \cdot 1 \cdot -1 = -1 \Rightarrow \text{no sol}^n$$

② Find the sol^n of $x^2 \equiv 4 \pmod{5}$

Whenever p is prime in modulus, do $\left(\frac{4}{5}\right)$

$\left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$ So, one solution is $x = 2$

Other solution $= p - x = 5 - 2 = 3$.

$(3^2 \equiv 4 \pmod{5})$

Page No

Q. Find sol^n of $x^2 \equiv 4 \pmod{15}$ → (1)

$\Rightarrow x^2 \equiv 4 \pmod{3 \times 5}$

We can write :
$$\left.\begin{aligned} x^2 &\equiv 4 \pmod 3 \\ \& \; x^2 &\equiv 4 \pmod 5 \end{aligned}\right\} \rightarrow (2)$$
(It's called as a sys.)

(1) has a sol^n iff (both) congruence in (2) are solvable.

As $\left(\frac{4}{3}\right) = 1$ & $\left(\frac{4}{5}\right) = 1$ ⇒ both congruence are solvable.

So, (1) has a sol^n.

(I) $x^2 \equiv 4 \pmod 3$

$x_0 = 2$ satisfies.

Other sol^n is $3 - 2 = 1$.

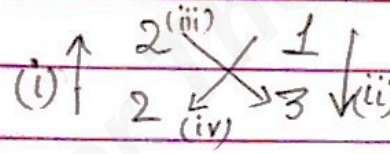
(II) $x^2 \equiv 4 \pmod 5$

$x_0 = 2$ is initial sol^n

Other sol^n is $5 - 2 = 3$

From (I) & (II) $x_0 = 2, 1, 3$ are not sol^{ns} of (1)

Now, these sol^{ns} like :-



Step (i) $x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 5$ → (3)

Step (ii) $x \equiv 1 \pmod 3$, $x \equiv 3 \pmod 5$ → (4)

Step (iv) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ → (5)

Step (v) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$ → (6)

Each set is solved using Chinese remainder theorem

Solving (3)

$x \equiv 2 \pmod 3$ & $x \equiv 2 \pmod 5$

M1 Observation Clearly, $x = 2$ satisfies.

Page No

M2 Chinese remainder

$x \equiv 2 \pmod 3$

$x \equiv 2 \pmod 5$

$c_1 = 2, n_1 = 5, \bar{n_1} = ?$

$c_2 = 2, n_2 = 3, \bar{n_2} = ?$

$n_1 \cdot \bar{n_1} \equiv 1 \pmod 3$

$\Rightarrow 5(\bar{n_1}) \equiv 1 \pmod 3 \Rightarrow \bar{n_1} = 2$

& $n_2 \bar{n_2} \equiv 1 \pmod 5$

$\Rightarrow 3(\bar{n_2}) \equiv 1 \pmod 5 \Rightarrow \bar{n_2} = 2$

$\Rightarrow$ Sol^n $= x_0 = c_1 n_1 \bar{n_1} + c_2 n_2 \bar{n_2}$

$= 2(5)(2) + 2(3)(2)$

$= 4(8) = 32.$

Now, $32 \equiv ? \pmod{15}$

$\Rightarrow ? = 2$ So, $\boxed{2}$ is the sol^n.

Solving (4)

$x \equiv 1 \pmod 3$ & $x \equiv 3 \pmod 5$

$c_1 = 1, n_1 = 5, \bar{n_1} = 2$

$c_2 = 3, n_2 = 3, \bar{n_2} = 2$

$x_0 = 1 \times 5 \times 2 + 3 \times 3 \times 2 = 28 \equiv ? \pmod{15}$

$? = \boxed{13}$ So, 13 is another sol^n.

Solving (5)

$x \equiv 2 \pmod 3$ & $x \equiv 3 \pmod 5$

$c_1 = 2, n_1 = 5, \bar{n_1} = 2$

$c_2 = 3, n_1 = 3, \bar{n_2} = 2$

$\Rightarrow x_0 = 2 \times 5 \times 2 + 3 \times 3 \times 2 = 38 \equiv ? \pmod{15}$

$\Rightarrow ? = 8$

$\Rightarrow \boxed{8}$ is a sol^n.

Solving (6)

$x \equiv 1 \pmod 3$ & $x \equiv 2 \pmod 5$

$c_1 = 1,\ n_1 = 5,\ \bar{n}_1 = 2$

$c_2 = 2,\ n_2 = 3,\ \bar{n}_2 = 2$

$x_0 = 1 \times 5 \times 2 + 2 \times 3 \times 2 = 22 \equiv ? \pmod{15}$

$\Rightarrow ? = 7$

So, $\boxed{7}$ is a sol^n

$S = \{2, 7, 8, 13\}$ are the incongruent solutions

(2) Solve: $x^2 \equiv 196 \pmod{1357} \longrightarrow (1)$

Sol^n: We solve: $x^2 \equiv 196 \pmod{23 \times 59}$.

Note: we need to find the set of all incongruent solutions.

System is: $\left.\begin{aligned} x^2 &\equiv 196 \pmod{23} \\ \& \quad x^2 &\equiv 196 \pmod{59} \end{aligned}\right\} \longrightarrow (2)$

Find $\left(\frac{196}{23}\right) = \left(\frac{14^2}{23}\right) = \left(\frac{a^2}{\text{prime}}\right) = 1$.

Illy, $\left(\frac{196}{59}\right) = 1$

They both have a sol^n.

So, eq^n is solvable

(I) $x^2 \equiv 196 \pmod{23}$.

(Note: 196 can be replaced by residue)

By observation, $x_0 = 14$ is one sol^n.

Other sol^n = 9 (23 − 14)

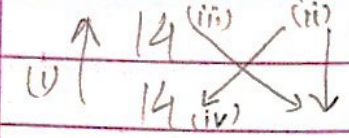
(II) $x^2 \equiv 196 \pmod{59}$

$x_0 = 14$ is one sol^n.

Other $59 - 14 = 45$

Page No

Write the soln as:



(i) :- $x \equiv 14 \pmod{23}$ & $x \equiv 14 \pmod{59}$ → (3)

(ii) :- $x \equiv 9 \pmod{23}$ & $x \equiv 45 \pmod{59}$ → (4)

(iii) :- $x \equiv 14 \pmod{23}$ & $x \equiv 45 \pmod{59}$ → (5)

(iv) :- $x \equiv 9 \pmod{23}$ & $x \equiv 14 \pmod{59}$ → (6)

Solving (3), (4), (5) & (6).

(By Chinese remainder or any other way).

we have, Set of incongruent solution is:

$S = \{14, 635, 722, 1343\}$

Q. Solve: $x^2 \equiv 23 \pmod{7^2}$.

↳ Break 7^2 into 7×7 & write a system of 2 congruences:-

$$\begin{cases} x^2 \equiv 23 \pmod{7} \\ \& \; x^2 \equiv 23 \pmod{7} \end{cases}$$

Sol① Show $\left(\frac{23}{7}\right) = 1$ to know if sol^n exists or not

Now, → Replace 23 by its residue (mod 2)

$$\left(\frac{23}{7}\right) = \left(\frac{2}{7}\right) = 1$$

$$\left\{ \because \frac{2}{p} = 1 \; ; \; 7 \equiv -1 \pmod{8} \right\}$$

So, sol^n exists.

Sol② Solve $x^2 \equiv 23 \pmod{7}$

↳ $a = 23$

↳ $p = 7$.

Replace 23 by its residue.

$x^2 \equiv 2 \pmod 7$

$x_0 = 3$ is the initial sol^n

Now, we find b from

$$\boxed{x_0^2 = a + bp^k}$$ for S(2), $k = 1$

$\Rightarrow 3^2 \equiv 23 + b(7)$

$\Rightarrow b = -2$.

Now, find y_0 from :

$$\boxed{2 x_0 y_0 \equiv -b \pmod p}$$

$\Rightarrow 2(3) y_0 = 2 \pmod 7$

$\Rightarrow 3 y_0 \equiv 1 \pmod 7$

$y_0 = -2$ or $(-2+7) = 5$

$\Rightarrow y_0 = 5$

To find x_1, which is the sol^n, we take :

$$\boxed{x_1 = x_0 + y_0 p^k}$$

Here $k = 1$

$\Rightarrow x_1 = 3 + 5(7)^1 = 38$.

Putting $x_1 = 38$ in eq^n, we get sol^n

So, $x_1 = \pm 38$ are sol^{ns}

Q Solve : $x^2 \equiv 23 \pmod{7^3}$

S1) From prev, $\left(\frac{23}{7}\right) = 1$. So, sol^n exists.

S2) Follow the same steps to get $x_1 = 38$.

Page No

(53) Now, $k=2$ & initial sol^n got was $x_1 = 38$

We will find x_2.

To find b.

$$x_1^2 = a + bp^2$$

$$\Rightarrow (38)^2 = 23 + (b)(7)^2$$

$$\Rightarrow b = \frac{1600+4-160-23}{49}$$

$$\Rightarrow b = 29$$

Now, find y_1

$$\Rightarrow 2x_1 y_1 \equiv -b \pmod{p}$$

$$\Rightarrow 2(38)(y_1) \equiv -29 \pmod{7}$$

↳ note: don't do $\pmod{7^2}$ as not done in the formula

$\Rightarrow y_1 = 1$ satisfies.

Now, find sol^n (i.e, x_2)

$$x_2 = x_1 + y_1 p^2$$

$$= 38 + 1(7)^2$$

$$= 38 + 49$$

$$\Rightarrow x_2 = 87$$

This is the final sol^n. (as it satisfies)

So, $x_2 = \pm 87$ is sol^n

Extra: had it been $(\text{mod } 7^4)$, go one more step after this....

* Theorem: Let a be an odd integer & $p=2$ then, (i) $x^2 \equiv a \pmod 2$ always has a sol^n.

(ii) $x^2 \equiv a \pmod{2^2}$ has a sol^n if $a \equiv 1 \pmod{2^2}$.

(iii) $x^2 \equiv a \pmod{2^n}$ for $n \geq 3$ has a sol^n if $a \equiv 1 \pmod{2^3}$.

* here,

$x_0^2 = a + b2^k$

$x_0 y_0 = -1 \pmod 2$

Sol^n :- $x_1 = x_0 + y_0 2^k$

Q. Find if it has a sol^n :-

$x^2 \equiv 5 \pmod 8$

here, $5 \not\equiv 1 \pmod 8$

$\Rightarrow \exists$ no sol^n.

Q. $x^2 \equiv 17 \pmod{16}$

i.e $x^2 \equiv 17 \pmod{24}$

It has sol^n because $17 \equiv 1 \pmod 8$.

Q. $x^2 \equiv 17 \pmod{32}$

$17 \equiv 1 \pmod 8$

So, sol^n exists

eg Quadratic congruences :

$x^2 + 5x \equiv 12 \pmod{31}$

Formula : given :

$ax^2 + bx + c \equiv 0 \pmod p$.

we can say, $(2ax + b)^2 \equiv (b^2 - 4ac) \pmod p$.

$= y$, say

$\Rightarrow y^2 \equiv (c_1) \pmod p$

(Similar to what we just did)

Now,

$(2 \cdot 1 \cdot x + 5)^2 \equiv (5^2 - 4 \cdot 1 \cdot (-12)) \pmod{31}$

$\Rightarrow (2x+5)^2 \equiv 73 \pmod{31}$

let $2x+5 = y$

$\Rightarrow y^2 \equiv 73 \pmod{31}$

Find $\frac{73}{31}$ i.e $\left(\frac{a}{p}\right) = 1$

$= \left(\frac{11}{31}\right)$

Now, $11 \equiv 3 \pmod 4$

& $31 \equiv 3 \pmod 4$

So, $\left(\frac{73}{31}\right) = -\left(\frac{31}{11}\right)$

$= -\left(\frac{9}{11}\right) = -\left(\frac{3^2}{11}\right) = -1$

$\neq 1$

$\Rightarrow$ No sol^n.

Q. Solve : $5x^2 - 6x + 2 \equiv 0 \pmod{13}$

$(2ax+b)^2 \equiv b^2 - 4ac \pmod p$

$\Rightarrow (10x - 6)^2 \equiv 36 - 40 \pmod{13}$

$\Rightarrow (10x-6)^2 \equiv -4 \pmod{13}$

let $10x - 6 = y$

$\Rightarrow y^2 \equiv -4 \pmod{13}$

or $y^2 \equiv 9 \pmod{13}$

Now, $\left(\frac{9}{13}\right) = \left(\frac{3^2}{13}\right) = 1$

So, sol^n exists.

$\Rightarrow y^2 \equiv 9 \pmod{13}$

$\Rightarrow y = 3$ is one of the sol^{ns}.

So, other sol^n $= 13 - 3 = 10$.

Hence, soln's are $y = 3, 10$.

$$\boxed{2ax \equiv y - b \pmod{p}}$$

$\Rightarrow 2 \cdot 5 \cdot x \equiv 3 - (-6) \pmod{13}$

$\Rightarrow 10x \equiv 9 \pmod{13}$

$\Rightarrow x = 10$.

Also, $2 \cdot 5 \cdot x \equiv 10 - (-6) \pmod{13}$

$\Rightarrow 10x \equiv 16 \pmod{13}$

or $5x \equiv 8 \pmod{13}$

$x = 12$ solves this congruence

So, 2 soln's of this problem are $x = 10, 12$

Ch: Continued Fractions

eg: $\frac{26}{60} = 1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{3}}}$

Later on, it was changed to writing like

$$1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5}}}}}$$

* General form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

↳ $a_1, \ldots a_n$ are +ve integers.

↳ a_0 can be +ve or -ve integers.

If all a_i are integers, fraction is called a simple continued fraction.

↳ can be finite (terminating) & infinite (non-terminating)

Result : The value of any finite continued fraction will always be a rational numbers.

eg Write $\frac{19}{51}$ as a continued fraction

$\frac{19}{51}$ (Den > Num)

$19 \overline{)51} (2$
$\underline{38}$
13

$51 = 19 \times 2 + 13$

$\Rightarrow \frac{51}{19} = 1 \times 2 + \frac{13}{19}$

$19 = 13 \times 1 + 6$

$\Rightarrow \frac{19}{13} = 1 + \frac{6}{13}$

$13 = 6 \times 2 + 1$

$\Rightarrow \frac{13}{6} = 2 + \frac{1}{6}$ → Stop when we get 1

$\Rightarrow \frac{19}{51} = \frac{1}{\frac{51}{19}} = \frac{1}{2 + \frac{13}{19}}$

$= \frac{1}{2 + \frac{1}{\frac{19}{13}}}$

$= \frac{1}{2 + \frac{1}{1 + \frac{6}{13}}}$

$$= \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\frac{13}{6}}}}$$

$$\Rightarrow \frac{19}{51} = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}}$$

$$\left(\equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \frac{1}{\quad}}}} \right)$$

$\Rightarrow a_0 = 0, a_1 = 2, a_2 = 1, a_3 = 2, a_4 = 6.$

Doing back calculation :

$$1 + \frac{1}{\frac{13}{6}} = 1 + \frac{6}{13} = \frac{19}{13}$$

$$\& \quad \cfrac{1}{2 + \cfrac{1}{\frac{19}{13}}} = \frac{1}{2 + \frac{13}{19}} = \frac{19}{51} = \text{original quotient}$$

(2) $\frac{333}{19}$

$$333 = 19 \times 17 + 10$$

$$\Rightarrow \frac{333}{19} = 17 + \frac{10}{19}.$$

$19 = 10 \times 1 + 9$

$\Rightarrow \frac{19}{10} = 1 + \frac{9}{10}$

& $10 = 9 \times 1 + 1$

$\Rightarrow \frac{10}{9} = 1 + \frac{1}{9}$ → stop.

$\Rightarrow \frac{333}{19} = 17 + \frac{10}{19}$

$= 17 + \cfrac{1}{\frac{19}{10}}$

$= 17 + \cfrac{1}{1 + \frac{9}{10}}$

$= 17 + \cfrac{1}{1 + \cfrac{1}{\frac{10}{9}}}$

$\Rightarrow \frac{333}{19} = 17 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{9}}}$ Ans

↳ $a_0 = 17,\ a_1 = 1,\ a_2 = 1,\ a_3 = 9$

* Numerator > Denominator : a_0 has a value
* Numerator < Denominator : $a_0 = 0$

$\frac{170}{53}$

$170 = 53 \times 3 + 11$

$\Rightarrow \frac{170}{53} = 3 + \frac{11}{53}$

$53 = 11 \times 4 + 9$

$\Rightarrow \frac{53}{11} = 4 + \frac{9}{11}$

$11 = 9 \times 1 + 2$

$\Rightarrow \frac{11}{9} = 1 + \frac{2}{9}$

$9 = 2 \times 4 + 1$

$\Rightarrow \frac{9}{2} = 4 + \frac{1}{2}$ → Stop.

Now, $\frac{170}{53} = 3 + \frac{11}{53}$

$= 3 + \cfrac{1}{4 + \frac{9}{11}}$

$= 3 + \cfrac{1}{4 + \cfrac{1}{1 + \frac{2}{9}}}$

$\Rightarrow \frac{170}{53} = 3 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{2}}}}$

$\hookrightarrow a_0 = 3, a_1 = 4, a_2 = 1, a_3 = 4, a_4 = 2$

$= [3; 4; 1, 4, 2]$

Standard Notation : $[a_0; a_1, a_2, a_3, \dots]$

Note : Simple continued fraction is not unique.

like,

$$\frac{170}{53} = 3 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1}}}}} = [3; 4, 1, 4, 1, 1]$$

we got extra term. So, not unique

* If last no. is $a_n = a_{n-1} + 1$.

$\Rightarrow a_n = a_{n-1} + \frac{1}{1}$.

Note: If we take a quotient of two successive Fabonacci numbers

$$\frac{U_{n+1}}{U_n} = [1; 1, 1, 1, \ldots 1]$$

eg: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ----

Taking 2 successive numbers, say 34 & 55

$\frac{55}{34}$

$55 = 34 \times 1 + 21$ $\quad$ $8 = 5 \times 1 + 3$

$\frac{55}{34} = 1 + \frac{21}{34}$ $\quad$ $\frac{8}{5} = 1 + \frac{3}{5}$.

$34 = 21 \times 1 + 13$ $\quad$ $5 = 3 \times 1 + 2$

$\frac{34}{21} = 1 + \frac{13}{21}$ $\quad$ $\frac{5}{3} = 1 + \frac{2}{3}$

$21 = 13 \times 1 + 8$ $\quad$ $3 = 2 \times 1 + 1$

$\frac{21}{13} = 1 + \frac{8}{13}$. $\quad$ $\Rightarrow \frac{3}{2} = 1 + \frac{1}{2}$

$13 = 8 \times 1 + 5$. $\quad$ $\Rightarrow 2 = 1 + \frac{1}{1}$.

$\Rightarrow \frac{13}{8} = 1 + \frac{5}{8}$.

$$\Rightarrow \frac{55}{34} = 1 + \frac{21}{34}$$

$$= 1 + \cfrac{1}{1 + \frac{13}{21}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{8}{13}}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{5}{8}}}}$$

$$\Rightarrow \frac{55}{34} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}}}$$

§ SOLVING DIOPHANTINE EQUATIONS.

Defin^n: C_K are continued fractions made from cutting off expansion after K^{th} partial denominator.

→ $C_K = [a_0; a_1, a_2, \ldots, a_K]$

→ $C_0 = a_0$.

eg $\frac{19}{51} = [0; 2, 1, 2, 6]$

$\Rightarrow \frac{19}{51} = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}}$

cut off like this → gives $C_1 = 1/2$

$C_2 = \frac{1}{2+1/1} = 1/3$

$C_3 = \frac{1}{2 + \frac{1}{1+1/3}} = \frac{3}{8}$

$C_4 = \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}}} = \frac{19}{51}$

→ $C_0 = a_0 = 0$.

$C_1 = 1/2$

$C_2 = 1/3$

$C_3 = 3/8$

$C_{(4)} = 19/51$

$a_K = a_{(4)} = 6$

So, $K = 4$

Theorem: $C_K = \frac{P_k}{q_k}$; $0 \le k \le n$

where $P_0 = a_0$ (by default), $P_1 = a_1 a_0 + 1$

$q_0 = 1$, $q_1 = a_1$

& $P_K = a_K P_{K-1} + P_{K-2}$

$q_K = a_K q_{K-1} + q_{K-2}$, for $k \ge 2$.

So, finding C_1, C_2, C_3 & C_4 using theorem:

$k=0$ $P_0 = a_0 = 0$, $q_0 = 1$

$k=1$ $P_1 = 1$, $q_1 = 2$

$(a_0 = 0, a_1 = 2, a_2 = 1, a_3 = 2, a_4 = 6)$

$k=2$ $P_2 = a_2 P_1 + P_0 = (1)(1) + (0) = 1$

$q_2 = a_2 q_1 + q_0 = (1)(2) + (1) = 3$

$k=3$ $P_3 = a_3 P_2 + P_1 = (2)(1) + 1 = 3$.

$q_3 = a_3 q_2 + q_1 = (2)(3) + 2 = 8$.

$k=4$ $P_4 = a_4 P_3 + P_2 = (6)(3) + 1 = 19$

$q_4 = a_4 q_3 + q_2 = (6)(8) + 3 = 51$

Now,

$C_0 = \frac{P_0}{q_0} = 0$, $C_1 = \frac{P_1}{q_1} = \frac{1}{2}$, $C_2 = \frac{P_2}{q_2} = \frac{1}{3}$.

$C_3 = \frac{3}{8}$, $C_4 = \frac{19}{51}$. (same as found before)

So, verified

* Theorem:

$$P_k q_{k-1} - q_k P_{k-1} = (-1)^{k-1}, \quad 1 \leq k \leq n.$$

eg $172x + 20y = 1000$. $\equiv (ax + by = c)$

$\div 4$ (make in simplest form).

$\Rightarrow 43x + 5y = 250$.

Sl Make RHS = 1 (i.e. replace the value for the time being)

So, $43x + 5y = 1$

$(\equiv ax + by = 1)$

S2 Solve $\left(\frac{a}{b}\right) = \left(\frac{43}{5}\right)$

Write $\left(\frac{a}{b}\right)$ as a continued fraction

$43 = 5 \times 8 + 3.$

$\Rightarrow \frac{43}{5} = 8 + \frac{3}{5}$

Use the $\frac{\text{num}}{\text{den}}$ form s.t num > den

$\frac{5}{3} = 1 + \frac{2}{3}$

$\frac{3}{2} = 1 + \frac{1}{2}$

$\frac{2}{1} = 1 + \frac{1}{1}$

$\Rightarrow \frac{43}{5} = 8 + \frac{3}{5}$

$= 8 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}$

C_1, C_2, C_3, C_4

S3 Find the values of C_0 & C_k

$C_0 = a_0 = 8.$

$C_1 = 8 + \frac{1}{1} = 9$

$C_2 = \frac{17}{2}$

$C_3 = \frac{26}{3}$

$C_4 = \frac{43}{5}$

Page No

S4 Use the last two C_k's
↳ here, C_3 & C_4.
$\parallel$ $\parallel$
$\frac{P_3}{q_3}$ $\frac{P_4}{q_4}$.

$\frac{P_4}{q_4} \times \frac{P_3}{q_3}$

↳ cross multiply. (Just like we find determinant of matrix)

$= P_4 q_3 - q_4 P_3 = (-1)^{k-1}$ (by theorem)

$\Rightarrow \frac{43}{5} \times \frac{26}{3}$

$= 43(3) - 26(5)$

$(= 129 - 130 = -1 = (-1)^{4-1} = -1$
(So, theorem verified)$)$

$\Rightarrow 43(3) + 5(-26) = 1$

$(\equiv 43x + 5y = 1)$

$\times 250$ (to make it $43x + 5y = 250$)

$\Rightarrow 43(3 \times 250) - 5(26 \times 250) = 250.$

$\Rightarrow 43(750) + 5(-6500) = 250.$

$\Rightarrow x_0 = 750$

$y_0 = -6500.$

(Note: If we do only till C_3 i.e., $2 = 1 + \frac{1}{1}$ & is not done, we CAN get diff^t answer)

$\Rightarrow x = x_0 + b/d\, t = 750 + 5t$

$y = y_0 - \frac{a}{d} t = -6500 - 43t$

↳ by same prev. formulas.

Page No

eg Solve the diophantine eqn :-
$17x + 15y = 143$
(Solving a previously done problem)
$\equiv (ax + by = c)$

S1) Make RHS = 1
$\Rightarrow 17x + 15y = 1$

S2) Find continued fraction of
$\left(\frac{a}{b}\right) = \frac{17}{15}$

$17 = 15 \times 1 + 2$
$\Rightarrow \frac{17}{15} = 1 + \frac{2}{15}$
&
$15 = 2 \times 7 + 1$
$\Rightarrow \frac{15}{2} = 7 + \frac{1}{2}$ → step

$\frac{17}{15} = 1 + \cfrac{1}{7 + \cfrac{1}{2}}$ (c_1, c_2)

S3) Find c_0, c_1, c_2
$c_0 = a_0 = 1$
$c_1 = 1 + \frac{1}{7} = \frac{8}{7}$

$c_2 = \frac{17}{15}$

S4) Use last two c_k's (c_1 & c_2)
$\frac{17}{15} \times \frac{8}{7}$
$\Rightarrow 17(7) - 15(8) = (-1)^{k-1} = (-1)^{2-1} = -1$
$= 17(7) + 15(-8) = -1$
$\Rightarrow 17(7 \times 143) + 15(-8 \times 143) = -143$

Page No

$= 17(-1001) + 15(+1144) = 143$

$\Rightarrow x_0 = -1001$

$y_0 = +1144$

$\Rightarrow x = x_0 + \frac{b}{d}t = -1001 + \frac{15}{1}t$

$y = y_0 - \frac{a}{d}t = +1144 - 17t$

M2 $P_0 = a_0, \; P_1 = a_1 a_0 + 1, \; q_0 = 1, \; q_1 = a_1$

$k \geq 2 \quad P_k = a_k P_{k-1} + P_{k-2}$

$q_k = a_k q_{k-1} + q_{k-2}$

$C_k = \frac{P_k}{q_k}$

$C_0 = \frac{P_0}{q_0} = \frac{1}{1} = 1$

$P_1 = 8, \; q_1 = 7, \; C_1 = \frac{8}{7}$

$P_2 = 17, \; q_2 = 15, \; C_2 = \frac{17}{15}$

Then, solve as above

Q. Check if the following eqn has a soln:

$100x - 12y = 42$

$g.c.d(100, 12) = 4$

g.c.d (a, b) should divide c. Only then solution exists.

As $4 \mid 42$ So, solution ✓

Page No

Q. $100x - 12y = 44$

$g.c.d(100, 12) = 4 \mid 44.$

So, solution exists.

$\div 4$

$\Rightarrow 25x - 3y = 11$

S1) Make RHS = 1

$\Rightarrow 25x - 3y = 1$

S2) Find continued fraction for $\frac{a}{b} = \frac{25}{3}$

$25 = 3 \times 8 + 1$

$\Rightarrow \frac{25}{3} = 8 + \frac{(1)}{3.}$ → stop

S3) Find C_0, C_1

$C_0 = 8$

$C_1 = 25/3$

For last two C_k's, we have

$\frac{25}{3} \times \frac{8}{1}$

$\Rightarrow 25(1) - 3(8) = (-1)^{k-1} = (-1)^0 = 1$

$\Rightarrow 25(1) - 3(8) = 1$

$\Rightarrow 25(11) - 3(88) = 11$

$\Rightarrow x_0 = 11, y = 88$

$x = x_0 + \frac{b}{d}t = 11 + \frac{3}{1}t$

$y = y_0 + \frac{a}{d}t = 88 + 25t$ Ans

Q. Find continued fraction for $\frac{19}{51}$

M1 Euclidean Algorithm

The Multiples

$51 = 19 \times 2 + 13$

$19 = 13 \times 1 + 6$

$13 = 6 \times 2 + 1$

$6 = 1 \times 6 + 0$

These are the values of a_1, a_2, a_3, a_4.

So, continued fraction = $[0; 2, 1, 2, 6]$

$\therefore$ Num < Den

So, continued fraction = $0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}}$

M2 like done before.

Q. Find Continued fraction of $\frac{158}{57}$

Using Euclidean Algorithm

$158 = 57 \times 2 + 44$

$57 = 44 \times 1 + 13$

$44 = 13 \times 3 + 5$

$13 = 5 \times 2 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 0$

$\therefore$ Num > Den.

values of $a_0, a_1, a_2, a_3, a_4, a_5, a_6$

158
−114
44

Ex. continued fraction: $[2; 1, 3, 2, 1, 1, 2]$

Sol.

$$\frac{158}{57} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}}}$$

✡ Continued...

APPLICATIONS OF CONGRUENCES

Q. Find the last two digits of 3^{1492}.

Idea: Find

$$3^{1492} \equiv ? \pmod{100}$$

↳ for hundredth's place

Firstly, find $\phi(m)$

$$3^{\phi(m)} \equiv 1 \pmod{100}$$

$$\phi(100) = \phi(2^2)\,\phi(5^2) = (2^2-2)(5^2-5)$$
$$= (20)(2) = 40$$

$$\Rightarrow 3^{40} \equiv 1 \pmod{100}$$

So, $1492 = 40 \times 37 + 12$

So,

$$3^{1492} = (3^{40})^{37} \cdot 3^{12} \equiv (1)^{37} \cdot 3^{12} \pmod{100}$$

Now, $(3^4) = 81 \equiv -19 \pmod{100}$

$$\Rightarrow (3^4)^3 \equiv (-19)^3 \pmod{100}$$
$$\equiv (-6859) \pmod{100}$$
$$\equiv -59 \pmod{100}$$
$$\equiv (41) \pmod{100}$$

↳ So, these are the last two digits.

Ans

Q. Find last two digits of 5^{2048}.

Find :-

$$5^{2048} \equiv ? \pmod{100}$$

Find :- $\phi(100) = 40$

$\Rightarrow 5^{40} \equiv 1 \pmod{100}$

$\Rightarrow 2048 = 40 \times 51 + 8$

$\Rightarrow 5^{2048} \equiv (5^{40})^{51} \cdot 5^8 \equiv 5^8$

Now

$5^3 \equiv 125 \equiv 25 \pmod{100}$

& $5^4 = 625 \equiv 25 \pmod{100}$

$\Rightarrow (5^4)^2 \equiv 25^2 \pmod{100} = 625$

$\Rightarrow 5^{2048} \equiv (25) \pmod{100}$

→ last two digits

This is wrong

So, Solving

$5^{2048} \equiv ? \pmod{100}$

$5^4 \equiv 25 \pmod{100}$

$5^8 \equiv 25 \pmod{100}$

⋮

Solve it

**Note :-

$g.c.d(5, 100) \neq 1$

So, $5^{\phi(m)} \equiv 1 \pmod{100}$

i.e Euler's theorem cannot be used.

HW $2^{100} \equiv ? \pmod{100}$

Ans = 76 (last 2 digits)

Previous Section Q : Solve : $x^2 \equiv 25 \pmod{2^5}$

$\Rightarrow \left(\frac{25}{32}\right) \Rightarrow \left(\frac{5}{2}\right)\left(\frac{5}{2}\right)\cdots\left(\frac{5}{2}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{5}\right)\cdots\left(\frac{2}{5}\right) = 1$

So, solution exists

(S1) $x^2 \equiv 25 \pmod{2}$

$x_0 = 5$ is initial sol^n

If $p \neq 2$, use $2x_0y_0 \equiv -b \pmod p$

Now, $x_0y_0 \equiv -1 \pmod 2$

$\Rightarrow 5y_0 \equiv -1 \pmod 2$

$\Rightarrow y_0 = 1$

$\Rightarrow x_1 = x_0 + y_0 2^{(1)}$

$= 5 + (1)(2)^1$

$\Rightarrow x_1 = 7$ $(x^2 \equiv 25 \pmod{2^2})$

(S2) Now, $x_1y_1 \equiv -1 \pmod 2$

$\Rightarrow y_1 = 1$, when we know $x_1 = 7$

& $x_2 = 7 + 1(2^2) = 11$ $(x^2 \equiv 25 \bmod (2^3))$

(S3) $11 \cdot y_2 \equiv -1 \pmod 2$

$\Rightarrow y_2 = 1$

& $x_3 = 11 + (1)(2)^3 = 19$ $(x^2 \equiv 25 \bmod 2$

(S4) $19 \cdot y_3 \equiv -1 \pmod 2$

$\Rightarrow y_3 = 1$

& $x_4 = 19 + (1)2^4 = 35$

$35 \cdot y_4 \equiv -1 \pmod 2$

$\Rightarrow y_4 = 1$

$\Rightarrow x_4 = 35$ satisfies for $(\bmod 2^5)$ Ans

Q. Find the least +ve integer that satisfies:

$$7^{128} \equiv x \pmod{13}$$

we know $7 \equiv -6 \pmod{13}$

$7^2 \equiv -3 \pmod{13}$

$7^3 \equiv 5 \pmod{13}$

& $7^{12} \equiv 1 \pmod{13}$ $\because p = 13$ = prime

→ By Euler's Formula.

Now, $128 = 12 \times 10 + 8$

$\Rightarrow$

$$7^{128} = (7^{12})^{10} \cdot 7^8 \equiv 7^8 \pmod{13}$$
$$= (7^2)^4 \pmod{13}$$
$$\equiv (-3)^4 \pmod{13}$$
$$= 81 \pmod{13}$$
$$\equiv 3 \pmod{13}$$

$\Rightarrow 7^{128} \equiv 3 \pmod{13}$

Ans

Q. Show : $2^{341} \equiv 2 \pmod{341}$

$2^{10} \equiv 1 \pmod{341}$

Now, $2^{341} = (2^{10})^{34} \cdot 2$

$\equiv 2 \pmod{341}$

Q. Solve :- $x^2 + x + 1 \equiv 0 \pmod{11}$

M2

$$(2x+1)^2 \equiv (8) \pmod{11}$$

$$\left[\equiv (2ax+b)^2 \equiv (b^2-4ac) \pmod{m}\right]$$

$\Rightarrow y^2 \equiv 8 \pmod{11}$

Now, Checking $\left(\frac{8}{11}\right) = 1$ or not

$$\left(\frac{8}{11}\right) = \left(\frac{4}{11}\right)\left(\frac{2}{11}\right) = \left(\frac{2^2}{11}\right)\left(\frac{2}{11}\right) = 1\left(\frac{2}{11}\right)$$

$$= (1)(-1)^{\frac{p^2-1}{8}}$$

$$= (-1)$$

So, ∄ NO SOLUTION

Page No

Q. $x^2 \equiv 5 \pmod{7^2}$: Check if solution exists.

Make a system:

$x^2 \equiv 5 \pmod 7$

& $x^2 \equiv 5 \pmod 7$

$\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)$ $\left(\because 5 \not\equiv 3 \pmod 4\right)$

$= \left(\frac{2}{5}\right)$

Now, $\frac{2}{p} = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{25-1}{8}} = -1$

$= -1$

So, solution doesn't exist.

Q. Let $n = 203$

Find whether 203 is prime or not?

$2^{202} \equiv 1 \pmod{203}$ or not?

$2^8 = 256 \equiv 53 \pmod{203}$

$2^8 \equiv 53 \pmod{203}$

Now,

$2^{10} \equiv 9 \pmod{203}$

$202 = 10 \times 20 + 2$

$2^{202} = (2^{10})^{20} \cdot 2^2$

$\equiv 9^{20} \cdot 2^2$

$= (9^4)^5 \cdot 2^2$

$\equiv 65^5 \cdot 2^2 = 116029025$

$\equiv 74 \cdot 4 = 296 \equiv 93$

So, $\neq 1$. So, not satisfied.

#

Q. Take $n = 31$

Let $n = 2$

$\Rightarrow 2^{30} \equiv ? \pmod{31}$

We know

$2^5 = 32 \equiv 1 \pmod{31}$

$\Rightarrow (2^5)^6 \equiv 1^6 \pmod{31}$

$\therefore 2^{30} \equiv 1 \pmod{31}$

↳ 1st cond^n of Lucas Theorem Satisfied

Now,

$n-1 = 30 = 2 \times 3 \times 5$.

Only prime factors are 2, 3, 5

①. $x^{\frac{31-1}{2}} = 2^{15} \equiv ? \pmod{31}$

Now, $2^5 \equiv 1 \pmod{31}$

$\Rightarrow (2^5)^3 \equiv 1^3 \pmod{31}$

$\Rightarrow 2^{15} \equiv 1 \pmod{31}$

By the theorem, we should have got

$2^{15} \not\equiv 1 \pmod{31}$

But we didn't get it. So, choose some other x.

& try.

For some x, we will get it as a prime no.

If not, it's composite.

NOTE: IN EXAMS, VALUE OF X WILL BE GIVEN.

NOT FOR EXAMS

Extra: 8 CRYPTOGRAPHY

Terms:

- Plain Text: Whatever message has to be hidden
- ~~Hidden Text: C~~
- Crypted Text, Cipher: When we hide the message

eg

A = 00
B = 01
C = 02
D = 03
E = 04
F = 05
⋮
X = 23
Y = 24
Z = 25

Caesar, while sending messages, he used to replace every alphabet by an alphabet, +3 shifted.

If P = Plain
C = Crypted

Then, $C \equiv (P+3) \pmod{26}$

eg:

If P = A Boy.

⇒ 00 01 14 24

+3

03 04 17 (27) >25

↳ replace by

= 03 04 17 01 $\quad 27 \equiv ? \pmod{26}$

= D E R B $\quad \Rightarrow 27 \equiv 01 \pmod{26}$

↳ Crypted message

Flaw: Pattern could be seen

Monoalphabetic Cipher: Use one code at all times for any alphabet.

eg: If B = 01, wherever I have 01 ⇒ its B.

☆ UPDATED WAY

eg: Suppose, message is

A B OY IS WAITING

Choosing a key 00 01 14 24 08 18 ---------- → (1)

= AM

⇒ we get A M AM AM AMAMAMA

00 12 0012 0012 ---------- → (2)

Adding (1) & (2)

= 00 13 14 36 ----------

Replace by residue (mod 26) = 00 13 14 10 ----------

Convert to alphabets = A N O K ----------

↳ Send this message (encrypted)

☆ RSA ALGORITHM (1977)

→ Rivest, Shamir, Adleman

Idea: Take two very large prime numbers p & q.

& make $n = pq$

↳ n: crypted message.

RSA defined a no. for every type of char. like:

A = 00 2 = 31

⋮ ⋮

Z = 25

; = 26 Space = 99

. = 27

? = 28

0 = 29

1 = 30.

Eg: Let $p = 29$, $q = 53$

$n = pq = 1537$

Now, find $\phi(n) = \phi(pq) = (p-1)(q-1) = 28 \cdot 52$

$\Rightarrow \phi(n) = 1456$

Then, select a no. e s.t $g.c.d(e, \phi(n)) = 1$

Let $e = 47$ (mostly, we take $e > p, q$)

We need a recovery exponent, say d.

d is taken, s.t $ed \equiv 1 \bmod (\phi(n))$

$\Rightarrow 47 \cdot d \equiv 1 \pmod{1456}$

$\Rightarrow d = 31$

Now, suppose the message to be encrypted is:

NO WAY

↳ space.

Let the code = M

So, M = 13 14 99 22 00 24

↳ Its a large no.

So, break into blocks & send.

Breaking into blocks → 131, 499, 220, 024

Each block will be called M_1, M_2, M_3, M_4

Now,

do: $M_1^e \equiv ? \pmod n$

i.e $131^{47} \equiv ? \pmod{1537}$

The residue ("?") is the code.

Next, do for M_2

$\Rightarrow 499^{47} \equiv ? \pmod{1537}$

Thus, find codes of blocks.

For decryption, the recovery exponent, d is used
So, if we had

$$131^{47} \equiv (570) \pmod{1537}$$

$$570^{31} \equiv ? \pmod{1537}$$

Solving it, we get ? = 131

So, receiver gets the message sent by sender = 131

end of course.