

3. Congruent modulo n:

Two integers a & b are said to be congruent modulo n, if

 $a \mod n = b \mod n$ i.e. we get same remainder when a is divided by n & b is divided by n .

The notation is, $a \equiv b \pmod{n}$

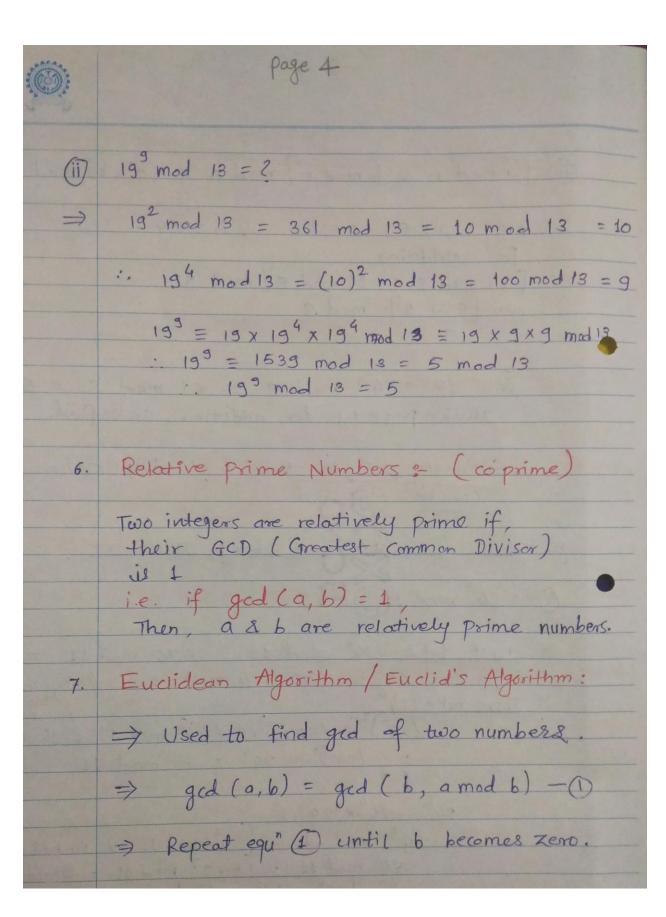
e.g. 1 73 mod 23 = 4 mod 23 ux get same remainder i.e. 4 Hence,

73 = 4 (mod 23)

- (2) 21 mod 10 = -9 mod 10 21 = -9 (mod 10)
- Modulas Asithmetic: properties:
- a mod n + b mod n mod n $= (a+b) \mod n$
- (i) a mod n b mod n] mod n = (a-b) mod n

i.e. $24^2 = 576 = 4 \mod 11 = 4$ Then take 24^4 $\therefore (24^2)^2 = (576)^2 = (4)^2 \mod 11 = 16 \mod 11$ $\therefore (24^2)^2 = 24^4 = 5 \mod 11$

 $24^{5} = 24^{4} \times 24^{4}$ $\therefore 24^{5} \mod 11 = [24^{4} \mod 11 \times 24 \mod 11] \mod 11$ $24^{5} \mod 11 = [5 \times 2] \mod 11 = 10 \mod 11$ $\therefore 24^{5} \mod 11 = 10$



```
Page 5
8. Example of Euclid's Algorithm
     gcd (161, 112) = gcd (112, 161 mod 112)

= gcd (112, 49)

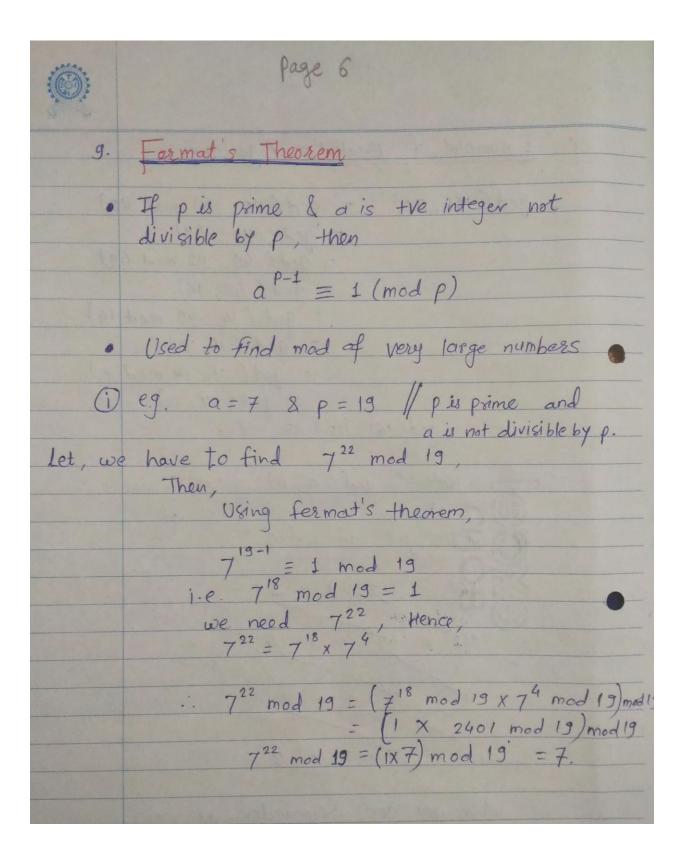
= gcd (49, 112 mod 49)

= gcd (49, 14)

= gcd (14, 49 mod 14)

= gcd (7, 14 mod 7)

= gcd (7, 0)
           = gcd(7,0)
: gcd(161,112) = 7.
             Note: gcd(a, 0) = a
     In steps, we can write,
            161 = 112 x 1 + 49
            112 = 49 \times 2 + 14
            49 = 14 × 3 + 7
            14 = 7x2 + 0
        when you get remainder as zero,
The ged is obtained in its above step
ie. ged (161, 112) = 7.
```



10. Extended Euclidean Algorithm:

i.e. ged of a &b is written as linear combination of two integers x & y.

Let's say, gcd (888, 54) = 888 x + 54 y we have to find out values of x & y

Step 1: Use Euclidean Algorithm to find out

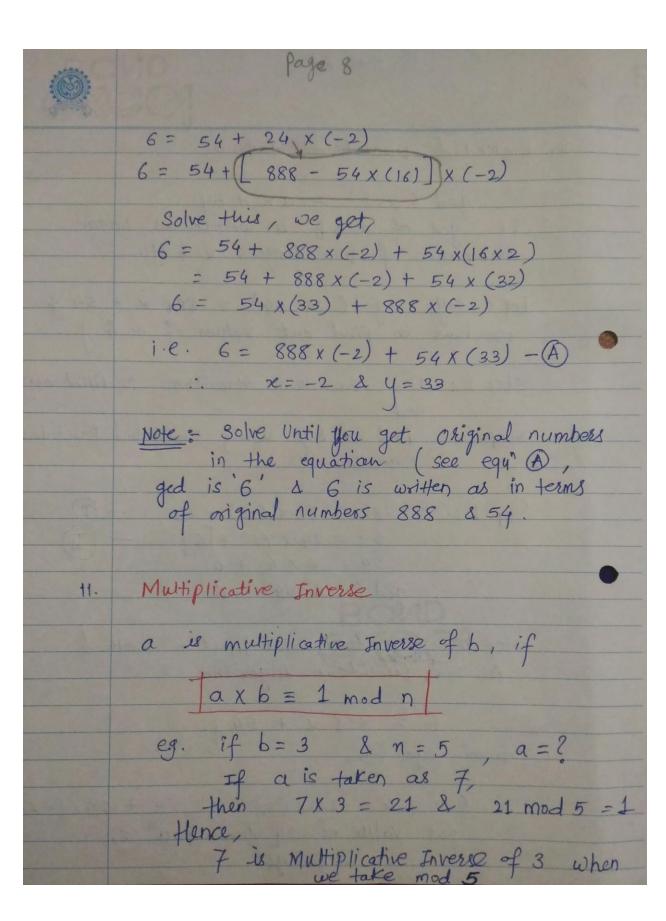
Step 2: find x & y using Extended Euclidean Algorithm.

Step 1: 888 = 54x (16) + 24 54 = 24 x (2) + 6 $24 = 6 \times 4 + 0$ ged (888, 54) = 6

Step 2:- Use Back Substitution Method.
As, per Euclidean Algorithm,

6 = 888 x + 54 y. from equ" (I)

> $6 = 54 - 24 \times (2) = 54 + 24 \times (-2)$ put value of 24 from equ" (=), we get,



12. Euler's Totient function o(n):

It is the number of positive integers less than n & relatively prime to n.

for prime number p, $\phi(p) = p-1$ e.g. $\phi(5) = 5 - 1 = 4$ o (7) = 7-1 = 6 ·

for Non-prime number,

eg. $\phi(4) = 1$ step 1: Take all nos. less than 4, here, 1,2,43

Step 2: Out of 1, 2 43,

ged (1,4)=1 => 184 are co-prime/relative gcd (2,4) = 2 > Not relative prime & ged (3,4) =1 => Relative prime.

Hence, $\phi(4) = 2$ Because only 1 & 3 are Lielative prime to 4

\$\(\phi(6) = 2 \quad \text{Because only 1 \$\pm\$ 5 are relative prime \$ (10) = 4 [Because only 1, 3, 7 & 9 are

relative prime to 10).

 $\phi(30) = \phi(5) \times \phi(6) = 4 \times 2 = 8$ $\phi(77) = \phi(7) \times \phi(10) = 6 \times 10 = 60$ 13. Euler's Theorem :

for Every a & n, that are relatively prime,

a (mod n)

Again, it is also used for finding mod of very large numbers.

eg. 97 mod 143 = ?

a=97, n= 143

 $\phi(n) = \phi(143) = 3$

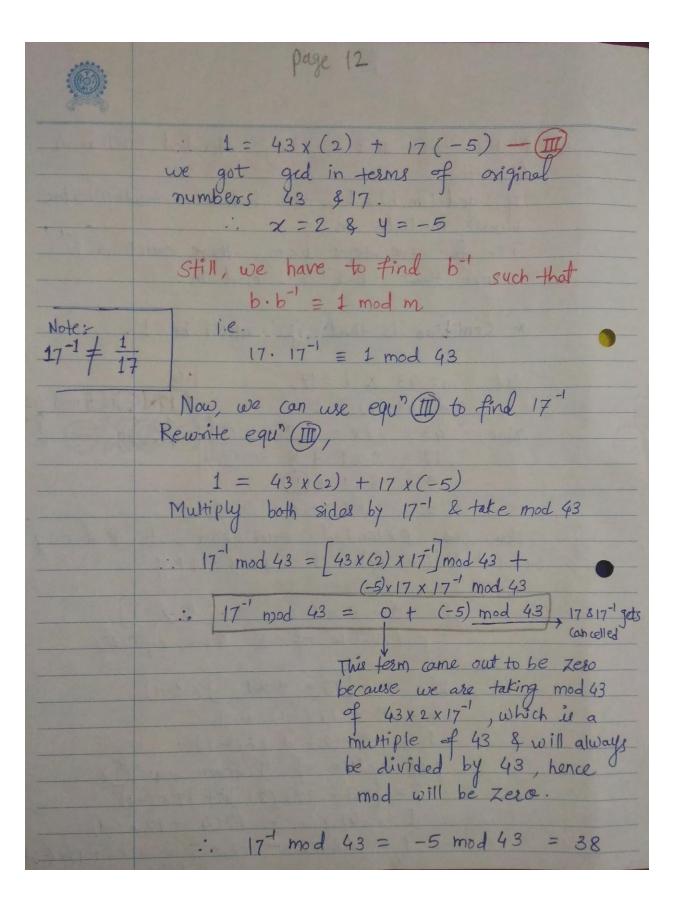
143 is not prime \$\(\phi(13) = \phi(11) \times \phi(13) \)

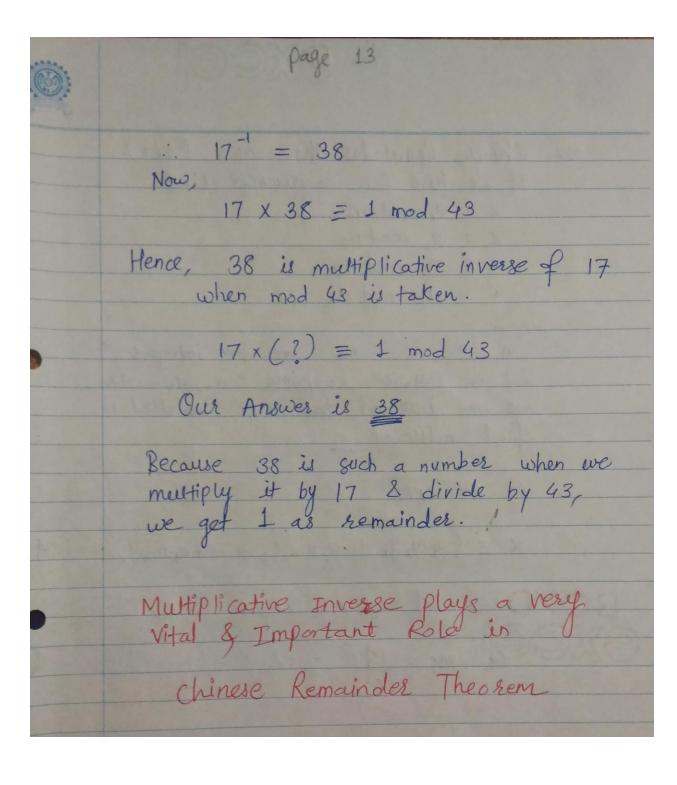
\$ (143) = 10 x 12 = 120

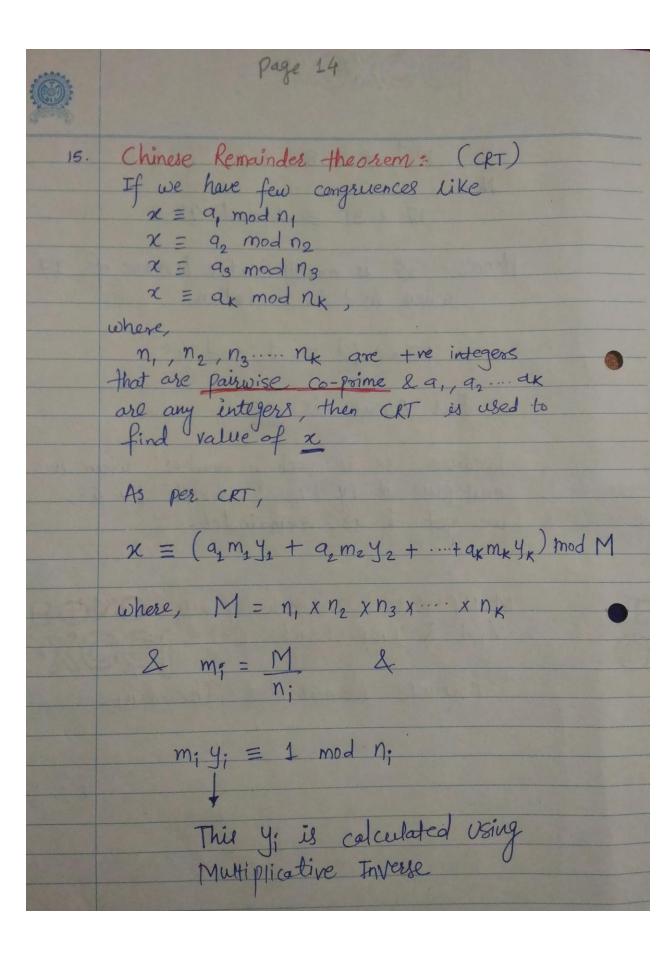
:. 97 120 x 97 = (1x97) mod 143

:. 97 = 97 mod 143

:. 97 121 mod 143 = 97.







	Page 15
16.	Solve Using chinese Remainder Theorem: $x = 1 \mod 5$, $x = 6 \mod 7$ by $x = 8 \mod 11$
>	Here, 5, 7 & 11 are pairwise co-prime 1.e. (5,7), (7,11) & (11,5) are coprimes
	Here, $n_1 = 5$, $n_2 = 7 \ 8 \ n_3 = 11$ $M = 5 \times 7 \times 11 = 385$ $m_1 = M - 385 = 77$ $n_1 = 5$ $q_2 = 6$
tent says	$m_2 = \frac{M}{n_2} = \frac{385}{7} = \frac{55}{7}$ $q_3 = 8$
	$8 \text{ m}_3 = \frac{M}{n_3} = \frac{385}{11} = 35$ As per CRT, $M = (2 \text{ m} \text{ U} + 2 \text{ m} \text{ U}) \approx 1 \text{ M}$
•	$x \equiv (a, m, y, + a_2 m_2 y_2 + a_3 m_3 y_3) \mod M$ $\therefore x \equiv (1x77xy, + 6x55xy_2 + 8x35xy_3) \mod 385$ $ \bigcirc$
	Now, we have to find y_1 , y_2 & y_3 from equ's 77 $y_1 \equiv 1 \mod 5$
	$55 y_2 \equiv 1 \mod 7$ $2 35 y_3 \equiv 1 \mod 11$
	(i) To find y_1 use Multiplicative Invesse. $5 = 77 \times 0 + 5$ (I) $77 = 5 \times 15 + 2$ (II)
	$5 = \pm x + 1$ $2 = 1 \times 2 + 0$ P.T.O.

```
· Page 16
    1 = 5 - 2x2 = 5 + 2x(-2)
     put value of 2 from (I)

:. 1 = 5 + (77 - 5 \times 15) \times (-2)

:. 1 = 5 + 77(-2) + 5 \times 30

:. 1 = 7.7(-2) + 5(31)
Now, y = 77-1 => is to be found.
         Multiply both sides of equ' III)
by 77-1 & take mod 5
     77^{-1} \mod 5 = 77^{-1} \times 77 \times (-2) \mod 5 + (5 \times 31 \times 77^{-1}) \mod 5

= -2 \mod 5 + 0 dividible by 5

\therefore 77^{-1} = 3 completely
             Hence y, = 3
      i.e. 77 x 3 = 1 mod 5
(ii) y_0 = \ell
     we have 55 y2 = 1 mod 7.
 7 = 55 \times 0 + 7 — \sqrt{2}
55 = 7 \times 7 + 6 — \sqrt{2}
6 = 1 \times 6 + 0
              () 1 = 7 - 6 x 1 = 7 + 6 x (-1)

put value of 6 from equ' (2)
```

```
Page 17
  1 = 7 + [55 - 7x7](-1)
 |\cdot| = 7 + 55 (-1) + 7×7
  1.1 = 55(-1) + 7(8) - (1)
Naw, To find 55-1 ie. y2,
 Multiply both sides of equ" (1) by 55-1 & take
 mod 7.
  55-1 mod 7 = 55.(-1). 55-1 mod 7 + (7x8x55-1 mod 7)
  :. 55 mod 7 = -1 mod 7 + 0
  :. 55 -1 =
     : [y2 = 6]
(iii) Similarly solve for y3.
    35 y = 1 mod 11.
  11 = 35 x 0 + 11
   35 = 11 × 3 + 2 - ($1)
   11= 2×5 +17
   2= 1/2+0
    ( 1= 11-2×5 = 11+2×(-5)
    1 = 11 + (35 - 11x3) x (-5)
    : 1 = 11 + 35 (-5) + 11 x 15
      . 1 = 35(-5) + 11(16) - (11)
```



To find 35%, i.e. y3, multiply both sides of equ" (III) by 35% & take mod 11.

 $35^{-1} \mod 11 = 35 \times 35^{-1} \times (-5) \mod 11 + 11 \times 16 \times 35^{-1} \mod 11$ $35^{-1} \mod 11 = -5 \mod 11 + 0$

35 1 mod 11 = 6

from equ" A,

2 = (1x77x y, + 6x55 x y2 + 8x35 x y3) mod 385 put values of y1, y2 & y3

 $\chi \equiv (77 \times 3 + 6 \times 55 \times 6 + 8 \times 35 \times 6) \mod 385$ $\chi \equiv (231 + 1980 + 1680) \mod 385$ $\chi \equiv 3891 \mod 385$

·. 2 = 41

Thus, $41 \equiv 1 \mod 5$ $41 \equiv 6 \mod 7$ $41 \equiv 8 \mod 11$

Hence, x = 41 solves all the equations