Euclidean (Algorithm)

> Reputition / Iteration.

Calculate g.c.d (567, 315) and expres. g.c.J (567, 315) = 567M + 315V.

By division algorithm

 $\frac{253}{63}$ = 4.

315)567(1

252/315 (1

567: 315×1 + 252 - (1)

315 = 252 × 1 + 63 - (II)

63)252 (4

63 is the last non-zero

g.c.1 of (567,315) = 63.

01.1. - 17

XM +yV

Find two integers u and v satisfying
63 u + 55 v = 1.

$$\rightarrow (63,55) \rightarrow co-prime to$$
each other.

 $g.c. \perp (63,55) = 63 M + 55 V.$ ox, 63 M + 55 V = 1.

W=7, V=-8

L.C.M (hart Common Multiple)

-2, -6, 10 -> what is L.C.M.)

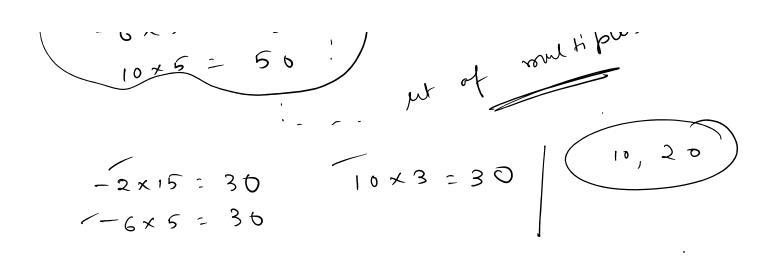
$$-6 \times 5 = -10$$

$$-6 \times 5 = -30$$

$$10 \times 5 = 50$$

1 multiplus.

Lecture 19 Page 2



Prime Numbers.

An integer p>1 is haid to be a prime no.
if only puritive divisors are only 1 and p.
even prime -> 2.

Thm: If p be a prime number and []

1 < a < p, then p is prime to a.

Thm: - If p be a prime and a is an integer > p such that p is not a divisor of a then p is prime to a.

Lecture_19 Page

of a, then p is prime to a. p=10.) a=21 co-prime. p x 21 Thm: If p be a prime number and a is an integer > p such that p is a divisor of a then g.c.2 (a,b)= b. Thm; If p be a prime number and p) ab. then either bla or blb. Proof! If pla, then the thm is done If $p \times a$. then $g \in A = (f, a) = 1$. Since, g.c. 2 of (1, p) = 1., 7 m and v such that an t p V = 1.

=> b(an+pv) = b.

Lecture_19 Page 4

 $\Rightarrow \begin{pmatrix} ab \end{pmatrix} + \begin{pmatrix} bb \end{pmatrix} = b.$ Now, plab and plpb >> pdivides => p | (ab) M + (bb) V. P Cy p | b PROVED ! Corrollary: If p be a prime and p/22...an Jan plak for some K where 1 & K & n. Examples:-1. P. T for n)3, the integer cannot be all primes. n, n+2, n+9 => 4,4+2,4+9 = (4,6,8) 5, 5+2, 5+4 = 5, 7, 5) non-prime Any positive integer n is one of the forems $3k \cdot 3k + 1 \cdot 3k + 2$

Lecture 19 Page 5

of the forms 3k, 3k+1, 3k+2, $k \in \mathbb{Z}^{+}$ 2f n = 3k, n = not prime. $1 = n + 2 = 3k + 1 + 2 = 3(k + 1) \neq prime$. $1 = n + 4 = 3k + 2 + 4 = 3(k + 2) \neq prime$. 1 = not primes. 1 = not primes. 1 = not primes. 1 = not primes. 1 = not primes.

#IND p is a positive integer and p, 2p+1,
4p+1 are primes. Find p.

3K, 3K+1, 3K+2

b= 3K+2.

 $= \frac{2(3k+2)+1}{6k+4} = \frac{2(3k+2)+1}{6k+4}$

= 6K+5 G So prime.

Cheek !

Check!