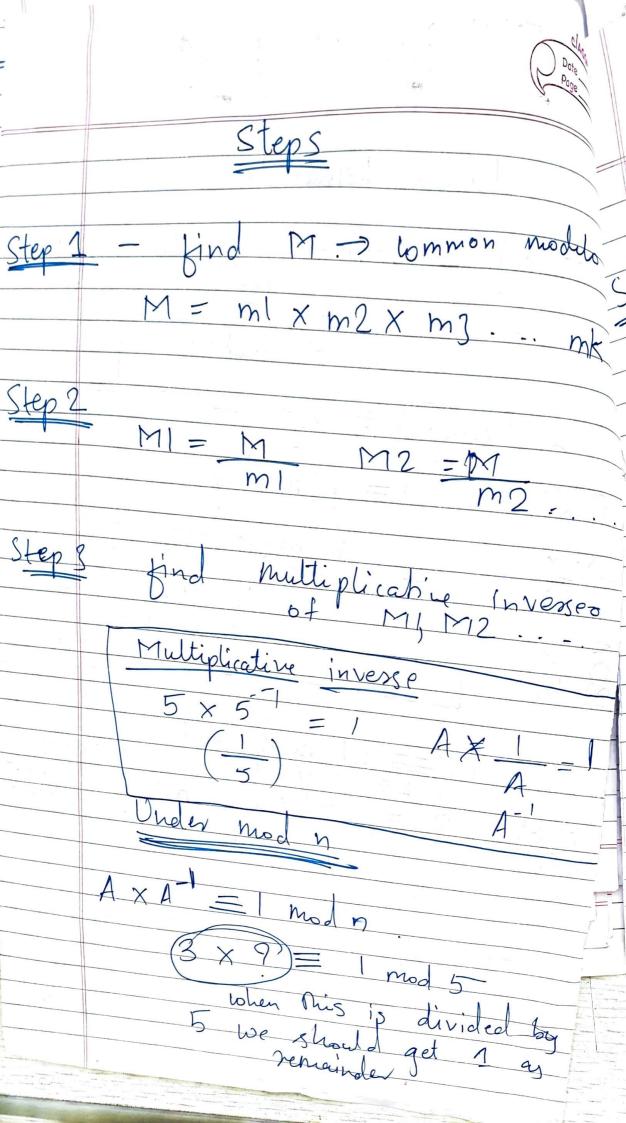
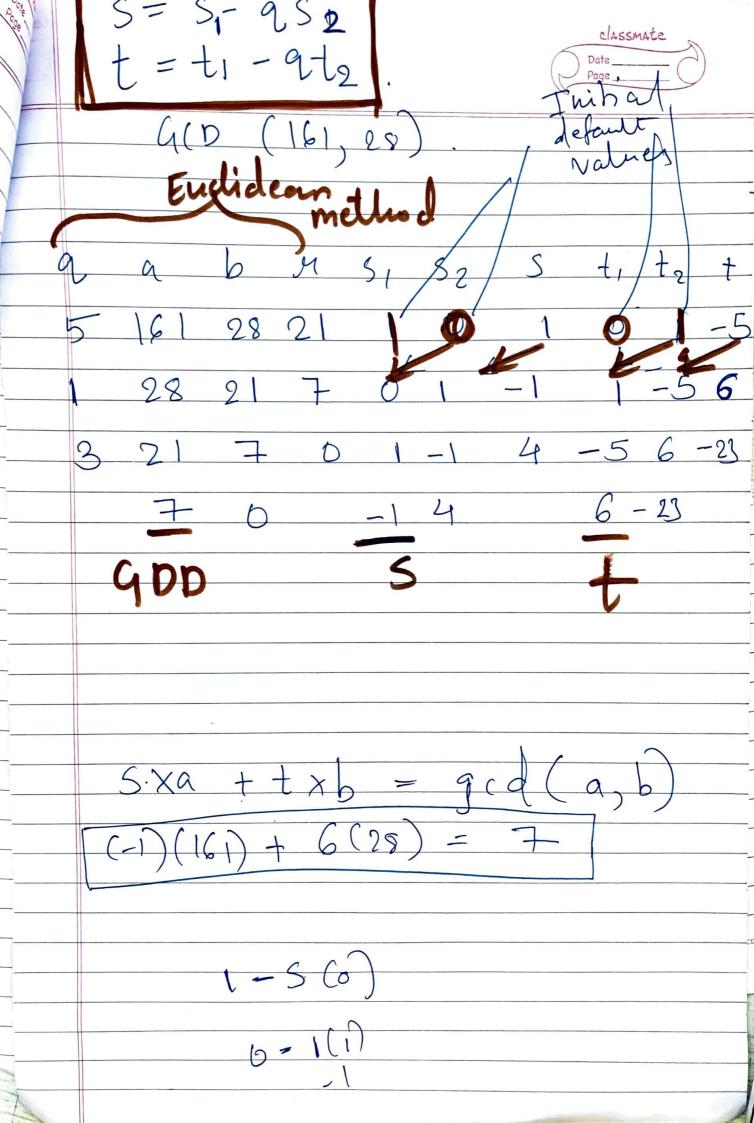
IS Pradical 1 Date Page Chinese Remainder Theorem -> solve bongruent equation (set of) withe one variable but different modulus which are relatively prince. Longruent egn a = b (mod m) a d b are wongreent modulo m $\rightarrow X$ Same remainder by m nou abou egt > urique solution it moduli are relatively prine relatively prime = no hommon factors except ±



6 mod 5 Step 4 Put Values in egh $X = (al \times M \times MI + a2 \times M2 \times M2)$ mod M. Example X = 4 mod 5 X = 6 mod 8 X = 8 mod 9 $\frac{5 \times 9 \times 9}{260}$ 360 M = 360 = = 366 = 45 M3 = 40



IS Practical Bie



RSA Algorithm

200 prime nos p=17

n = P2 = 187

 $\phi(n) = (P-1)(9-1) = 160$

Select c. such that relatively prime to $\phi(n)$ A less than $\phi(n)$ $(\phi_n, e) = e = 7$. g(d)

n 2 2 + t1 t2

	classmat	e
	Date	=
	William St.	
\sim	Eh "	
6)	E C C C C C C C C C C C C C C C C C C C	
,/	2 h 2 1	
	C= Memd n	
		-
7	Da h	
)		
	M = Cd mod n.	
		7
		1.7
7		
-1,		
\	T. J. va. 1. 18 d	
		_
	4	