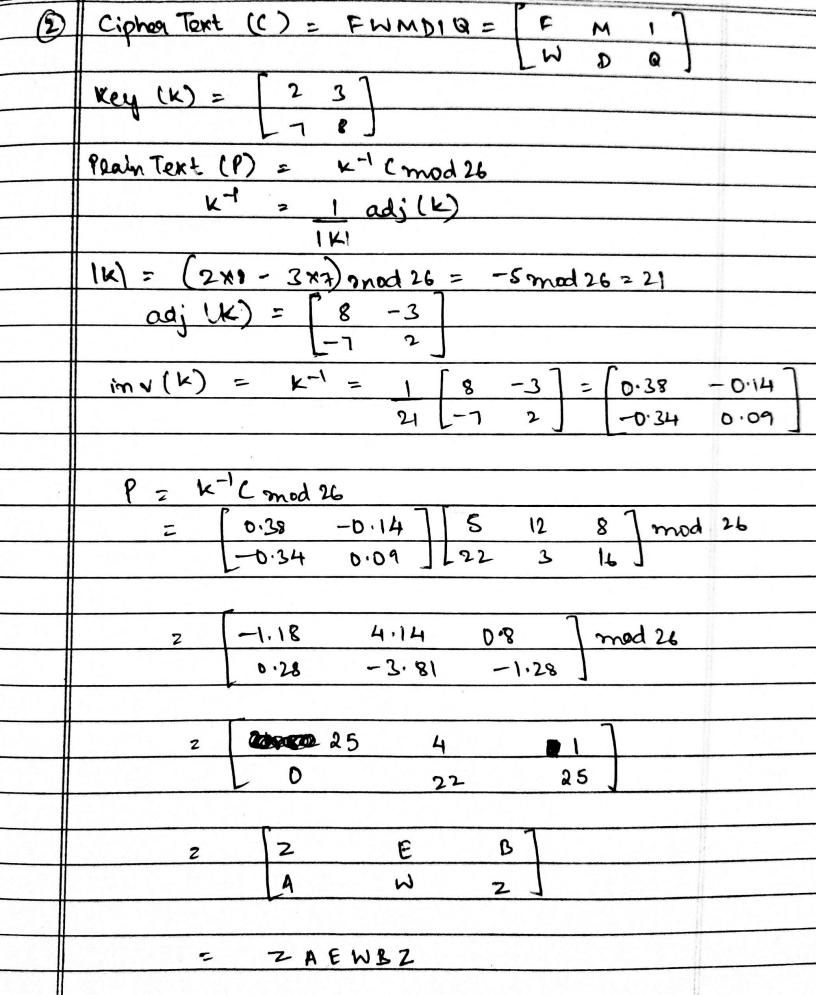
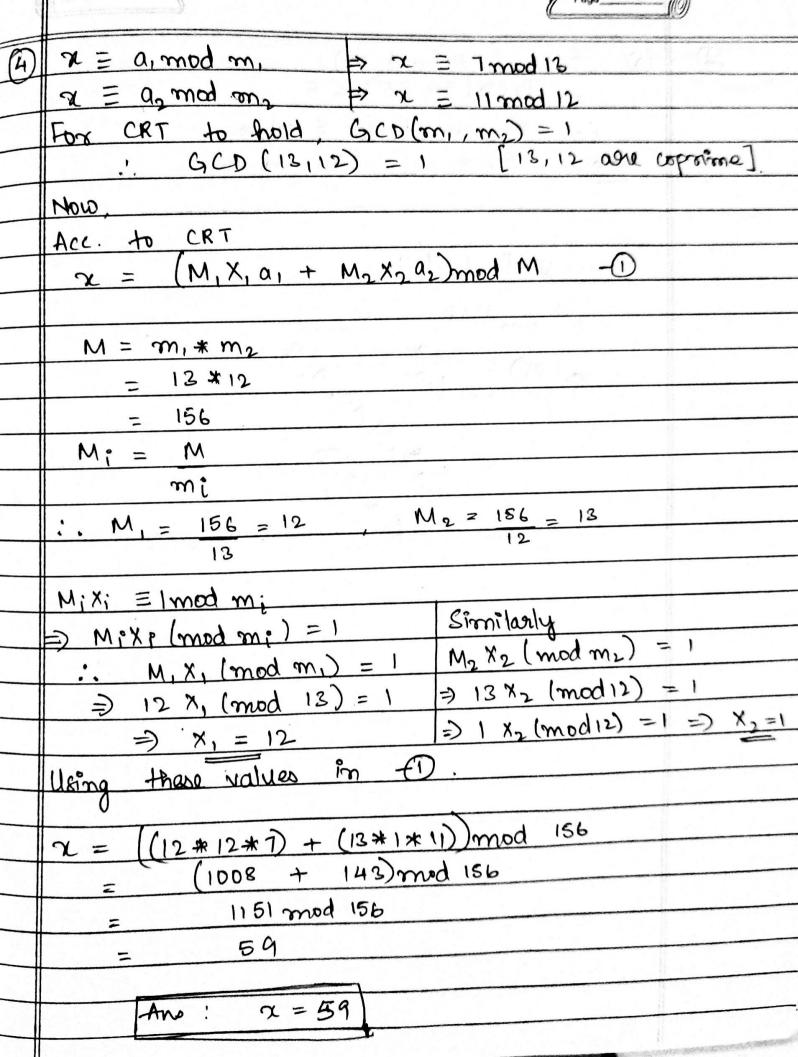
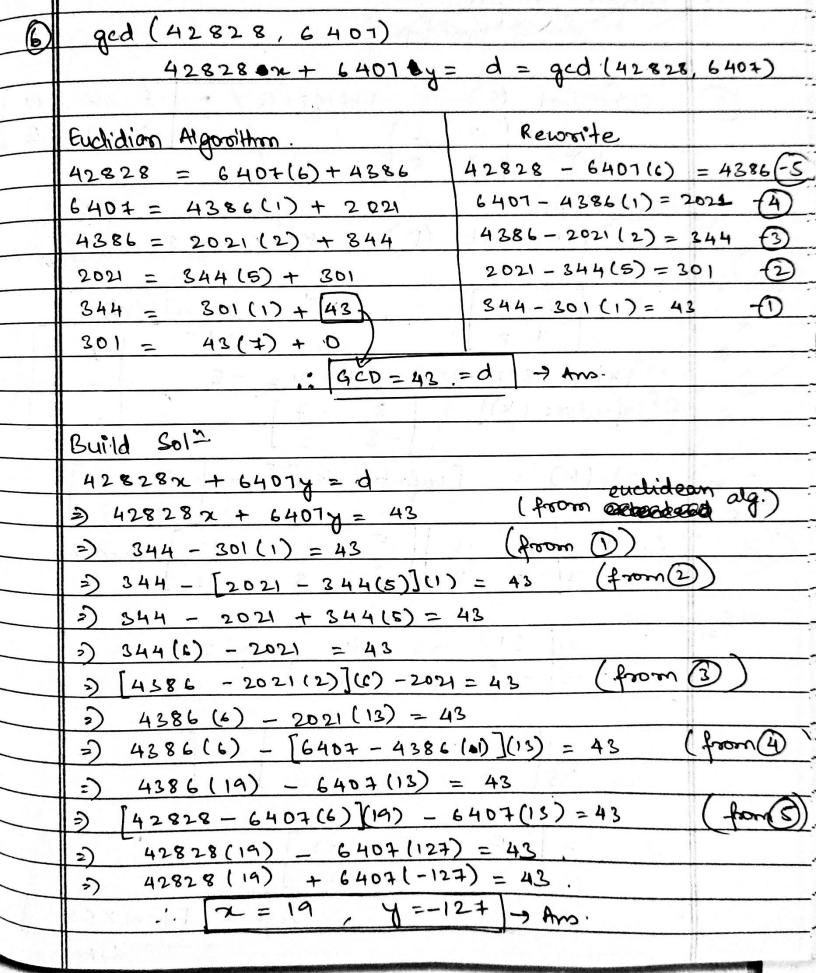
1	and C	(6)) Duto	2	
	KULVIK SINGH.			
	19BCE2074			
	n = 561			
(I)	90 = 561	11. 1		
	Acc. to Miller Rabin Algorithm.			
	m-1 = 5C1 - 1 (32872) p	2	560	
	= 56000	2	280	
	560 = m + 2K	2	140	
	= 35 * 2	2	70 35	
	K = 4, m = 35,			
	Random Ponteger a, (1Kakm-1 => 1Kak 560)			
det a = 2.			1.7	
	Check: am mod n = 1 = (a)			
LHS = 25 mod 561 (x2 16 6 6)				
	$= 2 \cdot (2^{17})^2 \mod 56$			
	= a (131072) 2 mod s61	- Lue	ing calculator]	
= 2(20) mod S612/2002 [1				
	= a. 400 mod 561			
	= 21.802 mod SG1 14 00 11 00			
	= 239 + 1			
	:. Check: $(a^{m})^{2} \mod 88 = n - 1$ LHS: $= (2^{35})^{2} \mod 561$ $= a^{35} \times 2^{35} \mod 561$ $= (239 \times 239) \mod 561$ $= 57121 \mod 561$			
	= 460 + 20-1		Company of the Compan	
	50)			
	:. 561 is COMPOSITE			

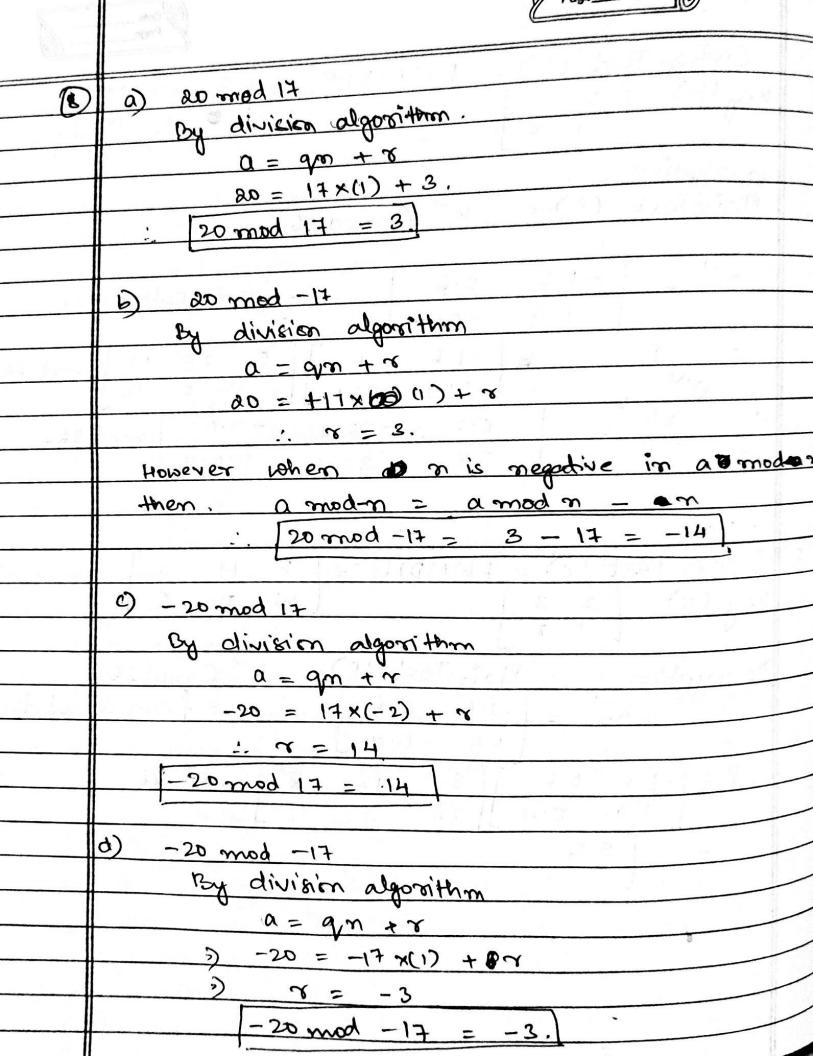


2x" = 22 mod 19 13 $22 \mod 19 = 3$ 22" = logarithm both sides
logar' = 1 log 2
2 11 kg x = 0.4771 - 0.3010 = 0.1761 0.1761 = 0.0160 0.0160 10 n = 1.0375





55x = 35 mod 75 Acd (55, 75) = 15. 25 = 500 5 x1 552 = 35 mod 75 112 = 7 mad 15 - n = 13 mod 15 2 = 2 mod 15 9 = 2, 17, 32, 47, 62 (mod 75) 422 = 12 (mod 90) gcd (42,90) = 6. 422 = 12 mod 90 72 = 2 mod 15 -14x = -4 mod 15 ·2 = 11 mod 15 2 = 11, 26, 41, 56, 71, 86 (mod 90)



According to Fermat's Theorem. 9 $= a \pmod{p}$ $a = 9 \pmod{73}$ 73 is prime, we want to break up the exponent 794 Porto a form of 739 + 8 794 = 73 * 10 + 64So, (73*10+64) a = 9 (mod 13) $= (9^{10})(9^{64})(mod 13)$ $= 9^{10}(9^{64})(mod 13)$ $= 9^{10}(9^{64})(mod 13)$ $= 9^{10}(mod 13)$ $= 9^{10}(mod 13)$ $= 9^{10}(mod 13)$ = 9 * 9 mod 73 = 81 mod 73 a = 8 mod 73. Hena

