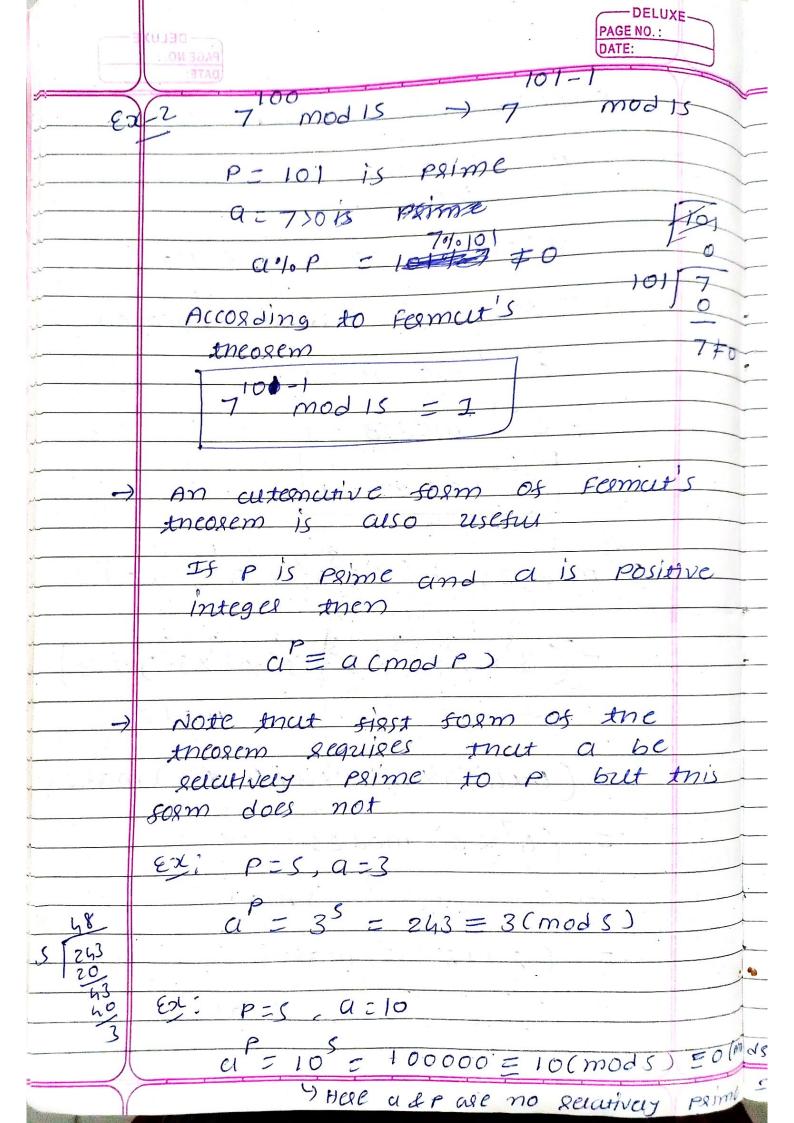


suppose a=3, P=23 P = 23 Prime a = 3 > 0a 1.0 = 3 % 23 = 3 #0 according to feamut's theosem a mod P =) mod 28 = 1 3 mod 23 = 1 3 mod 23 = ((3) × 3) mod 23 =[(3³×3³×3³×3³×3³×3³)×3 mod 23. = (4x4x4x4x4x4x4x4x3) mod 23 = (47 x 3) mod 23 = (43×43×4×3) mod 23 (18 × 18 × 12) mod 23 (32×2×32×2×12) mod 23 (12×2) mod 23 24 mod 23 = 1



DELUXE.

Eruci's Theorem Eucl's theosem states that sox every a en that are relatively prime $a^{(n)} = I(modn) = a^{(n)}$ 100 7 mod 15 a=7, n=15 that are relatively Prime so, apply eures's theosem $\phi(n) = \phi(1s)$ ф(3)× ф (3XS) = \$\phi(3) \times \phi(5) = 2×4 \$(15) Z 8 According ewer's theosem 78 mod15 = 1 Note: -5 (atb) modn

K

= (amodn + 6 modn) modn

