

Page No. M. x = 1 mod m, -> 20x, = 1 mod 3 20x2 = 40 40 +13 = 39 remainder =1 12 2 1.5=1 -> 2 = 3 n = (M, n, a, + M, & 2 a 2 + M 3 a 3 & 3) mod M = [(20×24/1×2)+(15×3×3)+(12×3×1)] mod 60 $\alpha = 1 \mod 5$, $x = 1 \mod 7$, $x = 3 \mod 1$

M2 = 385/7 = 55 M3 = 385/11 = 35 M, x, = 1 mod 5 -> 17 x, = 1 mod 5

= 251 mod 60 = 11

77 7, 9.5 5 1 -> 7, 53

M, n2 = 1 mod 7 -> 55 %. 7 a2 = 1 -> n2 = 6 M3 82 = 3 mod 11 -> 35 % 11 2 = 3 -> 2 = 6 X,=3 x2=6=x3

x, 5 2

M2 x, = 1 mod 4

15×2 1.4=1 -> x2=3

M=m, xm, + m2 = 385

MM, = M = 385 = 77

M3 x3 = Imod5

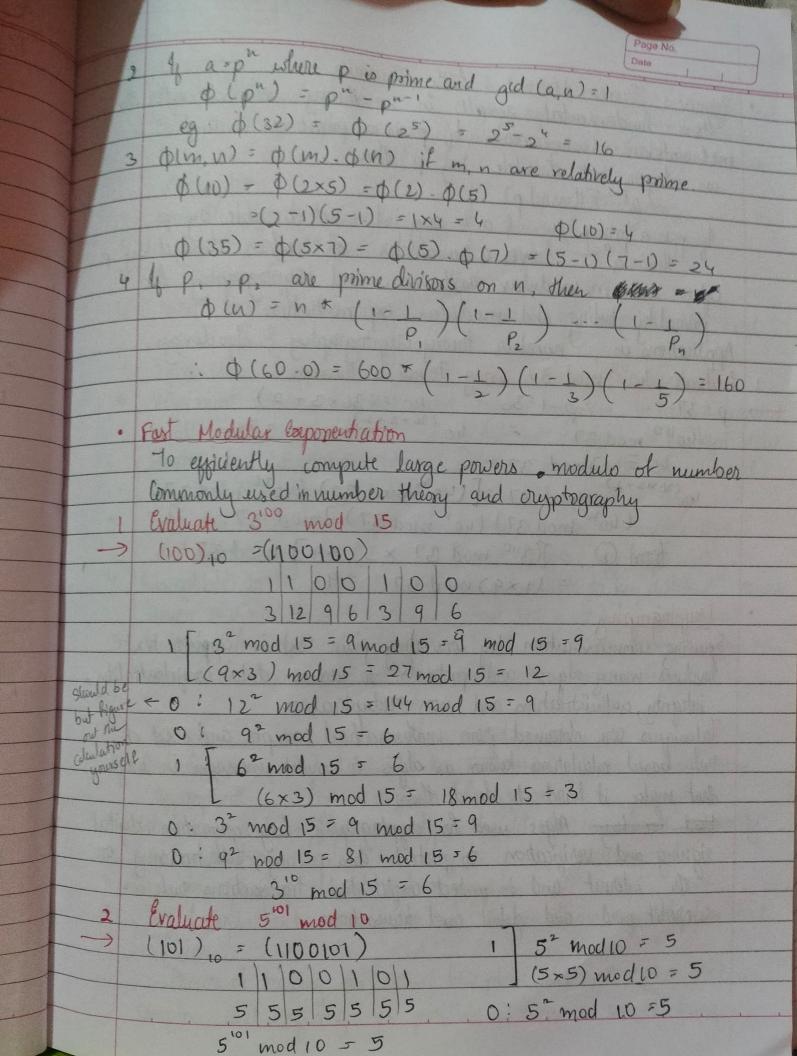
Dl = [77×3×1+ 55×6×1+35×6×3] a mod 385 = 1191 mod 385 = 36

Euler's Tokient Function

O(n) = \{n\ | 1 \le n < n\ \}, \gcd (x; ,n) = 1

eg N = 10 p(n) = 21,3,07,93 → gcd =1

O(p)= p-1 if p is prime eg. 0(2) = 2-1=1= {1} \$ (41) = 41-1= 40



Page No Fermat's Thorem / Fermat's Little Theorem Its a hundamental result in no theory, named after the mathematician (who caves). It p is a prime up, and a an integer not divisible by p, then: Jap-1 = (Lonodp) opten used in modular asithmetic and cryptography for primality testing and modular exponentiation Applications in number theory, etyptography & algoderican fundable 40"0 mod 37 wring Fermat's theorem

p = 37

i.p -1=36

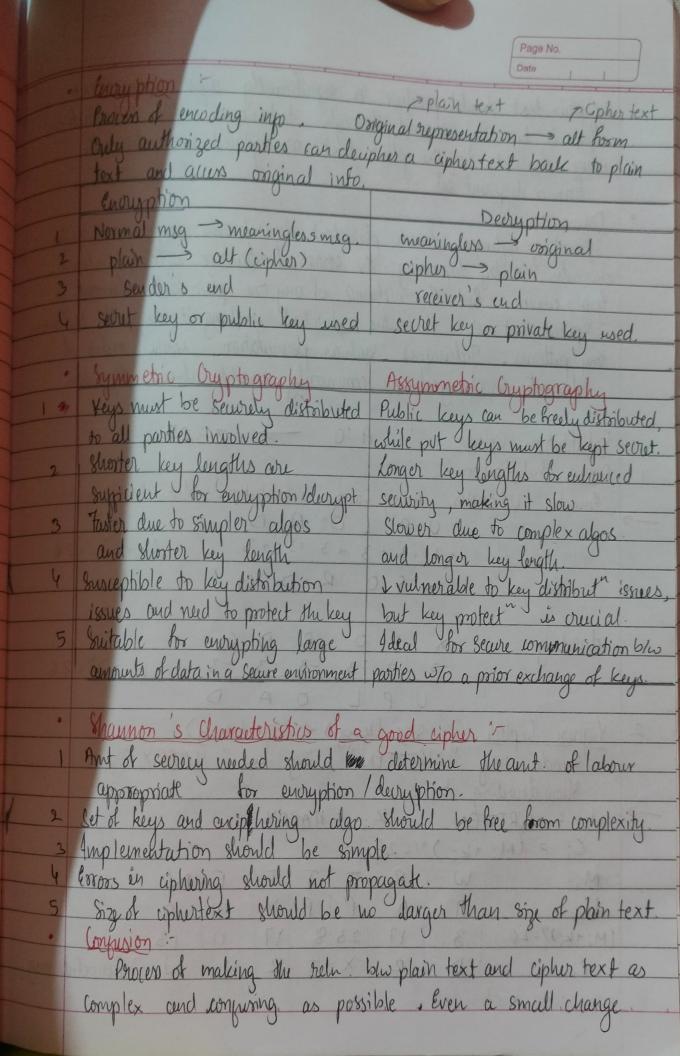
lip = (36 × 3 + 2)

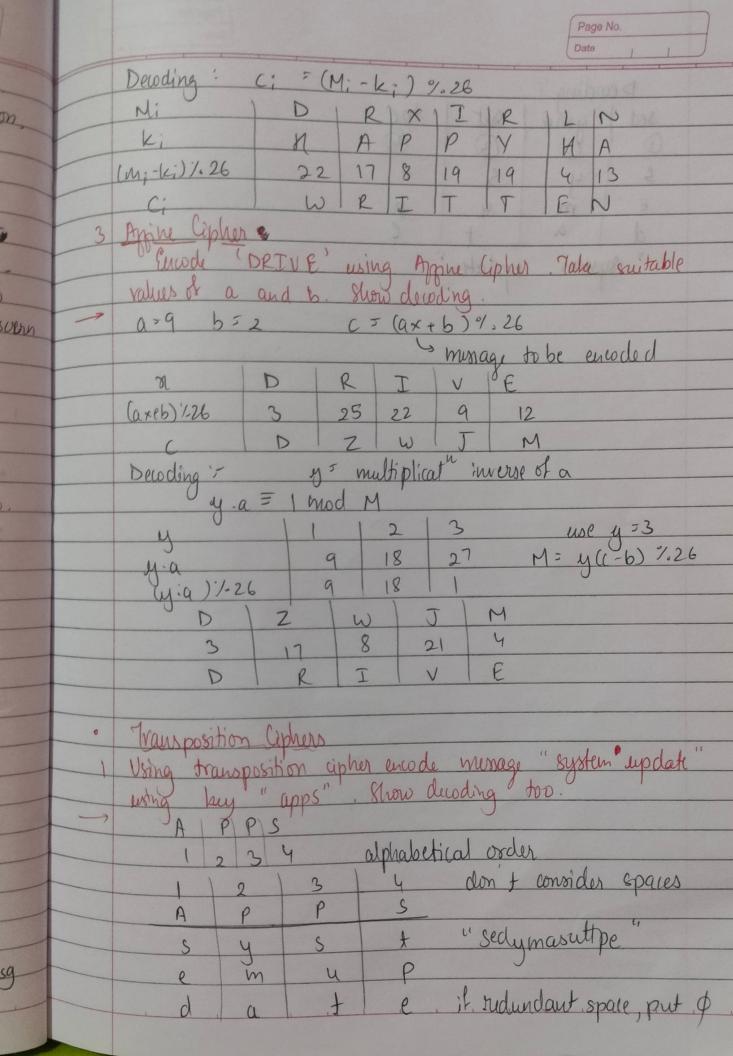
40 = 3 mod 37 = 40 (36 × 3 + 2)

40 = 3 mod 37 = (40 % mod 37) (40 % mod 37)

(40 % mod 37) (40 % mod 37) (40 % mod 37)

(40 % mod 37) (40 % mod 37) J mod 37 from (), [(3110 mod 37 x3) x9] mod 37 = (1x9) mod 37 = 9 Securing communication by converting plain text in cippher text had ves many algos and protocols to ensure data confidentiality. integrity, authentication and non reduplication. Techniques we obtained from mathematical concepts and a set of rule based calculations known as algos to convert messages in ways that make it hard to decode them. signing and verification to protect data privally, web browsing on the internet and to protect confidential transactions such as credit card and delsit card transactions





Decoding " sed 13 endate