

Tutorial 3

Or Find the value of $\phi(29)$, $\phi(80)$, $\phi(100)$

Theorem. $X = 2 \mod 7$, and $X = 3 \mod 9$ $X = 4 \mod 5$, and $X = 10 \mod 11$

O3 find the nesults of the following, using fearmat's little theorem.

5-1 mod 13

to a primary from

 $\phi(29) = (29-1) = 28$

\$\phi(80) = \phi(2 \times 40)

 $= \phi(2 \times 2 \times 20)$ $= \phi(2 \times 2 \times 20)$

= \$\phi(2x3x2x10)

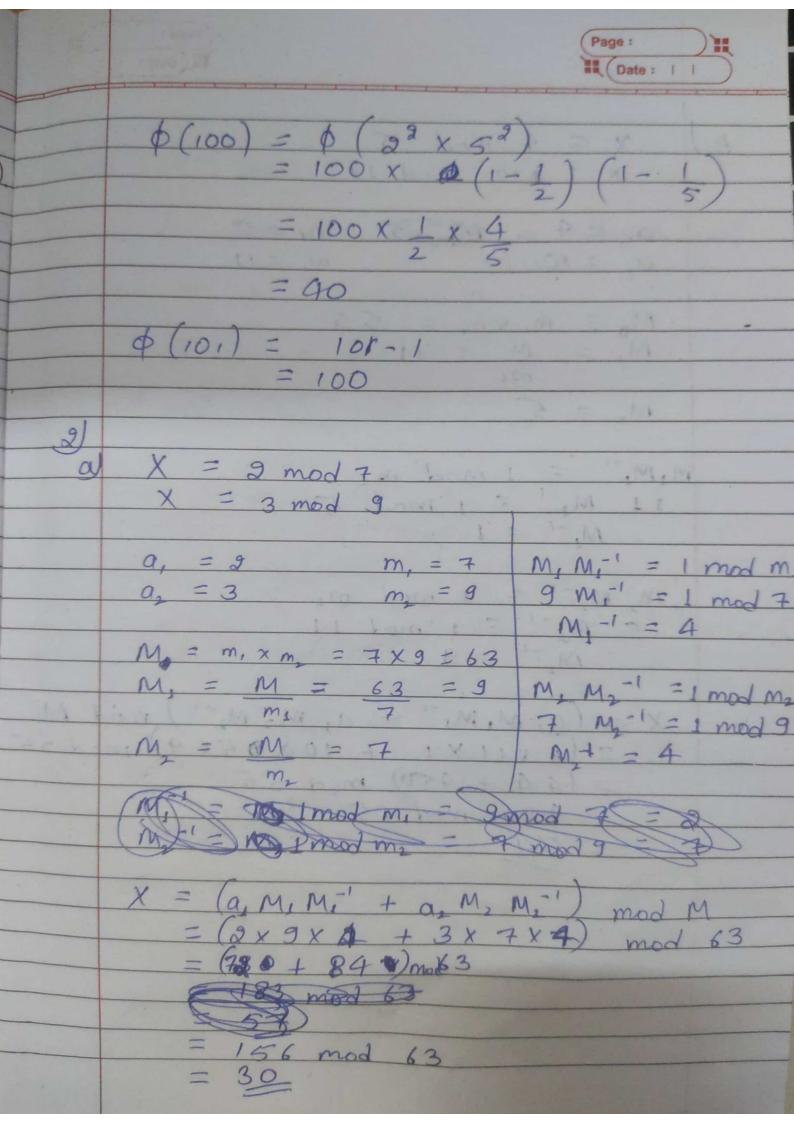
 $=\phi(16\times5)=\phi(2^4\times5^1)$

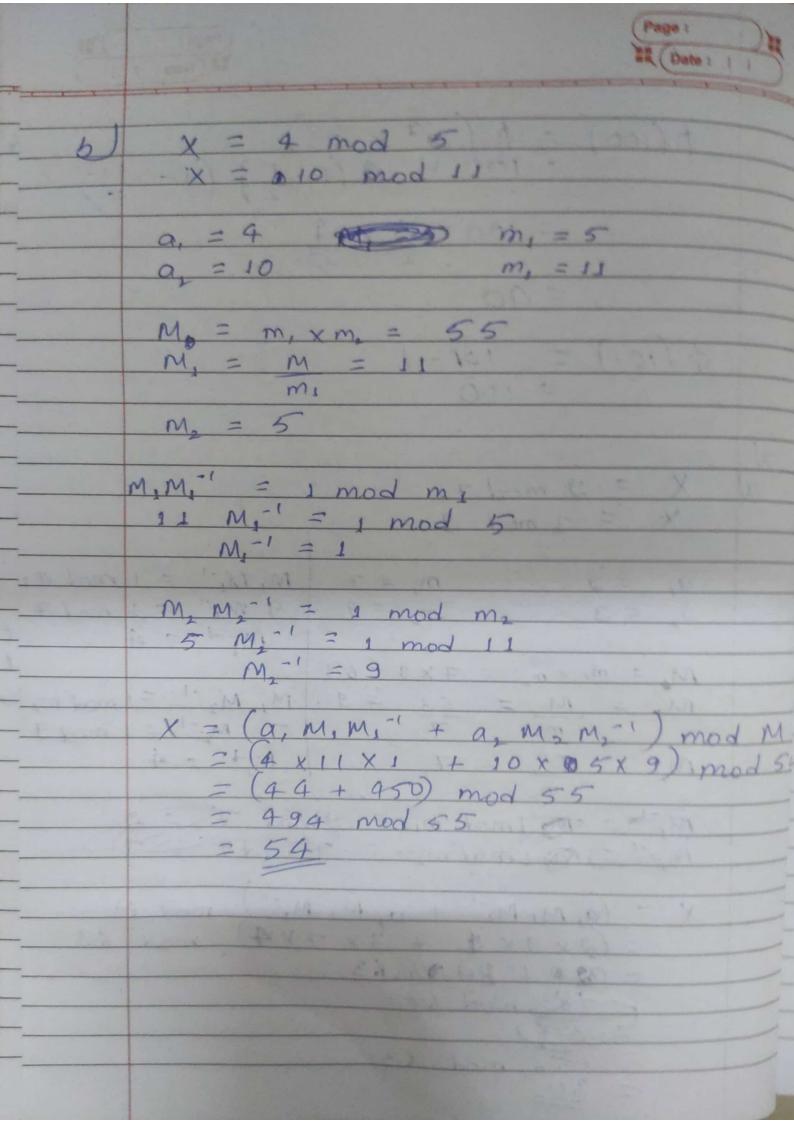
80 X 19 X 4

 $= 0.80 \times (1-\frac{1}{2})(1-\frac{1}{5})$

= 80 x 1 x 4

3 3 %





5-1 mad 13 b = prime, a = + ve integer not divisible by b ab -1 = 1 mod p a=5 p-1= a^{-1} mod $p = a^{p-2}$ mod p $= 5^{13-2} \mod 13$ $= 5^{11} \mod 13$ $= 5 \times 5^{10} \mod 13$ $= 5 \times 25^{5} \mod 13$ = $5 \times (26-1)^{5} \mod 13$ = $5 \times (26-1)^{5} \mod 13$ = $6 \times 5 \times 5 \times (26^{5}(-1)^{6} + 5 \times (26^{4}(-1)^{5})$ + ... $5 \times (26^{5}(-1)^{6}) \times (-1)^{5}$ mod 13 CORDE = [13 I + 5x(-1) 5] mod 13 (13I - 5) mod 13 $\begin{array}{rcl}
15^{-1} & \text{mod } & 17 \\
a^{-1} & \text{mod } & p = a^{p-2} & \text{mod } & p \\
& = 15^{17-2} & \text{mod } & 17 \\
& = 15^{15} & \text{mod } & 17 \\
& = (-2)^{15} & \text{mod } & 17 \\
& = (-2) & (2^4)^3 \times 2^2 & \text{mod } & 17
\end{array}$