Class 13

Friday, August 19, 2022 10:09 PM

$gcd(a_i, x) == 1$

$x = 2 \longrightarrow$ 3

1 2 3 4

2 2 2 2

$n - c$

2 3 4 6 7

2 3 2 2,3 7

$c(2) = 7$ $c(3) = 5$ $c(6) = 2$

$x = 12 \longrightarrow 2, 3$

gcd (

$n(A \cup B \cup C) = n(\overline{A}) + n(\overline{B}) +$

$n(\overline{A \cap B})$ $n(\overline{A \cap C})$

3
2-1

$+ n(\overline{A \cap B \cap C})$

2, 3, 7

$+c(2)$ $-c(2\cdot3$

$+c(3)$ $-c(2\cdot$

$+c(7)$ $-c(3$

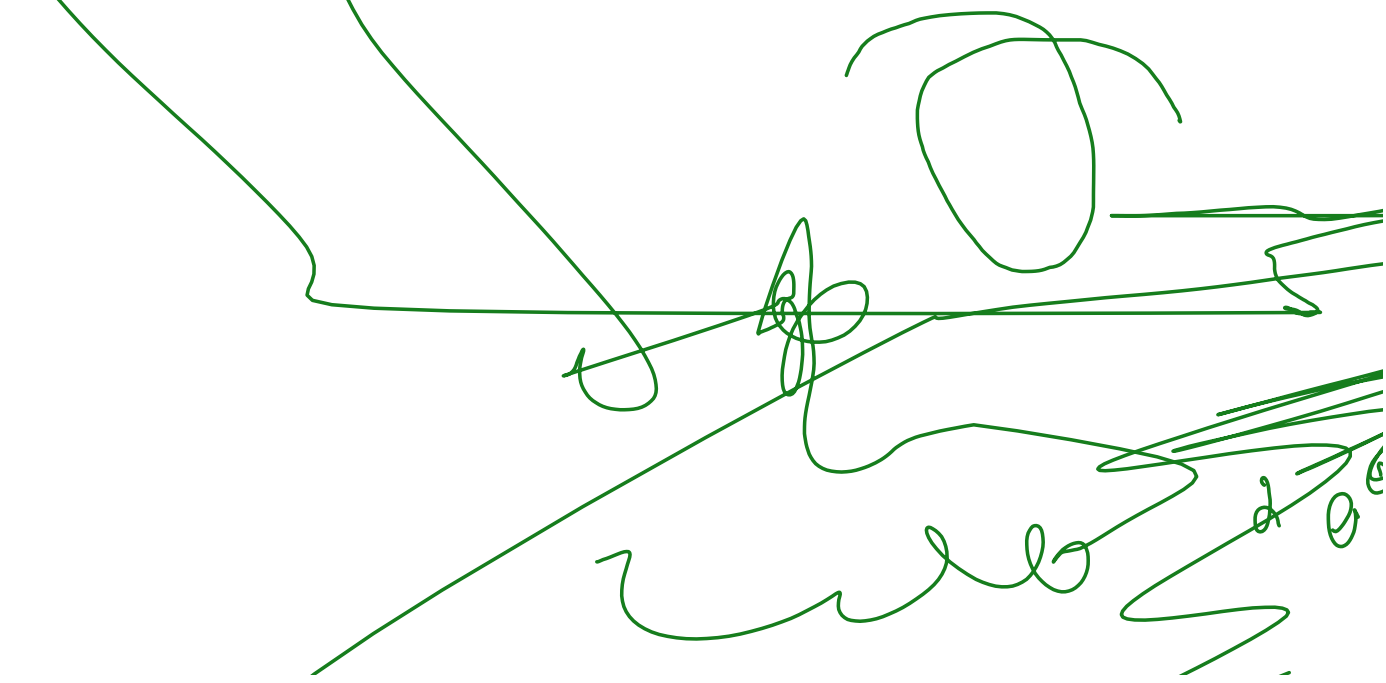
Sieve ✓

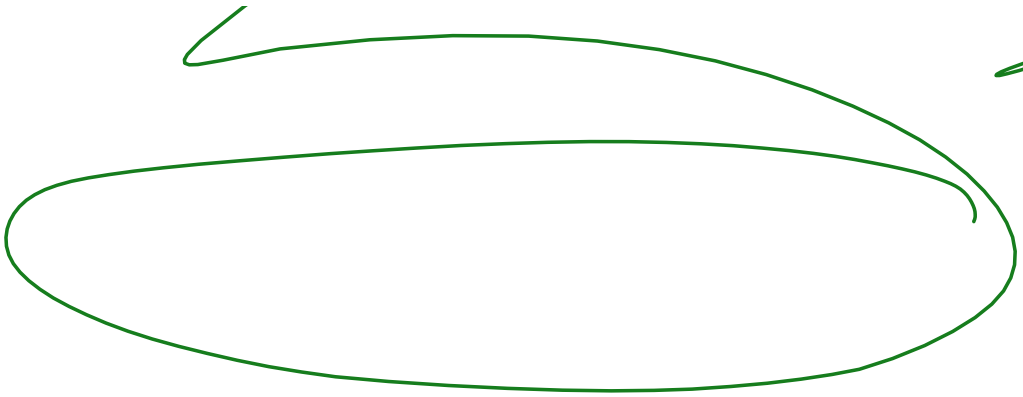
factoring ✓

IEP X

Observation + analysis X

n.





$12^2 = 144$

$12 \rightarrow (2^2 \times 3)$

Modular Arithmetic

$(a \pm b)\%M = ((a\%$

$(a * b)\%M = ((a\%$

$(7\%$

$a - b < 0$

$(2$

$(4+7k)\%7 = 4$

$(4\%7) + (7k\%7)$

$7($

$7($

$(a/b)\%M = (a \times$

$= (a$

b^{M-2}

$= ((a\%$

$b^{-1} \% M \longrightarrow$ Mod

$b < M$ gcd

M यदि prime

Fermat's Theorem

$a^{p-1} \% p$

$2 \cdot 3^{3} \cdot 5^{1} \cdot 7^{1} \cdot 11^{1}$

$2^{4} \% 5$

$b^{p-1} \%$

Congruence

Corollary:

$b^{p-1} \equiv 1 \pmod{p}$

$\cdot\ b^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow b^{-1} \cdot b^{p-1} \equiv b^{-1} \pmod{p}$

$\Rightarrow b^{p-2} \equiv b^{-1} \pmod{p}$