1. Prime
2. Relative prime number

$gcd = (1)$

3. congruent

a module b = remainder.

if a mod n = b mod n

$\Downarrow$

$a \equiv b \bmod n$

a mod n = b

n is multiple (a - b) whereas at least one of them should be primono

40 - 6 = 34

40 mod 17 6 mod 34

= 6 6

a - b

40 - 11 = 29

a b

40 mod 29 11 mod 29

11 11

13 - 11 = 2

13 md 2 11 md 2

1 1

doubt

Fermat's Theorem

+ no. a
Prime p

where as a is not divisible by p

Proof $P = \{1, 2, \ldots, P-1\}$

$X = \{a \bmod P,\ 2a \bmod P \ldots a(P-1) \bmod P\}$

$\{1, 2 \ldots P-1\}(\bmod p \equiv \{a, 2a \ldots (P-1)\} \bmod P$

$(P-1)! \bmod p = \{a \ldots (P-1)\} \bmod P$

$(P-1)! \bmod \cancel{\bmod p} = a^{P-1} \cdot (P-1)!$

(1) $a^{P-1} = 1 \bmod p$

$a^{P} = a (\bmod p)$

$5^{18} \bmod 19$

$5^{19-1} \bmod 19$

As $A^{P-1} = 1 \bmod$

$15^{19-1} \bmod 19 = 1$ Ans

(2) $\cancel{19}$ $5^{19} \bmod 19$

$a^{p} \bmod 19 = a \bmod p$

$5^{19} \bmod 19 \rightarrow 5 \bmod 19$

5 Ans

(3) $5^{20} \bmod 19$ $(a \cdot b) \cdot C$

$5^{19+1} \bmod 19$ $a \cdot c$ $b \cdot c$

$5^{19} \cdot 5^{1} \bmod 19$

$5 \cdot 5 \bmod 19$

$25 \bmod 19$

6 Ans

$\Rightarrow a = 7, \ p = 19$

$a^{p-1} \bmod 19 = 1$

$7^{18} \bmod 19 \rightarrow 1$

7^{19-1}

$7^{19-1} \bmod 19 = 1$

x^{26} mod 19

Euler's theorem

if $\phi(n)$ if n is prime no

$n-1$ Ans

if $\phi(n)$ P & Q are multiple of n

$\phi(P-1) \cdot \phi(q-1)$

$\phi(5)$

Ans = 4

$\phi(32)$

$\phi(8-1)(4-1)$

$\phi(7 \times 3)$

21

Proof

$$\prod_{i=1}^{\phi n} (a x_1 \bmod n) = \prod_{i=1}^{\phi n} x_1$$

$$\prod_{i=1}^{\phi n} a x_i \equiv \prod_{i=1}^{\phi n} x_1 \bmod n$$

$$a^{\phi(n)} \left[\prod_{i=1}^{\phi n} x_i \right] = \prod_{i=1}^{\phi n} x_1 \bmod n$$

$$\boxed{a^{\phi(n)} = 1 \bmod n}$$

$$3^{\phi(10)}$$

$$3^{4} = 1 \bmod 10$$

$81 \bmod 10 = 1$