Number - Theory

CHAPTER - FIVE (5)

Fermat's Factorization method -

Let n be any odd positve integer which is the differena of squire of two integers

ie $n = x^2 - y^2$

$= (x+y)(x-y)$

If $n = ab$, $a \geq b \geq 1$ then

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

we have a and b odd integers and consequently $\left(\frac{a+b}{2}\right)$ and $\left(\frac{a-b}{2}\right)$ will be non-negative integers

and $n = x^2 - y^2$

$x^2 - n = y^2$

for this we observe number

$k^2 - n$, $(k+1)^2 - n$, $(k+2)^2 - n$. -- --

Ex Show that $5^{38} \equiv 4 \pmod{11}$

Sol^{n} Since 11 is a prime and $(5, 11) = 1$

We have

$$5^{11} \equiv 5 \pmod{11}$$

$$5^{33} \equiv 5^{3} \pmod{11}$$

Now

$$5^{38} \times 5^{5} \equiv 5^{3} \times 5^{5} \pmod{11}$$

$$5^{38} \equiv 5^{8} \pmod{11}$$

$$= (5^{4})^{4} \pmod{11}$$

$$= (3^{4}) \pmod{11}$$

$$\equiv 81 \pmod{11}$$

$$\equiv 4 \pmod{11}$$

ABSOLUTE PSEUDO PRIMES →

A composite nomber n is called an absolute pseudo primes. If

$a^{n} \equiv a \pmod{n}$ for all integer a

The least absolute pseudo prime is 561