Ittate Jahan Nilima
ID: IT-21063

Fermat's Little Theorem

Proof:

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod p$. Furtheremorre, for every integer a we have,

$a^p \equiv a \pmod p$

Fermat's Little thorem is useful in computing the remainderes modulo p of large powers of integers.

Example:

Find $7^{222} \bmod 11$

By Fermat's Little theorem, we know that

$7^{11-1} \equiv 1 \pmod{11}$

and $7^{10} \equiv 1 \pmod{11}$ and so,

$7^{10} \equiv 1 \pmod{11}$

for every positive integer k therefore,

$7^{222} = 7^{22 \cdot 10 + 2}$

$= (7^{10})^{22} \cdot 7^2 = 1^{22} \cdot 49 \equiv 5 \pmod{11}$

So, $7^{222} \bmod 11 = 5$

- Does Fermat's theorem hold the true for $p=5$ and $a=2$?

$\rightarrow$ Given,

$p=5$, $a=2$

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

Or $2^{5-1} \equiv 1 \bmod 5$

Or $16 \equiv 1 \bmod 5$

Example:

$11^{13-1} \equiv 1 \pmod{13}$

$11^{12} \equiv 1 \bmod 13$

$-2^{12} \equiv 1 \bmod 13$

$-2^{4\times3} \equiv 1 \bmod 13$

$3^{3} \equiv 1 \bmod 13$

$27 \equiv 1 \bmod 13$

- Find an inverse of 101 modulo 4620

→ First have to use Euclidian algorithm to show that $gcd(101, 4620) = 1$

$4620 = 45 \times 10 + 15$

$\Rightarrow 101 = 1 \times 75 + 26$

$\Rightarrow 75 = 2 \times 26 + 23$

$\Rightarrow 26 = 1 \times 23 + 3$

$\Rightarrow 23 = 7 \times 3 + 2$

$\Rightarrow 3 = 1 \times 2 + 1$

$\Rightarrow 2 = 2 \times 1$

$gcd(101, 4260) = 1$

<u>Bezout's Theorem:</u>

<u>Lemma</u>: If a, b, c are positive integers such that $gcd(a, b) = 1$ and a / bc then $a | c$

Proof

Assume $\gcd(a,b) = 1$ and $a \mid bc$

- Since $\gcd(a,b) = 1$ by Bezout's theorem there are integers s and t such that $sa + tb = 1$
- Multiplying both sides of the equation by c yields $sac + tbc = c$
- We conclude $a \mid c$, since $sac + tbc = c$