Khadija Arefn Meen

ID: IT21059

Formstis Little Theore

Fermal's little Theorem:

If P is prime and a is an integer not divisible by P, then $a = 1 \pmod{P}$

Furthormore, for every integer a we have, $a^p = a \pmod{p}$

foremat's Little theorem is useful in computing the remaindows modulo P of large powers of integers.

Example

Find 7²²² mod 11

By fermat's little theoriem, we know thation $7''-1' = 1 \pmod{11}$

and 710 = 1 (mod 11) and 50,

(7") = 1 (mod 11)

fore every positive integer in thore-force; 7222 = 722.10+2 $=(7)^{2^2}$ $7^2=1^{2^2}$. $49 \equiv 5 \pmod{7}$ Hence, 7222 mod 1175 Does formal's theorem hold time for. P=5 and a=2? Given, 2 1 1 P=5, a=2 il bow a = 1 (mod P) orest25-10=4 modossont ettil étomos or 16 = 1 mod 5 (11 bon)

S CamScanner

Elample!-113-1 = 1 (mod 13) -2 = 1 mod 13 = 2 and 13 = 1 mod 13 = (d, n) bogg some 1 $3^{3} = 1 \mod 13$ $27 = 1 \mod 13$ $2 \approx 1000 \mod 13$ Find an inverse of 101 modulo 4620. Solictions out to abie Alad Michigania -that ged (101, 4620) = 410 shows on. 4620 = 45×101+45 -> 101 = 1×75 + 26 $\Rightarrow 75 = 2 \times 26 + 23$ =) 26 = 1×23+3 923 = 4x3 + 27321X2+1 9 = 2.1

first have to use Euclidian todgorithmito show ged (101, 4260) = 1

Bezout's theorem:

Lemma: II a,b,c are positive integers such that gcd (a,b)=1 and alber then ale

P1700]:

Assume gcd(9,b)=1 and albc

· since gcd (a,b) = 1, by Bezout's theorem there are integers 3 and + such that

ossisatibora 101 to soomi us bridge

· Multiplying both sides of the equation by continued to sides of the

· we conclude are; since sagt the = c

1 - (00 1 - 101) 1099

24-4101X211-C2: 38467