FERMAT'S THEOREM

Fermat's theorem states the following: if *p* is a prime and *a* is a positive integer not divisible by *p*, then

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

Consider the set of positive integers less than *p:*{1,2,3..p-1}

Multiply each element by *a modulo p* to get the set

X ={ a mod p,2a mod p….(p-1)mod p}.

None of the elements of X is equal to zero because *p* does not divide *a*. No two of the integers in X are equal.(p-1) elements of X are all positive integers with no two elements are equal. Multiplying the numbers in both sets and taking the result mod *p* yields.

$$a * 2a * \ldots *(p-1)a \equiv [(1*2* \ldots *(p-1)](\bmod p)$$

$$\{1 * 2 * \ldots *(p-1)\}\ a^{p-1} \equiv [(1*2* \ldots *(p-1)](\bmod p)$$

$$(p-1)!\ a^{p-1} \equiv (p-1)!(\bmod p)$$

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

Example

a = 7, *p* = 19

7^2 = 49≡ 11 (mod 19)

7^4 = 121 ≡ 7 (mod 19)

7^8≡ 49 ≡ 11 (mod 19)

7^{16}≡ 121 K 7 (mod 19)

$a^{p-1} = 7^{18} = 7^{16} * 7^2 \equiv 7 * 11 \equiv 1$ (mod 19

An alternative form of Fermat's theorem is also useful: If *p* is prime and *a* is a positive integer, then

$$a^p \equiv a(\text{mod } p)$$

Euler's totient function

It is represented as *ø(n)*.Euler's totient function is defined as the number of positive integers less than *n* and relatively prime to *n*. *ø(1)=1*

It should be clear that for a prime number *p*

$$\phi(p)=p-1$$

Suppose that we have two prime numbers *p* and *q*, with *p* not equal to *q*. Then we can show that

$$n=pq.$$

$$\phi(n)= \phi(pq)= \phi(p)* \phi(q)=(p-1)*(q-1)$$

$$\phi(n)=(pq-1)-[(q-1)+(p-1)]$$

$$= pq-(p+q)+1$$

$$=(p-1)*(q-1)$$

$$= \phi(p)* \phi(q)$$

To determine f(35), we list all of the positive integers less than 35 that are relatively prime to it:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18

19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34

There are 24 numbers on the list, so f(35) = 24.

f(21) = f(3) * f(7) = (3 - 1) * (7 - 1) = 2 * 6 = 12