
Wilson’s Theorem

> In number theory, Wilson's theorem states that a natural number $n > 1$ is a prime number if and only if $(n-1)! \equiv -1 \pmod n$.

This asserts that $(n-1)!$ is exactly 1 less than a multiple of n when n is prime.

Elementary Proof

$(n-1)!$ contains product of $[1, 2, \dots n-1]$. Since n is a prime, every element from 1 to $n-1$ has their modular inverse, which is among $[1, 2, \dots n-1]$.

This inverse is unique and each number is inverse of its inverse. But some numbers can be inverse of themselves. In that case:

$$a \times a \equiv 1 \pmod n$$
$$a^2 - 1 \equiv (a-1)(a+1) \equiv 0 \pmod n$$

Hence, $a = 1$ or $a = -1 = n-1$. Therefore, 1 and $n-1$ are the only numbers which are modular inverse of themselves.

So all the numbers from 2 to $n-2$ form pairs whose multiplication modulo n results in 1. So in the end, we are only left with $n-1$, as stated before.

Resource: Art of Problem Solving

Extension

Using Wilson’s Theorem, it can be shown that:

> If N is a composite number (except for 1 and 4), then $(N-1)! \equiv 0 \pmod N$.

This can be proved easily.

Proof

Since N is composite, there must p and q $(p, q > 1)$ for which $N = p \times q$.

Now if $p \neq q$, then $pq|(N-1)!$

If $p = q$, then for $N > 4$, $2p < N$. Thus p^2 is possible in $(N-1)!$. Hence $p^2|(N-1)!$.

Therefore, $(N-1)! \equiv 0(\text{mod N})$, no matter what when N is composite (except for $N = 1$ or $N = 4$)

Problem: CF 278 Div1 C

Gauss's Generalization

For a number M, product of all numbers that are less than M and coprime to it, modulo M is 1 or -1.

$$\prod*{k=1,gcd(k,m)=1}^{m}k \equiv 1 \text{ (mod m) --- if } m = 4, p^a, 2p^a*

prod{k=1,gcd(k,m)=-1}^{m}k \equiv 1 \text{ (mod m) --- otherwise }$$

where p is an odd prime.

Resources: Wiki