Wilson's Theorem

Lemma : (6.2)

$$x^2 \equiv 1 \mod p$$

has exactly 2 solutions, 1 and $p-1$.

Proof. Let r be any solution of $x^2 \equiv 1 \mod p$. Then, it follows that $r^2 - 1 \equiv 0 \mod p$. Thus, by definition of congruence,

$$p \mid \left(r^2 - 1\right) \quad \text{so} \quad p \mid (r-1)(r+1)$$

Hence, $r + 1 \equiv 0 \mod p$, or $r - 1 \equiv 0 \mod p$. Since r is a least residue modulo p, we get that $r = p - 1$ or $r = 1$. □

Definition : Modular Multiplicative Inverse

The modular multiplicative inverse of an integer a is an integer a' such that

$$aa' \equiv 1 \mod m$$

If $(a, p) = 1$, we know that $ax \equiv 1 \mod p$ has exactly one solution. Thus, the inverses exist for each non-zero element.

Lemma : (6.3)

Let p be an odd prime, and let a' be the solution of $ax \equiv 1 \mod p$, for $a = 1, 2, \ldots, p-1$. Then, $a' \equiv b' \mod p$ if and only if $a \equiv b \mod p$. Furthermore, $a \equiv a' \mod p$ if and only if $a = 1$ or $a = p - 1$.

Proof. Suppose that $a' \equiv b' \mod p$. Then, it follows that

$$b \equiv aa'b \equiv ab'b \equiv a \mod p$$

Conversely, suppose $a \equiv b \mod p$. Then it follows that

$$b' \equiv baa' \equiv b'ba \equiv a' \mod p$$

If $a = 1$ or $a = p - 1$, then

$$1 \cdot 1 \equiv 1 \mod p \quad \text{and} \quad (p-1) \cdot (p-1) \equiv 1 \mod p$$

Conversely, if $a \equiv a' \mod p$, then it follows that

$$1 \equiv aa' \mod p \equiv a^2 \mod p$$

From Lemma 6.2, this implies that $a = 1$ or $a = p - 1$ □

Theorem : Wilson's Theorem

p is a prime if and only if

$$(p-1)! \equiv -1 \mod p$$

Proof. From Lemma 6.3, we know that we can separate the numbers

$$2, \quad 3, \quad \ldots, \quad p-2$$

Into $(p-3)/2$ pairs such that each pair consists of an integer a and its associated multiplicative inverse a'. The product of the two integers in each pair is congruent to 1 modulo p, so it follows that

$$2 \times 3 \times \cdots \times (p-2) \equiv 1 \mod p$$

Therefore, it follows that

$$(p-1)! \equiv 1 \times 2 \times \cdots \times (p-2) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \mod p$$

Suppose that $n = ab$ for some integers a and b, with $a < n$. If $(n-1)! \equiv -1 \mod n$, then we have that

$$n \mid ((n-1)! + 1)$$

Since $a \mid n$, we also have that

$$a \mid ((n-1)! + 1)$$

Since $a \leq n-1$, one of the factors of $(n-1)!$ is a itself. This gives that $a \mid (n-1)!$ However, this implies that $a \mid 1$. The only positive divisors of n are 1 and n, and therefore n is a prime. $\square$