1 Wilson's Theorem

In number theory, Wilson's Theorem states that if integer $p > 1$, then $(p-1)!+1$ is divisible by p if and only if p is prime. It was stated by John Wilson.
The French mathematician Lagrange proved it in 1771.

1.1 proof

1.1.1 Elementary Proof

Suppose p is a prime. Then each of the integers $1, \ldots, p-1$ has an inverse modulo p. (Indeed, if one such integer a does not have an inverse, then for some distinct b and c modulo p, $ab \equiv ac \pmod{p}$, so that $a(b-c)$ is a multiple of p, when p does not divide a or $b-c$—a contradiction.) This inverse is unique, and each number is the inverse of its inverse. If one integer a is its own inverse, then

$$0 \equiv a^2 - 1 \equiv (a-1)(a+1) \pmod{p}, \tag{1}$$

so that $a \equiv 1$ or $a \equiv p-1$. Thus we can partition the set $\{2, \ldots, p-2\}$ into pairs $\{a, b\}$ such that $ab \equiv 1 \pmod{p}$. It follows that $(p-1)$ is the product of these pairs times $1 \cdot (-1)$. Since the product of each pair is conguent to 1 modulo p, we have

$$(p-1)! \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}, \tag{2}$$

as desired.

1.1.2 Algebraic Proof

Let p be a prime. Consider the field of integers modulo p. By Fermat's Little Theorem, every nonzero element of this field is a root of the polynomial

$$P(x) = x^{p-1} - 1. \tag{3}$$

Since this field has only $p-1$ nonzero elements, it follows that

$$x^{p-1} - 1 = \prod_{r=1}^{p-1} (x - r). \tag{4}$$

Now, either $p = 2$, in which case $a \equiv -a \pmod{2}$ for any integer a, or $p-1$ is even. In either case, $(-1)^{p-1} \equiv 1 \pmod{p}$, so that

$$x^{p-1} - 1 = \prod_{r=1}^{p-1} (x - r) = \prod_{r=1}^{p-1} (-x + r). \tag{5}$$

If we set x equal to 0, the theorem follows.