Wilsons Theorem

1 Theorem:

Wilsons Theorem states that if integer $p > 1$, then $(p-1)! + 1$ is divisible by p if and if only if p is prime.

2 Proofs

Suppose first that p is composite. Then p has a factor $d > 1$ that is less than or equal to p-1. Then d divides $(p-1)!$, so d does not divide $(p-1)! + 1$. Therefore p does not divide $(p-1)! + 1$.
Two proofs of the converse are provided: an elementary one that rests close to basic principles of modular arithmetic, and an elegant method that relies on more powerful algebraic tools.

Elementary Proof Suppose p is a prime. Then each of the integers $1, ..., p-1$ has an inverse modulo p. This inverse is unique, and each number is the inverse of its inverse. If one integer a is its own inverse then:

$$0 \equiv a^2 - 1 \equiv (a-1)(a+1) \quad (mod\ p)$$

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

$$(p-1)! \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \quad (mod\ p),$$

as desired.

2.1 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

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

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

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

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

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

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

References

1. $https://artofproblemsolving.com/wiki/index.php?title = Wilson$