Wilson Theorem

i.e. if p is prime, $p \mid (p-1)!+1$

1. Wilson Thm.: If p is a prime number, then $(p-1)!+1 \equiv 0 \pmod p$

proof: Considering $S = \{1, 2, \dots, p-1\}$.

Since p is a prime and $\forall s \in S$, s is a natural num, and obviously $p \nmid s$ as $s < p$, by theorem 5.1.5., gives $\exists x \in \mathbb{N}$, s.t. $sx \equiv 1 \pmod p$.

Also $p \nmid x$, x is congruent to one of num. in S mod p.

I'll igore 1 and $p-1$. as 5.1.7. states, the number con. to their own mod. p is 1 or $p-1$.

Let $S' = \{2, 3, \dots, p-2\}$.

WTS: no two num. in set S' has same inverse.

Assume for contra. that $s_1, s_2 \in S'$, $s_1 \neq s_2$.

$s_1 \cdot x_0 \equiv 1 \pmod p$, $s_2 \cdot x_0 \equiv 1 \pmod p$. s.t.

By 5.1.6., gives. $s_1 \equiv s_2 \pmod p$.

Since $s_1, s_2 \in S'$, $s_1 < p$, $s_2 < p$, which $s_1 \equiv s_1 \pmod p$. gives.

$s_1 = s_2$. contradicts $s_1 \neq s_2$.

? Thus, we can arrange numbers in S' in pairs of a num and its inverse. gives. $2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1 \pmod p$.

Also. $1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1 \pmod p$ by multiplying 1.

Since $(p-1) \equiv -1 \pmod p$. gives. $(p-1)! \equiv -1 \pmod p$. which $(p-1)!+1 \equiv 0 \pmod p$. ∎

$(m-1)!+1 \equiv 1 \pmod m$.

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

proof: Assume m is composite $m > 4$.

WTS: $(m-1)! \equiv 0 \pmod m$. i.e. $m \mid (m-1)!$

① Let $m = a \cdot b$. where $a < m$, $b < m$, $a \neq b$. then a and b occurs as distinct factors in $(m-1)!$, which $m = a \cdot b$ is a factor of

$(m-1)!$, gives. $(m-1)! \equiv 0 \pmod m$.

② Let $m=p^2$ where $p<m$. p is a prime. (m can't write as a product of two distinct numbers).

Since $m>4$, gives $p>2$, which $p^2>2p$. which $p^2-1 \geq 2p$., gives.

$(p^2-1)!$ contains a factor $2p$.

Since $2p>p$. $(p^2-1)!$ contains $2p \cdot p = 2p^2$

Also. $2p^2 > p^2$. $(p^2-1)!$ contains p^2. which $p^2 \mid (p^2-1)!$

$\Rightarrow m \mid (m-1)!$

2) If m is a natural number, $m \neq 1$. then $\underbrace{(m-1)!+1 \equiv 0 \pmod m}_{A}$ iff. $\underbrace{m \text{ is a prime number}}_{B}$.

proof: $B \to A$: wilson thm.

$A \to B$: contra positive of 1). except for $m=4$.

when $m=4$. $(m-1)!+1 = 3!+1 = 7 \Rightarrow 7 \equiv 3 \pmod 4$.

■