Wilson's theorem

n	1	2	3	4	5	6	7	8	9	...
$n!+1$	2	3	7	5^2	11^2	$7 \cdot 103$	71^2	$61 \cdot 661$	$19 \cdot 71 \cdot 269$	

any prime factor must be $> n$

data suggests: $p \mid (p-1)! + 1$

THM Wilson's theorem

$$(p-1)! \equiv -1 \pmod{p}$$

Pf

$1 \cdot 2 \cdot 3 \cdots (p-1)$

$=$ product of all invertible residues mod p

$\equiv (+1) \cdot (-1) \cdots \underbrace{x \cdot x^{-1}} \cdots$ ($x \cdot x^{-1} \equiv 1$)

$\equiv -1$

idea: pair each residue x with its inverse x^{-1}

except if $x \equiv x^{-1} \pmod{p}$

$\Leftrightarrow x^2 \equiv 1$

only 2 solutions: ± 1

COR $(n-1)! \equiv -1 \pmod{n}$

$\Leftrightarrow$ n is a prime

Pf "$\Leftarrow$" Wilson's theorem

"$\Rightarrow$" $-1 \equiv (n-1)!$ is invertible mod n

$\Rightarrow \gcd((n-1)!, n) = 1$

$\Rightarrow$ n is a prime