Converse of Wilson's Theorem

Vincent Mercieca

Theorem 1 (Wilson's Theorem) *If p is prime, then $(p-1)! = -1$ mod p.*

Theorem 2 (Converse to Theorem 1) *If $(p-1)! = -1$ mod p, then p is prime.*

Lagrange's Proof of Theorem 2:

It is clear that every prime greater than 2 can be written in the form of $4m+1$ or $4m-1$.
If we assume that $4m+1$ is prime, $\left((2m)!\right)^2 = -1 \text{ mod } n \Rightarrow n$ is prime.
And, if $4m-1$ is prime, $(2m-1)! = \pm 1 \text{ mod } n \Rightarrow n$ is prime.

Let $n = 4m+1$, then

$$\begin{aligned}(n-1)! = (4m)! &= 1.2\cdots(2m)\cdots(4m)\\ \therefore (n-1)! \text{ mod } n &= 1.2\cdots(2m)\cdots(4m) \text{ mod } (4m+1)\\ &= 1.2\cdots(2m)(-2m)\cdots(-1) \text{ mod } n\\ &= (-1)^{2m}.1.2\cdots(2m)(2m)\cdots 1 \text{ mod } n\\ &= \left((2m)!\right)^2 \text{ mod } n\end{aligned}$$

But $(n-1)! = -1 \text{ mod } n \Rightarrow \left((2m)!\right)^2 = -1 \text{ mod } n \Rightarrow n$ is prime.

Let $n = 4m-1$, then

$$\begin{aligned}(n-1)! = (4m-2)! &= 1.2\cdots(2m-1)(2m)\cdots(4m-2)\\ \therefore (n-1)! \text{ mod } n &= (2m-1)!(2m)\cdots(4m-2) \text{ mod } (4m-1)\\ &= (2m-1)!(-2m+1)\cdots(-1) \text{ mod } n\\ &= (-1)^{2m-1}\left((2m-1)!\right)^2 \text{ mod } n\\ &= -\left((2m-1)!\right)^2 \text{ mod } n\end{aligned}$$

$$\begin{aligned}\textit{But } (n-1)! = -1 \text{ mod } n &\Longrightarrow -\left((2m-1)!\right)^2 = -1 \text{ mod } n\\ &\Longrightarrow \left((2m-1)!\right)^2 = 1 \text{ mod } n\\ &\Longrightarrow (2m-1)! = \pm 1 \text{ mod } n\\ &\Longrightarrow n \text{ is prime.} \qquad \text{QED}\end{aligned}$$

Alternative proof:

Let $(n-1)! = -1 \bmod n$.
Then $\exists \lambda \in \mathbb{Z}$ *s.t.* $(n-1)! = \lambda n - 1 \Rightarrow \lambda n - (n-1)! = 1$

Suppose n is not prime.
Then $\exists a, b \in \{2, 3, \ldots, n-1\}$ *s.t.* $n = ab \Rightarrow n | (n-1)!$
Also $n | \lambda n$, hence $n | 1$, which is a contradiction.

$\therefore n$ is prime. QED