Wilson's Theorem

Definition: Given $n \in \mathbb{N}$, define $n! = \prod_{j=1}^{n} j$.

Examples: $1! = 1$, $2! = 1 \cdot 2 = 2$, $3! = 1 \cdot 2 \cdot 3 = 6$, and $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Wilson's Theorem: $\forall p \in \mathbb{P} \left((p-1)! \equiv -1 \bmod p \right)$

Examples:

$p = 2$ $\quad (p-1)! = 1! = 1 \quad 1 \equiv -1 \bmod 2$

$p = 3$ $\quad (p-1)! = 2! = 2 \quad 2 \equiv -1 \bmod 3$

$p = 5$ $\quad (p-1)! = 4! = 24 \quad 24 \equiv -1 \bmod 5$ as $24 = 5 \cdot 5 - 1$

$p = 7$ $\quad (p-1)! = 6! = 720 \quad 720 \equiv -1 \bmod 7$ as $720 = 103 \cdot 7 - 1$

Lemma: $\forall p \in \mathbb{P}\ \forall n \in \mathbb{Z} \left(n^2 \equiv 1 \bmod p \leftrightarrow n \equiv 1 \bmod p \vee n \equiv -1 \bmod p \right)$

Proof:

If $n \equiv 1 \bmod p$ or $n \equiv -1 \bmod p$ then $n^2 \equiv 1 \bmod p$.

Conversely, if $n^2 \equiv 1 \bmod p$ then $p \mid (n^2 - 1)$ so $p \mid (n+1)(n-1)$.

By the prime property, $p \mid (n+1)$ or $p \mid (n-1)$.

If $p \mid (n+1)$ then $n \equiv -1 \bmod p$. If $p \mid (n-1)$ then $n \equiv 1 \bmod p$.

Wilson's Theorem

Lemma: $\forall p \in \mathbb{P}\ \forall n \in \mathbb{Z}\ (n^2 \equiv 1 \bmod p \leftrightarrow n \equiv 1 \bmod p \vee n \equiv -1 \bmod p)$

Wilson's Theorem: $\forall p \in \mathbb{P}\ ((p-1)! \equiv -1 \bmod p)$

Proof:

Consider $(p-1)!$ in $\mathbb{Z}_p$.

Key idea: We can pair up the elements in $\{2,3,\ldots,p-2\}$ with their inverses (which are also in $\{2,3,\ldots,p-2\}$).

This leaves only -1 and 1. Thus, $(p-1)! \equiv -1 \cdot 1 \equiv -1 \bmod p$

Examples:

$p=7 \quad 6! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 \equiv 1\cdot 6 \equiv -1 \bmod 7$

$p=11 \quad 10! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10 \equiv 1\cdot 10 \equiv -1 \bmod 11$

To see why this works, observe that in $\mathbb{Z}_p$:

1) $1^{-1} = 1$ and $(-1)^{-1} = -1$

2) $\forall x \in \{2,3,\ldots,p-2\}\ (x \not\equiv 1 \bmod p \wedge x \not\equiv -1 \bmod p)$ so $x^2 \not\equiv 1 \bmod p$. Thus, $x^{-1} \neq x$ so $x^{-1} \in \{2,3,\ldots,p-2\} \setminus \{x\}$. Since $x^{-1} \neq x$, x and x^{-1} can indeed be paired up.