Compléments sur le théorème de Wilson.

Soit p un entier naturel.

Le nombre p est premier ssi $(p-1)! \equiv -1 \ (p)$

Idée : critère simple pour dire si un nombre est premier ou non.

Un exemple pour comprendre.

- $p=7$. $6! = 6\times5\times4\times3\times2\times1$

pour calculer ce produit, regroupons les termes deux à deux.

$2\times4 \equiv 1 \ (7)$, $3\times5 \equiv 1 \ (7)$

donc $(7-1)! = (2\times4)\times(3\times5)\times1\times6$

$= 6 \equiv -1 \ (7)$

Si p est premier, on cherche à regrouper les termes 2 à 2 tels que 1 et $p-1$ par que le produit soit égal à $1 \ (8)$

- $p=8$, 8 n'est pas premier, $8 = 2\times4$ et 2 et 4 vont apparaître comme facteurs dans la décomposition de $(8-1)!$

$(8-1)! = (2\times5)\times1\times3\times5\times6\times7 = 8\times1\times3\times5\times6\times7$

d'où $(8-1)!$ est divisible par 8

Preuve : sens direct. Si p est premier alors $(p-1)! \equiv -1 \ (p)$

On va utiliser l'idée de l'exemple précédent.

Prop : Si p est premier et si $a \in \{1, 2, \dots, p-1\}$ alors il existe un unique nombre b (p) tel que $ab \equiv 1 \ (p)$

Preuve : existence. Comme p est premier, il ne partage aucun diviseur commun avec a tel que $1 \leq a \leq p-1$

$p \wedge a = 1$, d'après Bezout, $\exists b, m$ tels que $ab + mp = 1$

donc $ab \equiv 1 \ (p)$

unicité : S'il existe b et b' tels que $\begin{cases} ab \equiv 1 \ (p) \\ ab' \equiv 1 \ (p) \end{cases}$ (*)

avec (*) $bab' \equiv b \ (p)$ et $ab = ba \equiv 1 \ (p)$

donc $b' = b \ (p)$

Donc on peut regrouper les facteurs par paire. Mais attention, il se peut que certains nombres ne puissent être regroupés qu'avec eux-mêmes.

ex le seul nombre b qui peut être regroupé avec le nombre 1 est lui-même

$1 \times b \equiv 1 \ (p) \Rightarrow b \equiv 1 \ (p)$

Etude des nombres tels que $a \times a \equiv 1 \ (p)$

Prop : Si p est premier alors $a \times a \equiv 1 \ (p)$ ssi : $a \equiv 1 \ (p)$ ou $a \equiv p-1 \ (p)$

Preuve : $a \times a \equiv 1 \ (p) \Leftrightarrow a^2 - 1 \equiv 0 \ (p)$

ou $(a+1)(a-1) \equiv 0 \ (p)$

Comme p est premier $p \mid a+1$ ou $p \mid a-1$

donc $a \equiv 1 \ (p)$ ou $a \equiv -1 \ (p)$

$a \equiv p-1 \ (p)$

Avec ces résultats, si p est premier, on peut regrouper tous les facteurs de $(p-1)!$ 2 à 2 de sorte que le produit de chaque paire vaille $1 \ (p)$ sauf 1 et $p-1$ (qui se regroupent avec eux-mêmes)

$(p-1)! \equiv 1 \times (p-1) \equiv p-1 \ (p) \equiv -1 \ (p)$

Réciproque : Si $(p-1)! \equiv -1 \ (p)$ alors p est premier

Passons à la contraposée

Si p n'est pas premier alors $(p-1)! \not\equiv -1 \ (p)$

- Cas $p=4$

$(p-1)! = 3! = 6$ et $6 \equiv 2 \neq -1 \ (4)$

- $p>4$ un nombre qui n'est pas premier

$p = a \times b$ avec $1 < a, b < p-1$

Deux cas :

a) $a \neq b$, on peut regrouper dans a et b dans le produit de $(p-1)!$, de sorte que

$p = ab \mid (p-1)!$

donc $(p-1)! \equiv 0 \ (p)$

b) $a = b$ (p est le carré d'un nombre premier, c'est 2^2)

alors $p = a^2$

Comme $p>4$ alors $a>2$ donc $p = a^2 > 2a$

Ainsi les nombres a et $2a$ apparaissent comme facteurs de $(p-1)!$ qui est donc divisible par a et $2a$

Donc $(p-1)!$ est divisible par $a \times a = a^2 = p$ d'où

$(p-1)! \equiv 0 \ (p) \neq -1 \ (p)$

Donc $(p-1)! = \begin{cases} -1 \ (p) & \text{si } p \text{ premier} \\ 2 \ (p) & \text{si } p=4 \\ 0 \ (p) & \text{sinon.} \end{cases}$