Math 4460
3/26/25

<u>Ex:</u> Let's illustrate the next theorem with an example.

Let $p = 13$. prime

Check out what happens when we multiply all the elements of $\mathbb{Z}_{13}^{\times} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \ldots, \overline{12}\}$

together.

$$\overline{12!} = \overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\overline{4}\cdot\overline{5}\cdot\overline{6}\cdot\overline{7}\cdot\overline{8}\cdot\overline{9}\cdot\overline{10}\cdot\overline{11}\cdot\overline{12}$$

$$= \overline{1}\cdot(\overline{2}\cdot\overline{7})(\overline{3}\cdot\overline{9})(\overline{4}\cdot\overline{10})(\overline{5}\cdot\overline{8})(\overline{6}\cdot\overline{11})\cdot\overline{12}$$

these are inverses

their own inverse

$$= \overline{1}\cdot\overline{14}\cdot\overline{27}\cdot\overline{40}\cdot\overline{40}\cdot\underbrace{\overline{66}}\cdot\overline{12}$$

$$\begin{array}{r} 5 \\ 13\,\overline{)\,66} \\ -65 \\ \hline 1 \end{array}$$

$$= \overline{1}\cdot\overline{1}\cdot\overline{1}\cdot\overline{1}\cdot\overline{1}\cdot\overline{1}\cdot\overline{12}$$

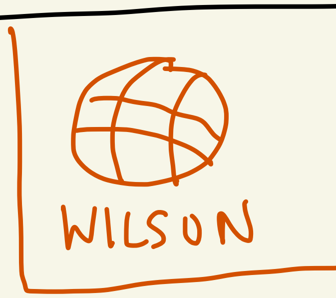
$$= \overline{12} = \overline{-1}$$

$12 \equiv -1 \pmod{13}$

So in $\mathbb{Z}_{13}^{\times}$ we get $\overline{12!} = \overline{-1}$

or $12! \equiv -1 \pmod{13}$

---




## Theorem (Wilson's theorem)

Let $p$ be a prime.

Then, $\overline{(p-1)!} = \overline{p-1} = \overline{-1}$ in $\mathbb{Z}_p^{\times}$

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

Proof:

If $p=2$, then

$$\overline{(p-1)!} = \overline{1!} = \overline{1} = \overline{-1}$$

in $\mathbb{Z}_2^\times = \{\overline{1}\}$

Let $p$ be an odd prime.

Then, $\mathbb{Z}_p^\times = \{\overline{1}, \underbrace{\overline{2}, \overline{3}, \ldots, \overline{p-2}}_{\text{these each have an inverse not equal to themselves}}, \overline{p-1}\}$

$\overline{1}$ and $\overline{p-1}$ are their own inverse

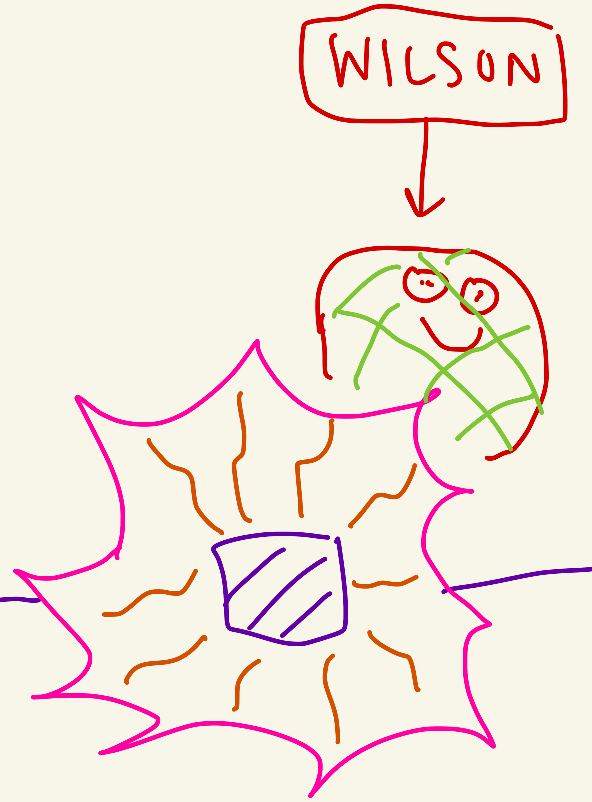
So, $\overline{(p-1)!} = \overline{1} \cdot \boxed{\overline{2} \cdot \overline{3} \cdot \overline{4} \cdots \overline{p-2}} \cdot \overline{p-1}$

every element in this range cancels out with its inverse

$$= \overline{1} \cdot \overline{p-1}$$

$$= \overline{p-1}$$

$$= \overline{-1}$$




Recall when $p$ is prime then one of three cases holds:

- $p = 2$ ← only even prime
- $p \equiv 1 \pmod{4}$
- $p \equiv 3 \pmod{4}$

odd primes

Ex:

$5 \equiv 1 \pmod{4}$

$11 \equiv 3 \pmod{4}$

Theorem: Let $p$ be a prime.
If $p = 2$ or $p \equiv 1 \pmod{4}$,
then there exists $\overline{x} \in \mathbb{Z}_p^\times$
with $\overline{x}^2 = \overline{-1}$

$$\begin{array}{r} 3 \\ 4\,\overline{)\,13} \\ -12 \\ \hline 1 \end{array}$$

Ex: $p = 13$ is prime

$13 \equiv 1 \pmod{4}$

Let

$$\overline{x} = \underbrace{\overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\overline{4}\cdot\overline{5}\cdot\overline{6}}_{\text{first half of } \mathbb{Z}_{13}^\times}$$

$(p-1)/2 = 6$

Then,

$$\overline{x}^2 = \overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\overline{4}\cdot\overline{5}\cdot\overline{6}\cdot\underbrace{\overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\overline{4}\cdot\overline{5}\cdot\overline{6}}_{\text{even \# of numbers}}$$

$$= \overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\overline{4}\cdot\overline{5}\cdot\overline{6}\cdot\overline{-1}\cdot\overline{-2}\cdot\overline{-3}\cdot\overline{-4}\cdot\overline{-5}\cdot\overline{-6}$$

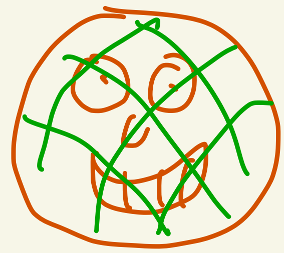
$$= \overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\overline{4}\cdot\overline{5}\cdot\overline{6}\cdot\underbrace{\overline{12}\cdot\overline{11}\cdot\overline{10}\cdot\overline{9}\cdot\overline{8}\cdot\overline{7}}$$

$= \bar{1}\cdot\bar{2}\cdot\bar{3}\cdot\bar{4}\cdot\bar{5}\cdot\bar{6}\cdot\underbrace{\bar{7}\cdot\bar{8}\cdot\bar{9}\cdot\overline{10}\cdot\overline{11}\cdot\overline{12}}$

$= \overline{12!}$

$= \overline{-1}$

WILSON!



Note: $\bar{x} = \bar{5}$

So, $\bar{5}^2 = \overline{-1}$ in $\mathbb{Z}_{13}^{\times}$.

---

<u>Proof of theorem:</u>

When $p = 2$, let $\bar{x} = \bar{1}$

Then $\bar{x}^2 = \bar{1}^2 = \bar{1} = \overline{-1}$ in $\mathbb{Z}_2^{\times}$

Let $p$ be an odd prime

where $p \equiv 1 \pmod 4$.

Then, $4 \mid (p-1)$.

So, $p - 1 = 4k$ where $k \in \mathbb{Z}$

That is, $p = 4k+1$.

Note $\frac{p-1}{2} = \frac{4k+1-1}{2} = 2k$ is even.

Let

$$\bar{x} = \underbrace{\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{\left(\frac{p-1}{2}\right)}}_{(p-1)/2 \text{ terms}} \qquad (*)$$

Since there an even number of terms in $(*)$ we have

$$\bar{x} = \overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdots \overline{\left[-\left(\frac{p-1}{2}\right)\right]}$$

Also, note

$$\overline{p-k} = \overline{-k}$$

in $\mathbb{Z}_p^{\times}$.

Thus,

$$\bar{x}^2 = \underbrace{\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{\frac{p-1}{2}}}_{\bar{x}} \cdot \underbrace{\overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdots \overline{\left[-\frac{p-1}{2}\right]}}_{\bar{x}}$$

$$= \overline{1}\cdot\overline{2}\cdot\overline{3}\cdots\overline{\tfrac{p-1}{2}}\cdot\overline{p-1}\cdot\overline{p-2}\cdot\overline{p-3}\cdots\overline{\left[p-\tfrac{p-1}{2}\right]}$$

$$\overline{\left(\tfrac{p+1}{2}\right)}$$

$$= \overline{1}\cdot\overline{2}\cdot\overline{3}\cdots\overline{\tfrac{p-1}{2}}\cdot\overline{\tfrac{p+1}{2}}\cdots\overline{p-3}\cdot\overline{p-2}\cdot\overline{p-1}$$

$$= \overline{(p-1)!}$$

$$= \overline{-1}$$

WILSON!

∎

Theorem: If $p$ is an odd prime with $p \equiv 3 \pmod 4$ then there is no $\overline{x} \in \mathbb{Z}_p^\times$ with $\overline{x}^2 = \overline{-1}$.

proof:

Suppose there is an $\overline{x} \in \mathbb{Z}_p^\times$ with $\overline{x}^2 = \overline{-1}$.

Since $p \equiv (3 \bmod 4)$ we can write $p = 4k+3$ for some $k \in \mathbb{Z}$.

Then,

$$\overline{x}^{p-1} = \overline{x}^{4k+2} = (\overline{x}^4)^k \, \overline{x}^2$$

$$= \overline{1}^k \cdot (\overline{-1}) = \overline{-1}$$

$$\overline{x}^2 = \overline{-1} \rightarrow \overline{x}^4 = \overline{1}$$

We will see later a theorem by Fermat that says $\bar{x}^{p-1} = \bar{1}$. This is a contradiction.

since $\bar{1} \neq \overline{-1}$ in $\mathbb{Z}_p^\times$ since $p>2$.

So there is no such $\bar{x}$. $\blacksquare$