Proof of Fermat’s Little Theorem Via the Binomial Theorem

Restatement of Fermat's Little Theorem:

$\forall p \in \mathbb{P}\ \forall x \in \mathbb{Z}\ (x^p \equiv x \pmod{p})$ Note: If $p \nmid x$, $x^p \equiv x \pmod{p} \leftrightarrow x^{p-1} \equiv 1 \pmod{p}$
If $p \mid x$, $x^p \equiv x \equiv 0 \pmod{p}$

Proof:

Proposition: $\forall j \in [p-1]\ \left(\binom{p}{j} \equiv 0 \pmod{p}\right)$

Proof: Observe that $\binom{p}{j} = \frac{p!}{j!(p-j)!}$, $p \mid p!$, $p \nmid j!$, and $p \nmid (p-j)!$

$p \mid \binom{p}{j} \cdot j! \cdot (p-j)!$ so by the prime property, $p \mid \binom{p}{j}$.

We'll now use induction.

Base case: If $x=0$, $x^p \equiv x \equiv 0 \pmod{p}$

Inductive step: Assume $k^p \equiv k \pmod{p}$ and consider $x=k+1$

By the Binomial Theorem, $(k+1)^p = \sum_{j=0}^{p} \binom{p}{j} k^{p-j} \cdot 1^j$

$(k+1)^p \equiv k^p + 1^p \equiv k+1 \pmod{p}$

Note: This proves the result for $x \geq 0$.

If $p>2$ and $x \in \mathbb{N}$ then $(-x)^p = -(x^p)$ so $(-x)^p \equiv -(x^p) \equiv -x \pmod{p}$.

If $x \in \mathbb{N}$, $-x \equiv x \pmod{2}$ so $(-x)^2 \equiv x^2 \equiv x \equiv (-x) \pmod{2}$