In this part, we will give a second proof for Fermat's Little Theorem. (Chapter 38 $P_{319-322}$)

Recall:

Theorem (Fermat's Little Theorem): Let $p$ be a prime, and let $a$ be any number such that $a \not\equiv 0 \pmod{p}$. Then:

$$a^{p-1} \equiv 1 \pmod{p}.$$

To prove this, it suffices to show:

$$(*) \quad a^{p} \equiv a \pmod{p}.$$

Remark: (1) Since $a \not\equiv 0 \pmod{p}$, we can cancel one $a$ on each side and the theorem is valid.

(2) $(*)$ is true even if $a \equiv 0 \pmod{p}$.

Idea for the 2nd proof:

(1) a special property for $\binom{p}{k}$

(2) induction.

Theorem (38.3 Binomial Theorem mod $p$) Let $p$ be a prime number.

(a) $\binom{p}{k} \equiv 1 \pmod p$ if $k=0$ or $k=p$.

(b) $\binom{p}{k} \equiv 0 \pmod p$ if $1 \le k \le p-1$

(c) For any number $A, B$, we have:

$$(A+B)^p \equiv (A+B) \pmod p.$$

Recall: we showed $p \mid \binom{p}{2}$ when $p>2$.

This is a special case of (b).

Proof: (a) This is obvious since

$$\binom{p}{0} = \binom{p}{p} = 1 \qquad 1 \equiv 1 \pmod p.$$

(b) Assume that $1 \le k \le p-1$.

$$\binom{p}{k} = \frac{p\,(p-1)\cdots(p-k+1)}{k(k-1)\cdots 2\cdot 1}.$$ this is a number!!!

Suppose that $p \nmid \binom{p}{k}$, we have

$$p \mid 1 \cdot 2 \cdot 3 \cdots (k-1)$$

since we have a $p$ in the numerator

This is impossible since $1, 2, 3, \cdots, k-1 < p$.

Therefore $p \mid \binom{p}{k}$ and $\binom{p}{k} \equiv 0 \pmod{p}$

(C) By the definition of binomial numbers:

$$(A+B)^p = \binom{p}{0} A^p + \binom{p}{1} A^{p-1} B + \cdots \binom{p}{k} A^{p-k} B^k + \cdots \binom{p}{p-1} A B^{p-1} + \binom{p}{p} B^p$$

$$= A^p + \binom{p}{1} A^{p-1} B + \cdots \binom{p}{k} A^{p-k} B^k + \cdots \binom{p}{p-1} A B^{p-1} + B^p$$

$$\equiv A^p + 0 A^{p-1} B + \cdots 0 A^{p-k} B^k + \cdots 0 A B^{p-1} + B^p \pmod{p}$$

This gives: $(A+B)^p \equiv A^p + B^p \pmod{p}$. $\square$.

Then we give the 2nd proof for Fermat's Little Theorem:

we know, we only need to show:

for any integer $a$, $a^p \equiv a \pmod{p}$.

We prove this by induction:

$P(a)$: for any integer $a$, $a^p \equiv a \pmod{p}$.

Step I: $P(1)$ $\quad 1^p = 1 \equiv 1 \pmod p$ ✓

Step II: Suppose that $P(a)$ is true, that is,

$$a^p \equiv a \pmod p.$$

$P(a+1)$:

$$(a+1)^p \equiv a^p + 1^p \pmod p \qquad \text{Theorem 1C)}$$

$$\equiv a+1 \pmod p \qquad \text{induction hypothesis.}$$

Therefore, if $P(a)$ is true, then $P(a+1)$ is true.

By induction, we showed, for any number $a$,

$$a^p \equiv a \pmod p. \qquad \square.$$