

In this part, we will give another proof for Fermat's Little Theorem. (Chapter 38 P319-322)

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.

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

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

(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

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

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

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

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 $1, 2, 3, \dots, k-1 < p$.

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

(C) By the definition of binomial numbers:

$$\begin{aligned}(A+B)^p &= \binom{p}{0} A^p + \binom{p}{1} A^{p-1} B + \cdots + \binom{p}{k} A^{p-k} B^k + \cdots + \binom{p}{p-1} A B^{p-1} + \binom{p}{p} B^p \\ &= A^p + \binom{p}{1} A^{p-1} B + \cdots + \binom{p}{k} A^{p-k} B^k + \cdots + \binom{p}{p-1} A B^{p-1} + B^p \\ &\equiv A^p + 0 A^{p-1} B + \cdots + 0 A^{p-k} B^k + \cdots + 0 A B^{p-1} + B^p \pmod{p}\end{aligned}$$

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: $P(1) \quad 1^p = 1 \equiv 1 \pmod{p} \quad \checkmark$

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

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

$P(a+1)$:

$$(a+1)^p \equiv a^p + 1^p \pmod{p} \quad \text{Theorem 1c)}$$

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

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

By induction, we showed, for any number a ,

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

□.

An application of Fermat's Little Theorem.

Example: Solve the congruent equation:

$$X^{86} \equiv 6 \pmod{7}$$

Solution: Note: $X \equiv 0 \pmod{7}$ is not a solution.

We can assume $X \not\equiv 0 \pmod{7}$. Then by Fermat's Little Theorem:

$$X^6 \equiv 1 \pmod{7}$$

By Euclidean's algorithm, $86 = 14 \cdot 6 + 2$

$$X^{86} = X^{6 \cdot 14 + 2} = (X^{6 \cdot 14}) (X^2) = (X^6)^{14} \cdot (X^2)$$

$$\equiv 1 \cdot X^2 \pmod{7}.$$

$$\equiv X^2 \pmod{7}$$

So it suffices to solve $X^2 \equiv 6 \pmod{7}$

$$X=1 \quad X^2 = 1 \not\equiv 6 \pmod{7}$$

$$X=2 \quad X^2 = 4 \not\equiv 6 \pmod{7}$$

$$X=3 \quad X^2 = 9 \not\equiv 6 \pmod{7}$$

$$X=4 \quad X^2 = 16 \not\equiv 6 \pmod{7}$$

$$X=5 \quad X^2 = 25 \not\equiv 6 \pmod{7}$$

$$X=6 \quad X^2 = 36 \not\equiv 6 \pmod{7}$$

Therefore, there is no solution for $x^{86} \equiv x^2 \pmod{7}$