Fermat's theorem

Statement: — If a is an integer and P a prime, then $a^P \equiv a \pmod{P}$.

Proof: — Ist We shall make use of the following lemma (In order to prove that theorem).

Lemma. If G is a finite group and $a \in G$, then $a^{O(G)} = e$.

The proof of the theorem starts.

If $a = 0$, the theorem is obviously true.
Consider the case in which $a \neq 0$.

Let G be the multiplicative group of residue modulo P. Then G contains $P-1$ distinct elements namely

$$[1], [2], [3], \text{——} [P-1].$$

$$O(G) = P-1, \quad e = [1]$$

by definition of congruent modulo P,

this $a^{P-1} \equiv 1 \pmod{P}$. Since P is a prime.

Hence the last implies

$$a^{P-1} \cdot a = 1 \pmod{P}$$

i.e. $a^P \equiv a \pmod{P}$ —— (1)

Proved.

Problem: — Let P be a positive prime integer and a an integer not divisible by P. Then show that P divides $a^{P-1} - 1$. Does 11 divide $(108)^{11} - 108$?

Solution — For Fermat's theorem

$$a^{P-1} \equiv 1 \pmod{P}. \quad \text{——} (1)$$

This $\Rightarrow P$ divides $a^{P-1} - 1$ —— (2)

take $p = 11$, $a = 108$

Now (2) $\Rightarrow$ 11 divides $(108)^{10} - 1$

$\Rightarrow$ 11 divides $108 \{(108)^{10} - 1\}$.

$\Rightarrow$ 11 divides $108 \{(108)^{10} - 1\}$.

$\Rightarrow$ 11 divides $(108)^{11} - 108$.