Fermat's Little Theorem

Theorem

If p is prime, then

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

Proof.

We will prove by induction. First note that if $a = 0$ then $0^p = 0$ and if $a = 1$ then $1^p = 1$.

Now assume the theorem is true for a. We compute

$$(a+1)^p \equiv a^p + 1^p \pmod{p} = a + 1 \pmod{p},$$

the first step using Lemma 2, and the second using the induction hypothesis.

□