Theorem 0.1 (Fermat's Little Theorem)**.**
Let p be a prime number and let $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$*. Then*

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

Proof. Let p be a prime number and let $a \in \mathbb{Z}$ such that $p \nmid a$.

Consider the set of integers

$$S = \{1, 2, \ldots, p-1\}.$$

Multiplying each element of S by a, we obtain the set

$$aS = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}.$$

We claim that the elements of aS are pairwise distinct modulo p.
Indeed, suppose that

$$ai \equiv aj \pmod{p}.$$

Then

$$a(i-j) \equiv 0 \pmod{p}.$$

Since p is prime, $p \mid a(i-j)$ and $\gcd(a, p) = 1$, it follows that $p \mid (i-j)$,

hence $i \equiv j \pmod{p}$.

As $1 \leq i, j \leq p-1$, we conclude that $i = j$.

Thus, the set aS is a permutation of S modulo p.

Taking the product of all elements in S, we obtain

$$1 \cdot 2 \cdots (p-1) \equiv (a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \pmod{p}.$$

The right-hand side simplifies to

$$a^{p-1} \cdot (1 \cdot 2 \cdots (p-1)).$$

Hence,

$$1 \cdot 2 \cdots (p-1) \equiv a^{p-1} \cdot (1 \cdot 2 \cdots (p-1)) \pmod{p}.$$

Since none of the integers $1, 2, \ldots, p-1$ is divisible by p, their product is invertible modulo p.

Therefore, we may cancel it from both sides, yielding

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

□

Exercise: Compute:

$$50^{100} \bmod 13$$

using Fermat's Little Theorem.

Solution.

We Compute:

$$50^{100} \bmod 13$$

using Fermat's Little Theorem.

Since 13 is a prime number and $\gcd(50, 13) = 1$, Fermat's little theorem gives

$$50^{12} \equiv 1 \pmod{13}.$$

We reduce the exponent modulo 12: $100 = 12 \cdot 8 + 4$. Hence,

$$50^{100} = (50^{12})^8 \cdot 50^4 \equiv 1^8 \cdot 50^4 \equiv 50^4 \pmod{13}.$$

Next, compute 50 mod 13: $50 \equiv 11 \pmod{13}$. Thus, $50^4 \equiv 11^4 \pmod{13}$.
We compute:

$$11^2 = 121 \equiv 4 \pmod{13}, \quad 11^4 \equiv 4^2 = 16 \equiv 3 \pmod{13}.$$

Therefore, $50^{100} \equiv 3 \pmod{13}$.

□