FERMAT'S little THEOREM

Yamini Singh

January 2026

Fermat's Little Theorem. Let p be a prime number and let a be any integer. Then

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

that is,

$$p \mid (a^p - a).$$

Proof. **Base step:** $a = 1$

$$1^p - 1 = 0,$$

hence $p \mid (1^p - 1)$.

Induction hypothesis:

Assume that

$$p \mid \big((a-1)^p - (a-1)\big).$$

Induction step:

Let us suppose we have a number of colours.

Consider a set of necklaces with p beads, each of which can be coloured with any of the a colours.

We partition this set using the following strategy.

Choose any colour, say x, from the a choices. The number of beads of colour x satisfies

$$0 \leq \text{number of beads of colour } x \leq p.$$

Let A_i be the set of necklaces having exactly i beads of colour x.

Then,

$$\bigcup_{i=0}^{p} A_i = \text{the set of all necklaces possible.}$$

The cardinality of this union is

$$\left|\bigcup_{i=0}^{p} A_i\right| = a^p.$$

For $1 \leq i \leq p-1$, the cardinality of A_i is

$$|A_i| = \binom{p}{i}(a-1)^{p-i}.$$

For the case $i = p$, there is one monochromatic necklace of colour x.

For $i = 0$, we have

$$|A_0| = (a-1)^p.$$

(Note that A_0 can still contain $(a-1)$ monochromatic necklaces.)

Observe that

$$\sum_{i=1}^{p-1} \binom{p}{i} (a-1)^{p-i} + (a-1)^p + 1 = a^p.$$

Removing the monochromatic necklaces, which appear only in A_0 and A_p, we obtain

$$\sum_{i=1}^{p-1} \binom{p}{i} (a-1)^{p-i} + \big((a-1)^p - (a-1)\big).$$

Hence,

$$\sum_{i=1}^{p-1} \binom{p}{i} (a-1)^{p-i} + \big((a-1)^p - (a-1)\big) = a^p - a.$$

For $1 \le i \le p-1$, we know that $\binom{p}{i}$ is divisible by p.

For the last term, by the induction hypothesis,

$$p \mid \big((a-1)^p - (a-1)\big).$$

Since each term in the sum

$$\sum_{i=1}^{p-1} \binom{p}{i} (a-1)^{p-i}$$

is divisible by p, and

$$p \mid \big((a-1)^p - (a-1)\big),$$

it follows that

$$p \mid (a^p - a).$$

This completes the proof of Fermat's Little Theorem.

$\square$