Proving Fermat's Little Theorem using Groups

Adhiraj Agarwal • 19 Aug 2026

This article presents Fermat's little theorem from a group theory perspective. This article assumes rudimentary knowledge of groups. In particular, the reader is expected to know the meaning of groups and inverses of elements.

Modular Arithmetic from A Group Perspective

Definition A group is a triple $(G, *, 1)$ where G is a non-vacuous set, $*$ is an associative binary composition in G and 1 is an element of G such that $\forall a \in G(1 * a = a * 1 = a)$ and $\forall a \in G \exists b \in G(a * b = b * a = 1)$. If in addition, the operator is commutative, the group is called an abelian group.

Definition A number a is congruent to b if $m \mid a - b$

Proposition The set of numbers nonzero modulo a prime number p form an abelian group with the binary operator as multiplication and 1 as the identity element.

Proof The operator is both associative and commutative. We only need to check if every element is invertible. If an element a is not invertible then the pigeonhole principle yields that there exist $b, c < p$ such that $ab \equiv ac \pmod{p}$ and since $\gcd(a, p) = 1$, from elementary number theory $p \mid a(b - c) \implies p \mid b - c$ so $b \equiv c \pmod{p}$ but this is impossible as $1 \leq |b - c| < p$ so every element is invertible. □

Fermat's Little Theorem

Fermat's Little Theorem (Fermat's Little Theorem) For a prime number p and an integer n coprime to it, that is $\gcd(n, p) = 1$,

$$n^p \equiv n \pmod{p}$$

We will attempt to provide a proof of Fermat's Theorem using group theory but this requires some sophisticated tools that we will develop before proving this theorem. First, we introduce the notion of cosets and use it to deduce Lagrange's theorem. Then we will employ cyclic subgroups to complete the proof. A subgroup is simply a subset of a group that follows the group axioms.

Definition The order of a finite group, G is the number of elements contained in G.

Definition Suppose we have an arbitrary group G and a non-empty subset H of G, then for $x \in G$, the right coset of H in G is defined as the set

$$Hx = \{hx | h \in H\}.$$

Lemma All right cosets of H in G have the same number of elements and any two cosets of H in G are equal or disjoint.

Proof We can prove the first hypothesis by establishing a one-to-one correspondence between Hx and H. Observe that if $h_1 x = h_2 x$ then by the cancellation law, $h_1 = h_2$ and clearly this is a surjection.

To prove the second hypothesis, suppose two cosets are not equal, then $h_1 x_1 = h_2 x_2$ for some $h_1, h_2 \in H$ and our selected x_1, x_2, then if $h' = h_1^{-1} h_2$, then $x_1 = h' x_2$ and thus if $g \in Hx_1$ then $g = hx_1 = hh' x_2$ for some $h \in H$ so $Hx_1 \subseteq Hx_2$. Repeating the argument in the reverse direction, we get $Hx_2 \subseteq Hx_1$. Therefore, $Hx_1 = Hx_2$. □

From this lemma and the fact that each element $g \in G$ must be in Hg as $1 \in H$, we can state Lagrange's theorem.

Lagrange's Theorem The number of elements in a coset of H in G divides the order of G. In particular, if S is a subgroup of G, then $|S|$ divides $|G|$.

Definition A finite cyclic subgroup generated by a is defined as

$$\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$$

where $a^n = 1$ and n is the order of the cyclic subgroup.

It is easy to verify that this is indeed a subgroup. We are almost ready to prove Fermat's theorem.

Corollary If a is an element in a finite group G of order n, then $a^n = 1$

Proof Consider the subgroup $\langle a \rangle$. Suppose it has order m, then $a^m = 1$. By Lagrange's theorem, $n = mk$ and so we have $a^n = (a^m)^k = 1$ □

Now using the above corollary to Lagrange's theorem, one can make out an algebraic proof of Fermat's Little Theorem.

Proof of Fermat's Theorem Suppose $p \mid n$, then this is trivial. Now suppose $p \nmid n$, then we can treat n as a part of the multiplicative group of integers not congruent to zero modulo p. This group has an order of $p - 1$, whence

$n^{p-1} \equiv 1 \pmod{p}$ by the corollary to Lagrange's theorem. Finally since $\gcd(n, p) = 1$, we can multiply n on both sides without changing the result to get

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

A point to remark is that we have developed tools of group theory motivated to prove Fermat's theorem, some of these results can be generalised but this would take considerable time and hence it is not pursued here. □