An algebraic proof of Fermat's little theorem

Ifan Howells-Baines

January 2025

Introduction

In this short project we will prove Fermat's little theorem using basic group theory. Only the fundamentals of group theory and modular arithmetic are needed to understand this proof. Any other ideas, such as Euler's totient function, are given.

Fermat's little theorem

Juxtaposing the name of the famous theorem by Fermat, the result is the following.

Theorem (Fermat's little theorem)**.** *Let p be a prime number. For any $a \in \mathbb{Z}$,*

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

The original result, which Fermat sent in a letter to his friend in October 1640, is slightly different; he only considers the case where a is not divisible by p, and he did not prove his assertion in the letter. The first published proof of the general result was written by Euler in 1736, though a proof by Leibniz has been dated earlier in some unpublished manuscripts.

Proof

To prove the theorem, we need to know a few results. All of these are common in any introductory course in group theory, and are among the first concepts a new student learns.

Lemma. *Let G be a finite group with subgroup H, and let $g \in G$. Then*

- *the order of G, $|G|$, divides $|H|$;*
- $g^{|G|} = e$.

Proof. The first part of this lemma is Lagrange's theorem, which we will not prove here. The second result is true since if $k = \frac{|G|}{|(g)|}$, then $g^{|G|} = g^{|(g)|k} = e^k = e$.* □

*The group (g) is the subgroup generated by g.

Modular arithmetic is needed to understand the proof, though not anything someone with a brief familiarity would not understand. We provide Bézout's identity as a reminder, but do not prove it. We will use this lemma to show that every element in the group we will construct has an inverse.

Lemma (Bézout's identity)**.** *Let a and b be integers, and let $d = (a, b)$, the greatest common divisor of a and b. Then there exists $u, v \in \mathbb{Z}$ such that $au + bv = d$.*

We define a function next, whose purpose is to make notation easier for us later. This function is interesting in it's own right, and readers can learn more about it from it's Wikipedia page.

Definition (Euler's totient function)**.** Let $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ be a function which maps a positive integer to the number of positive integers less than or equal to it, which are also relatively prime to it. In other words, for any $n \in \mathbb{Z}^+$,

$$n\phi = |\{x \in \mathbb{Z}^+ : (n, x) = 1 \text{ and } x \leq n\}|.$$

For example, $1\phi = 1$, since it is only relatively prime to itself, and $10\phi = |\{1, 3, 7, 9\}| = 4$. Notice that if p is prime, then $p\phi = p - 1$. This number will become the order of the group will be interested in.

Lemma. *Let $N_n = \{x \in \mathbb{Z}^+ : (n, x) = 1$ and $x \leq n\}$. This is a group with respect to multiplication modulo n.*

Proof. To prove this is a group, we need to show

1. N_n is closed under multiplication modulo n;
2. there exists an identity element;
3. multiplication modulo n is associative in N_n;
4. there exists an inverse for every element.

From now on, we will associate each integer $x \in N_n$ with it's equivalence class $[x]$. Let $[x_1], [x_2] \in N_n$, then $[x_1][x_2] = [x_1x_2]$. Since x_1 and x_2 share no prime factors with n, neither does x_1x_2, hence $[x_1x_2] \in N_n$. We have proved (1). For (2), note that $[1] \in N_n$, and for any $x \in N_n$, $[x_1][1] = [1][x_1] = [x_1]$. The associativity axiom in (3) is inherited from the regular multiplication in modular arithmetic.

To prove (4), we will use Bézout's identity. Let $[x] \in N_n$. Then we can find $u, v \in \mathbb{Z}$ such that $xu + nv = 1$, since $(x, n) = 1$. Rearranging, we get $1 - xu = nv$, which implies that $xu \equiv 1 \pmod{n}$. We have shown that there exists an integer u such that $[x][u] = 1$, so to complete the proof, we need to show that u is relatively prime to n. If u was not relatively prime to n, then we can find a prime p such that $u = pu'$ and $n = pn'$. Then $p(xu' + nv') = 1$, but as $p > 1$, this is impossible. Therefore $(n, u) = 1$ and $[u] \in N_n$.[†]

□

[†]Note that u might be greater than n, but since we are associating elements of N_n with their equivlance class, this does not pose an issue.

The proof of Fermat's little theorem now comes by combining what we have discussed.

Proof of Fermat's little theorem. Let p be a prime. Then N_p is a group of order $p\phi = p - 1$. For any integer a which is relatively prime to p, $[a] \in N_p$, and therefore $[a]^{p\phi} = [a]^{p-1} = [1]$. This is equivalent to writing $a^{p-1} \equiv 1 \pmod{p}$. Since $a \equiv a \pmod{p}$, we get $a^p \equiv a \pmod{p}$. Finally, if a is not relatively prime to p, then $a \equiv 0 \pmod{p}$, which means that $a^p \equiv 0 \pmod{p}$, and combining these gives $a^p \equiv a \pmod{p}$. $\square$