1 Introduction: Powers that Loop

Fermat's Little Theorem is one of the most elegant results in number theory. It was stated by Pierre de Fermat in 1640, and it asserts that:

Theorem 1.1 If p is a prime number and $p \nmid a$, then

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

This result also leads directly to the more general identity:

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

which holds for all integers a. Indeed, if $p \mid a$, both sides are congruent to 0. If $p \nmid a$, then multiplying both sides of $a^{p-1} \equiv 1 \pmod{p}$ by a yields the result.

This deceptively simple theorem lies at the foundation of modular arithmetic and has various consequences in algebra, primality testing and modern cryptography. In this paper, we explore Fermat's Little Theorem from multiple angles; starting with a classical number-theoretic proof followed by presenting a more abstract group and field-theoretic perspective. By comparing these approaches, we aim to illustrate the theorem's versatility and how different areas of mathematics naturally converge around its truth.

Before delving into the proofs, consider some elementary examples. Consider $a^k \pmod 5$ with $a \in \{1, 2, 3, 4\}$ and $k \in \{1, 2, 3, 4\}$. The table illustrates that for each a not divisible by 5, $a^4 \equiv 1 \pmod 5$.

a	a^1	a^2	a^3	a^4	$a^4 \bmod 5$
1	1	1	1	1	**1**
2	2	4	3	1	**1**
3	3	4	2	1	**1**
4	4	1	4	1	**1**

On the other hand, consider when n is non prime, such as 4.

a	a^1	a^2	a^3	$a^3 \bmod 4$
1	1	1	1	**1**
2	2	0	0	**0**
3	3	1	3	**3**

In contrast, when $n = 4$ is not prime, we see that $a^3 \not\equiv 1 \pmod 4$ in general. In particular, even though $\gcd(3, 4) = 1$, we have $3^3 = 27 \equiv 3 \not\equiv 1 \pmod 4$.

In a prime modulus, everything except 0 has an inverse. Consider $\mathbb{Z}/p\mathbb{Z}$ where p is prime, the non-zero numbers form a multiplicative group. This means:

1. There are no zero divisors.
2. Every $a \not\equiv 0 \pmod p$ has a unique inverse.

That is you can multiply, cancel, rearrange — it behaves like traditional multiplication but is wrapped around a circle of p points.

Example 1.2 Consider $p = 5$ where $\mathbb{Z}/5\mathbb{Z} := \{0, 1, 2, 3, 4\}$. All the non-zero elements have inverses mod 5.

- $2 \cdot 3 = 6 \equiv 1 \pmod 5$
- $4 \cdot 4 = 16 \equiv 1 \pmod 5$
- $1 \cdot 1 = 1 \pmod 5$

On the other hand, in a non-prime modulus, not everything has an inverse. In $\mathbb{Z}/n\mathbb{Z}$ with composite n, there are zero divisors. That is, you could multiply two non-zero numbers and get 0.

Example 1.3 Consider $n = 4$. Then, $2 \cdot 2 = 4 \equiv 0 \pmod 4$. Thus, 2 has no inverse and cancellation fails. This is why Fermat's Little Theorem does not hold when p is not prime.

2 Number-Theoretic Proofs

2.1 Binomial Expansion

Proof. Consider some integer $a \in \mathbb{Z}$ and expand $(a + b)^p$ modulo p using the binomial theorem:

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

When p is prime, the binomial coefficients $\binom{p}{k}$ are divisible by p for all $1 \leq k \leq p - 1$. Thus, modulo p, we obtain:

$$(a + b)^p \equiv a^p + b^p \pmod p$$

This is because, for every $1 \leq k \leq p - 1$, $\binom{p}{k} \equiv 0 \pmod p$. This is called the **Freshman's Dream**.

We now prove by induction that $a^p \equiv a \pmod p$ for all $a \in \mathbb{Z}$.

Base Case: Let $a = 0$. Then, $0^p = 0 \equiv 0 \pmod p$, so the base case holds.

Inductive step: Assume $a^p \equiv a \pmod p$ for some a. Then, taking $b = 1$:

$$(a + 1)^p \equiv a^p + 1 \equiv a + 1 \pmod p$$

Hence, by induction, the result holds for all $a \in \mathbb{Z}$.

Finally, if $p \nmid a$, we can cancel a from both sides of $a^p \equiv a$ to get:

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

which is Fermat's Little Theorem. □

2.2 Cancellation and Inverses

Proof. Let p be prime and $a \in \mathbb{Z}$ with $p \nmid a$. Consider the set:

$$S = \{a, 2a, 3a, \ldots, (p-1)a\} \pmod{p}$$

where each of these is taken modulo p and we want to understand how they relate to the set $\{1, 2, \ldots, p-1\}$.

Suppose $ia \equiv ja \pmod{p}$ for some $1 \leq i, j \leq p-1$. Then:

$$(ia - ja) \equiv 0 \pmod{p} \implies (i-j)a \equiv 0 \pmod{p}$$

Since $p \nmid a$, it follows that $p \mid (i-j)$, thus $i = j \pmod{p}$. But $1 \leq i, j \leq p-1$ so $i = j$. Hence, all elements in $S \pmod{p}$ are distinct and $S \pmod{p}$ is simply a reordering of the elements $\{1, 2, \ldots, p-1\} \pmod{p}$.

Now, take the product of all elements in the set:

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a = a^{p-1} \cdot (p-1)!$$

Since the set is a permutation of $\{1, 2, \ldots, p-1\}$, we also know that

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

Thus giving us

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

Since $p \nmid (p-1)!$ and $(p-1)! \not\equiv 0 \pmod{p}$, it has a multiplicative inverse modulo p. Thus, multiplying both sides by $((p-1)!)^{-1} \pmod{p}$ we obtain

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

□

3 Abstract Geometric Proofs

3.1 Lattice Point Rotation and Fixed Points

Let $a \in \mathbb{N}$ and p be a prime. Consider the p-dimensional cube $\{1, 2, \ldots, a\}^p$ whose elements are integer lattice points $(x_1, x_2, \ldots, x_p)$ with each $x_i \in \{1, 2, \ldots, a\}$. The total number of points is clearly a^p.

Before proceeding, the following are useful definitions for the upcoming proof:

- **Orbit**: The **orbit** of an element $x \in S$ under a map ϕ is the set of all elements that can be reached by repeatedly applying ϕ to x. That is,

  $$O(x) = \{\phi^n(x) \mid n \in \mathbb{N}\}$$

  where $\phi^n(x)$ denotes applying ϕ n times to x.

- **Disjoint Orbits**: Orbits are said to be **disjoint** if they do not share any common elements.

Define the rotation map $\phi : \mathbb{Z}^p \to \mathbb{Z}^p$ by

$$\phi(x_1, x_2, \ldots, x_p) = (x_2, x_3, \ldots, x_p, x_1)$$

This is a cyclic left rotation on the coordinates. Since p is prime, ϕ generates a $\mathbb{Z}_p$-action on the set $\{1, 2, \ldots, a\}^p$ where each orbit is either of size 1 (a fixed point) or size p (non-fixed points).

Lemma 3.1.1 A lattice point $(x_1, x_2, \ldots, x_p) \in \{1, 2, \ldots, a\}^p$ is fixed under ϕ if and only if $x_1 = x_2 = \cdots = x_p$.

Proof. Suppose $\phi(x_1, x_2, \ldots, x_p) = (x_1, x_2, \ldots, x_p)$. Then

$$(x_2, x_3, \ldots, x_p, x_1) = (x_1, x_2, \ldots, x_p)$$

which implies $x_1 = x_2 = \cdots = x_p$. Conversely, if all x_i are equal, then rotation clearly leaves the point unchanged. So the fixed points are precisely those with all coordinates equal. □

Since each coordinate must be one of the integers 1 to a, there are exactly a such constant tuples:

$$(1, 1, \ldots, 1), (2, 2, \ldots, 2), \ldots, (a, a, \ldots, a)$$

Lemma 3.1.2 Let S be a finite set with a map $\phi : S \to S$ such that every non-fixed point lies in a disjoint orbit of size p, where p is prime. Then:

$$|S| \equiv (\text{number of fixed points of } \phi) \pmod{p}$$

Proof. First define the following:

$$F = \{x \in S \mid \phi(x) = x\} \text{ - the set of fixed points under } \phi$$
$$R = S \setminus F \text{ - the remaining non-fixed points}$$

The orbits in R have size p, so $|R| = kp$ for some $k \in \mathbb{Z}$. Hence $|S| = |F| + kp \equiv |F| \pmod{p}$. □

We are now ready to apply the results from both lemmas to derive Fermat's Little Theorem. Recall that Fermat's Little Theorem states that if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Set,

$$S = \{1, 2, \ldots, a\}^p, \quad |S| = a^p$$

By **Lemma 3.1.1**, the fixed-point set has size a and thus by **Lemma 3.1.2**, we therefore obtain

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

Finally, if $p \nmid a$, we can cancel a to get

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

which is Fermat's Little Theorem.

4 Abstract Algebraic Proofs

4.1 Group-Theoretic Proof via Lagrange's Theorem

Let $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ denote the integers modulo p. Since p is prime, $\mathbb{Z}_p$ is a field and its multiplicative group of non-zero elements denote:

$$\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$$

forms a finite **abelian group** under multiplication modulo p of order $p-1$.

Recall Lagrange's Theorem:
If G is a finite group and $H \leq G$ is a subgroup, then:

$$|H| \mid |G|$$

In particular, for any element $g \in G$, the order of g (i.e. the smallest k such that $g^k = e$) divides $|G|$. Therefore, we have:

$$g^{|G|} = e$$

Let $a \in \mathbb{Z}_p^\times$. Then a is an element of the finite group $\mathbb{Z}_p^\times$, which has order $p-1$. By **Lagrange's Theorem**, the order of a divides $p-1$ and thus:

$$a^{p-1} = 1 \in \mathbb{Z}_p \implies a^{p-1} \equiv 1 \pmod{p}$$

4.2 Frobenius Homomorphism

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denote the finite field of order p. Define a map $\phi : \mathbb{F}_p \to \mathbb{F}_p$ by:

$$\phi(x) = x^p$$

This is called the **Frobenius homomorphism**.

Proposition 4.2.1 The map $\phi(x) = x^p$ is a **ring homomorphism** in characteristic p. That is,

$$\phi(x+y) = \phi(x) + \phi(y), \quad \phi(xy) = \phi(x)\phi(y)$$

Proof. Let $x \in \mathbb{F}_p$. We apply the **Freshman's Dream** identity:

$$(x+y)^p = x^p + y^p \text{ in characteristic } p$$

since all binomial coefficients $\binom{p}{k}$ with $1 \leq k \leq p-1$ are divisible by p and hence vanish in $\mathbb{F}_p$.

So the map $\phi(x) = x^p$ satisfies:

$$\phi(x+y) = (x+y)^p = x^p + y^p = \phi(x) + \phi(y)$$

and clearly $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$. Thus, ϕ is a ring homomorphism.

But $\mathbb{F}_p$ is a finite field of characteristic p, and any ring endomorphism of a finite field that fixes the identity is necessarily the identity map. Hence:

$$x^p = x \ \ \forall x \in \mathbb{F}_p \implies a^p \equiv a \pmod{p} \ \ \forall a \in \mathbb{Z}$$

□

Thus, Fermat's Little Theorem (the standard form) is a corollary. That is, if $p \nmid a$, then $a \in \mathbb{F}_p^\times$, so multiplying both sides of $a^p \equiv a \pmod{p}$ by $a{-}1$ yields:

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

Remark. This proof is powerful since it works in any ring of characteristic p, not just integers mod p. The Frobenius map plays a central role in modern algebraic geometry and field theory, especially in the study of algebraic varieties over finite fields.