# Fermat's Little Theorem and Euler's Theorem

Alston Yam

## 1 Fermat's Little Theorem

**Theorem 1.1 – Fermat's Little Theorem (FLT)** Let $p$ be a prime, and let $a$ be any positive integer not divisible by $p$. Then

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

There's also an alternate formulation:

**Theorem 1.2 – Alternate form of FLT** Let $p$ be a prime and let $a$ be any positive integer. Then we have

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

We can see that to go from the first formulation to the second, we have essentially multiplied both sides by $a$. However to go from the second formulation back to the first, we must introduce the new condition that $\gcd(a, p) = 1$. This is because of the edge case of $p \mid a$.

"If something is worth proving once, it's worth proving twice."

Therefore, we will present two different proofs of FLT.

**Proof 1: Induction**

*Proof.* We will use a key lemma:

**Lemma 1:** $(a+b)^p \equiv a^p + b^p \pmod{p}$ (*Side note: this lemma is called "Freshman's Dream"*).
**Proof of Lemma:**

$$\begin{aligned}(a+b)^p &= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p \\ &\equiv a^p + b^p \pmod{p}\end{aligned}$$

This is because all of the "middle" terms have a binomial coefficient, and we know that $p \mid \binom{p}{i}$ for all $1 \leq i \leq p-1$. Therefore, all of the middle terms disappear when we take mod $p$, and the lemma is proven.

I claim $a^p \equiv a \pmod{p}$ for all integers $a$ and prime $p$. We induct on $a$.

*Base case:* $a = 1$

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

And we know this will hold true for any prime $p$.

*Inductive Hypothesis:* Assume that for $k = a$, we have $k^p \equiv k \pmod{p}$ for all primes $p$.

*Inductive Step:* Now we will consider $k + 1$. Notice that:

$$\begin{aligned}(k+1)^p &\equiv k^p + 1^p \pmod{p} \\ &\equiv k + 1 \pmod{p}\end{aligned}$$

Where the first line is from Lemma 1 and the second line is from the Inductive Hypothesis. Hence our induction is complete, and we have proven FLT. □

**Proof 2: Inverses**

*Proof.* Here I will claim that $a^{p-1} \equiv 1 \pmod{p}$, for positive integers $a$ that are coprime with $p$.

Let's consider the sets $\{1, 2, 3, \ldots, p-2, p-1\}$, and $\{a, 2a, 3a, \ldots, (p-2)a, (p-1)a\}$. The main claim is that the two sets are **permutations** of one another under mod $p$. Notice that the elements in the first set are all distinct under mod $p$, and since $a$ is coprime to $p$, we know that all the elements in the second set are not multiples of $p$. Therefore if we prove all elements in the second set are distinct under mod $p$, we would have proven the claim.

Suppose not. Then, we must have two elements such that $ia \equiv ja \pmod{p}$. Since $a$ is coprime to $p$, we may multiply both sides of the congruence by $a^{-1}$. This implies $i \equiv j \pmod{p}$ which is a contradiction.

So now we know the second set is a permutation of the first, under mod $p$. We will multiply all the elements in both sets together which implies

$$\prod_{k=1}^{p-1}(k) \equiv a^{p-1}\prod_{k=1}^{p-1}(k) \pmod{p}$$

However, $\gcd\left(p, \prod_{k=1}^{p-1}(k)\right) = 1$, so we can may multiply both sides by the inverse of $\prod_{k=1}^{p-1}(k)$ to imply

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

as desired. □

There is also a cool combinatorial proof that does not require any words, which you are welcome to look up.

# 2 Euler's Theorem

To recap, we define the Euler Totient Function again:

**Definition 2.1 – Euler's Totient Function** $\varphi(n)$ is defined as the number of positive integers $k$ with $k \leq n$ such that $\gcd k, n = 1$.

The most important result relating to this function is Euler's Theorem:

**Theorem 2.1 – Euler's Theorem** For any positive integers $n \geq 2$ and an integer $a$ coprime to $n$, we have

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

The statement of Euler's Theorem closely resembles FLT, and we might notice that this theorem is actually a generalisation of it. In fact, this lets us extend our computation from a prime mod to any general positive integer mod.

**Proof of Euler's Theorem**

*Proof.* The proof of Euler's Theorem is extremely similar to the proof by inverses for FLT, and you're encouraged to ponder it before reading on. For the sake of completeness, I will present a proof here.

Consider the set $S = \{k \mid \gcd(k, n) = 1\}$. We know $|S| = \varphi(n)$ by definition. Also consider the set $T = \{ak \mid \gcd(k, n) = 1\}$. We know that all elements in both $S$ ad $K$ are coprime to $n$, and we know that $K$ is a permutation of $S$ under mod $n$ (this can be proven in exactly the same way as the proof by inverse previously).

Now, we also multiply all elements in both sets together and equate them.

$$a^{|S|} \prod_{1 \leq k \leq n, \gcd(k,n)=1} (k) \equiv \prod_{1 \leq k \leq n, \gcd(k,n)=1} (k) \pmod{p}$$

Then we will multiply both sides by the inverse of the large producted term, to arrive at $a^{\varphi(n)} \equiv 1 \pmod{n}$, as desired. □

# 3 Problems

**Problem 3.1** Find

$$2^{50} \pmod{7}$$

**Problem 3.2** Let $a, b$ by integers and $p$ a prime. Show that $p$ divides $ab^p - a^p b$.

**Problem 3.3** Show that $n \mid 2^{n!} - 1$ for all odd integers $n$.

**Problem 3.4** A positive integer $n$ is called *groovy* if, for every positive integer $a$, $n^2$ divides $a^n - 1$ whenever $n$ divides $a^n - 1$.

Show that all primes are *groovy*.

**Problem 3.5** Show that for every positive integer $n$ not divisible by 2 or 5, there exists a multiple of $n$ all of whose digits are ones.