FERMAT'S LITTLE THEOREM, EULER'S THEOREM

YIPING DENG

Abstract. The aim of this paper is to give a concrete proof of Fermat's little theorem, as well as Euler-Fermat's theorem.

1. Introduction

Fermat's little theorem is one of the most fundamental theorem in number theory. It provides a method to test whether a arbitray natural number is a prime number. Euler's theorem, however, is the more general case for Fermat's little theorem.

This paper is aiming at proving Euler's theorem, and later use it to prove its special case, Fermat's little theorem.

Now we present Euler's theorem.

Theorem 1.1. [1] *if n and a are coprime positive integer, then*

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

2. Theorem 1.1 explained

To understand the theorem, proper definition of Euler's totient function should be introduced.

Definition 2.1. (Euler's Totient Function). Euler's Totient Function, denoted Φ, is the number of integers k in the range $1 \leq k \leq n$ such that $gcd(n, k) = 1$. [1]

Once given Definition 2.1, consider its special case that n is a prime number. $\Phi(p) = p - 1$. Such case is exactly Fermat's little theorem.

Theorem 2.2. *(Fermat's little theorem).*[1] *For any integer a relatively prime to prime p, then*

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

Hence, we shall only focus on the proof of Theorem 1.1.

3. Theorem 1.1 and Reduced Residue System

We shall see that Theorem 1.1 is closely connected with reduced residual system.

Definition 3.1. (Reduced Residue System). Any subset $R \subset \mathbb{Z}$ is called a reduced residue system modulo n if

(1) $\forall r \in R. gcd(r, n) = 1$
(2) $|R| = \Phi(n)$
(3) no two elements are congrulent modulo n

Consider the simplest Reduced Residue System, called Least Positive Coprime Residues.

Key words and phrases. Fermat's little theorem, Euler's theorem.

Definition 3.2. (Least Positive Coprime Residues). The Least Positive Coprime Residues modulo n is a Reduced Residue System that satisfies $\forall r \in R. 0 < r < n$.

It is intuitive that there is a bijection between two Reduced Residue System. A proof that there exists a bijection between Reduced Residue System and Least Positive Coprime Residues is sufficient.

Lemma 3.3. *(Bijection Between Reduced Residue System and Least Positive Coprime Residues). There exists a bijection $\omega : R \to L$, where R is a Reduced Residue System modulo n and L is a Least Positive Coprime Residues modulo n, and $\omega(r) \equiv r \pmod{n}$*

The proof for Lemma 3.3 is straight forward

Proof. First, we need to prove that ω will not map into any elements outside of L.

Assume $\exists r \in R. \forall l \in L. r \not\equiv l \pmod{n}$. We know that $\exists 0 \leq r < n. r \equiv p \pmod{n}$. Such $p \notin L$ $gcd(p, n) \neq 1 \implies gcd(r, n) \neq 1$. Contradiction.

For "Injectivity", we assume not. $\exists r_1, r_2 \in R, r_1 \neq r_2. \omega(r_1) = \omega(r_2)$ It implies that $r_1 \equiv l \equiv r_2 \pmod{n} \implies r_1 \equiv r_2 \pmod{n}$. Another Contradiction.

For "Surjectivity", it is sufficient to show that $|R| = |L| = \Phi(n)$.

Hence, such bijection exists. □

Also, there is another interesting property of Reduced Residue System.

Lemma 3.4. *Let $n > 0$. For any Reduced Residue System modulo n, denoted R, and any interger a coprime to n, $R' = \{ar \mid r \in R\}$ is also a Reduced Residue System.*

Proof for Lemma 3.4 is the following

Proof. First, $\forall r \in R. gcd(r, n) = 1$ and $gcd(a, n) = 1 \implies gcd(ar, n) = 1$ Also, assume $\exists r_1, r_2 \in R, r_1 \neq r_2. ar_1 \equiv ar_2 \pmod{n}$. This implies that $ar_1 - ar_2$ is divisible by n, also $gcd(a, n) = 1 \implies r_1 - r_2$ is divisible by $n \implies r_1 \equiv r_2 \pmod{n}$ □

4. Proof of Theorem 1.1

We can uses any Reduced Residue System to prove Theorem 1.1

Proof. Let n, a to be two coprime positive integer. Pick a Reduced Residue System modulo n, then $R' = \{a \cdot r \mid r \in R\}$ is also a Reduce Residue System modulo n. Pick a bijection ω. Thus

$$\prod_{r \in R} r \equiv \prod_{r \in R} \omega(r) \pmod{n}$$

$$\text{having } \prod_{r \in R} \omega(r) = \prod_{r \in R'} r \implies$$

$$\prod_{r \in R} r \equiv \prod_{r \in R'} r \pmod{n}$$

$$\prod_{r \in R} r \equiv \prod_{r \in R} a \cdot r \pmod{n}$$

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

□

References

[1] Annie Xu, and Emily Zhu. *Euler's Totient Function and More!*
http://www.math.cmu.edu/~mlavrov/arml/16-17/number-theory-09-18-16.pdf

P.O 182 College Ring 7, 28759 Bremen, Germany
E-mail address: y.deng@jacobs-university.de