Proofs, Generalizations and Applications of Fermat's Little Theorem

Zichuan Wang*

Department of Mathematics, Imperial College London, the United Kingdom

*Corresponding author: zichuan.wang20@imperial.ac.uk

Abstract. This paper introduces Fermat's little theorem (FLT), which says that any integer a raised to power p is congruent to a modulo p. This paper will give several proofs of FLT, using methods including number theory and group theory, together with generalizations of FLT in different directions. FLT is an important result in number theory and group theory. It has multiple generalizations and corollaries, and one of its corollaries is the foundation of RSA cryptography. The effort made trying to prove FLT stimulated researches in many fields in mathematics, and FLT is crucial and fundamental in research of modern cryptography.

Keywords: Number theory, Group theory, Fermat's little theorem, Euler's totient theorem.

1. Introduction

Fermat's little theorem (FLT) claims that for any natural number a, and any prime p, $a^p \equiv a \pmod{p}$. If a is coprime to p, then $a^{p-1} \equiv 1 \pmod{p}$. To help understand and apply FLT see [1], which gives multiple exercises on modular arithmetics, divisibility and FLT. It is mentioned that some primality tests work as an application of FLT: for a very large number n, it is extremely hard and time-consuming to conclude whether it is prime by trying every prime between 1 and $\sqrt{n}$, but if for some integer a, $a^n \bmod n$ does not equal a, then n is not prime by FLT [2]. Notice n need not be prime given it passes a test with a specific integer a, but this method can be applied on different integers to increase the confidence that n is prime.

Fermat was a pioneer in analytic geometry, number theory, probability theory, calculus, and was the first to give the integral of general power functions. Fermat discovered FLT while studying perfect numbers, but there was no record of his proof for FLT. The first formal proof of FLT was published by Euler in 1749, who also proposed and proved a generalization of the theorem, which will be mentioned later in this paper. More proofs have been proposed since then, and several of them are available at Ref. [3]. In addition, it is shown in Ref. [4] that a new proof, which is neither algebraic nor arithmetic, is constructed by using the fact that the polynomial $f(x) = 1 - x - dx^2 + \sum_{k\geq 3} a_k x^k$ can be written in the form

$$f(x) = \prod_{i\geq 1} \left(1 - m_k x^i\right) \tag{1}$$

in a unique way. Notably, this result is further proved elegantly [5]. Based on Burnside's lemma, a geometric proof is presented by coloring the vertices of a regular polygon [6]. This proof is suitable for intuitive visualisation.

The paper is organized as follows. Section 2 will give two common proofs of FLT in detail, in number theory and group theory respectively. Section 3 will propose several generalizations of FLT and prove some of them. In section 4, some applications of FLT are discussed. Finally, Section 5 is devoted to the conclusion of this paper.

2. Proofs of FLT by Various Methods

2.1. Number Theoretic Proof

This subsection is a proof of FLT using methods in number theory. A lemma is needed for the proof:

Lemma. For any prime p, and any $i \neq 0, i \neq p, p \mid \binom{p}{i}$.

Proof. Prove by contradiction. Assume $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is not divisible by p, then there must be some factor in the denominator dividing p which is not 1 or p, but this is impossible since p is prime.

□

Next, the theorem is proved by induction on a. The base case $a = 0$ and $a = 1$ are trivial. Assume for all $n < a$, for any prime p, one has

$$n^p \equiv n \pmod{p}. \tag{2}$$

Then for any prime p,

$$a^p = \big((a-1)+1\big)^p = \sum_{i=0}^{p} \binom{p}{i} (a-1)^i \tag{3}$$

$$= 1 + \binom{p}{1}(a-1) + \cdots + \binom{p}{p-1}(a-1)^{p-1} + (a-1)^p \tag{4}$$

as a binomial expansion.

Finally, one needs to show that the aforementioned summation is equivalent to a modulo p. Since $a - 1 < a$, the last term in Eq. 4 is equivalent to $a - 1$ modulo p by induction step, and by previous lemma, all other terms except the first term are divisible by p, thus are equivalent to 0 modulo p. Therefore, the sum in Eq. 4 is equivalent to $1 + 0 + \cdots + 0 + (a-1) = a$ modulo p, as claimed.

Notice this result could also follow from the fact, by similar proof as above,

$$(x+y)^p \equiv x^p + y^p \pmod{p}. \tag{5}$$

2.2. Group Theoretic Proof

The theorem could also be proven using group theory in multiple ways. In the followings, the group version of the theorem is stated and an example proof is given.

For any prime number p, consider the multiplicative group of the Z_p, where Z denote the integers, that is, $G = \{a \in Z : 1 \leq a \leq p-1\}$. For any $a, b \in G$, mutiplication of ab is defined as the residue of usual product ab divided by p. For $\forall a \in G, a^p = a$.

Proof. First the Bezout's identity is used to verify G is indeed a group. Notice multiplication modulo p fulfills closedness and associativity, 1 is the unit element, and for any $g \in G, g$ is coprime with p, thus by Bezout's identity, there are integers a, b satisfying $ag + bp = 1$. This is identical to $ag = 1$ taking modulo p, therefore any element in G has an inverse.

Now the theorem is proved as follow. For any element $a \in G$, consider the subgroup $\langle a \rangle = \{1, a, a^2, \cdots, a^{m-1}\}$, where m is the order of a. Clearly this subgroup has order m. By Lagrange's theorem, the order of $\langle a \rangle$ divides the order of G, that is, $m \mid p-1$. Assume $p - 1 = ms$ for some integer s, then

$$a^p = a \cdot a^{p-1} = a \cdot a^{ms} = a \cdot 1^s = a. \tag{6}$$

3. Generalizations of FLT

3.1. Euler's Totient Theorem

As a generalization of FLT, Euler published a proof of the following Euler's totient theorem in 1736: For any pair of coprime integers a and n, $a^{\phi(n)+1} \equiv a \pmod{n}$. Here $\phi(n)$ denotes Euler's totient function, defined as the amount of a such that $a \in Z,\ 1 \leq a < n$ and $\gcd(a,n) = 1$. One states the group version of the theorem and gives an example proof.

For any integer n, consider the multiplicative group of the ring Z_n, where Z denote the integers, that is $G = \{\, a \mid 1 \leq a < n, \gcd(a,n) = 1 \,\}$, with multiplication modulo n. For $\forall a \in G$, $a^{\phi(n)+1} = a$.

Proof. First verify G is indeed a group, by similar argument used in Section 2.2 to prove FLT by group theory. Also notice the size of G is precisely $\phi(n)$.

For any element $a \in G$, consider the subgroup $\langle a \rangle = \{1, a, a^2, \cdots, a^{m-1}\}$, where m is the order of a. Clearly this subgroup has order m. By Lagrange's theorem, the order of $\langle a \rangle$ divides the order of G, that is, $m \mid \phi(n)$. Assume $\phi(n) = ms$ for some integer s, then

$$a^{\phi(n)+1} = a \cdot a^{\phi(n)} = a \cdot a^{ms} = a \cdot 1^s = a. \tag{7}$$

Notice this proof is analogue to the second proof of FLT.

3.2. Further Generalization

Since the rings Z_p and Z_n has been studied, a natural question to ask is whether there are other rings with similar property. In Ref. [7], the authors generalized Euler's totient theorem to rings that has ideals $\{N_1, \ldots, N_r\}$ that the statements below hold:

1. N_r is the trivial subring $\{0\}$, and each N_i is included in N_{i-1};
2. For all $i, 1 \leq i < r, \exists t_i \geq 2, N_i^{t_i} \subset N_{i+1}$;
3. For all $i, 1 \leq i < r, \exists s_i \geq 1, s_i N_i \subset N_{i+1}$. and the prime factors of s_i are not smaller than t_i.

Also, Example 3.8 of Ref. 7 showed how its main result could derive Euler's totient theorem. The paper also contains some applications of its main result.

4. Applications of FLT

4.1. The AKS Test

AKS is a primality test based on FLT. M. Agrawal, N. Kayal and N. Saxena (AKS) developed the AKS test [8], and named it with abbreviations of their names. While FLT determines the primality of a natural number with probability, AKS is a deterministic test.

The test for an integer n works as followings:

1. If $n = a^b$ for natural numbers a and $b > 1$, n is COMPOSITE;
2. Find the smallest r such that $O_r(n) > (\log_2 n)^2$;
3. If $1 < gcd(a,n) < n$ for some $a \leq r$, n is COMPOSITE;
4. If $n \leq r$, n is PRIME;
5. For $a = 1$ to $\phi(r) \log_2 n$:

If $(x+a)^n \neq x^n + a \pmod{x^r - 1, n}$, n is COMPOSITE;

6. otherwise n is PRIME,

where

- $O_r(n)$ is the order of n modulo r, that is, the smallest value k such that $n^k = 1 \pmod{r}$;
- $\pmod{x^r - 1, n}$ means divide by the polynomial $x^r - 1$ and take the remainder.

In addition, Ref. [9] also gives examples of running AKS on several numbers.

4.2. the RSA Algorithm

RSA was created by and named after Ron Rivest, Adi Shamir and Leonard Adleman (RSA) in 1977 [10]. It is one of the most widely used public-key cryptosystems. Encryption and decryption using RSA involves a public key e, a private key d, and an auxiliary value n. e and n are published and known by everyone, but d is kept secret.

Starting with the original message m, with $0 \leq m < n$, and the public key e, calculate the encrypted message $k = m^e \pmod n$. Given the encrypted message k and the private key d, restore the original message $m = k^d \pmod n$. Combining both cases, it is found that

$$m^{ed} = m \pmod n. \tag{8}$$

Here, n, e and d must be chosen carefully to fulfill Eq. 8 for any integer m with $0 \leq m < n$. They are generated as follows:

1. Choose a pair of large primes p and q. Calculate $n = pq$ and $\phi(pq) = (p-1)(q-1)$;
2. Choose the private key e and public key d, such that $0 \leq e, d < n$ and $ed \equiv 1 \left(\mathrm{mod}\ \phi(pq)\right)$. Notice that to fulfill the second condition, both e and d need to be coprime with $\phi(pq)$.

The correctness of RSA is based on a corollary of Euler's totient theorem: $m^{ed} \equiv m \pmod n$ indeed holds.

Proof. Since $ed \equiv 1 \left(\mathrm{mod}\ \phi(n)\right)$, there is an integer s such that $ed = s\phi(n) + 1$. Thus

$$m^{ed} = m^{s\phi(n)+1} = m \cdot \left(m^{\phi(n)}\right)^s \equiv m \cdot 1^s = m \pmod n. \tag{9}$$

The second last step follows from Euler's totient theorem.

The safety of RSA is based on the following fact. Given two very large primes p and q, it is easy to obtain their product n. However, the reverse process, namely given the product n, try to find its two prime factors p and q, is extremely hard. Assume someone knowing only the auxiliary value n, and the public key d, but not the private key e, would like to derive the original message m from the encrypted message k. That is, to find the integer m such that $m^e = k \pmod n$, knowing only $ed \equiv 1 \left(\mathrm{mod}\ \phi(n)\right)$. Since the values of p and q are needed to calculate $\phi(n)$, one needs to first factorize $n = pq$. There is no known algorithm to obtain this in a reasonable time.

5. Conclusion

In this paper, an important number theoretical result, namely Fermat's little theorem (FLT), is proposed and then proved by multiple methods, including number theory and group theory. Research for new proofs of FLT has led to some, and could lead to more, useful branches of studies in mathematics. FLT has many important corollaries and generalizations, one of the most commonly used generalization is Euler's totient theorem, which could be further generalized to a class of rings with certain properties. Euler's totient theorem could be applied to multiple different fields and derive important results, such as the ASK primality test in number theory, and the RSA encryption algorithm in cryptography.

References

[1] Nga N. T. Application of Little Fermat Theorem Solving some Problems about Division. Turkish Online Journal of Qualitative Inquiry, 2021, 12(10): 5046-5059.

[2] Kappor Vivek, Gupta Rati. Hybrid symmetric cryptography approach for secure communication in web application. Journal of Discrete Mathematical Sciences and Cryptography, 2021, 24(5): 1179-1187.

[3] Wang Zhilan. Several Ways to Testify the Fermat's Little Theorem and Examples of Its Application. Journal of Langfang Teachers College (Naturnal Science Edition), 2009, 9(6): 11-13.

[4] Yuan Jinchen. Examples of Applying Fermat's Little Theorem. Studies in College Mathematics, 2020, 23(1): 49-50.

[5] Koblitz N. p-adic Numbers, p-adic Analysis, and Zeta Functions, 2nd ed., Springer-Verlag, New York, 1984.

[6] Beatty T., Barry M., Orsini A. A Geometric Proof of Fermat's Little Theorem. Advances in Pure Mathematics, 2018, 8: 41-44.

[7] de M. Hern´andez F. D., Melo C. A. H. Tapia-Recillas H. Fermat's Little Theorem and Euler's Theorem in a class of rings. Communications in Algebra, 2022, 50(7): 3064-3078.

[8] Li Gao, Chang Xiufang. New Method of Finding Prime Numbers. Journal of Shanxi Datong University(Natural Science Edition), 2021, 37(6): 33-35.

[9] Khumanthem MJ S., Singh Kh. M. Generalization of Fermat's Little Theorem. International Journal of Mathematics Trends and Technology, 2019, 65(7): 56-59.

[10] Wu Yandong. Symbolic Dynamics and Fermat's Little Theorem. College Math, 2009, 25(5): 120-123.