Fermat's Little Theorem and RSA Codes

Jaiden Goerlitz

Novemener 2022

1 Introduction

In this paper, we will discuss *Fermat's Little Theorem* and how it relates to RSA Codes. *Fermat's Little Theorem* was written by Pierre de Fermat, a French Mathematician, in 1640 in a letter to wrote Bernard Frenicle de Bessy in response to the question if some large numbers were prime. In this letter, Fermat did not write a proof of the theorem, but in 1736, Leonhard Euler wrote the first proof. While Fermat's Little Theorem was written in 1640 when electricity still had not been discovered, it still is highly prevalent today.

This little theorem discusses whether a number is prime or not, which is used in RSA codes. RSA, which stands for Rivest, Shamir, and Adleman, the inventors of the code, is an encryption algorithm that is widely used to transmit secured messages and data over the internet. Things like banking data, passwords, and private communications rely on the techniques of the RSA Code to remain secure when being transferred over the internet. Pierre de Fermat's "Little Theorem" is the key to it all.

2 Pierre de Fermat

Pierre de Fermat was born in France around 1607-1608. He was an attorney who had a knack for mathematics. While he was not a mathematical scholar, he corresponded with many famous mathematicians and scholars like Jean Beaugrand and Marin Mersenne, often challenging them to problems that he had already solved himself. Fermat even offended the famous René Descartes by calling Descartes' *La Dioptrique* "groping about in the shadows" in a letter to Mersenne.

In this paper, we will be discussing Fermat's Little Theorem, but Fermat developed many new mathematical ideas ahead of his time. Fermat never published his own work, but the mathematicians and scholars he corresponded with did. In the 1630s, Fermat sent two manuscripts to Mersenne about minima, maxima, and tangents for curved lines. We now know this as differential calculus. Sir Isaac Newton, the father of calculus, credited Fermat for his work and findings in differential calculus.

The most famous of Fermat's works is *Fermat's Last Theorem* which took over 350 years to solve. Fermat wrote in the margins of his copy of *Arithmetica* that he found discovered a great proof but there was not enough room in the margins to finish the proof. This half-finished proof would then stump mathematicians for centuries. In the margins, he only proved this for even numbers, not odd. This theorem would finally be proved by Andrew Wiles in 1994. Fermat's Last Theorem states if n is a whole number bigger than 2, the equation has no whole number solutions for x, y, and z.

$$x^n + y^n = z^n \tag{1}$$

In the 1640s, Fermat wrote a letter to Frenicle de Bessy, stating what would later be called *Fermat's Little Theorem*, without a proof in classic Pierre de Fermat fashion. Leonhard Euler later proved and generalized this theorem in 1736. Fermat's little theorem would give rise

to the Fermat primality test for the RSA algorithm.

3 Mathematical Background

Fermat's Little Theorem is involved in primality testing, which testing whether a number is prime or not prime. A prime number is a natural number greater than one and is not the product of two smaller natural numbers.

3.1 Modular Arithmetic

In the Little Theorem, modular arithmetic is used. I will be explaining modular arithmetic here and give examples. When we divide a positive integer a (the dividend) by another positive integer b (the divisor), the answer sometimes results in a quotient q and a remainder r.

In modular arithmetic, the operation is done by 'modulo' or 'mod'. Modulo is the remainder after diving one number by another. As an example, if we want to divide 31 by 5, we find $31 = 6 \times 5 + 1$ where 31 is the dividend, 5 is the divisor, the quotient is 6, and the remainder is 1. For this example, the remainder is 1, 31 mod 5 = 1, where 1 is the.

3.2 Congruence Modulo

The definition of the congruence modulo:

$$a \equiv b \pmod{n} \iff n|(a-b) \tag{2}$$

For example,

$$even\,numbers \equiv 0 \pmod{2} \tag{3}$$

$$odd\,numbers \equiv 1 \pmod{2} \tag{4}$$

$$91 \equiv 1 \pmod{9} \tag{5}$$

Another way to think of this is by the Remainder Lemma.

$$a \equiv b \pmod{n} \iff (a \div n)remainder = (b \div n)remainder \tag{6}$$

For example,

$$30 \equiv 12 \pmod{9} \tag{7}$$

This is true because 30 divided by 9 equals a quotient of 3 with a remainder of 3 and 12 divided by 9 is 1 with a remainder of 3. We can say that the Congruence Modulo is symmetric because

$$a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n} \tag{8}$$

We can also say it is transitive because

$$a \equiv b \, and \, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n} \tag{9}$$

3.3 Fermat's Little Theorem

Fermat's Little Theorem states that if p is prime, then

$$a^p \equiv a \, mod \, p \tag{10}$$

for all integers that are not divisible by p. One other way Fermat's Little Theorem states: Let p be any prime number and a belong to {1, 2, . . . , p-1}. Then

$$a^{p-1} \equiv 1 \pmod{p} \tag{11}$$

We will present an example to further explain the theorem. Let p=7. We verify Fermat's little theorem for a=3 and then for a=6. For the example, we will use

$$a^{p-1} \equiv 1 \pmod{p} \tag{12}$$

$$3^{7-1} \equiv 3^6 \equiv 729 \equiv 1 \pmod{7} \tag{13}$$

$$a = 6 \;\; 6^7 - 1 = 6^6 = 46,656 = 1 \pmod{7} \tag{14}$$

Another way to think of these examples is if we were to divide 729 by 7 we would have a remainder of 1 and if we were to divide 46,656 by 7 we would have a remainder of 1.

3.4 Proof

Assume p is a prime number and p does not divide a. Every integer is congruent to one of 0, 1, 2,..., *p-1 (mod p)*. We need to only focus on nonzero congruence classes because *0 (mod p)* contains all the multiples of p (and p does not divide a). So, focus on 1, 2,..., *p-1*. Multiply all of these by a:

$$a, 2a, ..., (p-1) * a \tag{15}$$

Claim 1: None of these is congruent to 0 *(mod p)*. Suppose for contradiction that:

$$r * a \equiv 0 \mod p \tag{16}$$

$$p | r * a \tag{17}$$

This is impossible since p does not divide a and r is less than p.

Claim 2: These are distinct *(mod p)*, that is, no two are congruent to each other. Pick

two values from the list **16**, r^*a and s^*a where r and s are integers with r$\neq$ s and

$$0 < r < p \tag{18}$$

$$0 < s < p \tag{19}$$

Let's show that r^*a is not congruent to s^*a *(mod p)*

$$r * a - s * a = a(r - s) \tag{20}$$

By assumption, p does not divide a. But can p divide *(r-s)*?

$$0 < r < p \tag{21}$$

$$-p < -s < 0 \tag{22}$$

Hence:

$$-p < r - s < p \tag{23}$$

(r-s) cannot equal 0 because r $\neq$ s. So the claim is true.

$$p \not| (r - s) \Rightarrow a, 2a, ..., (p - 1) * a \tag{24}$$

$$1, 2, ..., (p - 1) \tag{25}$$

$$a * 2a. \ldots * (p - 1) \equiv 1 * 2 * ... * (p - 1) \mod p \tag{26}$$

$$\Rightarrow (p - 1)! * a^{p-1} \equiv (p - 1)! \pmod{p} \tag{27}$$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p} \quad \blacksquare \tag{28}$$

4 Fermat's Little Theorem and RSA Codes

RSA Codes, named for its developers, is an algorithm used for public key cryptography. Cryptography takes some secret key, which is then used to encode some information that transfers it from its readable form to an unreadable form. This unreadable information is sent to someone and then they can decrypt the information back to its readable form. This is the foundation of security systems in the modern and technological age. Cryptography keeps our personal information safe, passwords, banking information, and many other things secure.

A public-key cryptosystem is one in which someone places an encryption E into a public file. Then, someone else has a corresponding decryption key D and the details are not released to anyone else, making it very private. Using the D to decrypt the encrypted message, *(E(M))*, where M, is the message, applying D will make the message readable.

The RSA algorithm was the first public key encryption created, and it is still widely used today. It is most widely used for online payments and encrypted emails. One thing that made RSA so special was that people could "sign" their name so the receiver of the message could know who it was from.

In RSA encryption, a *public key* is made; this key is open to anyone. The only way this message can be decrypted once it has been sent is using the *private key.* In RSA, we have two large prime numbers p and q, a modulus $N = pq$, an encryption exponent e and a decryption exponent d, such that:

$$ed \equiv 1 \mod (p-1)(q-1) \tag{29}$$

The public key is the pair *(N, e)* and the private key is d. To encrypt message M,

$$C = M^e(\mod N) \tag{30}$$

and we want

$$M = C^d \mod N \tag{31}$$

We decrypt by raising the ciphertext C to the d power and reducing the result *Modulo N*.

One thing we must understand before showing how Fermat's Little Theorem relates to RSA is *Relatively Prime Numbers*. Two integers are relatively prime if they share no common positive factors except 1. For example, 12 and 13 are relatively prime because the only common factor they share is 1. On the other hand, 12 and 10 are not relatively because they share 1 and 2 as common factors.

Moving forward with this fact, for a positive integer n, define ϕ to be the number of integers less than n that are relatively prime with n. For example:

$$\phi(12) = 4, \tag{32}$$

because 11, 7, 5, and 1 are less than 12 and relatively prime to 12. Similarly,

$$\phi(5) = 4 \tag{33}$$

since 4,3, 2, and 1 are less than 5 and relatively prime to 5. So, for any prime number p we have $\phi(p) = p-1$. Now, Suppose the prime factorization of n is given by:

$$n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r} \tag{34}$$

We then can note:

$$\phi(N) = (p-1)(q-1) \tag{35}$$

Finally, we use Fermat's Little Theorem. If p is prime and p does not divide x, then

$$x^{p-1} \equiv 1 \pmod{p} \tag{36}$$

Using a generalization of Fermat's Little Theorem, known as *Euler's Theorem*, we can rewrite the above equation. If x is relatively prime to n then:

$$x^{\phi(n)} = 1 \pmod{n} \tag{37}$$

Using the claims from above, we can now decrypt a message. We want to show that

$$M = C^d = (M^e)^d = M^{ed} \pmod{N} \tag{38}$$

$$Recall : ed = 1 \mod (p-1)(q-1) \; and \; N = pq \tag{39}$$

$$\phi(N) = (p-1)(q-1) \Rightarrow ed = 1 \pmod{\phi(N)} \tag{40}$$

By the definition of *mod*, there is some k such that $ed - 1 = k\phi(N)$. We now have:

$$M^{ed} = M^{(ed-1)+1} = MM^{ed-1} = MM^{k\phi(N)} \pmod{N} \tag{41}$$

Finally, Fermat's Little Theorem (in the form of Euler's Theorem) can be applied to yield the desired result:

$$M^{ed} = M(M^k)^{\phi(N)} \equiv M \pmod{N} \tag{42}$$

So, using the public key *(N, e)* and the private key d, we can decrypt the message M.

5 Conclusion

Pierre de Fermat was an interesting man and scholar. He was an attorney who had a passion for mathematics. Fermat was a secretive man and often stumped other scholars. His most famous theorem, *Fermat's Last Theorem*, was ahead of its time. This theorem took centuries to prove. In contrast, Fermat's Little Theorem, developed in the 1640s, was proven in the 1730s by Euler.

In this paper, we explained and proved Fermat's Little Theorem. We also showed how Fermat's Little Theorem relates to RSA codes and the mathematics behind them. The applicability of Fermat's Little Theorem is still substantial to this day. This theorem helps us deliver messages we want to keep safe every single day, and the RSA algorithm is only growing and getting bigger, faster, and more complex. A lawyer from France impacted the world of mathematics, something he would not live to know, but his family and friends were able to share his great work with the world.