Applications of Fermat's Little Theorem

Noormal Samandari [a], Nazar Mohammad Nazari [a], Janat Akbar Olfat[a] , Rafiullah Rafi [b] , Ziaulhaq Azizi[b], Wali Imam Ulfat [c] , Ikramullah waqar [b] , Mansoor Zahirzai[b] , Mohammad Jawad Niazi[b]

[a] Department of Mathematics, Faculty of Science, Nangarhar University, Afghanistan

[b] Department of Physics, Faculty of Science, Nangarhar University, Afghanistan

[e] Department of Chemistry, Faculty of Science, Nangarhar University, Afghanistan

Correspondence E-mail : noormalsamandari9@gmail.com

Abstract: Fermat's Little Theorem that is used to simplify the progression of converting a power of a number to a prime modulus is known as the most crucial theorem in elementary number theory. The credit of this theorem goes to Pierre de Fermat. This theorem is an exclusive situation of Euler's theorem and is pretty helpful in application of number theory such as congruence relation modulo n and public-key cryptography. Compared to Fermat's Last theorem which notes that when $n > 2$, $x^n + y^n = z^n$ has no solutions $x.y.z \in N$.(Riehm & Dudley), Fermat's this theorem is titled as "little". Fermat's Last Theorem remained unsolved for several years in the field of mathematics. Fermat described this theorem some 350 years ago and Andrew Wiles proved it in 1995. It is simple to prove Fermat's Little Theorem, but it has a wide implication for cryptography.

Keywords: Euler's theorem, public-key cryptography, Fermat's Last theorem, Congruence

1. Introduction

The most significant of Fermat's correspondents in number theory was Bernhard Frenicle de Bessy (1605 – 1675), an official at the French mint who was renowned for his gift of manipulating large numbers(Riehm & Dudley, 1971). (Frenicle's facility in numerical calculation is revealed by the following incident: On hearing that Fermat had perposed the problem of finding cubes which when increased by their proper divisors become squares, as is the case with $7^3 + (1 + 7 + 7^2) = 20^2$, he immediately gave four different salutions; and supplied six more the next day.) though in no way Fermat's equal as a mathematician, Frenicle alone among his contemporaries could challenge him in number theory and his challenges had the distinction of coaxing out of Fermat some of his carefully guarded secrets(Armytage, 2013). One of the most striking is the theorem which states: if p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$. Fermat communicated the result in a letter to Frenicle dated October 18, 1640, along with the comment, "I would send you the demonstration, if I did not fear its being too long." This theorem has since become known as "Fermat's Little Theorem," to distinguish it from Fermat's "Great" or "Last" theorem." Almost 100 years were to elapse before Euler published the first proof of the Little Theorem in 1736. Leibniz however, seems not to have received his share of recognition; for he left an identical argument in an unpublished manuscript sometimes before 1683.(Riehm & Dudley, 1971)

Fermat's Little Theorem is so called to specify it from the famous "Fermat's Last Theorem," a result which has compromised mathematicians for over 300 years. Fermat's Last Theorem was only recently proved, with great difficulty, in 1994. Before proving the Little Theorem, we need the following result on binomial coefficients.

2. Significance of The Study

The study we conducted is about Fermat's Little Theorem and its applications. As a result of the study we reached the conclusion that the Fermat's Little Theorem is one of the most famous theorems in elementary number theory. This study also indicated that Fermat's Little Theorem is derived from Fermat's "Last" Theorem. Fermat's Little Theorem's application includes but are not limited to labor-saving device, testing the primality of given integer *n*, congruence relation modulo *n*, and public-key cryptography.

3. Review Of Related Studies

Michael O. Rabin (1990) conducted study on probabilistic algorithm for testing primality, they used fermat's Little Theorem to describe the primality of integers. **Mr. Shady Ayesh and Dr. Mohammed Dweib (2016)** conducted a study on SMA CRYPTOGRAPHY ALGORITHM DECRYPT MD5 SOLUTION, they describe and discuss a new algorithm of cryptography which makes the application in any type more secure and let all the users and administrators keep their critical data in safe. They depend on Md5 and RSA. **Sergey Nikitin (2018)** conducted a study on Eluer-Fermat algorithm and some of its applications. They used fermat's Little Theorem to prove the Euler-Carmichael function $s(r,n)$. **Giedrius Alkauskas (2009)** conducted study on classical proof of Fermat's Little Theorem by the use of properties of binomial coefficients. **Kevin Iga (2003)** conducted to proof Fermat's Little Theorem by use of dynamical systems.

.

4. Objectives of The Study

- To find out that which numbers have congruence relation modulo.
- To find out that how we can generate the public and private keys.

I. congruence relation modulo *n*

Theorem 1. If p is a prime, then $\binom{p}{i}$ is divisible by p for $0 < i < p$. Otherwise put $\binom{p}{i} \equiv 0(mod\ p)$ for $0 < i < p$.

For example, if we consider the Pascal's triangle, then we know that the 7th row of Pascal's triangle is 1 7 21 35 35 21 7 1. Here, $p = 7$ and the row itself consist of $\binom{7}{i}$ for $0 < i < 7$. Other than these, the numbers are$\binom{7}{i}$ for $0 < i < 7$ and we see that they are all divisible by 7, as predicted by the theorem.(Mathematics, 2016)

Theorem 2. (Fermat's Little Theorem (Riehm & Dudley, 1971)) If p is a prime number and a is any other natural number not divisible by p, then the number $a^{p-1} \equiv 1\ (mod\ p)$, which is also equivalent to $a^p \equiv a\ (mod\ p)$.

Proof. We begin by considering the first p-1 positive multiples of a; that is, the integers

$$a.\,2a.\,3a.\,\ldots\ .(p-1)a.$$

None of these numbers are congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that

$$ra \equiv sa(mod\ p).\ 1 \le r < s \le p-1$$

then a could be cancelled to give $r \equiv s(mod\ p)$. which is impossible. Therefore, the above set of integers must be congruent modulo p to $1.\,2.\,3.\,\ldots\ .p-1.$ taken in some order. Multiplying all these congruences together, we find that

$$a.\,2a.\,3a.\,\ldots\ .(p-1)a \equiv 1.\,2.\,3.\,\ldots\ .(p-1)(mod\ p).$$

whence

$$a^{p-1}(p-1)! \equiv (p-1)!\,(mod\ p).$$

Once $(p-1)!$ Is cancelled from both sides of the preceding congruence (this is possible since pł$(p-1)!$, our line of reasoning culminates in $p^{p-1} \equiv 1(mod\ p)$, which is fermat's theorem.

Remark 1. Fermat's Little Theorem can also be referred as:

If p is a prime number and a is any other natural number, then $a^p - a$ is divisible by p.

Example 1. Consider a prime p and any number a not divisible by that prime.

$$p = 5$$
$$a = 6$$

As per theorem we know, $a^{p-1} - a$ is divisible by p, so: $6^{(5-1)} - 6 = 1290$ which is a multiple of 5. For any p is a prime number the Fermat's Little Theorem state that, then $gcd(x.p) = 1$ and $x^{p-1} \equiv x(mod\ p)$. We may say $x^p \equiv x(mod\ p)$. For any integer x if the constraint $gcd(x.p) = 1$ is lifted. This last congruence will be referred to as a generalization form of Fermat's Little Theorem. Euler generalized Fermat's theorem as follows.

If $gcd(x.p) = 1.x^{\phi(n)} \equiv 1(mod\ p)$. where ϕ is Euler's phi function. Obviously, like Fermat's theorem, Euler's result cannot be extended to all integers x. In other words, congruence $x^{\phi(n)+1} \equiv x(mod\ n)$ is not always valid. For example, if $n = 10$, then congruence holds for all values of x, but if $n = 12.x = 2.6$ and 10 fail.

In this paper, we explore the following question: for what values of x is the congruence $x^{\phi(n)+1} \equiv x(mod\ n)$ valid, given any natural integer n with $n > 1$.When n is a prime number, this congruence is an extension of Fermat's Little Theorem and holds true for all x.

The authors believe that the results would be ideal issues to present in an introductory number theory course because they require just simple methods to show. This paper's terminology may be found in ((Riehm & Dudley, 1971)).

I. Euler's Generalization

Step I :(n is prime)

Theorem 3. Let p is a prime number, then show that when the congruence $x^{\phi(n)+1} \equiv x(mod\ p)$ is valid, when n is prime.

Proof. If n is prime, then

$$\phi(n) \equiv n - 1$$

Euler's generalization form it becomes

$$x^{\phi(n)} \equiv 1(mod\ n)$$

From Fermat's Little Theorem, we know that $x^{n-1} \equiv 1(mod\ p)$ $[When\ n\ is\ a\ prime],[gcd\ (x.n) = 1]$
Then here we have,

$$(x_1 + x_2)^n(x) = [x_1^n + \binom{n}{1} x_1^{n-1}x_2 + \binom{n}{2} x_1^{n-2}x_2^2 + \cdots + \binom{n}{2} x_1^{n-n}x_2^n](x) =$$
$$[x_1^n + x_2^n\ terms\ divisible\ (by\ n)](x)$$
$$=> [(x_1 + x_2)^n - (x_1^n + x_2^n)](x) = \big((\mathrm{x})\ terms\ divisible\ by\ n\big) => (x_1 + x_2)^n(\mathrm{x}) \equiv (x_1^n + x_2^n)(\mathrm{x})(\mathrm{mod\ n})$$
$$=> (x_1 + x_2 + \cdots + x_n)^n(x) \equiv (x_1^n + x_2^n + \cdots + x_n^n)(x)(mod\ n)$$

Putting $x_1 = x_2 = \cdots = x_n = x$

$$=> (x)^n(x) \equiv x \cdot x(mod\ n) => x^{n-1}(x) \equiv x(mod\ n) => x^{\phi(n)+1} \equiv x(mod\ n)$$

Example 2. Apply Euler's Theorem to Solve the following Problem

a) $for\ any\ integer\ x, x^{11} \equiv x(mod\ 2310)$

Ans.

a) Euler's theorem show that for $gcd(x.n) = 1$ has $x^{\phi(n)} \equiv 1(mod\ n)$.which is also relevant in this instance Fermat's Little Theorem $x^{p-1} \equiv 1(mod\ n)$. The exceptional case when $n = p$ is prime, let $n = 2310 =$ 2.3.5.7.11. Then, according to Fermat's Little Theorem,

$$x \equiv 1(mod\ 2)$$
$$x^2 \equiv 1(mod\ 3)$$
$$x^4 \equiv 1(mod\ 5)$$
$$x^6 \equiv 1(mod\ 7)$$
$$x^{10} \equiv 1(mod\ 11)$$

For x, the modules are relatively prime. Each power on the left once again congruent to 1, and so on.

$$x^{10} \equiv 1(mod\ 2)$$
$$x^{10} \equiv 1(mod\ 3)$$
$$x^{10} \equiv 1(mod\ 5)$$
$$x^{10} \equiv 1(mod\ 7)$$
$$x^{10} \equiv 1(mod\ 11)$$

Again, for x the modules are relatively prime. Multiply each of these by x to get $x^{11} \equiv x$ for all modulo and all integers x and all integers x. According to the Chinese remainder theorem

$$x^{11} \equiv x\ (mod\ 2.3.5.7.11)$$

For every integer x

step II: (n is not prime)

Theorem 4. Suppose that n be a positive natural number with prime factorization with $n = \prod_{i=1}^{k} p_i^{\gamma_i}$ for $1 \le i \le k$. If x is an integer, then $x^{\phi(n)+1} \not\equiv x(mod\ n)$ there exists at least one of $i,\ for\ \ which\ p_i^{\delta_i} | x\ and\ p_i^{\delta_i+1}\ Xx\ with$ $0 < \delta_i < \gamma_i$.

Proof. Assume that for each $i, p_i^{\delta_i} | x\ and\ p_i^{\delta_i+1}\ Xx\ have$ either $\delta_i = 0\ or\ \delta_i > \alpha_i$. We may presume that for any $\delta_i > \gamma_i$ for $1 \le i \le \gamma$ and $\delta_i = 0$ for $a + 1 \le i \le k$ since $x \equiv 0(mod\ p_i^{\gamma_i})$ for$1 \le i \le a$, we have got

$$x^{\phi(n)+1} \equiv x\big(mod\ p_i^{\gamma_i}\big) \qquad (i)$$

For $1 \le i \le a$. We have $gcd(x.p_i^{\gamma_i}) = 1$ for $a+1 \le i \le k$, which implies $gcd(x_m.p_i^{\gamma_i}) = 1$ for all positive integer m. By Euler's Theorem we also know $\phi(p_i^{\gamma_i})|\phi(n)$ for $1 \le i \le k$ so we have

$$x^{\phi(n)+1} = x^{\phi(n)} = \left(x^{\frac{\phi(n)}{\phi(p_i^{\gamma_i})}}\right)^{\phi(p_i^{\gamma_i})} \quad x \equiv 1 \cdot x \equiv x\left(mod\ p_i^{\gamma_i}\right) \qquad (ii)$$

From the identities (i) and (ii), we have the following congruence system:

$$x^{\phi(n)+1} \equiv x\left(mod\ p_1^{\gamma_1}\right)$$
$$x^{\phi(n)+1} \equiv x\left(mod\ p_2^{\gamma_2}\right)$$
$$\vdots \qquad \vdots$$
$$x^{\phi(n)+1} \equiv x\left(mod\ p_k^{\gamma_k}\right)$$

According to the Chinese Remainder Theorem, Now we can conclude that $x^{\phi(n)+1} \equiv x(mod\ n)$.

To proceed it, we assume that for $i, p_i^{\delta_i}|x \ \ and\ p_i^{\delta_i+1} Xx \ \ with\ 0 < \delta_i < \gamma_i$. Then we obtain $p_i^{\delta_i} Xx \ \ and\ p_i|x$; indicating that for $m > 1$,

$$x^m - x = x(x^{m-1} - 1) \not\equiv 0(\text{mod}\ p_i^{\gamma_i})$$

Now we have that for any $m > 1. x^m \not\equiv x(mod\ n)$ in this case, we have $x^{\phi(n)+1} \not\equiv x(mod\ n)$. This finding directly results in the 2 corollaries listed below.

Corollary 1. Suppose n is a natural number and x is an integer. If $x^{\phi(n)+1} \not\equiv x(mod\ n)$, then $x_m \not\equiv x(mod\ n)$ for every $m > 1$.

Corollary 2. Assume n is a natural number. If and only if n is that the product of distinct primes then $x^{\phi(n)+1} \equiv x\left(mod\ p_k^{\gamma_k}\right)$ for any integer x.

Example 3. Use Euler's Theorem to Solve the following problem. For any odd integer $x, x^{33} \equiv x(mod\ 4080)$.

Ans. Euler's theorem indication that for $gcd(x.n) = 1$ has $x^{\phi(n)} \equiv x(mod\ n)$,which is also relevant in this instance Fermat's Little Theorem $x^{p-1} \equiv 1(mod\ n)$. The special case when n is not prime. Let $n = 1729 = 3 \cdot 5 \cdot 16 \cdot 17$ Then, according to Fermat's Little Theorem,

$$x^2 \equiv 1(mod\ 3)$$
$$x^4 \equiv 1(mod\ 5)$$
$$x^8 \equiv 1(mod\ 16)$$
$$x^{16} \equiv 1(mod\ 17)$$

For x, the modules are relatively prime. Each power on the left once again congruent to 1, and so on.

$$x^{32} \equiv 1(mod\ 3)$$
$$x^{32} \equiv 1(mod\ 5)$$
$$x^{32} \equiv 1(mod\ 16)$$
$$x^{32} \equiv 1(mod\ 17)$$

Again, for x the modules are relatively prime. Multiply each of these by x to get

$$x^{32} \equiv x(mod\ 3)$$
$$x^{32} \equiv x(mod\ 5)$$
$$x^{32} \equiv x(mod\ 16)$$
$$x^{32} \equiv x(mod\ 17)$$

The first, second and fourth congruence hold for all integers x. Multiplication by x also makes the congruence hold for all integers x. The third is for all integers relatively prime to 16, where all integers are odd. According to the Chinese remainder theorem

$$x^{33} \equiv x\ (mod\ 3 \cdot 5 \cdot 16 \cdot 17\ )$$

For every integer x.

II. Fermat Little Theorem in RSA correctness

Fermat's Little Theorem can also be used to prove that RSA operates correctly and accurately. The abbreviation RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, the developers of this algorithm. RSA is a asymmetric cryptographic technique for sending and receiving sensitive information or messages (Rabin, 1980) (Ayesh & Dweib., 2016) (Nikitin, 2018).

Generating public key and private key

- Public Key: All network users are aware of it.

- Private Key: It is kept private and not revealed to others.

If we use A's public key for encryption, we need to decrypt using A's private key only. Now we will go through the process of generating public key and private key. A chooses two distinct primes p, p_1 and then computes $n = p \cdot p_1$, where n is used as the modulus for both keys. Then A finds the totient function n where:

$$\phi(\mathrm{n}) = (\mathrm{p} - 1)(p_1 - 1)$$

Now, A chooses $e \in \mathbb{Z}$, where $1 < e < \phi(\mathrm{n})$ such that e and $\phi(\mathrm{n})$ are relatively prime. The public key consists of $\{e\,.n\}$, which user A sends to user B. The public key will then be used by B to encrypt the data that must be transferred to A.

Let $d \in \mathbb{Z}$ be the private key, where $1 < d < \phi(\mathrm{n})$ such that,

$$e \cdot d \equiv 1(mod\ \phi(\mathrm{n}))$$

A computes d using extended Euclidean algorithm.(Raghunandan et al., 2020)

Example 4. Let p = 13 and $p_1 = 11$ be two primes numbers. Then,

$$n = p \cdot p_1 = 13 \cdot 11 = 143$$

Then,

$$\begin{aligned}\phi(\mathrm{n}) &= (\mathrm{p} - 1)(p_1 - 1)\\ &= (13 - 1)(11 - 1)\\ &= 12 \cdot 10 = 120\end{aligned}$$

Select any arbitrary integer e = 13, such that gcd(13,120) = 1. Computing d using $d \equiv e^{-1}\ (mod\ \phi(\mathrm{n}))$ or $ed \equiv 1\ (mod\ \phi(\mathrm{n}))$ we get, $13d \equiv 1\ (mod\ 143)$.

For some integer k, we need to find the number d that achieves $13d = 1 + 143k$. We can also write this as:

$$d = \frac{(1 + 120k)}{e}$$

For $k = 1$,

$$d = \frac{(1 + 120 \cdot 1)}{13} = 9.30$$

For $k = 2$,

$$d = \frac{(1 + 120 \cdot 2)}{13} = 18.53$$

For $k = 3$,

$$d = \frac{(1 + 120 \cdot 3)}{13} = 26.76$$

For $k = 4$,

$$d = \frac{(1 + 120 \cdot 4)}{13} = 37$$

Therefore, $d = 37$. As a result, public key $= \{e, n\} = \{13,143\}$ and private key $= \{d, n\} = \{37,143\}$.

Encryption using public key

User A shares the public key with B, keeping the private key secret. If B wants to send a message or information X to A, B first converts X to an integer such that $0 < x < n$ using a wadding scheme. Therefore, a plaintext x is encoded by computation(Simonson, 2005)

$$c = x^e (mod\ n).$$

Here, c is a encryption text.

Example 5. We have public key as {13,143} and private key as {37,143}.

Let the simple text be $x = 13$. Then,

$$\begin{aligned}c &= x^e (mod\ n)\\ c &= 13^{13} (mod\ 143)\end{aligned}$$

By using division algorithm, we can solve this as below:

$$\begin{aligned}13^{13} (mod\ 143) &= (13^2)^6 \cdot 13 (mod\ 143)\\ &= (26^2)^3 \cdot 13 (mod\ 143)\\ &= (104)^2 \cdot 104 \cdot 13 (mod\ 143)\\ &= 91 \cdot 104 \cdot 13 (mod\ 143)\\ &= 26 \cdot 13 (mod\ 143)\end{aligned}$$

$$= 52(mod\ 143)$$
$$=> c = 52$$

(Luciano & Prichett, 1987)

Decryption
B sends an encrypted text message to A. A decrypts the message using a cipher private key d and by calculation

$$x = c^d(mod\ n).$$

Example 6. We have $x = c^d(mod\ n)$

$$x = 52^{37}(mod\ 143)$$

By using division algorithm, we can solve this as below:

$$\begin{aligned} 52^{37}(mod\ 143) &= (52^2)^{18} \cdot 52(mod\ 143) \\ &= (130^2)^9 \cdot 52(mod\ 143) \\ &= (26^2)^2 \cdot 26 \cdot 52(mod\ 143) \\ &= 91^2 \cdot 26 \cdot 52(mod\ 143) \\ &= 130 \cdot 26 \cdot 52(mod\ 143) \\ &= 13(mod\ 143) \\ => x &= 13 \end{aligned}$$

5. Recommendation

- We can find the units digit of 3^{100} by the use of Fermat's theorem.
- with Fermat's Little Theorem we can confirm that some integers are absolute pseudoprimes.
- For any integer a, we can verify that a^5 and a have the same units digit.
- When the base of the exponentiation is allowed to be a non-integer, such bases we call Fermat factors. To find out that irrational factors Satisfying the Fermat's Little Theorem.
- To find out whether we can calculate labor-saving device in certain calculations with Fermat's Little Theorem.
- To find out whether we can test the primality of a given integer number.

6. Conclusion

Fermat's Little Theorem is generalized by Euler; we know that this theorem is a fundamental theorem in elementary number theory that facilitate the calculation of powers of integers modulo prime numbers. This theorem is specified Euler's theorem and is useful in elementary number theory's applications such as primality checking and labor-saving device in certain calculations.

References

Armytage, W. H. G. (2013). *The rise of the technocrats: A social history*. Routledge.

Ayesh, M. S., & Dweib., D. M. (2016). Sma Cryptography Algorithm Decrypt Md5 Solution. *International Journal of Advanced Research*, *4*(11), 290–296. https://doi.org/10.21474/ijar01/2081

Luciano, D., & Prichett, G. (1987). Cryptology: From Caesar ciphers to public-key cryptosystems. *The College Mathematics Journal*, *18*(1), 2–17.

Nikitin, S. (2018). Euler-Fermat algorithm and some of its applications. *Arizona State University*, *August*, 1–15.

Rabin, M. O. (1980). Probabilistic algorithm for testing primality. *Journal of Number Theory*, *12*(1), 128–138. https://doi.org/10.1016/0022-314X(80)90084-0

Raghunandan, K. R., Ganesh, A., Surendra, S., & Bhavya, K. (2020). Key generation using generalized Pell's equation in public key cryptography based on the prime fake modulus principle to image encryption and its security analysis. *Cybernetics and Information Technologies*, *20*(3), 86–101.

Riehm, C., & Dudley, U. (1971). Elementary Number Theory. *The American Mathematical Monthly*, *78*(7), 805. https://doi.org/10.2307/2318039

Simonson, S. (2005). Public Key Cryptography. *MAA NOTES*, *68*, 109.