Mathematics Analysis and Approaches HL

PROVING FERMAT'S LITTLE THEOREM

INTRODUCTION

The aim of this investigation is to prove Fermat's little theorem. The topic is of significance because by making use of Fermat's Little Theorem; it becomes possible to analyze big-digit numbers and determine whether they are prime or composite numbers. This topic is important to me because I am very interested in learning more about prime numbers. What makes prime numbers so interesting to me is because of their usefulness and vast properties in mathematics such as the whole number line can be produced using prime numbers. I have read a vast amount of math number theory related to prime numbers, such as the Eratosthenes Sieve Algorithm and The Prime Number Theorem. For instance Sieve's Algorithm allows anyone to quickly identify prime numbers up to a limit. That is possible by crossing out the numbers composite by the prime numbers .On the other hand, the prime number theorem discovered by Jacques Hadamard allows mathematicians to determine the amount of prime numbers until a specific range. The most unique characteristic of prime numbers is that the further away you go, the rarer they become and thus harder for us to identify them. This is why Fermat's little theorem is so famous and relevant. We are able to try out numbers and prove whether they are prime or composite with a simple expression, and that is why it was even more exciting for me to carry out this project.

FERMAT'S LITTLE THEOREM[1]

Fermat's little theorem states: Let p be a prime number, and a be and integer.
Then a^p-a is always divisible by p.

In **modular arithmetic notation**, this theorem can be written as:

$$a^p \equiv a \bmod p$$

This notation has the meaning that if we take an integer a and set it in power of p (where p is a prime) and then a^p is divided by p, we would be able to obtain the same **remainder** as if we divided a by p.

For instance; let's take the integer a=4 and the prime number p=3.
From Fermat's little theorem we would obtain:

[1] "Fermat's Little Theorem | Brilliant Math & Science Wiki." https://brilliant.org/wiki/fermats-little-theorem/. Accessed 5 Jul. 2020.

$$4^3 \equiv 4 \bmod 3$$

Now if we write these numbers in the remainder form we would get:

$$4^3 = 64$$

$64 = 3 \times 21 + \boldsymbol{1}$

$4 = 3 \times 1 + \boldsymbol{1}$

As it can be clearly seen in the example above, the remainder of 64 and 4 after divided by 3 is 1, meaning that for this scenario the theorem works.

The modular arithmetic notation form is going to be used in order to prove the theorem to be true, however in order to get into that much detail, we need to first understand what modular arithmetic is and what its principles are.

PRIME NUMBERS[2]

A prime number *p* is a natural number greater than 1, that is not a product of two smaller natural numbers. A natural number greater than 1 that is not a prime number is called a composite number.

For instance, number 7 is a prime number because the only ways of writing it as a product is through , 1×7 or 7×1. However 6 is a composite number because despite the fact that it can be written as 6×1; and 1×6, it can also be written as 3×2 and 2×3.

Prime numbers are **central in number theory**, because every natural number greater than 1 is either a prime itself or can be factorized as a product of primes that is *unique* up to their order.

MODULAR ARITHMETIC[3]

Modular arithmetic is a system of arithmetic that works with integers and their remainders. In modular arithmetic numbers (integres) reach upon a fixed quantity, which is called modulus in order to leave a remainder.

---

[2] "Prime Numbers | Brilliant Math & Science Wiki." https://brilliant.org/wiki/prime-numbers/. Accessed 21 Feb. 2021.
[3] "Modular Arithmetic | Brilliant Math & Science Wiki." https://brilliant.org/wiki/modular-arithmetic/. Accessed 5 Jul. 2020.

A famous usage of modular arithmetic is a 12-hour clock. For instance; if the time right now happens to be 9 o'clock in the morning , after 4 hours it is going to be 1 o'clock in the evening and not 13:00 o'clock. In the same way in this example the remainder of 13 modulus 12 is going to be 1.
In other words: $13 = 12 \times 1 + 1$.

The way how we would right this example in the modular arithmetic expression is going to be :

$$13 \bmod 12$$

This means that if we take the number 13 and divide it with the number 12 (or modulus 12) we would obtain the remainder equal to 1.

From this example we can get into a more general expression of modular arithmetic which is:

$$a \bmod N \quad \text{where a;N are integers}$$

CONGRUENT INTEGERS IN MODULAR ARITHMETIC

Two integers a and b are said to be congruent with each other if a mod N and b mod N have the same remainder after they have been divided by N. The word congruent is going to be meant through the usage of the symbol ≡ .

In this case the we say that:

$$a \equiv b \bmod N \quad \text{where a;b;N are integers}$$

For instance let's take again the modulus N as 12 and the inger a = 15 and the integer b= 27.

Then:

$$15 \bmod 12$$ will have a remainder of 3

and

$$27 \bmod 12$$ will have a remainder of 3

Since 15 mod 12 and 27 mod 12 have the same reminder we can say that

$$27 \equiv 15 \bmod 12$$

ADDITION IN MODULAR ARITHMETIC

When the remainder of *a mod N* is added to the remainder of *b mod N*, then it becomes possible to say that this remainder is equal to the remainder of *a+b mod N*.

Another way to present this principle is:

$$a \bmod N + b \bmod N = a+b \bmod N$$

For instance; let's take the integers *a=9* and the integer *b=10* and let's take *N=8*. By this we obtain:

$$9 \bmod 8 + 10 \bmod 8 = 9+10 \bmod 8$$

9 mod 8 has a remainder of 1 ($9 = 8\times1 + 1$)

10 mod 8 has a remainder of 2 ($10 = 8\times1 + 2$)

9+10 mod 8 = 19 mod 8 has a remainder of 3 ($19= 8\times2 + 3$)

So the remainder of *9 mod 8 = 1* plus the remainder of *10 mod 8 = 2* gives us the remainder of *19 mod 8* which is equal to 3 (2+1).

In case that the sum of the remainders of two integers mod N is equal to the modulus or bigger than the modulus, then you need to take the mod N of that integer too.

MULTIPLICATION IN MODULAR ARITHMETIC

When the remainder of *a mod N* is multiplied to the remainder of *b mod N*, then it becomes possible to say that this remainder is equal to the remainder of $a \times b \bmod N$.

Another way to present this principle is:

$$a \bmod N \times b \bmod N = a \times b \bmod N$$

For instance; let's take the integers $a=9$ and the integer $b=10$ and let's take $N=8$. By this we obtain:

$$9 \bmod 8 \times 10 \bmod 8 = 9 \times 10 \bmod 8$$

9 mod 8 has a remainder of 1 ($9 = 8 \times 1 + 1$)
10 mod 8 has a remainder of 2 ($10 = 8 \times 1 + 2$)
$9 \times 10 \bmod 8 = 90 \bmod 8$ has a remainder of 2 ($90 = 8 \times 11 + 2$)
So the remainder of *9 mod 8 = 1* multiplied to the remainder of *10 mod 8 = 2* gives us the remainder of *90 mod 8* which is equal to 2 (2×1).

In case that the multiplication of the remainders of two integers mod N is equal to the modulus or bigger than the modulus, then you need to take the mod N of that integer too.

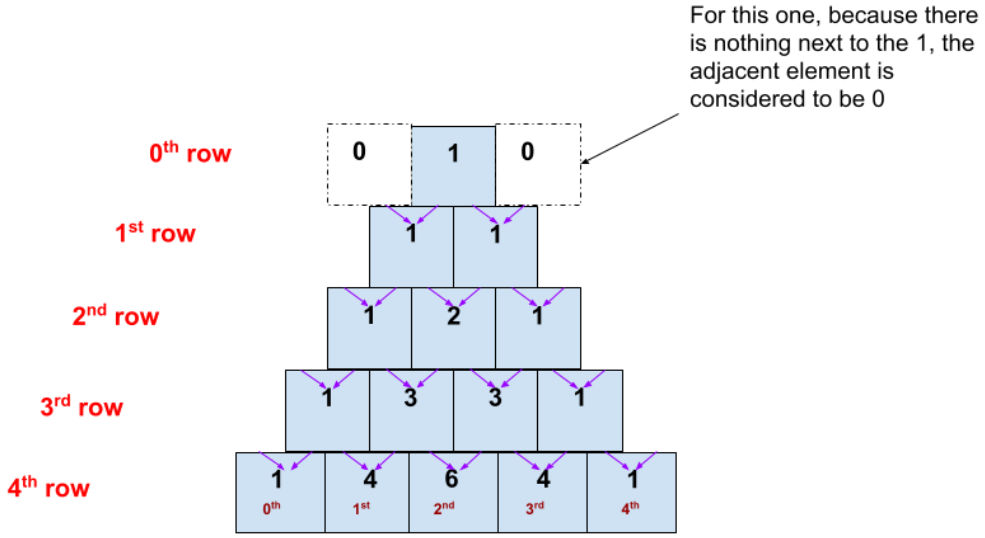
Note: The modulus N of a=0 is always going to have a remainder of 0.

PASCAL'S TRIANGLE[4]

Pascal's triangle is a triangular array of the binomial coefficients constructed by summing adjacent elements in preceding rows. It rises in combinatorics, algebra and probability theory. It was named after the 17th century French mathematician, Blaise Pascal.

[4] "Pascal's Triangle | Brilliant Math & Science Wiki." https://brilliant.org/wiki/pascals-triangle/. Accessed 27 Dec. 2020.

Fig. 1 Representation of the Pascal's triangle



It begins by placing a 1 at the top center of the triangle as shown in **Fig.1**. The following row down of the triangle is formed by summing adjacent elements in the previous row. Pascal's triangle has an *infinite number of rows*.

The top row is considered to be the **0th row** . The following one is the 1st, and the next one the 2nd and so on (infinitely). In each row the leftmost element is the **0th element of the row**, and the n to the right of that is the 1st element and then the 2nd and so on.

In less words each n^{th} (from n=0) row has an n+1 element/s.

Another way to find the binomial coefficients in the Pascal's Triangle is through ${}_nC_r$ formula, where n is the row and r is the element of the row.

$${}_nC_r=\frac{n!}{r!(n-r)!};\ (n,r\geq 0)$$

Example:

The binomial coefficient in the 2nd row and 2nd element of the row is:

$${}_2C_2=\frac{2!}{2!(2-2)!}=\frac{2\times 1}{2\times 1(0)!}=\frac{2}{2}=1$$

Now we can use ${}_nC_r$ in order to find the binomial coefficient of the expansion terms for every binomial in every power.

$(x+y)^n = x^n + nx^{n-1}y + \ldots + {}_nC_r\, x^{n-r}\, y^r + \ldots + nxy^{n-1} + y^n$ (The Pascal's triangle is going to be used later in the proof.)

PROVING FERMAT'S LITTLE THEOREM[5]

Lets restate what Fermat's little theorem says again:

Fermat's little theorem states: Let p be a prime number, and a be and integer.

Then a^p-a is always divisible by p.

$$a^p \equiv a \bmod p$$

1) First we are going to deal with $\{0\}$ or in other words when $a=0$.

   $a=0 \Rightarrow 0^p \bmod p = (0 \times 0 \times \dots \times 0) \bmod p \equiv 0 \bmod p \times \dots \times 0 \bmod p = 0$

   Thus $0^p \bmod \equiv 0$ □

2) Now we are going to prove the theorem to be prove for $a \in Z^+$

   For nonnegative a we give a proof by induction on a

   Basic step

   $a=1$;

   $a^p \bmod p = 1^p \bmod p = (1 \times \dots \times 1)^p \bmod p \equiv 1 \bmod p \times \dots \times 1 \bmod p \equiv 1 \bmod p$

   $1 \bmod p = a \bmod p$ □

   Assumption

   For a random but fixed $a \in Z^+$, $a \geq 1$ we assume that $a^p \bmod p \equiv a \bmod p$ is true.

   Inductive step

   Investigate for $a+1$: $(a+1)^p \equiv a+1 \bmod p$.

   Then using binomial theorem can write $(a+1)^p$ as:

$$(a+1)^p = \sum_{r=0}^{p} {}^pC_r \, a^{p-r}$$

$$(a+1)^p = {}^pC_0 \, a^p + {}^pC_1 \, a^{p-1} + {}^pC_2 \, a^{p-2} + \dots + {}^pC_{p-1} \, a + {}^pC_p \, 1$$

   Another thing we know is that ${}^nC_r$ or in this case ${}^pC_r$ can be written as:

$${}^pC_r = \frac{p!}{r!(p-r)!}$$

   This means that all the coefficients in front of a are $\equiv 0 \bmod p$ except for the first one and the last one.

$${}^pC_0 \, a^p + \dots + {}^pC_p \, 1$$

   Are the only ones *not* divisible by p

[5] "Fermat's Little Theorem | Brilliant Math & Science Wiki." https://brilliant.org/wiki/fermats-little-theorem/. Accessed 6 Jul. 2020.

The reason why is because ${}^{p}C_0$ and ${}^{p}C_p$ in Pascals Triangle are always equal to *1*.

$$ {}^{p}C_0 = \frac{p!}{r!(p-r)!} = \frac{p!}{0!(p-0)!} = \frac{p!}{p!} = 1 $$

$$ {}^{p}C_9 = \frac{p!}{p!(p-p)!} = \frac{1}{0!} = 1 $$

So the only part not divisible by *p* is:

$$ a^p + 1 \text{ so:} $$

$$ (a+1)^p \equiv (a^p+1) \bmod p $$

$$ (a^p+1) \bmod p \equiv a^p \bmod p + 1 \bmod p $$

However in the beginning of the Theorem proof , we have considered $a^p \bmod p$ as true and equal to $a \bmod p$. So:

$$ (a^p+1) \bmod p \equiv a^p \bmod p + 1 \bmod p \equiv a^p \bmod p + 1 \bmod p; $$

and

$$ a^p \bmod p + 1 \bmod p \equiv a^p + 1 \bmod p \ \square $$

Final Statement

Since a=1 was shown to be true and it was also shown that if the statement is true for some $a^p \bmod p \equiv a \bmod p$, *it is also true for* $(a+1)^p \equiv a+1 \bmod p$, $a \in Z^+$, *it follows by the principle of mathematical induction that the statement is true for all positive integers.*

3) Now we are going to prove the theorem to be true for $a \in Z^-$.

$(-a)^p \equiv (-a) \bmod p$.

Prime numbers can be:

- *Even:* only the number 2
- *Odd:* every other prime number like 1, 3, 5 ,7 etc.

Even:

$(-a)^2 = a^2 \equiv -(a) \bmod 2$; However we have proven that positive integers as a^2 are congruent with $a \bmod 2$, hence proving that $a^2 \equiv a \bmod 2$. □

Odd:

$(-a)^p \equiv (-a) \bmod p \Rightarrow -1 \times a^p \equiv -1 \times a \bmod p$ (so now we can remove -1) $\Rightarrow a^p \equiv a \bmod p$. □

Quod erat demonstrandum (Q.E.D)

APPLICATION OF THE THEOREM[6]

Fermat's little theorem has authentic applications in the world. Similar to other number theory based upon prime numbers, this one is likewise used in the RSA-cryptography. RSA is an encryption algorithm used from websites and companies to transmit messages over the internet securely. RSA is based upon the difficulty of factoring large composite numbers and hence allowing the person who knows the factoring numbers to see the message. Because of the difficulty in breaking RSA, it becomes usable everywhere encryption is needed, such as online shopping, banking, password exchange, etc. RSA strength is based upon the size of the number. For instance, when the number is 155 digits, it is insecure and simple for someone to factor the number since computers have innovated more and more over time. For instance, Israeli researchers were able to extract a 4096-bit number in under an hour.

CONCLUSION

Even though Pierre de Fermat wrote Fermat's little theorem in 1640, it required 96 years for Euler to provide the first proof of this theorem. Over the years, the theory has proven to possibly be one of the most important theorems in mathematics, making it possible for everyone to determine whether a number is prime or composite. Because of the proof of this theorem, Euler was able to come up with his phi function or Euler's totient function where it becomes possible to find the number of integers up to a given integer n that are relatively prime to n. Fermat's theorem has also led to new ideas and ways to improve the theorem itself, such as the AKS[7] - primality test, published in 2002 at the Indian Institute and Technology Kanpur. This test allows us to determine whether any given number is prime or composite, just as Fermat's theorem. A further extension to the theorem and the IA would be the investigation of the Rabin-Miller primality test.[8]Like Fermat's little theorem, this test allows us to determine whether a number is prime. Compared to Fermat, this theorem relies more upon the unproven Riemann hypothesis[9] instead of the modular arithmetic, thus making Fermat's theorem more reliable since the Riemann hypothesis has not been proven yet. The only limitation that Fermat's little theorem provides is that it proves to be va1lid only with prime numbers.

---

[6] "RSA Encryption | Brilliant Math & Science Wiki." https://brilliant.org/wiki/rsa-encryption/. Accessed 6 Jul. 2020.
[7] "AKS primality test - Wikipedia." https://en.wikipedia.org/wiki/AKS_primality_test. Accessed 27 Dec. 2020.
[8] "Miller–Rabin primality test - Wikipedia." https://en.wikipedia.org/wiki/Miller%E2%80%93Rabin_primality_test. Accessed 27 Dec. 2020.
[9] "Riemann hypothesis - Wikipedia." https://en.wikipedia.org/wiki/Riemann_hypothesis. Accessed 27 Dec. 2020.