_ Prime numbers and their analysis

Yousef Mohamed Hassan & Abdelrahman Mohamed Abdelbaky

Abstract- Primes are the fundamental units of the integer's universe. Prime numbers play a significant role in number theory. This paper comprehensively examines prime numbers and explains various prime types and testing procedures. Mathematicians and many other fields of science and technology still find prime numbers fascinating. Moreover, the usage of primes in nature and real life has been considered. It also has crucial uses for computer engineers and programmers in solving a wide range of myriad real problems. From antiquity to today, scientists have studied mathematical reasoning to comprehend prime numbers; prominent intellectuals labored on this topic before it was abandoned. Twenty different types of prime numbers have been presented in this paper, and corresponding Python applications are provided, along with the Python library. Due to the complexity of the prime factorization NP issue, an asymmetric technique has been utilized for crucial exchange between the client and the server. Prime factorization uses graphs to examine the relationship between the size of the Composite number and the amount of time it takes to Factorize. Three significant applications of prime numbers have also been covered in this paper. Mathematicians regarded prime numbers as "building blocks in contrasting natural numbers" and the most challenging aspect of Mathematics. Understanding natural numbers depend on the knowledge of prime numbers. Insight into the prime will facilitates comprehension of the supporting sciences. The prime numbers play a vital role in securing information technology hence the promotion of the NTIC. Every year, there is a price for persons who will discover the biggest prim. Using the methods provided in this article, we can calculate all the largest prime numbers that modern computers are capable of calculating.

keywords- Fermat, cryptography, python, number theory

I. INTRODUCTION

The prime number is a natural number with only two divisors: itself and one. Every integer bigger than one is either a prime number or can be represented as the product of prime numbers, according to the fundamental theorem of arithmetic, also called the unique factorization theorem or the unique-prime-factorization theorem. For instance, 15 is not a prime number but still an integer; it must be expressed using the product of prime numbers, i.e., 3×5. Many people find the question "Whether one is prime or not?" puzzling. Below is a metaphor that will help illustrate this point. One can be written as $1 = 1 \times 1 \times 1 \times \ldots \times 1$; it is not prime because this violates the prime number theorem. In the modern technological era, the study and application of prime numbers are in high demand due to the wide variety of exciting qualities. This is especially true with the advent of computers, a super computational capacity. No one can say for sure when prime numbers were first introduced. However, some Papyrus writings from the ancient Egyptians, dating back more than 3,500 years, seem to be the earliest hard evidence. But they had different definitions for primes and composites than what we talk about today. On the other hand, it is well-established that around 300 B.C.E., ancient Greek mathematicians began investigating prime numbers and their characteristics. Then Euclid, the great Greek mathematician, proposed that there exist an infinite number of primes. This achievement can be taken as the beginning of the abstract theory of prime numbers.

Using a paradox, Euclid demonstrated that the number of primes is infinite. Well-known mathematicians have since made significant advancements in our knowledge of primes. Pierre de Fermat made numerous contributions to mathematics. Still, he is best known today for "Fermat's last theorem," a 380-year-old issue involving primes that were only solved by Andrew Wiles 28 years ago. In the 18th, Leonhard Euler proved several conclusions, and 19th century, Carl Friedrich Gauss, Pafnuty Chebyshev, and Bernhard Riemann

had enormous advances, especially in the distribution of primes. This culminated with the still unsolved 'Riemann Hypothesis,' often considered the most important unsolved problem in all mathematics. The "Riemann Hypothesis" is one of the millennium problems. Despite its age, studying prime numbers remains an exciting and challenging topic.
The study of prime numbers dramatically benefits from such a strong foundation in mathematics. It's possible to generate many different kinds of prime numbers at random with the help of "Primelibpy", a library dedicated to prime numbers. In security systems such as online transactions and online communications, prime numbers are used in the asymmetric algorithm. The algorithm uses a 64-bit key, which necessitates two 32-bit prime values. The analysis of prime generation on several systems and factorization of composite numbers with Traditional, Fermat's Theorem, and Pollard's Rho has been accomplished.

2. FERMAT'S LAST THEOREM

Fermat's last theorem, also called Fermat's great theorem, the statement that there are no natural numbers (1, 2, 3,) x, y, and z such that xn + yn = zn, in which n is a natural number bigger than 2. For instance (3, 4, 5), (5, 12, 13). Even as early as 1500 B.C., the Babylonians had figured out the answer (4961, 6480, 8161).
Nowadays, Fermat is remembered mainly as a number theorist, in fact, as perhaps the most famous number theorist who ever lived. Thus, it comes as a surprise to learn that Fermat was a lawyer and an amateur mathematician at most. In the margin of a copy of Diophantus' Arithmetical, Pierre de Fermat noted in 1637 that the equation xn + yn = zn does not have any solutions in positive integers if n is greater than 2. This proposition shall be referred to from here on out as (F LT) n, he claimed to have a remarkable proof. This is questionable for verious reasons.
To begin with, his son, after his father's death, published this statement without his permission. Second, Fermat never mentions this supposed proof in his subsequent communication, even when discussing the instances n = 3, 4. So, it's probably just an off-the-cuff remark that Fermat forgot to cross out. Of course (F LT) n implies (F LT) αn, for α any positive integer, and so it suffices to prove (F LT)4 and (F LT) ` for every prime number ` > 2

3. Types of Prime Number

Even though there are 76 distinct kinds of prime numbers, just Twenty of the more significant ones are shown below.

3.1 Mersenne Prime:

Mersenne prime is defined as a prime number that is one fewer than a power of two. Adding one to the prime number is the simplest method to ensure, as a result, constantly forms a value in the form of 2n. They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17th century. The algebraic structure of Mersenne prime $\boldsymbol{Mn}$ **is** $\boldsymbol{Mn = 2n - 1.}$ where n is also a prime.

3.2 Twin Prime:

A twin prime is a prime that is either 2 less than or 2 more than another prime. Except for (3,5), every twin prime pair consists of the form (6n - 1,6n + 1), where n is a natural number. To be simple, a couple of prime numbers (such as 3 and 5 or 11 and 13) differ by two.

3.3 Wilson Prime:

A Wilson prime [1] is p such that $(p - 1)! \equiv (-1)^*(mod\ p2)$. Or, more simply, a prime integer p such that p2 divides (p 1)! + 1, where "!" signifies the factorial function. For example, 5, 13, and 563 are all Wilson primes. The value of the subsequent Wilson prime after 563 is bigger than 2 * 1013.

3.4 Factorial Prime:
It is a prime number, one more or less than any factorial. It can be expressed as $n! \pm 1$.
The first factorial primes are: 2, 3, 5, 7, 23, 719, 5039, 39916801, 479001599**.**

3.5 Sophie Germain prime:
A prime number p is a Sophie Germain prime [1] if $2 \times p + 1$ is also prime. The number $2 \times p + 1$ is associated with a Sophie Germain prime and is called a "safe prime". This represents the "initial case" of Fermat's theorem. A good illustration is the number 11, and $2 \times 11 + 1 = 23$ is its associated safe prime.

3.6 Wieferich prime:
A Wieferich prime is a prime number p such that p^2 divides 2^p−1 − 1 linking these primes with Fermat's little theorem, which claims that every odd prime p divides 2^p−1 −1.

3.7 Circular Prime:
It is a prime number with the property that the number generated at each intermediate step when cyclically permuting its (base10) digits will be prime, such as “1193”. Since 1931, 9311, and 3119 are also prime numbers, this one forms a circle of primes.

3.8 Cousin Primes:

Prime numbers of pair which differs by 4 with each other is known as cousin primes.
It's important to keep in mind that 7 is the only number with two sets of prime cousins (3, 7) and (7, 11).

3.9 Palindromic Prime:
A palindrome is a term used for words or numbers which reads the same from the forward or backward. Also, if a prime number is also a palindrome, we call it a Palindromic Prime all Palindromic primes have an odd number of digits except 11, because palindromic number with an even number of digits is a multiple of 11,131, 151 are Palindromic primes.

3.10 Reversible Prime:
Alternatively, it is called "emirp," which is means spelt backward. Reversible primes are those that may be transformed into another prime by just looking at them backwards or in the other direction.
For example, for a three-digit number abc which also written as, $d = a \times 10$^2 + $b \times 10 + c \times 1$. To be a reversible prime, cba must be a prime number, which can be represented as, $drev = c \times 10$^2 + $b \times 10 + a \times 1$. Here if d is reversible prime than e will be prime number.

3.11 Balanced Prime:
If we take out the Arithmetic means of prime numbers above & below a given integer, and if the arithmetic mean itself is a prime number, then we have a Balanced Prime.
In general, it is expressed as $pk = \sum$^n i=1(pk-i^+pk+i) /2n
Where pk-i and pk+i are also prime numbers and pk is i^th mode Balanced Prime, k is index of ordered prime.
For example, 5 is a balanced prime of mode 2 as it is the average of 3 and 7. Indeed (3 + 7) ÷ 2 = 5.

3.12 Pythagorean Prime:
In Fermat’s theorem, the sum of two squares yields an odd prime p, given as; $p = x$^2 + y^2 with x and y integers if and only if $p \equiv 1(mod\ 4)$.
Pythagorean Primes refer to the prime numbers for which this is true. They are the odd prime numbers p for which $\sqrt{p}$ is the length of the hypotenuse of right angle triangle with integer legs, and p itself is the hypotenuse of a primitive Pythagorean triangle.

For example, √13 is the hypotenuse for legs 3 and 2, also 13 is the hypotenuse for legs 12 and 5.

3.13 Permutable Prime:
Permutable primes remain prime when their digits are jumbled. Permutable primes are also circular primes, and like circular primes, they are likely to be only finite in number such as(13,17,37,79,113,199,337)

3.14 Wagstaff Prime:
Wagstaff number [9] in general form is given by
$Q\ (b, n) = bn+1/b+1$
Wagstaff prime p is a prime number given by $p = 2q+ 1/3$, where q is an odd number.

3.15 Fermat Pseudo primes to Base a:
A Fermat pseudo prime to base a, written $psp(a)$, is a composite number n such that, $a\text{^}n-1 \equiv 1(mod\ n)$. For an integer $a > 1$, Fermat Pseudoprimes are composite numbers which can be directly used in security algorithm but some pseudo primes have more than Four factors so algorithm should be such that it generates only primes which have only Four factors (one, the number itself and other two primes).

3.16 Semi Prime:
A natural number whose factors only contains 1 & two same or different prime number then that number is called Semi Prime. It can also be termed as the product of two prime numbers and if both are same then Semi-Prime number is the square of any prime number. If Sp is a Semi prime, then it is given below;
$Sp = \{p1 \times p2, p1\ and\ p2\ are\ different\ prime\ numbers$
P^2, p is the prime number

3.17 Primorial prime:

Primorial is a function similar to the factorial function, but here we do successive multiplication of only prime numbers. It is symbolized as #.
For nth prime number Pn, the primordial Pn # is defined as

$$P_n\# = \prod_{k=1}^{n} P_k$$

A primorial prime is a prime number of the form $Pn\# \pm 1$. Here $P\ n\# + 1$ is also known as Euclid Number (En) and $Pn\# - 1$ is also known as Kummer number (En). First few primordial primes are 2,3,5,7,29,31,211.

3.18 Good Prime:

Prime number $p(n)$ is a good prime[2] if $p(n) > p(n - i) * p(n + i)$, for all values of '$i$' is from $1\ to\ n - 1$.
For instance, we take a series of prime numbers like 11, 13, 17, 19 and 23 then
17^2 > 13 * 19 and, 17^2 > 11 * 23 this is fulfilled so 17 is a good prime. Series of good prime is 5,11,17,29,37,41

3.19 Gaussian Prime:
The Gaussian integer is a complex no. who's real and imaginary parts are in the form of integers. The complex plane is basically an integral domain. Gaussian integers are written
as Gp.
$Gp = x + iy, where\ x\ \&\ y\ are\ integers$
Gaussian primes are given if two conditions are satisfied:

(i) One of x *or* y is zero & the absolute value of the complex number is a prime number of the form $4n + 3$ (n is an integer).
(ii) Both x & y is nonzero and $|x2 + y2|$ i.e., modulo of Gaussian number is a prime number. (Not in form of $4n + 3$) If Gaussian primes less than some specific numbers are plotted on the Argand diagram, then it will form a circular pattern and lies within some radius equal to $\sqrt{x2 + y3}$. This pattern has been used for tablecloths and tiling floors.

3.20 Truncatable Prime

• Right truncatable prime number which does not have zero at any place (A zero free number). When the last right of that number is removed then we obtain the prime number.
For example, 31379 → 3137 → 313 → 31 → 3 all are primes.

• Left Truncatable Prime is a prime number, whose leading left digit is successively removed, then all resulting numbers are prime.
For example, 983 → 83 → 3 all are primes.

• Left and right truncatable prime is a prime number which remains prime if the leading (left) & last (Right) digits are simultaneously successively removed down to a one or two-digit prime.
For example, 739397 → 3939 → 93 all are primes.

One fact is that there are exactly 83 Right truncatable primes, 4260 Left truncatable primes, 920720315 Left-and-Right truncatable primes.

4. Distribution of prime numbers

We are aware that there are an unlimited number of primes, but can we provide an equation for locating the nth prime? It remains an issue that must be resolved. There is no consistent pattern of primes across composites; hence, they are random. In 1792, however, Gauss estimated a pattern that is the way to the prime number theorem.
In number theory, the Prime Number Theorem (PNT) describes the asymptotic distribution of the prime numbers. The PNT provides an overview of the distribution of primes among the positive integers. It formalizes the intuitive notion that primes become less frequent as their sizes increase.
In PNT, it states that, $\pi(x)$ as the prime-counting function that gives the number of primes less than or equal to x, for any real number x, where $\boldsymbol{\pi(x)} \sim \frac{x}{\ln x}$

In addition, it asserts that if a random number is taken from the range 0 to some enormous integer, the result is a prime.

N, the probability that the chosen integer is prime is about $\mathbf{1} / \boldsymbol{ln(N)}$, where $\boldsymbol{ln(N)}$ is the natural logarithm of N.

Consequently, a random number with at most 2n digits has about half the probability of being a prime as a random integer with at most n digits (for sufficiently large n).

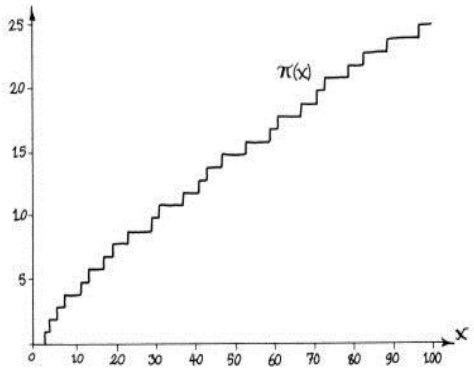

Figure 1. The diagram that illustrates the distribution of primes

5. Time Analysis

The following table provides an examination of how prime numbers are generated on various platforms. Below is a table containing the time required to create prime numbers between 1 and 106. Printing the prime numbers between 1 and 107 (up to 26 bits) using a C program took 7228 seconds.
As a key, modern security systems use 128-bit integers. Based on the table, Python is much slower than all other languages, except for R. However, the code is lot shorter when using Python, and millions of developers choose Python over other languages since troubleshooting is easier with Python.

O.S.	C	C++	Java	Python	R	
MacOS X	80.98 s	94.51 s	50 s	1826.23 s	2137 s	
Window10	114.31 s	106.29 s	82.57 s	3731.84 s	4586 s	
Ubuntu	99.62 s	102.21 s	88.67 s	2427.34 s	4094.88 s	

Table -1: Time to generate prime number between 1 to 10^6

6. Factorization Comparison

Prime factorization is an NP-Problem; thus, several cryptographic systems are based on it. There are numerous ways available for factoring prime numbers. This research may be broken down into three basic phases. In the first layer, we have created large integers using a novel method. After generation, the factorization algorithms are conducted, including the new technique. In the last step, the performance of the algorithms is assessed.

The factorization of composite numbers has been a fascinating topic of research from early times, and there exist techniques such as Sieve of Eratosthenes (276 – 194 BC). Also, by the spreading usage of modern cryptographic systems which some are built on the difficulty of factoring, like RSA, the factorization problem has been a studying area.

The following Graph shows the Composite numbers vs. Time to factorize that number is shown by the Traditional (Trial Division), Fermat Factorization and Pollard Rho Factorization method.

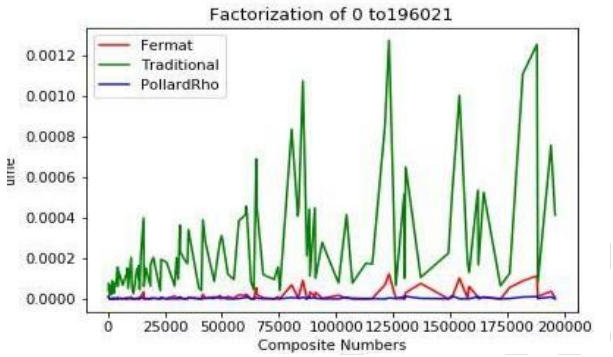

Chart -1: Prime factorization from 0 to 200000

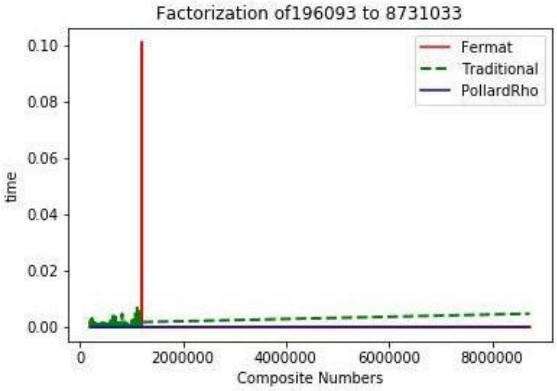

Chart -2: Prime factorization from 0 to 8000000

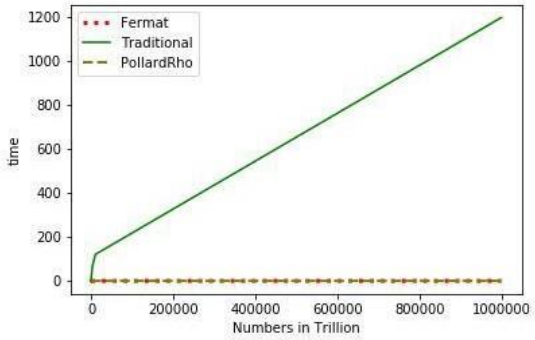

Chart -3: Prime factorization from 0 to 1000000

7. Applications

7.1 Cryptography

Prime numbers are used in cryptography since it is difficult to factor them. This indicates that it is impossible to determine the prime factors of a composite number without first knowing its factors. This makes it impossible for someone to intercept and decipher a communication without the correct key.

When Fermat, well known for Fermat's Last Theorem, found a sophisticated way for determining whether a number is prime or composite, his colleagues were unable to appreciate the value of the proof. Discoveries regarding prime numbers were lauded solely for the sake of discovery — for revealing and making sense of the hidden complexities in mathematics, and for solving an intriguing puzzle — despite the fact that they did not contribute any substantial solutions to real-world issues.

There are two types of cryptosystems, symmetric and asymmetric. Asymmetric encryption and decryption are accomplished using two distinct keys. The public may access the public key.

Only the secret key may reveal the private key. Prime numbers are essential to the RSA algorithm. If prime factorization is simple, this approach may be broken. As a result, brute-force searches cannot be used to discover the key. RSA is a component of the algorithm in real-time security systems.

Steps for RSA algorithm:

A. Generate two large prime number p = 17, q = 13

B. Calculate $n = p \times q = 17 \times 13 = 221$

C. Find Euler's Totient Function (ch-8.2).Calculate $f(n)$ = $(p-1) \times (q-1) = 16 \times 12 = 192$

D. Select e such that e is relatively prime to $f(n)$ = 192 and less than $f(n)$; we choose e = 7.

E. Generate d such that $d \times e \equiv 1 (mod\ 192)$ and $d < 192$. The correct value is d = 55 because 55 × 7 = 385 = (2 × 192) + 1; d can be calculated using the extended Euclid's algorithm.

F. Public Key = $\{e, n\}$ = {7 ,221}

G. Private Key = $\{d, n\}$= {55 ,221 }

H. Assume plaintext M = 88

I. Encryption: Cipher text: $CM = Ce\ mod\ n$ = $887\ mod\ 221 = 62$

J. Decryption: Plain text: $M = Cd\ mod\ n = 6255\ mod\ 221 = 88$

Value of n and e are public. If we know factor of n then we can easily generate "d". After calculating "d" we can encrypt and decrypt a message. Prime factorization is very difficult that is why this system is used in cryptography.

7.2 Biology to anticipate the predator-prey model for a specific insect

In certain biological situations, primes are utilized to anticipate the predator-prey model for a specific insect species to have a greater survival rate; this insect species is known as "Cicada." They essentially hide underground for an extended duration to avoid predators. Then, they emerged only for feeding and mating purposes.

For example, if the periodical cicada (another term given to them in the United States) has 17 years, they stay underground for 16 years and appear every 17 years.
Here, the usage of prime numbers comes into play; the analysis identifies another 13-year span. What justifies the choice of such a high prime number? Additionally, they may choose the numbers 3, 5, or other. The solution may be found in multiples of prime integers such as 13 or 17. For example, if the life cycle of predator is 4 years and for the cicada, if it is 17 years, then in order to consume cicada for their food, the predator has to wait

for 68(17 × 4) years, i.e. 4th generation will meet with a cicada. This way, nature uses the application of prime numbers to save itself from the foe.

Conclusion

This is a deep study of prime numbers. In this article, the properties of prime numbers, different types of prime numbers, and their real-life applications as well as the applications in nature have been analyzed. Furthermore, different types of primality tests have been studied and MATLAB programs for each of those tests have been constructed. Moreover, a summary of previous work regarding primes has been included.

REFERENCES

[1].“The Book of Prime Number Records” - Paulo Ribenboim; Springer. ISBN 978-1-4684-9938-4

[2].“PRIME NUMBERS: The Most Mysterious Figures in Math” - David Wells; John Wiley & Sons, Inc. ISBN-13 978-0-471-46234-7

[3].“Survey on prime numbers” by A.R.C.De Vas Gunasekara, A.A.C.A.Jayathilake and A.A.I.Perera

[4]. William Stallings, “Cryptography and Network Security: Principles and Practice”

[5] Dr. Chris K. Caldwell, University of Tennessee , USA, Prime pages .

[6] Ajay Chaudhuri, Introduction to Number Theory.

[7] W. Eric Weisstein, "Lucas Number." From *Math World*--A Wolfram Web.

[8] Zachary S. McGregor-Dorsey, Methods of Primality Testing.

[9] Manindra Agrawal, Is n a Prime Number? , IIT Kanpur, March 27, 2006, Delft.

[10] M.R Adhikari, Text Book of Linear Algebra: An Introduction to Modern Algebra, 2004 Allied publishers Pvt Ltd.

[11] David J. Wirian, Institute of Information & Mathematical Sciences, Massey University at Albany, Auckland, New Zealand, Research paper on Parallel Prime Sieve: Finding Prime Numbers.

[12] Chris K. Caldwell, Yeng Xiong – “What is the smallest prime?” , Journal of Integer Sequences, Vol. 15 (2012), Article 12.9.7 .

[13] D. Goldfeld, The Elementary Proof Of The Prime Number Theorem: An Historical Perspective.

Yousef Mohamed Hassan, email: 1020081@stemegypt.edu.eg

October Math Gems, STEM High school for boys – 6th of October.