Prime numbers and their analysis

Mit Patel[1], Alok M. Patel[2] , R.B.Gandhi[3]

[1] UG Student, Computer Department, B.V.M. Engineering College, V.V.Nagar, Anand, Gujarat, India

[2] UG Student, Electrical Department, B.V.M. Engineering College, V.V.Nagar, Anand, Gujarat, India

[3]Associate Professor, Mathematics Department, B.V.M. Engineering College, V.V.Nagar, Anand, Gujarat, India

Abstract

Prime numbers have always remained a matter fascination to the mathematicians, and many scientific and technical communities. Also, it has paramount applications for computer engineers to solve myriad real problems. In this paper, twenty different types of prime numbers have been covered and Python programs to generate them are given, with the Python library. Asymmetric algorithm has been used for key exchange between client and server; it is significant because of the prime factorization NP-problem. In the encryption system, prime number play the major role to crack security system where prime factorization is necessary, so the analysis for the same has been shown in this paper, by generating prime numbers on various platforms (Windows, Os X, and Ubuntu) and by prime factorization using three different algorithms. In prime factorization, the comparison between Composite numbers vs. the time it takes to Factorize is plotted on the graphs. Two of the major applications of prime numbers which are Cryptography and Cicada have also been covered in this paper.

Key Words: *Python, Python Library, Cryptography, Cicada, Brute Force, R programming, Asymmetric Cryptosystem and Factorization.*

1. Introduction

A prime number is a number which has only two factors, 'one' and 'the number itself'. The **fundamental theorem of arithmetic**, also called the unique factorization theorem or the **unique-prime-factorization theorem**[4] states that: "Every integer greater than one, either is a prime number or can be represented as the product of prime numbers, uniquely. For example, 15 is an integer which is not the prime number, so it has to be written using the product of prime numbers, i.e. 3×5. 'Whether one is prime or not?' is bit confusing for many people. This can be understood by the below metaphor. One can also be written as $1 = 1 \times 1 \times 1 \times \dots \times 1$, which contradicts the fundamental theorem of arithmetic, so it is not prime. With the invention of computers, a super computing power, in the technological era of today, prime numbers, their study and applications are greatly in demand because of so many peculiar properties they possess. No one knows that when does the prime number introduced. But, the first concrete evidence appears to be some Papyrus writings of the ancient Egyptians from over 3500 years ago[5]. The ancient Greeks were the first to introduce the prime numbers in their academic curriculum. Since then, many of the most famous mathematicians have made important contributions to our understanding of primes. Pierre de Fermat made many discoveries and is famous these days for '**Fermat's last theorem**'[8], a 380-year-old problem connected to primes which was solved by Andrew Wiles just 25 years ago. Leonhard Euler proved many results in the 18^{th} century, and in the 19^{th} century, there were huge advances due to Carl Friedrich Gauss, Pafnuty Chebyshev, and Bernhard Riemann, particularly on the distribution of primes. This culminated with still unsolved 'Riemann Hypothesis', often referred to as the most important unsolved problem in all of mathematics. The 'Riemann Hypothesis' is one of the millennium problems. Thus study of prime numbers is still very interesting and challenging. Because of such deep routed in mathematics, study of prime numbers is contributed immensely. The prime library, **primelibpy** provide much functionality for generating random specific types of prime numbers. In security system such as; online transactions and online communications prime numbers are being used in asymmetric algorithm. Currently, 64 bit key has been used for algorithm, for that two 32 bit prime numbers are required. So, the analysis of prime generation on various platform has been carried out, and factorization of the composite numbers using Traditional, Fermat Theorem, and Pollard Rho.

2. Types of Prime Number

There are in total 76 types of prime numbers[6], but in this paper twenty most important prime numbers are illustrated.

2.1 Mersenne Prime:

A Mersenne prime[2] is a prime number that is one less than a power of two. The easiest way to check is by adding one to the prime number and the result must be in the form of 2^n. The algebraic form of Mersenne prime M_n is $M_n = 2^n - 1$.

Program:https://colab.research.google.com/drive/14jMUpuWFMEroIWAfzHEOgHRYb5hLuguq

2.2 Twin Prime:

A Twin prime[1] is a prime number that is either 2 less or 2 more than another prime number. Every twin prime pair except (3,5) is in the form of $(6n - 1, 6n + 1)$, where n is a natural number.

Program:https://colab.research.google.com/drive/1faAK_yxySwzUYTv7RLdaYjWyBeVDTsli

2.3 Wilson Prime:

A Wilson prime[1] is p such that

$(p-1)! \equiv (-1)(mod\ p^2)$.

In other words, a prime number p such that p^2 divides $(p-1)!+1$, where "!" denotes the factorial function. Some Wilson primes are $5, 13, and\ 563$. The next Wilson prime after 563 is greater than 2×10^{13}.

Program:https://colab.research.google.com/drive/1AuJ5K6Ic2y7mbIrMNzs4Q3f7kGgF-sOs

2.4 Sophie Germain prime:

A prime number p is a Sophie Germain prime[1] if $2 \times p + 1$ is also prime. The number $2 \times p + 1$ associated with a Sophie Germain prime is called a safe prime. It is the "first case" of Fermat's theorem. As for example, 11 is a Sophie Germain prime and $2 \times 11 + 1 = 23$ is its associated safe prime.

Program:https://colab.research.google.com/drive/1VJRrHLCKKLdbUPnB_k6IJx9TfSmoxWN7

2.5 Wieferich prime:

A Wieferich prime[1] is a prime number p such that p^2 divides $2^{p-1} - 1$, therefore connecting these primes with Fermat's little theorem, which states that every odd prime p divides $2^{p-1} - 1$.

Program:https://colab.research.google.com/drive/1308JMgr9yp7Y0SZr7wR5SoYvOr3fZF4_

2.6 Factorial Prime:

It is a prime number which is one more or less than any factorial. It can be expressed as $n! \pm 1$. For example $2, 3, 5, 7, 23$.

Program:https://colab.research.google.com/drive/1e5w-RqaT8CQbI5o9BPWL0Uws6UUqhgpS

2.7 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. Example is 1193. It is a circular prime, since $1931, 9311$ & 3119 are also prime.

Program:https://colab.research.google.com/drive/1sjQBtzDYNXr8shj45xMbYL1PIerlCCV8

2.8 Balanced Prime:

If we take out the Arithmetic means of prime numbers above & below a specific number then that and if the Arithmetic mean value itself is a prime number and that value is known as Balanced Prime. In general, it is given as

$$p_k = \frac{\sum_{i=1}^{n}(p_{k-i}+p_{k+i})}{2n}$$

Where p_{k-i} and p_{k+i} are also prime numbers and p_k is i^{th} mode Balanced Prime, k is index of ordered prime.

For instance, 5 is a balanced prime of mode 2 as it is the average of 3 and 7. Indeed$(3 + 7) \div 2 = 5$.

Program:https://colab.research.google.com/drive/155mAW_WSEMjNpaCA_26YogleZFvIT_h4

2.9 Cousin Primes:

Prime numbers pair which differs by 4 with each other is known as cousin primes. Note that 7 is the only number that has two pairs of cousin prime, $(3, 7)$ and $(7, 11)$.

Program:https://colab.research.google.com/drive/1sLL_H5q2pWKkks7TWXNpX45LkZWa0olW

2.10 Palindromic Prime:

A palindrome is a term used for words or numbers which reads the same from the forward or backward. And a prime number which is a palindrome then it is known as Palindromic Prime[2]. Except 11, all palindromic primes have an odd number of digits, because palindromic number with an even number of digits is a multiple of 11,$131, 151$ are Palindromic primes.

Program:https://colab.research.google.com/drive/1DkIpsbOsQsHSdO3LTetjqd8nBTOSXQnY

2.11 Reversible Prime:

It is also termed as 'emirp' means spelled backward. When any prime number is reversed or see from way back and if we obtain another prime than it is Reversible Prime. 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, $d_{rev} = c \times 10^2 + b \times 10 + a \times 1$. Here if d is reversible prime than e will be definitely prime number.

Program:https://colab.research.google.com/drive/1RxTYbPNwLReOpzoY2z21NcUukueu3CrJ

2.12 Pythagorean Prime:

In Fermat's theorem, the sum of two squares gives an odd prime p, expressed as; $p = x^2 + y^2$ with x and y integers if and only if $p \equiv 1(mod\ 4)$.The prime numbers for which this is true are called Pythagorean Primes. They are the odd prime numbers p for which $\sqrt{p}$ is the length of the hypotenuse of a right-angle triangle with integer legs, and p itself is the hypotenuse of a primitive Pythagorean triangle.For example, $\sqrt{13}$ is the hypotenuse for legs 3 & 2, also 13 is the hypotenuse for legs 12 & 5.
Program:https://colab.research.google.com/drive/1qY-B_ftd_6O9sR0aYIufeGHF-s2t2EyL

2.13 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. For example; 13,17,37,79,113,199,337.

Program:https://colab.research.google.com/drive/1v50JY7Ke4ZJ3FD_iIBPyX-IhyZvyW46c

2.14 Wagstaff Prime:

Wagstaff number[9] in general form is given by

$$Q(b, n) = \frac{b^n+1}{b+1}$$

Wagstaff prime p is a prime number given by $p = \frac{2^q+1}{3}$, where q is an odd number.

Program:https://colab.research.google.com/drive/1pmuRjURSypJqlkVr6y8u3eG2uDwa0vJ3

2.15 Fermat Pseudo primes to Base a:

A Fermat pseudo prime to base a, written $psp(a)$, is a composite number n such that, $a^{n-1} \equiv 1(mod\ n)$. 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). For example, visit Fermat Pseudo prime[13].

Program:https://colab.research.google.com/drive/1X1yd6r1UHCqIy5G2cy5ZIhI2wdu852Ko

2.16 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 S_p is a Semi prime then it is given below;

$$S_p = \begin{cases} p_1 \times p_2\,, & p_1 \text{ and } p_2 \text{ are different prime numbers} \\ p^2, & p \text{ is the prime numbers} \end{cases}$$

Program:https://colab.research.google.com/drive/16jTpxY90UfbmKeSN1cASfJLXAQqcdcNi

2.17 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 P_n, the primorial $P_n\#$ is defined as

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

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

Program:https://colab.research.google.com/drive/1g29VxAJIybISSwIitNi3rcaxiTdoSbIb

2.18 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 .

Program:https://colab.research.google.com/drive/1EiL6l4BjjiyXdiHnb0pcq7ny0wy-LA5E

2.19 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 G_p.

$$G_p = x\ +\ iy, where\ x\ \&\ y\ are\ integers$$

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 $|x^2 + y^2|$ 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 $\sqrt{x^2 + y^2}$. This pattern has been used for tablecloths and tiling floors.

Program:https://colab.research.google.com/drive/1y5t3mTuuLK86z3o5nsH3VMUNu25E5m9t

2.20 Truncatable Prime

- Right truncatable prime number which does not have zero at any place. And 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.

  Program:https://colab.research.google.com/drive/1bVUpWdvyqm0ENbknxjIx5DzYdjYVD659

- Left truncatable 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.

  Program:https://colab.research.google.com/drive/16JVgBZtCJeuh6Lv-ZKOmxftw9AataJvv

- 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.

  Program:https://colab.research.google.com/drive/18je3fFJo1S4dQTvPZLYOK53jb8eyrTDN

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

3. Library Access

In order to print the prime numbers mentioned in this paper, the user can access the library name as primelibpy in the Python Library.

4. Time Analysis

In the following table, there is given an analysis of generating prime numbers on various platforms. In the table given below, time to generate prime numbers between 1 to 10^6 is given. If prime numbers between 1 to 10^7 (up to 26 bits) were print on C program, it took 7228 seconds. In security system nowadays system uses 128 bit numbers as a key. From the table, it can be seen that Python is much slower than other languages except R, but the benefit of using Python is that the code work is very short and millions of developers prefer Python nowadays over other languages as trouble shooting is very simple 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

5. Factorization Comparison

Prime factorization is NP Problem; therefore many cryptographic systems are built on it. There are many different methods available to factorize the prime numbers. In the paper of Connelly Barnes[12], comparison of the factorization method in which the Number of Decimal Digits vs. Number of Steps comparison has been done.

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[12].

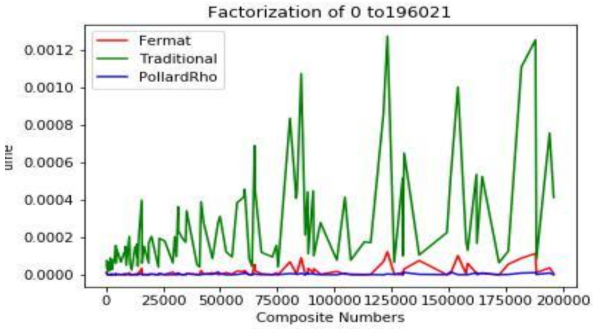

Chart -1: Prime factorization from 0 to 200000

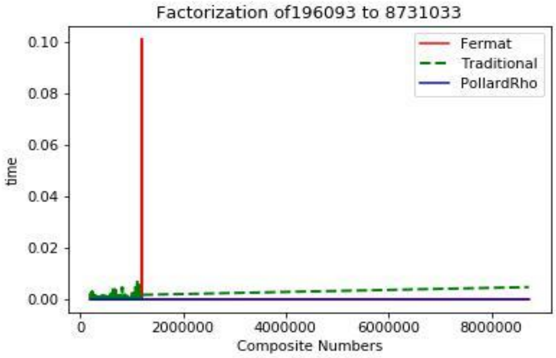

Chart -2: Prime factorization from 0 to 8000000

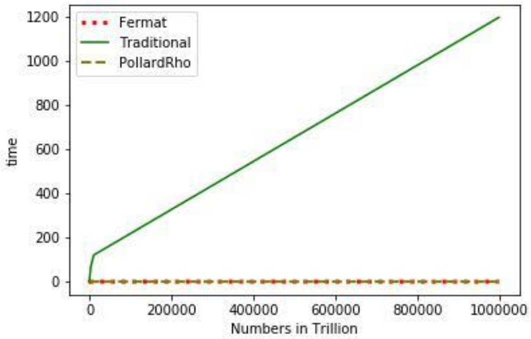

Chart -3: Prime factorization from 0 to 1000000

6. Applications

6.1 Biology

There are some biological instances in which primes are used to help in predicting the predator-prey model for a special type of insect to have a higher survival rate, this type of insects are known as "Cicada"[7]. They basically, hide underground for a long period in order to hide away from their predators. And they came out for a feed and mate purpose at particular instances only. For instance, if the periodical cicada (another name given to them in the United States) is of 17 years[11], then they reside underground for 16 years and after every 17 year they came out. Here the use of prime numbers comes into the picture; another period of 13 years is detected by the study. What is the reason for choosing such a large prime number? They can also choose the number 3,5, or other. The answer lies in the multiples of prime numbers 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.

6.2 Cryptography

There are two types of a cryptosystem which are symmetric and Asymmetric. Asymmetric encryption and decryption are done by two different keys. The public key is known to the public[2]. The private key can only be known by secret key. The RSA algorithm depends on the prime number. This algorithm can be crack if prime factorization is easy. Here the reason for choosing the prime number is we can get more relative prime numbers so that brute force searches will not work to find the key. In real-time security systems RSA is part of the whole algorithm.

Steps of RSA algorithm[2]:

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 $55 \times 7 = 385 = (2 \times 192) + 1$; 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: $CM = C^e \ mod\ n = 88^7 \ mod\ 221 = 62$

J. Decryption: Plain text: $M = C^d \ mod\ n = 62^{55} \ mod\ 221 = 88$

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

ACKNOWLEDGEMENT

The authors would like to thank computer engineering department of B.V.M Engineering College to allow for doing work on 8 core processor computer for factorizing the prime numbers and their analysis.

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].https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic

[5].http://serious-science.org/prime-numbers-6114

[6].https://en.wikipedia.org/wiki/Category:Classes_of_prime_numbers

[7].https://www.youtube.com/playlist?list=PL0D0BD149128BB06F

[8].http://web.math.rochester.edu/people/faculty/doug/UGpages/FLT.html

[9].https://cs.uwaterloo.ca/journals/JIS/VOL3/DUBNER/dubner.pdf

[10].http://www.numericana.com/answer/pseudo.htm#pseudoprime

[11].https://www.cicadamania.com/cicadas/cicadas-and-prime-numbers/

[12].Integer Factorization Algorithms, Connelly Barnes, Department of Physics, Oregon State University

[13].http://mathworld.wolfram.com/FermatPseudoprime.html

[14]. William Stallings, “Cryptography and Network Security: Principles and Practice”, by Pearson Publication; ISBN: 0133354695