SOME CHARACTERIZATIONS OF TWIN PRIME NUMBERS AND THEIR APPLICATIONS

By

S. M. Naser

MASTER OF SCIENCE

In

MATHEMATICS

Department of Mathematics
BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY(BUET)
DHAKA-1000

SOME CHARACTERIZATIONS OF TWIN PRIME NUMBERS AND THEIR APPLICATIONS

A Thesis Submitted to the
Department of Mathematics, BUET, Dhaka-1000
In partial fulfillment of the requirements for the award of the degree of

MASTER OF SCIENCE

In

MATHEMATICS

By

S. M. Naser

Student No. 1018092518, Session: October, 2018
Department of Mathematics
BANGLADESH UNIVERSITY OF ENGINEERING TECHNOLOGY
DHAKA-1000

Under the supervision of
Dr. KhandkerFarid Uddin Ahmed
Professor
Department of Mathematics
BUET, Dhaka-1000

The thesis entitled **"Some Characterizations of Twin Prime Numbers and Their Applications"**, submitted by S. M. Naser, Student No. 1018092518, Session: October 2018, to the Department of Mathematics, has been accepted as satisfactory in partial fulfillment of the requirements for the degree of Master of Science in Mathematics approved as to its style and contents on August 9, 2021.

Board of Examiners

(i) ______________________________

Dr. Khandker Farid Uddin Ahmed — Chairman (Supervisor)
Professor
Department of Mathematics, BUET, Dhaka

(ii) ______________________________

Dr. Khandker Farid Uddin Ahmed — (Ex-Officio)
Professor and Head
Department of Mathematics

(iii) ______________________________

Dr. Md. Abdul Hakim Khan — Member
Professor
Department of Mathematics

(iv) ______________________________

Dr. Mohammed Forhad Uddin — Member
Professor
Department of Mathematics

(v) Md. Elias.
____

Dr. Md. Elias — Member (External)
Ex-Professor
Department of Mathematics
48/7/A, Dhakeswari R/A, BUET, Dhaka

Dedicated to

My Teachers

and

to My Family.

Candidate’s Declaration

I, do, hereby, certify that the work presented in this thesis, titled, “Some Characterizations of Twin Prime Numbers and Their Applications”, is the outcome of the investigation and research carried out by me under the supervision of Dr. KhandkerFarid Uddin Ahmed, Professor, Department of Mathematics, BUET.

I also declare that neither this thesis nor any part thereof has been submitted anywhere else for the award of any degree, diploma or other qualifications.

S. M. Naser

S. M. Naser

1018092518

Acknowledgements

I would like to express my heartiest gratitude, profound indebtedness and deep respect to my supervisor, Dr. KhandkerFarid Uddin Ahmed, Professor and Head, Department of Mathematics, BUET, Dhaka, Bangladesh, for his constant supervision, affectionate guidance and great encouragement and motivation. His keen interest in the topic and valuable advice throughout the study helped to complete the thesis.

I would also like to thank the members of my thesis committee for their valuable suggestions. I thank Dr. Md. Abdul Hakim Khan, Dr. Mohammed Forhad Uddin and especially the external member Dr. Md. Elias.

I am especially grateful to the Department of Mathematics of Bangladesh University of Engineering and Technology (BUET) for providing me support during the thesis work. My sincere thanks go to the staffs of Mathematics Department to let me use the Lab to successfully complete my thesis work.

I want to thank my elder brother Rezaul Karim who was also a student of the CSE Department at BUET.Finally, my sincere gratitude goes to my family and friends for their continuous and unparallel love, help, support and constant encouragement throughout the whole journey.

Above all, I am thankful to Almighty Allah for his blessings for the successful completion of my thesis.

Dhaka	S. M. Naser
August 09, 2021	1018092518

ABSTRACT

Letting Bertrand‟s Postulate, Goldbach‟s Conjecture and Chen‟s theorem as base theorems, we find some new results. This research work proposesa theorem that every even number greater than 6 can be written as a sum of two primes, where at least one is a member of a twin prime. In addition, we propose a lemmawhich states that for any positive integer n, $2n > 12$has at least one twin prime in between n and $2n$. In this study, we establish two propositions. First proposition finds out few prime summations of two consecutive even integers if the prime summation of one is known and where one prime is one of a twin prime. Second proposition finds out the equality of two primes from the middle of the integer. The construction of the distance $6m + 4$ between two consecutive twin primes, where m is any nonnegative integer, is shown and illustrated by examples. The distance between two consecutive twin primes is calculated by congruence modulo. All those results are verified by programming language Python. Graphical representation of the distance between two consecutive twin primes is presented in this research by MS Excel.

There are a lot of different types of applications of primes in mathematics, science, engineering and technology. Among them, prime numbers used in cryptography has changed revolutionarily the whole secret communication system and greatly developed the cyber security system. This thesis work briefly enlighten on cryptography and two old models of cryptography,namely, Diffie-Hellman public key cryptography and RSA cryptosystem as applications of primes.

Table of Content

Page

CHAPTER 1

INTRODUCTION

CHAPTER 2

BASIC KNOWLEDGE

CHAPTER 3

MAIN RESULTS

CHAPTER 4

APPLICATIONS AND PRIMES IN CRYPTOGRAPHY

CHAPTER 5

CONCLUSION

List of Tables

Page

List of Program Codes

Pages

List of Graphs

Page

CHAPTER 1

INTRODUCTION

Prime numbers belong to a unique world of abstract conceptions. In modern times mathematicians are trying to find the profundity of primes. A huge effort and resources are spending toward the computational aspect, the task of finding, characterizing, and applying primes in other domains.

1.1 Motivation

This thesis work is about prime numbers specially twin prime numbers and further more little discussion on applications of primes in different areas of mathematics and information science. Based on the study on twin primes we proposed a theorem which shows that for any even integer 2n greater than 12, there is always a twin prime in the interval [n, 2n]. We have also shown that, every even integer greater than 6 can be written as a sum of two primes where at least one is a member of a twin prime. Our study presented that the difference between two consecutive twin prime numbersis $6m + 4$, where m is any of nonnegative integers 0,1,2,3,… .

The prominent study of prime numbers begins at 3000 B.C. with the proof of Euclid that there are infinitely many primes. Which, in later deduced that every positive integer factors as a product of primes. Prime numbers are used in Diffie and Hellman public-key cryptosystem which is supposed to be the bone of the revolution in digital communication, RSA public-key cryptosystem of Rivest, Shamir, and Adleman, elliptic curves revolutionized number theory, primality testing, Andrew Wiles resolution of Fermat"s Last Theorem. In this research paper we have shown a complete model of Diffie and Hellman public-key cryptography and RSA public-key cryptosystem. These two models showed how to encrypt a plaintext into ciphertext and again how to decrypt the cipher text into clear text so that two people can secretly communicate in public. To operate the whole process needs a clear view on some algorithms, theorems and some operations of primes which we included in the description part of the models.

1.1.1 Contemporary Study on Primes and Twin Primes

The prominent study of primes begins at 3000 B.C. with the proof of Euclid that there are infinitely many primes. With times, day by day the applications of primes are increasing. In modern era primes are used to be the key of cryptography [1].

Even though twin primes are still a mysterious figure in number theory but they play a vital role in number theory.An integer p>1 is a prime if it has no positive divisors other than 1 and itself. Examples include 2, 3, 5, 7, 11, 13,17, 19, etc. [1]. A twin prime is a prime number that is either 2 less or 2 more than another prime number. Thetwin primes include many pairs differing by 2 such as (3, 5), (5, 7), (11, 13), (17, 19) and so on ([2], [3]). Someimportant formulations of primes are Bertrand"s Postulate [4], Goldbach"s Conjecture [5], Chen"s Theorem [6] and TwinPrime Conjecture [7]. Jhang [8] proved that there are infinitely many twin prime pairs that differ by no more than70000000 numbers. Murty [9] illustrated the basic strategy of Jhang"s proof and Maynard [10] represented gapsbetween primes and proposed a proof for a limit of numbers. Yue [11] proposed a proof of Twin Prime Conjectureby computer programming language C.

Baoshan [12] proposed a theorem which states that for sufficiently largeenough prime p, there always exist a pair of twin prime number q, q+2 in the interval (p, 2p).

An integer $p \geq 2$is a prime if it has no positive divisors other than 1 and itself. $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$are examples of first few primes. 1 is not a prime number [20]. A twin prime is a prime number that is either 2 less or 2 more than another prime number ([14], [30]). For example, either member of the twin prime pair $(41, 43)$. In other word, a twin prime is a prime that has a prime gap of two [16]. Sometimes the term twin prime is used for a pair of twin primes; an alternative name for this is prime twin or prime pair. Normally twin prime appears in the form $6n \pm 1$. The only number that appears in two twin pairs is 5; and 3 is the only number in the sequence not in the form $6n \pm 1$ ([14], [27]).

The following characterization, found by Ruiz in 2000 and reported by Weisstein on the internet, is computationally friendlier to find the condition necessary for a number of pair to be primes. For $a \geq 0$, the pair $(n, n + 2)$ of integers are twin primes if and only if

$$\sum_{i=1}^{n} i^a \left(\left\lfloor \frac{n+2}{i} \right\rfloor + \left\lfloor \frac{n}{i} \right\rfloor \right) = 2 + n^a + \sum_{i=1}^{n} i^a \left(\left\lfloor \frac{n+1}{i} \right\rfloor + \left\lfloor \frac{n-1}{i} \right\rfloor \right)$$

where$\lfloor x \rfloor$is the floor function denoting the greatest integer not exceeding x [24]. A floor function converts the fraction to the nearest small integer ([25], [26]). As an example, a floor function converts the fraction 3.1416 to the nearest smallest integer 3.

The term twin prime was introduced by Paul Stackel. The set $(3, 5), (5, 7), (11, 13), \ldots$ of twin prime pairs $(q, q + 2)$ has been studied by Brun (1919), Hardy and Littlewood (1922), Selmer (1942), Fr¨oberg (1961), Weintraub(1973), Bohman(1973), Shanks and Wrench (1974), and Brent $(1975, 1976)$ [21].

There are few theorems and conjectures on prime. One of the most important conjectures is twin prime conjecture, which has no clear proof yet. There was an attempt to build a proof of the twin-prime conjecture, even in the stronger form of Hardy and Littlewood, namely that [22]

$$\lim_{N \to \infty} \frac{1}{N} \sum_{\substack{p < N \\ p, p+2 \text{ both primes}}} \log p . \log(p + 2) = B_2 > 0,$$

was presented using methods from classical analytic number theory with Dirichlet series [22].

A serious error was found in Arenstorf"s proof [22]. As a result, the paper has been retracted later.

N.A. Carella showed a proof of the De Polignac conjecture claims that for any fixed $\mathrm{k} \geq 1$, the Diophantine equation $\mathrm{q} = \mathrm{p} + 2\mathrm{k}$ has infinitely many prime pairs solutions [23]. Recent works of JhangYitang and others greatly promote the study of the problem. They are very close to the final proof of the problem [18]. JhangYitang proved that there are infinitely many pairs of prime that differ by no more than 7×10^7 numbers, by his method at 2013 [16].

1.1.2 Objectives of Cryptography

With the advancement of the world, people feel for a secret communication in public which none but only two sides- sender and receiver can understand what the message contains actually, to keep secure the information flow between two sides. With times, in this digital internet-based world people need for a strong lock system where they can keep secure their important personal and official documents to prevent entry of any intruder third party who can harm. Internet lock system builds up based on primes and prime factorization. In this age of universal internet connectivity it is the major issue to protect the data and resources from disclosure and to protect the systems from cyber attack to guarantee the authenticity of data and messages.

Many service providing companies needed to provide security of their client accounts through encryption to prevent attacks of third parties such as hackers, viruses, electronic eavesdropping and electronic fraud through e-banking, e-shopping, e-ticketing etc. One of the best recent technology to encrypt data is steganography- is a technique of hiding secret data within a non-secret image or file to avoid detection. In steganography, message bits are inserted as the LSBs of the arbitrary choosing pixels in the picture is a type of concealment of data so that the message won‟t look suspicious [33].

As cryptography is the study of converting a message into scramble message or unintelligible message and again converting it into readable message, it has become an integral part of securely data transmission. The basic cryptography started with the invention of Diffie-Hellman public key cryptography system and RSA system where using congruence modulo of integers of primes and integers one can send a secret message to other which only other can understand by using the key usually a prime number. Primarily cryptography was invented for secret communication of two parties so that if the message goes to another hand then it wouldn‟t be possible to read and seems to be a scramble message. Only one can read it who knows the common integer and own secret key which normally a prime, by which decrypting the message one can understand the message. The drawback of those systems is if one can find out the secret key number then one can read the message and can change it and resend to the actual receiver. So, to keep secure, cryptographer always try to use a prime number for secret key which should be a big prime number with lot of digits ([34], [35]).

1.2 Thesis Objective

It is the purpose to this thesis is to throw a light on the current study of primes and to provide few states on twin primes and to present how they behave in number theory. This thesis work shown that for any integer greater than 12 can be presented as a summations of two primes, where at least one is a part of a twin prime and there is always a twin prime in the interval of 3 to the half of that integer and one twin prime in the interval of half of the number and to the number. It is also shown that in natural number the distance between two consecutive twin prime numbers follow a definite form of sequence. This distance is presented by congruency.

Among the applications of primes the most important one is to carry a vital role on cryptography which is the backbone of secure communication and information security in the modern internet based world. Here, this research paper presented two old models of cryptography- Diffie-Hellman public key cryptography and RSA system. To learn the behavior of primes in number theory and in cryptography, Reduction map and lift, Solvability, Euler"s $\varphi - function$, Euler"s theorem, Chinese remainder theorem, Extended Euclidean representation, Primality test, The discrete log problem, Factoring an integer etc. are added in the applications part.

1.3 Contribution of the Thesis

If we take any integer $2\mathrm{n} > 12$, then we see that there is at least one twin prime in between n and $2\mathrm{n}$. If we analyze any two consecutive twin primes then we can find that the distance between two consecutive twin primes follows a definite manner. Between the first two twin prime pair i.e., between $(3, 5)$ and $(5, 7)$ the distance is 0 and the distance between any other twin prime pair can be presented in the form $6\mathrm{m} + 4$, where m is any nonnegative integer ,i.e., $\mathrm{m} = 0,1,2, \dots$. We can present this distance by using integer modulo as $\mathrm{d} \equiv 4 (\mathrm{mod}\ 6)$ where d is the distance between two consecutive prime pairs.

Based on Bertrand"s Postulate, Goldbach"s Conjecture and Chen"s theorem, we investigated some new results. These results are verified by programming language Python [13]. It is shown that every even integer greater than 6 can be written as a sum of two primes where at least one is a member of a twin prime. It is also shown that for any positive integer n, $2n > 12$ has at least one twin prime in between n and $2n$. The formulation of the distance $6m + 4$ between two consecutive twin primes, where m is any nonnegative integer, is shown and illustrated by examples. This formula is verified by programming language Python. The distance between two consecutive twin primes is calculated by congruence modulo. Graphical representation of the distance between two consecutive twin primes is presented in this research by MS Excel.

1.4 Organization of the Thesis

The main goal of this thesis is to present few characteristics on twin prime, applications and to show the uses of primes in cryptography.

In chapter 1 we discussed on primes and twin primes and a brief history of them. We have also included the contemporary study, thesis objective, contribution of the thesis and organization of the thesis in chapter 1.

Chapter 2 discussed some brief review of basic definitions and theorems related to prime numbers and twin prime numbers such as primes, twin primes, Mersenne primes, Fermat primes, prime number theorem, Bertrand‟s postulate, Goldbach‟s Conjecture, Chen‟s theorem, Twin prime conjecture, Zhang-Baoshan‟s theorem, Fundamental theorem of arithmatic, Seive of Eratosthenes and definitions of terms related to cryptography.

In chapter 3, we have discussed the main results of our thesis. This chapter is the contribution of our research work. Here we have presented few characteristics of twin primes and verified by programming language code.

In chapter 4, we mentioned applications of primes and discussed cryptography models. We have also shown two old cryptographic models. We have presented how to send secret messages using the prime numbers. We also included the applications of twin primes briefly in this chapter.

In chapter 5, we have presented the conclusion of this thesis and its future scope.

CHAPTER 2

BASIC KNOWLEDGE

Prime numbers act as the basic building blocks in the multiplicative structure of the integers. Behind the simplicity of the prime numbers lies a mysterious world of insights and results that has fascinated mathematicians for centuries. Among the different kinds of primes, twin primes is the most beautiful one that holds a definite structure and distance. In this chapter some basic knowledge of primes and twin primes are discussed.

2.1 Prime Number

A prime number or simply a prime is a natural number greater than 1 and that has no positive divisors other than 1 and itself [7]. Symbolically, a number p is said to be prime if

i) $p > 1$
ii) p has no positive divisors except 1 and p.

Example

It is well known that $2, 3, 5, 7, 11, 13, \ldots$ are the first few primes.

2.2 Twin Prime

A twin prime number is a pair of prime numbers where these two primes are differ by 2 [14].

Example

$(3,5),\ (5,7), (11,13), (17,19)$are twin primes.

2.3 Mersenne Primes

Primes of the form $2p - 1$ where p is also a prime is called the Mersenne primes.

Example

If $p = 2$, then $2p - 1 = 2.2 - 1 = 3$.
If $p = 7$, then $2.p - 1 = 2.7 - 1 = 13$.

2.4 Fermat Primes

Primes of the form $2^n + 1$ where n is a positive integer is called the Fermat Primes.

Example

If $n = 2$, then $2^n + 1 = 5$.
If $n = 5$, then $2^n + 1 = 31$.

2.5 Prime Number Theorem [31]

Let x be a positive real number, and let $\pi(x)$ be the number of primes $\leq x$. Then the prime number theorem asserts that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/log\, x} = 1, \qquad (1)$$

Where $\log x$ denotes the natural log of x. In other words, the prime number theorem asserts that

$$\pi(x) = \frac{x}{log\, x} + o\left(\frac{x}{log\, x}\right), \qquad (x \to \infty), \qquad (2)$$

Where $o(x/log\, x)$ stands for a function $f(x)$ with the property

$$\lim_{x\to\infty} \frac{f(x)}{x/log\, x} = 0.$$

2.6 Bertrand's Postulate [15]

For all $n \geq 1$ there is a prime p such that $n < p \leq 2n$.

This statement was first conjectured by Bertrand in 1845 and was verified by Bertrand for all $N < 3 \times 10^6$ and was first proved by chebychev in 1850.

2.7 Goldbach's Conjecture ([5], [28])

Every even integer greater than 2, can be expressed as the sum of two primes.

The conjecture has been shown to hold for all integers less than 4×10^8.

2.8 Chen's Theorem [29]

Chen‟s theorem states that every sufficiently large even number can be written as the sum of either two primes, or a prime and a semiprime(the product of two primes).
This theorem was first stated by Chinese mathematician Chen Jingrunin1966. P.M. Ross proved the theorem in 1975.

2.9 Twin Prime Conjecture

In 1849 De Polignac made a general conjecture that for every natural number k there are infinitely many primes p such that $p + 2k$ is also primes. For $k = 1$ Polignac"s conjecture becomes twin prime conjecture.

Statement

There are infinitely many twin primes ([30], [19]).

2.10 Zhang Baoshan's Theorem

For big enough prime p, there always exists a pair of twin prime number $q, q + 2$, in the interval$(p, 2p)$ [12].

2.11 Fundamental Theorem of Arithmetic [1]

Every natural number can be written as a product of primes uniquely up to order.

Example

Here,

$$6 = 2.3,$$

where 6 factors in 2.3.

2.12 Seive of Eratosthenes [32]

This is perhaps the most widely accepted algorithm which has been used since ancient times. This algorithm lists out all the numbers from 1 to n (or 2 to n, since 1 is known to be neither prime nor composite) and then marks off all the multiples of the first prime which is 2. After marking off all the multiples of 2, it is then begins to mark off all the multiples of the next prime, which is 3. It does this routine till the time there are no primes less than n. In the end all the unmarked numbers are all the primes less than n.

2.13 Cryptography

Cryptography, or cryptology is the practice and study of techniques for secure communication in the presence of "adversaries" (the third parties). More generally, cryptography is about burning the message in such a way that prevents third parties or the public from reading private messages [33]. Modern cryptology exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payments cards, digital currencies, computer passwords, and military communications.

2.14 Symmetric Key Cryptography

In symmetric key cryptography (also known as private-key cryptography) a secret key may be held by one person or exchanged between the sender and the receiver of a message. Private key cryptography is used to send secret messages between two parties, where both the sender and recipient must have a copy of the secret key.

2.15 Asymmetric Key Cryptography

In the two-key system (also known as the public key system), one key encrypts the information into ciphertext and anotherkey mathematically related to the first key, decrypts the ciphertext into plaintext. The sender uses a public key to encrypt the message. The recipient uses a private key to decrypt the message. By this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message [38].

2.16 Plaintext

In cryptography, plaintext usually means unencrypted information or the original intelligible message or data that someone wishes to another, fed into the algorithm as input [35].

2.17 Key

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa depending on the decryption algorithm. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

2.18 Secret Key

The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key[34].

2.19 Encryption Algorithm

The encryption algorithm performs various substitutions and transformations on the plaintext to converts it into the ciphertext.

2.20 Ciphertext

Ciphertext or cyphertext is the encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. This is the scrambled message produced as output. It depends on the plaintext and the secret key [38].

2.21 Decryption Algorithm

This is essentially the encryption algorithm run in receives. It takes the ciphertext and the secret key and produces the original plaintext.

2.22 Encryption

A process of converting plaintext into ciphertext is called encryption. Cryptographers use various encryption methods to send confidential messages via an insecure channel. The process of encryption requires two things – an encryption algorithm and a key. An encryption algorithm means the method that has been used in encrypting the data. Encryption happens at the senders side.

2.23 Decryption

The reverse process of encryption is called decryption. It is the process of converting ciphertext into plaintext. Cryptographers use the decryption algorithms at the receiver side to obtain the original message from non readable message, i.e. ciphertext. The process of decryption requires two things – a decryption algorithm and a key. A decryption algorithm means the method that has been used in decryption. Generally the encryption and decryption algorithm are identical but reverse.

2.24 Encoder

An encoder is the person that wants to send the message and uses encryption to make the messages secure.

2.25 Decoder

A decoder is the person who decrypts the message. This may be the intended recipient of the message or may be an intruder, trying to get access to the secret message.

2.26 Rotor Machines

In cryptography, a rotor machine is an electro-mechanical stream cipher device used for encrypting and decrypting messages. In the 1920s, various mechanical encryption devices were invented to automate the process of encryption. Most were based on the concept of a rotor, a mechanical wheel wired to perform a general substitution.

2.27 Reduction Map and Lift

We call the natural reduction map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, which sends a to $a + n\mathbb{Z}$, reduction modulo n. We also say that a is a lift of $a + n\mathbb{Z}$. Thus, e.g., 7 is a lift of $1\ mod\ 3$, since $7 + 3\mathbb{Z} = 1 + 3\mathbb{Z}$ [1].

2.28 Solvability

The equation $ax \equiv b(mod\ n)$ has a solution if and only if $\gcd(a, n)$divides b.

2.29 Euler's φ-function

For $n \in N$, let

$$\varphi(n) = \#\{a \in N: a \leq n\ and \gcd(a, n) = 1\}$$

For example,

$$\begin{aligned}
&\varphi(1) = \#\{1\} = 1,\\
&\varphi(2) = \#\{1\} = 1,\\
&\varphi(3) = \#\{1,2\} = 2\\
&\varphi(4) = \#\{1,3\} = 2,\\
&\varphi(7) = \#\{1,2,3,4,5,6\} = 6\\
&\varphi(9) = \#\{1,2,4,5,7,8\} = 6,
\end{aligned}$$

Also, if p is any prime number then

$$\varphi(p) = \#\{1,2, \dots, p - 1\} = p - 1$$

Using Euler‟s $\varphi - function$ it is simple to find out the number of relatively prime number of a given natural number and if the natural number is a prime number p then the number of relatively prime number less than p is $p - 1$.

2.30 Pseudoprimality

An integer $p > 1$ is prime if and only if for every $a \not\equiv 0(mod\ p)$,

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

2.31 Wilson's Theorem

An integer $p > 1$ is prime if and only if

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

For example, if $p = 7$, then

$$(p - 1)! = 6! = 720 \equiv -1(mod\ 7)$$

But if $p = 6$, then

$$(p - 1)! = 5! = 120 \equiv 1(mod\ 7)$$

So 6 is a composite number.

Wilson‟s theorem, from a computational point of view, probably one of the world‟s least efficient primality tests since computing $(n-1)!$ takes so many steps.

2.32 Computing $a^m(mod\ n)$

Let a and n be integers, and m a nonnegative integer. In this section we describe an efficient algorithm to compute $a^m(mod\ n)$. For cryptography applications,m will have hundreds of digits.

The naive approach to computing $a^m(mod\ n)$ is to simply compute $a^m = a.a\dots a\ (mod\ n)$ by repeatedly multiplying by a and reducing modulo m. Note that after each arithmetic operation is completed, we reduce the result modulo n so that the sizes of numbers involved do not get too large. Nonetheless, this algorithm is horribly inefficient because it takes $m-1$ multiplications, which is huge if m has hundreds of digits.

A much more efficient algorithm for computing $a^m(mod\ n)$ involves writing m in binary, then expressing a^m as a product of expressing a^{2^i}, for various i. These latter expressions can be computed by repeatedly squaring a^{2^i}. This more clever algorithm is not "simpler", but it is vastly more efficient since the number of operations needed grows with the number of binary digits of m.

Example-1

We can compute the last 2 digits of 3^{85} by finding $3^{85}(mod\ 100)$. First, because $gcd(3,100) = 1$, we have by Euler‟s theorem that $3^{\varphi(100)} \equiv 1(mod\ 100)$. Because φ is multiplicative,

$$\varphi(100) = \varphi(2^2.5^2) = (2^2-2).(5^2-5) = 40.$$

Thus $3^{40} \equiv 1(\ mod\ 100)$, hence

$$3^{85} \equiv 3^{40+40+5} \equiv 3^5(mod\ 100).$$

We now compute 3^5(mod 100)using the above algorithm. First write 5 in binary by repeatedly dividing by 2.

$$5 = 2.2 + 1$$
$$2 = 1.2 + 0$$
$$1 = 0.2 + 1$$

So in binary$(5)_2 = 101$, which we check

$$5 = 1.4 + 1.$$

Next, compute a, a^2, a^4 and output $a^4.a$. We have

$$a = 3$$
$$a^2 \equiv 3^2 \equiv 9$$

$$a^4 \equiv 9^2 \equiv 81$$

Finally,

$$3^{85} \equiv 3^5 \equiv a^4.a \equiv 81.3 \equiv 43(mod\ 100)$$

Example-2

Is $p = 143$ prime?

Solution

We compute $2^{142}\,(mod\ 143)$by making a table as follows.

Table 2.1: Computing $2^{142}\,(mod\ 143)$ by finding the values of i, M, ε_i, $2^{2^i}\ mod\ 143$.

I	M	ε_i	$2^{2^i}\ mod\ 143$
0	142	0	2
1	71	1	4
2	35	1	16
3	17	1	113
4	8	0	42
5	4	0	48
6	2	0	16
7	1	1	113

Thus

$$2^{142} \equiv 4.16.113.113 \quad \equiv 114\ (mod\ 143)$$

So, 143 is not prime.

Example-3

Is $p = 47$ prime?

Solution

We compute $2^{46}\,(mod\ 47)$ making a table as follows:

Table 2.2: Computing $2^{46}\,(mod\ 47)$by finding the values of i, M, ε_i, $2^{2^i}\ mod\ 47$.

I	M	ε_i	$2^{2^i}\ mod\ 47$
0	46	0	2
1	23	1	4
2	11	1	16
3	5	1	21
4	2	0	18
5	1	1	42

Thus

$$2^{46} \equiv 4.16.21.42 \equiv 1\ (mod\ 47)$$

So, by pseudoprimality theorem 47 is a prime.

2.33 The Discrete Log Problem

Let $a, b,$ and n be real numbers with $a, b > 0$ and $n \geq 0$. The "log to the base b" function is characterized by ,

$$\log_b(a) = n, \text{if and only if } a = b^n.$$

log_b function is used in algebra to solve the following problem: given a base b and a power a of b, find an exponent function n such that

$$a = b^n$$

Discrete Log Problem

Let G be a finite group, for example, $G = (\mathbb{Z}/p\mathbb{Z})^*$. Given $b \in G$ and a power a of b, find a positive integer n such that,

$$b^n = a$$

It is easy to give an inefficient algorithm that solves the discrete log problem. Simply try b^1, b^2, b^3, etc., until we find an exponent n such that $b^n = a$. For example, $a = 7, b = 3$ and $p = 19$. Working $modulo$ 19, we have

$$b^1 = 3, b^2 = 9, b^3 = 8, \ldots, b^6 = (b^3)^2 = 7,$$

So $n = 6$. This method can be used to simplify a large power of integer modulo to a small integer modulo. When p is large, computing the discrete log this way soon becomes impractical, because increasing the number of digits of the modulus makes the computation take vastly longer.

2.34 Factoring n When $\varphi(n)$ is Given

Suppose $n = pq$. Given $\varphi(n)$, it is very easy to compute p and q. We have,

$$\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1,$$

So we know both $pq = n$and $p + q = n + 1 - \varphi(n)$. Thus, we know the polynomial

$$x^2 - (p+q)x + pq = (x-p)(x-q)$$

Whose roots are p and q. These roots can be found using the quadratic formula.

Example-1

The number $n = pq = 55298377$ is a product of two primes, and $\varphi(n) = 55283476$. We have

$$\begin{aligned} f &= x^2 - (n + 1 - \varphi(n))x + n \\ &= x^2 - 14902x + 55283476 \end{aligned}$$

$$= (x - 7919)(x - 6983)$$

Where the factorizations step is easily accomplished using the quadratic formula:

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

$$= \frac{14902 + \sqrt{14902^2 - 4.55283476}}{2}$$

$$= 7919$$

We conclude that $f = 7919$.

When p and q are Close

Suppose that p and q are "close" to each other. Then it is easy to factor n using a factorization method of Fermat called the Fermat Factorization Method.

Suppose $n = pq$ with $p > q$. Then,

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$

Since p and q are "close",

$$s = \frac{p-q}{2}$$

is small,

$$t = \frac{p+q}{2}$$

is only slightly larger than $\sqrt{n}$; and $t^2 - n = s^2$ is a perfect square. So, we just try

$$t = \lceil\sqrt{n}\rceil, \quad t = \lceil\sqrt{n}\rceil + 1, \quad t = \lceil\sqrt{n}\rceil + 2, \ldots$$

Until $t^2 - n$ is a perfect square s^2. (Here $\lceil x \rceil$ denotes the least integer $n \geq x$.)

Then

$$p = t + s, \qquad q = t - s.$$

Example-2

Suppose $n = 10648251541$. Then

$$\sqrt{n} = 103190.37 \ldots.$$

If $t = 103191$, then $\sqrt{t^2 - n} = 361.86$ ....
If $t = 103192$, then $\sqrt{t^2 - n} = 580.8$ ....
If $t = 103193$, then $\sqrt{t^2 - n} = 737.37$ ....
If $t = 103194$, then $\sqrt{t^2 - n} = 866.08$ ....
If $t = 103195$, then $\sqrt{t^2 - n} = 978$.

Thus $s = 978$ We find that $p = t + s = 103195 + 978 = 104173$ and $q = t - s = 103195 - 978 = 102217$.

CHAPTER 3

MAIN RESULTS

In this chapter, we propose some characteristics of twin prime numbers. Those characteristics are verified by programming language Python. To build the programming code, Seive method of finding primes is used.

3.1 Theorem

If $2n > 6$ is a positive even integer and p_1 and p_2 are primes, then among all summations of two prime summation $p_1 + p_2 = 2n$, there is at least one summation where p_1 is one of any twin prime such that $n < p_1 < 2n$ and at least a summation (could be the same summation for p_1 andp_2) where p_2 is one of any twin prime such that $3 \leq p_2 < n$ or p_1 and $p_2$both are differently one of any two different or sametwin primes where there is a summation $p_1 + p_2 = 2n$ and $n < p_1 < 2n$ and $3 \leq p_2 < n$.

Example-1

Consider any integer

$$2n = 100$$

So,

$$n = 50$$

We can express $2n = 100$ as a collection of summations of two primes such that $2n = p_1 + p_2$, where p_1 and$p_2$are two primes, as follows:

Table 3.1: Prime summations of 100.

100=	97+3	89+11	83+17	71+29	59+41	53+47

Here, we got six $(p_1 + p_2)$ prime summationsfor $2n = 100$.
Let,
$p_1 + p_2 = 71 + 29 = 100 = 2n$.
So,$p_1 = 71$, $p_2 = 29$.
Here, 71 is one of a twin prime $(71, 73)$ and 29 is one of a twin prime $(29, 31)$.
Again,
$50 < 71 < 100$ and $3 < 29 < 50$.

Example-2

Let,

$$2n = 500$$

So,

$$n = 250$$

We can express 500 as a collection of summations of two primes $p_1$and p_2 as $2n = p_1 + p_2$ as follows:

Table 3.2: Prime summations of 500.

500=	487+13	463+37	457+43	439+61	433+67	421+79	397+103
	373+127	349+151	337+163	307+193	277+223	271+229	

Here, we got a collection of thirteen $(p_1 + p_2)$summations of primesfor 500.

Let,

$$p_1 + p_2 = 463 + 37 = 500 = 2n$$

So,
$p_1 = 463$ and$p_2 = 37$.

463 is one of a twin prime $(461, 463)$ and $250 < 463 < 500$.

Again, let,

$$p_1 + p_2 = 487 + 13 = 500 = 2n$$

So,
$p_1 = 487$ and $p_2 = 13$.
13 is one of a twin prime $(11, 13)$ and $3 < 13 < 250$.

3.1.1 Verification

We can verify the *Theorem 3.1*. Here we will verify the *Theorem 3.1*for all the even numbers from 8 to 200. We have added a program code to verify this theorem using programming language python at the end of this section.
The verification of the theorem is given by

$$2n = p_1 + p_2$$

$p_1 \in (p_1, p_3)$or, $p_1 \in (p_3, p_1)$ and $n < p_1 < 2n$
[where $p_3 = p_1 + 2$ or $p_3 = p_1 - 2$]

$p_2 \in (p_2, p_4)$or$p_2 \in (p_4,\ p_2)$ and $3 \leq p_2 < n$

[where $p_4 = p_2 + 2$ or $p_4 = p_2 - 2$]

Verification for 8 to 200Even Numbers

$8 = 5 + 3$
$5 \in (5, 7)$and$4 < 5 < 8$
$3 \in (3, 5)$and$3 \leq 3 < 4$

$10 = 7 + 3$
$7 \in (5, 7)$and$5 < 7 < 10$
$3 \in (3, 5)$and$3 \leq 3 < 5$

$12 = 7 + 5$
$7 \in (5, 7)$and$6 < 7 < 12$
$5 \in (3, 5)$and$3 \leq 5 < 6$

$14 = 11 + 3$
$11 \in (11, 13)$and$7 < 11 < 14$
$3 \in (3, 5)$and$3 \leq 3 < 7$

$16 = 11 + 5$
$11 \in (11, 13)$and$8 < 11 < 16$
$5 \in (3, 5)$and$3 \leq 5 < 8$

$18 = 11 + 7$
$11 \in (11, 13)$and$9 < 11 < 18$
$7 \in (5, 7)$and$3 \leq 7 < 9$

$20 = 13 + 7$
$13 \in (11, 13)$and$10 < 13 < 20$
$7 \in (5, 7)$and$3 \leq 7 < 10$

$22 = 17 + 5$
$17 \in (17, 19)$and$11 < 17 < 22$
$5 \in (3, 5)$and$3 \leq 5 < 11$

$24 = 17 + 7$
$17 \in (17, 19)\text{and } 12 < 17 < 24$
$7 \in (5, 7)\text{and } 3 \leq 7 < 12$

$26 = 19 + 7$
$19 \in (17, 19)\text{and } 13 < 19 < 26$
$7 \in (5, 7)\text{and } 3 \leq 7 < 13$

$28 = 17 + 11$
$17 \in (17, 19)\text{and } 14 < 17 < 28$
$11 \in (11, 13)\text{and } 3 \leq 11 < 14$

$30 = 17 + 13$
$17 \in (17, 19)\text{and } 15 < 17 < 30$
$13 \in (11, 13)\text{and } 3 \leq 13 < 15$

$32 = 19 + 13$
$19 \in (17, 19)\text{and } 16 < 19 < 32$
$13 \in (11, 13)\text{and } 3 \leq 13 < 16$

$34 = 29 + 5$
$29 \in (29, 31)\text{and } 17 < 29 < 34$
$5 \in (3, 5)\text{and } 3 \leq 5 < 17$

$36 = 29 + 7$
$29 \in (29,31)\text{and } 18 < 29 < 36$
$7 \in (5,7)\text{and } 3 \leq 7 < 18$

$38 = 31 + 7$
$31 \in (29, 31)\text{and } 19 < 29 < 38$
$7 \in (5, 7)\text{and } 3 \leq 7 < 19$

$40 = 29 + 11$
$29 \in (29, 31)\text{and } 20 < 29 < 40$
$11 \in (11, 13)\text{and } 3 \leq 11 < 20$

$42 = 31 + 11$
$31 \in (29, 31)\text{and } 21 < 31 < 42$
$11 \in (11, 13)\text{and } 3 \leq 11 < 21$

$44 = 31 + 13$
$31 \in (29, 31)$and $22 < 31 < 44$
$13 \in (11,13)$and $3 \leq 7 < 22$

$46 = 41 + 5$
$41 \in (41, 43)$and $23 < 41 < 46$
$5 \in (3, 5)$and $3 \leq 5 < 23$

$48 = 43 + 5$
$41 \in (41, 43)$and $24 < 41 < 48$
$5 \in (3, 5)$and $3 \leq 5 < 24$

$50 = 43 + 7$
$43 \in (41, 43)$and $25 < 43 < 50$
$7 \in (5, 7)$and $3 \leq 7 < 25$

$52 = 41 + 11$
$41 \in (41, 43)$and $26 < 41 < 52$
$11 \in (11, 13)$and $3 \leq 11 < 26$

$54 = 43 + 11$
$43 \in (41, 43)$and $27 < 43 < 54$
$11 \in (11, 13)$and $3 \leq 11 < 27$

$56 = 43 + 13$
$43 \in (41, 43)$and $28 < 43 < 56$
$13 \in (11, 13)$and $3 \leq 13 < 28$

$58 = 41 + 17$
$41 \in (41, 43)$and $29 < 41 < 58$
$17 \in (17, 19)$and $3 \leq 17 < 29$

$60 = 43 + 17$
$43 \in (41, 43)$and $30 < 43 < 60$
$17 \in (17, 19)$and $3 \leq 17 < 30$

$62 = 43 + 19$
$43 \in (41, 43)$and $31 < 43 < 62$
$19 \in (17, 19)$and $3 \leq 19 < 31$

$64 = 59 + 5$
$59 \in (59, 61)$and $32 < 59 < 64$
$5 \in (5, 7)$and $3 \leq 5 < 32$

$66 = 59 + 7$
$59 \in (59, 61)$and $33 < 43 < 66$
$7 \in (5, 7)$and $3 \leq 7 < 33$

$68 = 61 + 7$
$61 \in (59,\ 61)$and $34 < 61 < 68$
$7 \in (5, 7)$and $3 \leq 7 < 34$

$70 = 59 + 11$
$59 \in (59, 61)$and $35 < 59 < 70$
$11 \in (11, 13)$and $3 \leq 11 < 35$

$72 = 59 + 13$
$59 \in (59, 61)$and $36 < 59 < 72$
$13 \in (11, 13)$and $3 \leq 13 < 36$

$74 = 61 + 13$
$59 \in (59, 61)$and $37 < 59 < 74$
$13 \in (11, 13)$and $3 \leq 13 < 37$

$76 = 59 + 17$
$59 \in (59, 61)$and $38 < 59 < 76$
$17 \in (17, 19)$and $3 \leq 17 < 38$

$78 = 59 + 19$
$59 \in (59, 61)$and $39 < 59 < 78$
$19 \in (17, 19)$and $3 \leq 19 < 39$

$80 = 73 + 7$
$73 \in (71, 73)$and $40 < 73 < 80$
$7 \in (5, 7)$and $3 \leq 7 < 40$

$82 = 71 + 11$
$71 \in (71\,, 73)$ and $41 < 71 < 82$
$11 \in (11\,, 13)$ and $3 \leq 11 < 41$

$84 = 73 + 11$
$73 \in (71\,, 73)$ and $42 < 73 < 84$
$11 \in (11\,, 13)$ and $3 \leq 11 < 42$

$86 = 73 + 13$
$73 \in (71\,, 73)$ and $43 < 73 < 86$
$13 \in (11\,, 13)$ and $3 \leq 13 < 43$

$88 = 71 + 17$
$71 \in (71\,, 73)$ and $44 < 71 < 88$
$17 \in (17\,, 19)$ and $3 \leq 17 < 44$

$90 = 71 + 19$
$71 \in (71\,, 73)$ and $45 < 71 < 90$
$17 \in (17\,, 19)$ and $3 \leq 17 < 45$

$92 = 73 + 19$
$73 \in (71\,, 73)$ and $46 < 73 < 92$
$19 \in (17\,, 19)$ and $3 \leq 19 < 46$

$94 = 71 + 23, \qquad 89 + 5$
$71 \in (71\,, 73)$ and $47 < 71 < 94$
$5 \in (5\,, 7)$ and $3 \leq 5 < 47$

$96 = 73 + 23, \qquad 89 + 7$
$73 \in (71\,, 73)$ and $48 < 73 < 96$
$7 \in (5\,, 7)$ and $3 \leq 7 < 48$

$98 = 79 + 19\ \ , \quad 61 + 37$
$61 \in (59\,, 61)$ and $49 < 61 < 98$
$19 \in (17\,, 19)$ and $3 \leq 19 < 49$

$100 = 71 + 29$
$71 \in (71\,, 73)$ and $50 < 71 < 100$
$29 \in (29\,, 31)$ and $3 \leq 29 < 50$

$102 = 71 + 31$
$71 \in (71\,,73)$ and $51 < 71 < 102$
$31 \in (29\,,31)$ and $3 \leq 31 < 51$

$104 = 73 + 31$
$73 \in (71\,,73)$ and $52 < 73 < 104$
$31 \in (29\,,31)$ and $3 \leq 31 < 52$

$106 = 101 + 5$
$101 \in (101\,,103)$ and $53 < 101 < 106$
$5 \in (5\,,7)$ and $3 \leq 5 < 53$

$108 = 101 + 7$
$101 \in (101\,,103)$ and $54 < 101 < 108$
$7 \in (5\,,7)$ and $3 \leq 7 < 54$

$110 = 103 + 7$
$103 \in (101\,,103)$ and $55 < 103 < 110$
$7 \in (5\,,7)$ and $3 \leq 7 < 55$

$112 = 101 + 11$
$101 \in (101\,,103)$ and $56 < 101 < 112$
$11 \in (11\,,13)$ and $3 \leq 11 < 56$

$114 = 103 + 11$
$103 \in (101\,,103)$ and $57 < 103 < 114$
$11 \in (11\,,13)$ and $3 \leq 11 < 57$

$116 = 103 + 13$
$103 \in (101\,,103)$ and $58 < 103 < 116$
$13 \in (11\,,13)$ and $3 \leq 13 < 58$

$118 = 101 + 17$
$101 \in (101\,,103)$ and $59 < 101 < 118$
$17 \in (17\,,19)$ and $3 \leq 17 < 59$

$120 = 103 + 17$
$103 \in (101 , 103)$ and $60 < 103 < 120$
$17 \in (17 , 19)$ and $3 \leq 17 < 60$

$122 = 103 + 19$
$103 \in (101 , 103)$ and $61 < 103 < 122$
$19 \in (17 , 19)$ and $3 \leq 19 < 61$

$124 = 107 + 17$
$107 \in (107 , 109)$ and $62 < 107 < 124$
$17 \in (17 , 19)$ and $3 \leq 17 < 62$

$126 = 109 + 17$
$109 \in (107 , 109)$ and $63 < 109 < 126$
$17 \in (17 , 19)$ and $3 \leq 17 < 63$

$128 = 109 + 19$
$109 \in (107 , 109)$ and $64 < 109 < 128$
$19 \in (17 , 19)$ and $3 \leq 19 < 64$

$130 = 101 + 29$
$101 \in (101 , 103)$ and $65 < 101 < 130$
$29 \in (29 , 31)$ and $3 \leq 29 < 65$

$132 = 101 + 31$
$101 \in (101 , 103)$ and $66 < 101 < 132$
$31 \in (29 , 31)$ and $3 \leq 31 < 66$

$134 = 103 + 31$
$103 \in (101 , 103)$ and $67 < 103 < 134$
$31 \in (29 , 31)$ and $3 \leq 31 < 67$

$136 = 107 + 29$
$107 \in (107 , 109)$ and $68 < 107 < 136$
$29 \in (29 , 31)$ and $3 \leq 29 < 68$

$138 = 109 + 29$
$109 \in (107 , 109)$ and $69 < 109 < 138$
$29 \in (29 , 31)$ and $3 \leq 29 < 69$
$140 = 109 + 31$

$109 \in (107\,,109)$ and $70 < 109 < 140$
$31 \in (29\,,31)$ and $3 \leq 31 < 70$

$142 = 137 + 5$
$137 \in (137\,,139)$ and $71 < 137 < 142$
$5 \in (5\,,7)$ and $3 \leq 5 < 71$

$144 = 137 + 7$
$137 \in (137\,,139)$ and $72 < 137 < 144$
$7 \in (5\,,7)$ and $3 \leq 7 < 72$

$146 = 139 + 7$
$139 \in (137\,,139)$ and $73 < 139 < 146$
$7 \in (5\,,7)$ and $3 \leq 7 < 73$

$148 = 137 + 11$
$137 \in (137\,,139)$ and $74 < 137 < 148$
$11 \in (11\,,13)$ and $3 \leq 11 < 74$

$150 = 139 + 11$
$139 \in (137\,,139)$ and $75 < 139 < 150$
$11 \in (11\,,13)$ and $3 \leq 11 < 75$

$152 = 139 + 13$
$139 \in (137\,,139)$ and $76 < 139 < 152$
$13 \in (11\,,13)$ and $3 \leq 13 < 76$

$154 = 137 + 17$
$137 \in (137\,,139)$ and $77 < 137 < 154$
$17 \in (17\,,19)$ and $3 \leq 17 < 77$

$156 = 137 + 19$
$137 \in (137\,,139)$ and $78 < 137 < 156$
$19 \in (17\,,19)$ and $3 \leq 19 < 78$

$158 = 139 + 19$
$139 \in (137\,,139)$ and $79 < 139 < 158$
$19 \in (17\,,19)$ and $3 \leq 19 < 79$

$160 = 149 + 11$
$149 \in (149\,, 151)$ and $80 < 149 < 160$
$11 \in (11\,, 13)$ and $3 \leq 11 < 80$

$162 = 149 + 13$
$149 \in (149\,, 151)$ and $81 < 149 < 162$
$13 \in (11\,, 13)$ and $3 \leq 13 < 81$

$164 = 151 + 13$
$151 \in (149\,, 151)$ and $82 < 151 < 164$
$13 \in (11\,, 13)$ and $3 \leq 13 < 82$

$166 = 149 + 17$
$149 \in (149\,, 151)$ and $83 < 149 < 166$
$17 \in (17\,, 19)$ and $3 \leq 17 < 83$

$168 = 149 + 19$
$149 \in (149\,, 151)$ and $84 < 149 < 168$
$19 \in (17\,, 19)$ and $3 \leq 19 < 84$

$170 = 151 + 19$
$151 \in (149\,, 151)$ and $85 < 151 < 170$
$19 \in (17\,, 19)$ and $3 \leq 19 < 85$

$172 = 149 + 23$, $167 + 5$
$149 \in (149\,, 151)$ and $86 < 149 < 172$
$5 \in (5\,, 7)$ and $3 \leq 5 < 86$

$174 = 101 + 73$
$101 \in (101\,, 103)$ and $87 < 101 < 170$
$73 \in (71\,, 73)$ and $3 \leq 73 < 87$

$176 = 103 + 73$
$103 \in (101\,, 103)$ and $88 < 103 < 176$
$73 \in (71\,, 73)$ and $3 \leq 73 < 88$

$178 = 149 + 29$
$149 \in (149\,, 151)$ and $89 < 149 < 178$
$29 \in (29\,, 31)$ and $3 \leq 29 < 89$

$180 = 151 + 29$
$151 \in (149\,,151)$ and $90 < 151 < 180$
$29 \in (29\,,31)$ and $3 \leq 29 < 90$

$182 = 151 + 31$
$151 \in (149\,,151)$ and $91 < 151 < 182$
$31 \in (29\,,31)$ and $3 \leq 31 < 91$

$184 = 179 + 5$
$179 \in (179\,,181)$ and $92 < 179 < 184$
$5 \in (5\,,7)$ and $3 \leq 5 < 92$

$186 = 179 + 7$
$179 \in (179\,,181)$ and $93 < 179 < 186$
$7 \in (5\,,7)$ and $3 \leq 7 < 93$

$188 = 181 + 7$
$181 \in (179\,,181)$ and $94 < 181 < 188$
$7 \in (5\,,7)$ and $3 \leq 7 < 94$

$190 = 179 + 11$
$179 \in (179\,,181)$ and $95 < 179 < 190$
$11 \in (11\,,13)$ and $3 \leq 11 < 95$

$192 = 179 + 13$
$179 \in (179\,,181)$ and $96 < 179 < 192$
$13 \in (11\,,13)$ and $3 \leq 13 < 96$

$194 = 181 + 13$
$181 \in (179\,,181)$ and $97 < 181 < 194$
$13 \in (11\,,13)$ and $3 \leq 13 < 97$

$196 = 179 + 17$
$179 \in (179\,,181)$ and $98 < 179 < 196$
$17 \in (17\,,19)$ and $3 \leq 17 < 98$

$198 = 179 + 19$
$179 \in (179\,,181)$ and $99 < 179 < 198$
$19 \in (17\,,19)$ and $3 \leq 19 < 99$

$200 = 193 + 7$
$193 \in (191\,, 193)$ and $100 < 193 < 200$
$7 \in (5\,, 7)$ and $3 \leq 7 < 100$

Proceeding in this way, we can verify the *Theorem 3.1*for any even integer greater than 6.

3.1.2 Verification of Theorem 3.1 by Program Code

The *Theorem 3.1* can be verified by a program code which can be run by Python programming language.

Program code-1: Verification Theorem 3.1

```
#import numpy as np




def sieve(end):
   '''
   Sieve to get list of prime in a range,
   See: https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes
   '''
prime_list = []
sieve_list = [True] * (end+1)
   #sieve_list = np.ones(end+1,bool)
foreach_number in range(2,end):
ifsieve_list[each_number]:
prime_list.append(each_number)
for multiple in range(each_number*each_number, end+1, each_number):
sieve_list[multiple] = False
returnprime_list


defget_prime_sums(primes,n):
   '''
   Find p1, p2 from the list of primes in the range of n
   '''
prime_sums=[]  #this is a list of pairs (p,q) such that p+q=n
for p in primes:
if p>= n//2  :
break
      q=n-p
if q in primes:
prime_sums.append((p,n-p))
returnprime_sums
```

```
defget_twinprimes(n,primes,prime_sums):
all_twin_primes={} #Dictionary or results, n=p+q will be key, and the set of twin prime will be
values
forpq in prime_sums:
p,q=pq # pq is a pair in the form (p,q)           such that p+q=n
key='%d=%d+%d'%(n,p,q)
twin_primes={
p:[],
                q:[],
                      }
items=0
if p-2 in primes:
items=items+1
twin_primes[p].append((p-2,p))
if p+2 in primes:
items=items+1
twin_primes[p].append((p,p+2))
if q-2 in primes:
items=items+1
twin_primes[q].append((q-2,q))
if q+2 in primes:
items=items+1
twin_primes[q].append((q,q+2))
if items>0:
all_twin_primes[key]=twin_primes
returnall_twin_primes

def verify_theorem_1(n):
   #1. Any number n, remember this is 2n in your theorem, and in place on n, I used n//2
print('n: ',n )
   #2.a. all the prime p in 2..n
primes=sieve(n)
   #print('primes: ',primes)
   #2.b. all p1, p2 such that p1+p2=n
prime_sums=get_prime_sums(primes,n)
   #print('prime_sums: ',prime_sums)
   #import ipdb;ipdb.set_trace()
all_twin_primes=get_twinprimes(n,primes,prime_sums)
print('Showing results for n=%d'%n)
fork,v in all_twin_primes.items():
print('prime sum: '+k)
for p,v1 in v.items(): #v is also a dictionary
prange= '%d<=%d<%d'%(3,p,n//2) if p<=n//2 else '%d<%d<%d'%(n//2,p,n)
          #print(prange+' and, ')
fortwinprime in v1:
```

```
print('%d in %s and %s '%(p,str(twinprime),prange))
print('')

if __name__== '__main__':
   #Change value of n here
   n= 10000
   verify_theorem_1(n) #for a single number n
   '''ns=range(100,200,2) # this will do for all numbers in sequence
for n in ns:
verify_twin_primes(n)'''
print('---The End---')
```

3.2 Lemma

Any positive even integer $2n > 12$ has at least one twin prime $(p_{1,} p_2)$ in between n and $2n$ such that, $n < p_1, p_2 < 2n$.

Example-1

Let, $2n = 14$, so $\mathrm{n} = 7$.
Here, the twin prime $(11, 13)$ is in between 7 and 14 such that,

$$7 < 11, 13 < 14$$

Example-2

Let, $2\mathrm{n} = 100$, so $\mathrm{n} = 50$.
Here, the twin primes $(59, 61)$ and $(71, 73)$ are in between 50 and 100 such that,

$$50 < 59, 61 < 100 \quad \text{and} \quad 50 < 71, 73 < 100$$

Example-3

Let, $2\mathrm{n} = 1000$, so $\mathrm{n} = 500$.
Here the twin primes $(521,\ 523)$, $(569,\ 571)$, $(599, 601)$, $(617,\ 619)$, $(641,\ 643)$, $(809,\ 811)$, $(821,\ 823)$, $(827,\ 829)$ are in between 500 and 1000 such that,

$$500 < 521, 523 < 1000$$
$$500 < 569, 571 < 1000$$
$$500 < 599, 601 < 1000$$
$$500 < 617, 619 < 1000$$
$$500 < 641, 643 < 1000$$
$$500 < 809, 811 < 1000$$
$$500 < 821, 823 < 1000$$
$$500 < 827, 829 < 1000$$

3.2.1 Verification of Lemma 3.2 by Program Code

We can verify *Lemma 3.2* for large even positive integer by using program. The program code to verify *Lemma 3.2* which can be run by programming language Python is given below.

Program code-2: Verification Lemma 3.2

```
def sieve(end):
prime_list = []
sieve_list = [True] * (end+1)
foreach_number in range(2,end):
ifsieve_list[each_number]:
prime_list.append(each_number)
for multiple in range(each_number*each_number, end+1,each_number):
sieve_list[multiple] = False
returnprime_list
defget_number_of_twin_prime_upper_half(primes,n):
twin_primes=[]
for p in primes:
if p< n//2 :
continue #do nothing for for p smaller than n/2
if p+2 in primes:
twin_primes.append((p,p+2))
returntwin_primes

def verify_theorem_3(n):
print('verifying lemma-1 for 2n= %d'%(n))
if n<12:
print('n must be greater than 12!')
exit()
primes=sieve(n)
tp= get_number_of_twin_prime_upper_half(primes,n)
```

```
print('Showing the twin primes between %d and %d:'%(n//2,n))
print(str(tp))
print('number of twin primes between %d and %d is %d'%(n//2,n,len(tp)))

if __name__== "__main__":
   #1. Any number n
   n= 10000
   verify_theorem_3(n)
print("---The End---")
```

3.3 Distance between Two Consecutive Twin Primes

The distance between two consecutive twin primes (except the first two consecutive twin primes) can be represented by $6m + 4$, where m is any nonnegative integer. i.e., $= 0,1,2 \dots$. So we can say after a twin prime we will get one more twin prime exactly after $6m + 4$.
From *Lemma 4.2* we can see that in the inequality $n < p_1, p_2 < 2n$, when n becomes too large the number of twin primes in between n and $2n$ increases. The distance between two consecutive twin primes among those twin prime is $6m + 4$. For large n, m remains too small that we can say $m \ll n$.We discuss this matter later in details in Section 3.5 and 3.6.

3.4 Proposition-1

If $2n$ is an even positive integer, which is formed by the summation of two primes p_1 and p_2 where at least one (say p_1) is one of any twin prime, then

(i) If p_1 is the greater one of that twin prime, then $(2n - 2)$ integer has a summation of two primes where $(p_1 - 2)$ is one.

(ii) If p_1 is the smaller one of a twin prime then $(2n + 2)$ integer has a summation of two primes where $(p_1 + 2)$ is one.

(iii) If p_2 is also one of a twin prime then the same results happened as like p_1 for p_2.

Proof:

Let $2n$ is an even integer.
p_1 and p_2 be two primes such that,

$$p_1 + p_2 = 2n \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (3.4.1)$$

Further let, p_1 is one of any twin prime and it is the greater one of that twin prime.

So, it has a twin,

$$r = p_1 - 2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots\ldots\ldots\ldots\ldots\ldots\ldots. (3.4.2)$$

[By the definition of twin prime]

From equation (3.4.1), we get,

$$p_1 + p_2 = 2n$$

$$\Rightarrow p_1 + p_2 - 2 = 2n - 2$$

[Adding (-2) on both sides]

$$\Rightarrow\ p_1 - 2 + p_2 = 2n - 2$$

$$\Rightarrow \qquad r + p_2 = 2n - 2$$

[From equation (3.4.2)]

This completes the proof of (i).

Again letp_1 is the smaller one of any twin prime.
So, the other one of this twin prime is,

$$s = p_1 + 2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.4.3)$$

From equation (3.4.1),

$$p_1 + p_2 = 2n$$

$$\Rightarrow p_1 + p_2 + 2 = 2n + 2$$

[Adding „2" on both sides]

$$\Rightarrow p_1 + 2 + p_2 = 2n + 2$$

$$\Rightarrow s + p_2 = 2n + 2$$

[From equation (3.4.3)]

This completes the proof of (ii).

Similarly, we can prove (iii) for p_2.

Example-1

Let$2n = 50$ be an even positive integer.
We can express $2n = 50$ as the combination of summations of two primesp_1 andp_2 such that $p_1 + p_2 = 2n$ as follows:

Table 3.3: Prime summations of 50.

50=	47+3	43+7	37+13	31+19

We got a combination of 4 summations of primes for 50.

Let

$$p_1 + p_2 = 2n = 50,$$

Again,

$$47 + 3 = 5.$$

So, let

$$p_1 = 47 \text{ and } p_2 = 3$$

Here, $\mathrm{p}_2 = 3$ is one of a twin prime $(3, 5)$ and it is the smaller one.

So, $\mathrm{s} = \mathrm{p}_2 + 2 = 3 + 2 = 5$ is the other one.

By the proposition 3.4, $2n + 2 = 50 + 2 = 52$ has a combination of summations of two primes where $s = 5$ is one of a summation of primes of 52. So, $52 - 5 = 47$ is a prime.

Now, we express 52 as a combination of summations of two primes as follows:

Table 3.4: Prime summations of 52.

52 =	47+5	41+11	29+23

Here,

$2n + 2 = 52 = 47 + 5 = p_1 + s.$

Example-2

Again from Table 3.3,

Let

$$p_1 + p_2 = 43 + 7 = 50 = 2n.$$

Here,

$$p_1 = 43 \text{ and } p_2 = 7.$$

$p_1 = 43$ is one of the twin prime $(41, 43)$ and the greater one.

And $p_2 = 7$ is one of the twin prime $(5, 7)$ and the greater one.

So, by the *Proposition3.2*,$2n - 2 = 50 - 2 = 48$ must have combination of summations of two primes where, $r_1 = p_1 - 2 = 43 - 2 = 41$ exist and $r_2 = p_2 - 2 = 7 - 2 = 5$ exists. Here, $48 - 41 = 7$ and $48 - 5 = 43$ are two primes.

Now, express 48 as combination of summations of two primes as follows:

Table 3.5: Prime summations of 52.

48=					
	43+5	41+7	37+11	31+17	29+19

Here,

$$2n - 2 = 48 = 43 + 5 = p_1 + r_2$$

And,

$$2n - 2 = 48 = 41 + 7 = r_1 + p_2$$

Note thatthis is true for all other twin primes.

3.5 Proposition-2

If $2n$ is a positive even integer and p_1 and p_2 are two primes such that $p_1 + p_2 = 2n$, then either $p_1 = p_2$ or if $p_1 > n$ and $p_2 < n$ then $p_1 - n = n - p_2$, i.e., if the sum of two primes is equal to an even positive integer then they are equidistant from the half of that integer.

Proof:

Let,

$$p_1 + p_2 = 2n \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.5.1)$$

where,$2n$ is a positive even integer and p_1 and p_2 are two primes.

Now from $(3.5.1)$, we get

$$p_1 + p_2 = 2n$$

$$\Rightarrow p_1 + p_2 - p_2 = 2n - p_2$$

[By adding „$-p_2$' on both sides]

$$\Rightarrow p_1 = 2n - p_2$$

$$\Rightarrow p_1 - n = 2n - p_2 - n$$

[By adding „$-n$' on both sides]

$$\Rightarrow p_1 - n = n - p_2$$

Again,consider

$$2n = 20$$

We can express $2n = 20$ as combination of summations of primes as follows:

Table 3.6: Prime summations of 20.

20=	17+3	13+7

Here,

$$n = 10$$

$$p_1 = 17 \text{ and} p_2 = 3.$$

Then

$$\text{L. H. S.} = p_1 - n$$

$$= 17 - 10$$

$$= 7$$

$$\text{R. H. S.} = p_2 - n$$

$$= 10 - 3$$

$$= 7$$

$$\therefore \text{ L. H. S.} = \text{R. H. S.}$$

Hence the proposition is proved.

3.6 Number of Summations of a Prime Combination of an Even Positive Integer

The number of equidistant prime pair from the half of a positive even integer $2n$ (i.e., from n) is the number of the summations of prime combination of that integer.

We can denote this by

$$N(n \pm l) = q_i.$$

Where,

$$n = \text{half of the positive integer.}$$

$$l = \text{ any number.}$$

$$q_i = \text{symbol for two primes } q_1 \text{ and } q_2 \text{ which we got by adding or subtracting } l \text{ from } n.$$

So,

$$n + l = q_1$$

and

$$n - l = q_2.$$

implies that

$$q_1 - n = l$$

and

$$n + q_2 = l.$$

Note thatif n is even then l is odd and if n is odd then l is even.

Example-1

Let

$$2n = 40$$

$$\Rightarrow \ n = 20$$

All the prime summations of 40 is given as follows:

Table 3.7: Prime summations of 40.

40=	37+3	29+11	23+17

Here,

$$20 - 3 = 17$$
$$37 - 20 = 17.$$

Again,

$$20 - 11 = 9$$
$$29 - 20 = 9.$$

And,

$$23 - 20 = 3$$
$$20 - 17 = 3.$$

Hence the number of summations of prime combination of 40 is

$$N(n \pm l) = 3$$

Example-2

Let

$$2n = 18,$$

$$\Rightarrow \ n = 9$$

All the prime summations of 18 are given as follows:

Table 3.8: Prime summations of 18.

18=	13+5	11+7

Here,

$$13-9=4$$
$$9-5=4$$

Again,

$$11-9=2$$
$$9-7=2$$

Hence the number of summations of prime combination of 18 is

$$N(n \pm l)=2$$

3.7 Distance between Two Consecutive Twin Primes with Example

Let, (p_1, q_1) and (p_2, q_2) be two pair of consecutive twin prime, where

$$q_1 = p_1 + 2$$

and

$$q_2 = p_2 + 2$$

and,

$$p_2 > p_1$$
$$q_2 > q_1$$

Then if $p_1 > 3$ the distance between (p_1, q_1) and (p_2, q_2) can be written in the form

$d((p_1, q_1), (p_2, q_2)) = p_2 - q_1 = 6m + 4$, where$m = 0,1,2,3, \ldots$

If $p_1 = 3$, i.e., for the first two consecutive pair of twin primes(3,5) and (5,7), the distance is zero. Here, q_1 and p_2 are equal and it is 5.

Example

The first 10 successive twin primes are:

$(3\ 5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73), (101,103), (107,109).$

The distances between the two consecutive twin primes successively are given below:

$$\mathrm{d}\big((3,5),(5,7)\big) = 5-5 = 0$$

$\mathrm{d}\big((5,7),(11,13)\big) = 11 - 7 = 4 = 6.0 + 4$; here $m = 0$.
$\mathrm{d}\big((11,13),(17,19)\big) = 17 - 13 = 4 = 6.0 + 4$; here $m = 0$.
$\mathrm{d}\big((17,19),(29,31)\big) = 29 - 19 = 10 = 6.1 + 4$; here $m = 1$.
$\mathrm{d}\big((29,31),(41,43)\big) = 41 - 31 = 10 = 6.1 + 4$; here $m = 1$.
$\mathrm{d}\big((41,43),(59,61)\big) = 59 - 43 = 16 = 6.2 + 4$; here $m = 2$.
$\mathrm{d}\big((59,61),(71,73)\big) = 71 - 61 = 10 = 6.1 + 4$; here $m = 1$.
$\mathrm{d}\big((71,73),(101,103)\big) = 101 - 73 = 28 = 6.4 + 4$; here $m = 4$.
$\mathrm{d}\big((101,103),(107,109)\big) = 107 - 103 = 4 = 6.0 + 4$; here $m = 0$.

After generating so many steps we will find m=5 and m=3and other values can be found proceeding in this way.
So, we can say that, $\mathrm{d}((p_1,\ q_1),\ (p_2,\ q_2)) = p_2 - q_1 = 6m + 4$; where, $m = 0, 1,\ 2,\ 3, \dots$.
Let us consider the inequality $\mathrm{n} < \mathrm{p}_1, \mathrm{p}_2 < 2n$ from *Lemma 3.2*.
Let, $n = 100000000000$. Then $2n = 200000000000$. Then if we talk about few twin primes in between 100000000000 and 200000000000, then we will find the following matter.

$$\mathrm{d}\big((100000000817, 100000000819),(100000001237, 100000001239)\big) = 418 = 6.69 + 4;$$
Here, $m = 69$

$$\mathrm{d}\big((100000001237, 100000001239),(100000001837, 100000001839)\big) = 598 = 6.99 + 4;$$
Here, $m = 99$

$$\mathrm{d}\big((100000001837, 100000001839),(100000001921, 100000001923)\big) = 82 = 6.13 + 4;$$
Here, $m = 13$

$$\mathrm{d}\big((100000001921, 100000001923),(100000002059, 100000002061)\big) = 136 = 6.22 + 4;$$
Here, $m = 22$

$$\mathrm{d}\big((100000002059, 100000002061),(100000002497, 100000002499)\big) = 436 = 6.72 + 4;$$
Here, $m = 72$

$$\mathrm{d}\big((100000002497, 100000002499),(100000002911, 100000002913)\big) = 412 = 6.68 + 4;$$
Here, $m = 68$

$$\mathrm{d}\big((100000002911, 100000002913),(100000002941, 100000002943)\big) = 28 = 6.4 + 4;$$
Here, $m = 4$

$$\mathrm{d}\big((100000002941, 100000002943),(100000003067, 100000003069)\big) = 124 = 6.20 + 4;$$
Here, $m = 20$

$$\mathrm{d}\big((100000003067, 100000003069), (100000003379, 100000003381)\big) = 310 = 6.51 + 4;$$
$$\text{Here}, m = 51$$

$$\mathrm{d}\big((100000003379, 100000003381), (100000003757, 100000003759)\big) = 376 = 6.62 + 4;$$
$$\text{Here}, \mathrm{m} = 62$$

$$\mathrm{d}\big((100000003757, 100000003759), (100000005431, 100000005433)\big) = 1672$$
$$= 6.278 + 4;$$
$$\text{Here}, m = 278$$

In this case, $n = 100000000000$ and the highest value of $m = 278$. So, in this case we say that $m \ll n$.

3.7.1 Verification by Program Code

We can find out the distance between two consecutive twin primes and represent it as $6m + 4$ (where $m = 0, 1, 2, 3, ...$) by using the following program which can be run by using programming language python:

Program code-3: Verification distance between two consecutive primes

```
#import numpy as np

def sieve(end):
   '''
   Sieve to get list of all prime in a range up to end,
   See: https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes
   '''
prime_list = []
sieve_list = [True] * (end+1)
   #sieve_list = np.ones(end+1,bool)
foreach_number in range(2,end):
ifsieve_list[each_number]:
prime_list.append(each_number)
for multiple in range(each_number*each_number, end+1, each_number):
sieve_list[multiple] = False
returnprime_list

def verify_theorem_2(n):
print('Going to verify theorem 2 for primes upto %d'%(n))
status=True
primes=sieve(n) #get list of all the primes in range 2..n, so primes=[2,3,5,7....]
tp=(5,7)
```

```
size=len(primes)
start_index=primes.index(7) #start from the index of 7 in the list as (5,7) already taken
fori in range(start_index,size-1):
        p=primes[i] #prime at the i-th index in the list
pnext=primes[i+1] #prime at the (i+1)-th index, next prime after p
ifpnext== p+2: #if they have difference 2 then they are twin prime
tpnext=(p,pnext) #p,pnext are a pair of twin prime, insert them as pair to list
            #twin_primes.append(tp)
            d=tpnext[0]-tp[1] #d
            n=d//6
            r=d%6 #express d as d= 6*n+r , here r should be 4 according to theorem
            print('d=%3d = 6*%d+%d for: %s, %s '%(d,n,r,str(tp),str(tpnext)))
if r!=4:
print('\nTheorem found wrong for pair %s, %s!'%(str(tp),str(tpnext)))
status=False
break
tp=tpnext #next pair is now current pair as we are done with this pair and going for next pair
return status


if __name__== '__main__':
    #Change value of n here
    n= 1000
    verify_theorem_2(n) #for a single number n
print('---The End---')
```

Executing the program for $n = 10000$ we got the following result:

```
Going to verify the distance in the form 6m + 4 for primes upto 10000
d=  4 = 6*0+4 for: (5, 7), (11, 13)
d=  4 = 6*0+4 for: (11, 13), (17, 19)
d= 10 = 6*1+4 for: (17, 19), (29, 31)
d= 10 = 6*1+4 for: (29, 31), (41, 43)
d= 16 = 6*2+4 for: (41, 43), (59, 61)
d= 10 = 6*1+4 for: (59, 61), (71, 73)
d= 28 = 6*4+4 for: (71, 73), (101, 103)
d=  4 = 6*0+4 for: (101, 103), (107, 109)
d= 28 = 6*4+4 for: (107, 109), (137, 139)
d= 10 = 6*1+4 for: (137, 139), (149, 151)
d= 28 = 6*4+4 for: (149, 151), (179, 181)
d= 10 = 6*1+4 for: (179, 181), (191, 193)
d=  4 = 6*0+4 for: (191, 193), (197, 199)
```

```
d= 28 = 6*4+4 for: (197, 199), (227, 229)
d= 10 = 6*1+4 for: (227, 229), (239, 241)
d= 28 = 6*4+4 for: (239, 241), (269, 271)
d= 10 = 6*1+4 for: (269, 271), (281, 283)
d= 28 = 6*4+4 for: (281, 283), (311, 313)
d= 34 = 6*5+4 for: (311, 313), (347, 349)
d= 70 = 6*11+4 for: (347, 349), (419, 421)
d= 10 = 6*1+4 for: (419, 421), (431, 433)
d= 28 = 6*4+4 for: (431, 433), (461, 463)
d= 58 = 6*9+4 for: (461, 463), (521, 523)
d= 46 = 6*7+4 for: (521, 523), (569, 571)
d= 28 = 6*4+4 for: (569, 571), (599, 601)
d= 16 = 6*2+4 for: (599, 601), (617, 619)
d= 22 = 6*3+4 for: (617, 619), (641, 643)
d= 16 = 6*2+4 for: (641, 643), (659, 661)
d=148 = 6*24+4 for: (659, 661), (809, 811)
d= 10 = 6*1+4 for: (809, 811), (821, 823)
d=  4 = 6*0+4 for: (821, 823), (827, 829)
d= 28 = 6*4+4 for: (827, 829), (857, 859)
d= 22 = 6*3+4 for: (857, 859), (881, 883)
d=136 = 6*22+4 for: (881, 883), (1019, 1021)
d= 10 = 6*1+4 for: (1019, 1021), (1031, 1033)
d= 16 = 6*2+4 for: (1031, 1033), (1049, 1051)
d= 10 = 6*1+4 for: (1049, 1051), (1061, 1063)
d= 28 = 6*4+4 for: (1061, 1063), (1091, 1093)
d= 58 = 6*9+4 for: (1091, 1093), (1151, 1153)
d= 76 = 6*12+4 for: (1151, 1153), (1229, 1231)
d= 46 = 6*7+4 for: (1229, 1231), (1277, 1279)
d= 10 = 6*1+4 for: (1277, 1279), (1289, 1291)
d= 10 = 6*1+4 for: (1289, 1291), (1301, 1303)
d= 16 = 6*2+4 for: (1301, 1303), (1319, 1321)
d=106 = 6*17+4 for: (1319, 1321), (1427, 1429)
d= 22 = 6*3+4 for: (1427, 1429), (1451, 1453)
d= 28 = 6*4+4 for: (1451, 1453), (1481, 1483)
d=  4 = 6*0+4 for: (1481, 1483), (1487, 1489)
d=118 = 6*19+4 for: (1487, 1489), (1607, 1609)
d= 10 = 6*1+4 for: (1607, 1609), (1619, 1621)
d= 46 = 6*7+4 for: (1619, 1621), (1667, 1669)
d= 28 = 6*4+4 for: (1667, 1669), (1697, 1699)
d= 22 = 6*3+4 for: (1697, 1699), (1721, 1723)
```

```
d= 64 = 6*10+4 for: (1721, 1723), (1787, 1789)
d= 82 = 6*13+4 for: (1787, 1789), (1871, 1873)
d=  4 = 6*0+4 for: (1871, 1873), (1877, 1879)
d= 52 = 6*8+4 for: (1877, 1879), (1931, 1933)
d= 16 = 6*2+4 for: (1931, 1933), (1949, 1951)
d= 46 = 6*7+4 for: (1949, 1951), (1997, 1999)
d= 28 = 6*4+4 for: (1997, 1999), (2027, 2029)
d= 52 = 6*8+4 for: (2027, 2029), (2081, 2083)
d=  4 = 6*0+4 for: (2081, 2083), (2087, 2089)
d= 22 = 6*3+4 for: (2087, 2089), (2111, 2113)
d= 16 = 6*2+4 for: (2111, 2113), (2129, 2131)
d= 10 = 6*1+4 for: (2129, 2131), (2141, 2143)
d= 94 = 6*15+4 for: (2141, 2143), (2237, 2239)
d= 28 = 6*4+4 for: (2237, 2239), (2267, 2269)
d= 40 = 6*6+4 for: (2267, 2269), (2309, 2311)
d= 28 = 6*4+4 for: (2309, 2311), (2339, 2341)
d= 40 = 6*6+4 for: (2339, 2341), (2381, 2383)
d=166 = 6*27+4 for: (2381, 2383), (2549, 2551)
d= 40 = 6*6+4 for: (2549, 2551), (2591, 2593)
d= 64 = 6*10+4 for: (2591, 2593), (2657, 2659)
d= 28 = 6*4+4 for: (2657, 2659), (2687, 2689)
d= 22 = 6*3+4 for: (2687, 2689), (2711, 2713)
d= 16 = 6*2+4 for: (2711, 2713), (2729, 2731)
d= 58 = 6*9+4 for: (2729, 2731), (2789, 2791)
d= 10 = 6*1+4 for: (2789, 2791), (2801, 2803)
d=166 = 6*27+4 for: (2801, 2803), (2969, 2971)
d= 28 = 6*4+4 for: (2969, 2971), (2999, 3001)
d=118 = 6*19+4 for: (2999, 3001), (3119, 3121)
d= 46 = 6*7+4 for: (3119, 3121), (3167, 3169)
d= 82 = 6*13+4 for: (3167, 3169), (3251, 3253)
d=  4 = 6*0+4 for: (3251, 3253), (3257, 3259)
d= 40 = 6*6+4 for: (3257, 3259), (3299, 3301)
d= 28 = 6*4+4 for: (3299, 3301), (3329, 3331)
d= 28 = 6*4+4 for: (3329, 3331), (3359, 3361)
d= 10 = 6*1+4 for: (3359, 3361), (3371, 3373)
d= 16 = 6*2+4 for: (3371, 3373), (3389, 3391)
d= 70 = 6*11+4 for: (3389, 3391), (3461, 3463)
d=  4 = 6*0+4 for: (3461, 3463), (3467, 3469)
d= 58 = 6*9+4 for: (3467, 3469), (3527, 3529)
d= 10 = 6*1+4 for: (3527, 3529), (3539, 3541)
```

```
d= 16 = 6*2+4 for: (3539, 3541), (3557, 3559)
d= 22 = 6*3+4 for: (3557, 3559), (3581, 3583)
d= 88 = 6*14+4 for: (3581, 3583), (3671, 3673)
d= 94 = 6*15+4 for: (3671, 3673), (3767, 3769)
d= 52 = 6*8+4 for: (3767, 3769), (3821, 3823)
d= 28 = 6*4+4 for: (3821, 3823), (3851, 3853)
d= 64 = 6*10+4 for: (3851, 3853), (3917, 3919)
d= 10 = 6*1+4 for: (3917, 3919), (3929, 3931)
d= 70 = 6*11+4 for: (3929, 3931), (4001, 4003)
d= 16 = 6*2+4 for: (4001, 4003), (4019, 4021)
d= 28 = 6*4+4 for: (4019, 4021), (4049, 4051)
d= 40 = 6*6+4 for: (4049, 4051), (4091, 4093)
d= 34 = 6*5+4 for: (4091, 4093), (4127, 4129)
d= 28 = 6*4+4 for: (4127, 4129), (4157, 4159)
d= 58 = 6*9+4 for: (4157, 4159), (4217, 4219)
d= 10 = 6*1+4 for: (4217, 4219), (4229, 4231)
d= 10 = 6*1+4 for: (4229, 4231), (4241, 4243)
d= 16 = 6*2+4 for: (4241, 4243), (4259, 4261)
d= 10 = 6*1+4 for: (4259, 4261), (4271, 4273)
d= 64 = 6*10+4 for: (4271, 4273), (4337, 4339)
d= 82 = 6*13+4 for: (4337, 4339), (4421, 4423)
d= 58 = 6*9+4 for: (4421, 4423), (4481, 4483)
d= 34 = 6*5+4 for: (4481, 4483), (4517, 4519)
d= 28 = 6*4+4 for: (4517, 4519), (4547, 4549)
d= 88 = 6*14+4 for: (4547, 4549), (4637, 4639)
d= 10 = 6*1+4 for: (4637, 4639), (4649, 4651)
d= 70 = 6*11+4 for: (4649, 4651), (4721, 4723)
d= 64 = 6*10+4 for: (4721, 4723), (4787, 4789)
d= 10 = 6*1+4 for: (4787, 4789), (4799, 4801)
d=130 = 6*21+4 for: (4799, 4801), (4931, 4933)
d= 34 = 6*5+4 for: (4931, 4933), (4967, 4969)
d= 40 = 6*6+4 for: (4967, 4969), (5009, 5011)
d= 10 = 6*1+4 for: (5009, 5011), (5021, 5023)
d= 76 = 6*12+4 for: (5021, 5023), (5099, 5101)
d=130 = 6*21+4 for: (5099, 5101), (5231, 5233)
d= 46 = 6*7+4 for: (5231, 5233), (5279, 5281)
d=136 = 6*22+4 for: (5279, 5281), (5417, 5419)
d= 22 = 6*3+4 for: (5417, 5419), (5441, 5443)
d= 34 = 6*5+4 for: (5441, 5443), (5477, 5479)
d= 22 = 6*3+4 for: (5477, 5479), (5501, 5503)
```

```
d= 16 = 6*2+4 for: (5501, 5503), (5519, 5521)
d=118 = 6*19+4 for: (5519, 5521), (5639, 5641)
d= 10 = 6*1+4 for: (5639, 5641), (5651, 5653)
d=  4 = 6*0+4 for: (5651, 5653), (5657, 5659)
d= 82 = 6*13+4 for: (5657, 5659), (5741, 5743)
d=106 = 6*17+4 for: (5741, 5743), (5849, 5851)
d= 16 = 6*2+4 for: (5849, 5851), (5867, 5869)
d= 10 = 6*1+4 for: (5867, 5869), (5879, 5881)
d=208 = 6*34+4 for: (5879, 5881), (6089, 6091)
d= 40 = 6*6+4 for: (6089, 6091), (6131, 6133)
d= 64 = 6*10+4 for: (6131, 6133), (6197, 6199)
d= 70 = 6*11+4 for: (6197, 6199), (6269, 6271)
d= 28 = 6*4+4 for: (6269, 6271), (6299, 6301)
d= 58 = 6*9+4 for: (6299, 6301), (6359, 6361)
d= 88 = 6*14+4 for: (6359, 6361), (6449, 6451)
d=100 = 6*16+4 for: (6449, 6451), (6551, 6553)
d= 16 = 6*2+4 for: (6551, 6553), (6569, 6571)
d= 88 = 6*14+4 for: (6569, 6571), (6659, 6661)
d= 28 = 6*4+4 for: (6659, 6661), (6689, 6691)
d= 10 = 6*1+4 for: (6689, 6691), (6701, 6703)
d= 58 = 6*9+4 for: (6701, 6703), (6761, 6763)
d= 16 = 6*2+4 for: (6761, 6763), (6779, 6781)
d= 10 = 6*1+4 for: (6779, 6781), (6791, 6793)
d= 34 = 6*5+4 for: (6791, 6793), (6827, 6829)
d= 40 = 6*6+4 for: (6827, 6829), (6869, 6871)
d= 76 = 6*12+4 for: (6869, 6871), (6947, 6949)
d= 10 = 6*1+4 for: (6947, 6949), (6959, 6961)
d=166 = 6*27+4 for: (6959, 6961), (7127, 7129)
d= 82 = 6*13+4 for: (7127, 7129), (7211, 7213)
d= 94 = 6*15+4 for: (7211, 7213), (7307, 7309)
d= 22 = 6*3+4 for: (7307, 7309), (7331, 7333)
d= 16 = 6*2+4 for: (7331, 7333), (7349, 7351)
d=106 = 6*17+4 for: (7349, 7351), (7457, 7459)
d= 28 = 6*4+4 for: (7457, 7459), (7487, 7489)
d= 58 = 6*9+4 for: (7487, 7489), (7547, 7549)
d= 10 = 6*1+4 for: (7547, 7549), (7559, 7561)
d= 28 = 6*4+4 for: (7559, 7561), (7589, 7591)
d=166 = 6*27+4 for: (7589, 7591), (7757, 7759)
d=118 = 6*19+4 for: (7757, 7759), (7877, 7879)
d= 70 = 6*11+4 for: (7877, 7879), (7949, 7951)
```

d= 58 = 6*9+4 for: (7949, 7951), (8009, 8011)
d= 76 = 6*12+4 for: (8009, 8011), (8087, 8089)
d=130 = 6*21+4 for: (8087, 8089), (8219, 8221)
d= 10 = 6*1+4 for: (8219, 8221), (8231, 8233)
d= 58 = 6*9+4 for: (8231, 8233), (8291, 8293)
d= 94 = 6*15+4 for: (8291, 8293), (8387, 8389)
d= 40 = 6*6+4 for: (8387, 8389), (8429, 8431)
d=106 = 6*17+4 for: (8429, 8431), (8537, 8539)
d= 58 = 6*9+4 for: (8537, 8539), (8597, 8599)
d= 28 = 6*4+4 for: (8597, 8599), (8627, 8629)
d=190 = 6*31+4 for: (8627, 8629), (8819, 8821)
d= 16 = 6*2+4 for: (8819, 8821), (8837, 8839)
d= 22 = 6*3+4 for: (8837, 8839), (8861, 8863)
d=106 = 6*17+4 for: (8861, 8863), (8969, 8971)
d= 28 = 6*4+4 for: (8969, 8971), (8999, 9001)
d= 10 = 6*1+4 for: (8999, 9001), (9011, 9013)
d= 28 = 6*4+4 for: (9011, 9013), (9041, 9043)
d=196 = 6*32+4 for: (9041, 9043), (9239, 9241)
d= 40 = 6*6+4 for: (9239, 9241), (9281, 9283)
d= 58 = 6*9+4 for: (9281, 9283), (9341, 9343)
d= 76 = 6*12+4 for: (9341, 9343), (9419, 9421)
d= 10 = 6*1+4 for: (9419, 9421), (9431, 9433)
d= 4 = 6*0+4 for: (9431, 9433), (9437, 9439)
d= 22 = 6*3+4 for: (9437, 9439), (9461, 9463)
d=166 = 6*27+4 for: (9461, 9463), (9629, 9631)
d= 46 = 6*7+4 for: (9629, 9631), (9677, 9679)
d= 40 = 6*6+4 for: (9677, 9679), (9719, 9721)
d= 46 = 6*7+4 for: (9719, 9721), (9767, 9769)
d= 88 = 6*14+4 for: (9767, 9769), (9857, 9859)
d= 70 = 6*11+4 for: (9857, 9859), (9929, 9931)
---The End---

3.8 Congruent Modulo [1] of the Distance of Two Consecutive Twin Primes

In this section, we briefly discuss the distance between two consecutive twin primes.

3.8.1 Definition [20]

If $m \geq 0$,then the numbers a and b are congruent modulo m, denoted by $a \equiv b \ (mod\ m)$, if a and b leave the same remainder when divided by m. The number m is the modulus of the congruence. The notation $a \not\equiv b(mod\ m)$means that they are not congruent.

Consider the following examples:

1. $25 \equiv 1(\text{mod}4)\text{since } 4|24.$
2. $25 \not\equiv 2(\text{mod}4)\text{since } 4 \nmid 23.$
3. $1 \equiv -3(\text{mod}4)\text{since } 4|4.$

Let two consecutive twin primes be$(p_1, p_2)$and (p_3, p_4), where $p_1 > 3$. Then the distance between them can be expressed using congruence modulo as follows:

$$p_3 - p_2 \equiv 4(\text{mod } 6)$$

Example-1

Let $(17,19)$ and $(29,31)$ be two consecutive twin primes. Then

$$29 - 19 \equiv 4(\text{mod } 6)$$

$$\Rightarrow \qquad 10 \equiv 4(\text{mod } 6)$$

$$\Rightarrow \qquad 6|(10 - 4)$$

$$\Rightarrow \qquad 6|6$$

Example-2

Again, if we consider two consecutive twin primes $(10709, 10711)$ and $(10859, 10861)$,then

$$10859 - 10711 \equiv 4(\text{mod } 6)$$

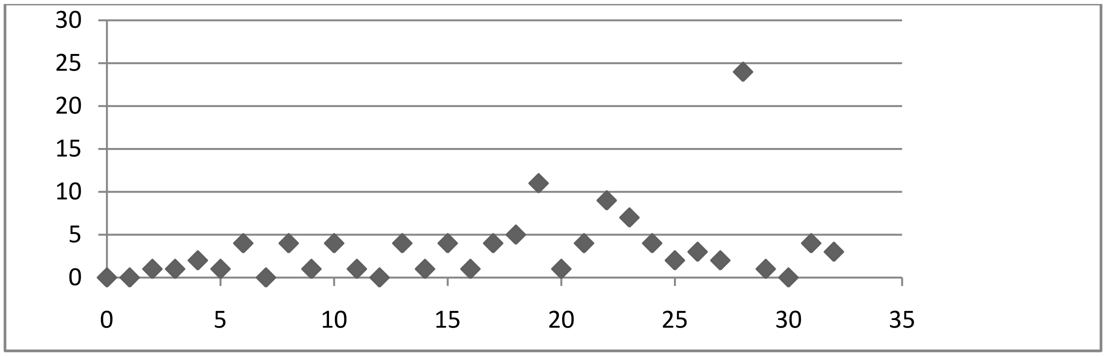
$$\Rightarrow \qquad 148 \equiv 4(\text{mod } 6)$$

$$\Rightarrow \qquad 6|(148 - 4)$$

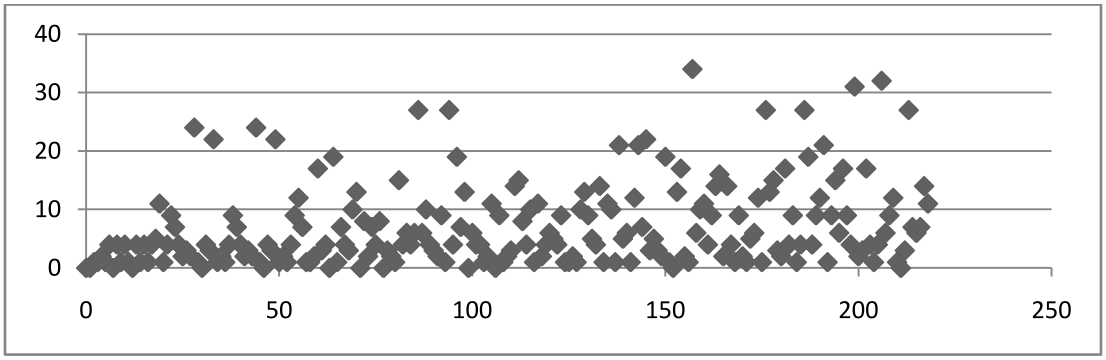
$$\Rightarrow \qquad 6|144$$

3.8.2 Graph of m

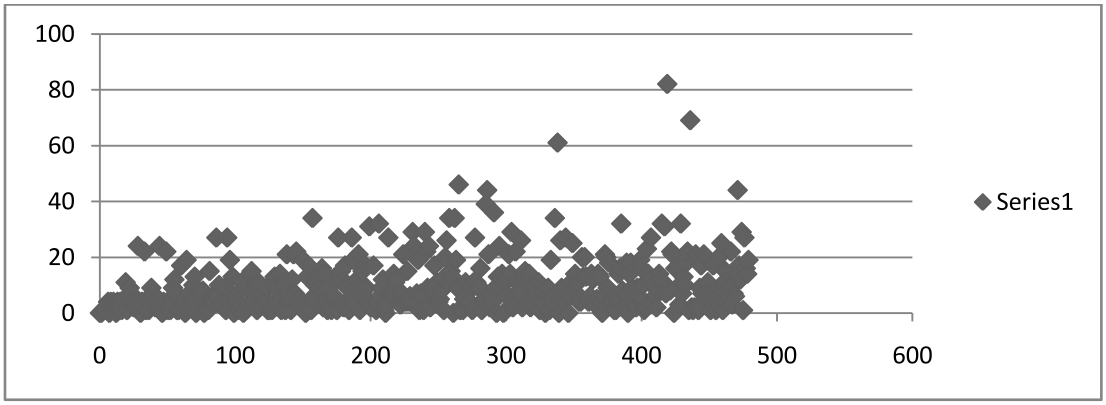
The highest values of m for different values of n from the distance $d = 6m + 4$ of two consecutive twin primes are shown below using Microsoft Office Excel.Here, values of n is presented along the horizontal axis and the values of m is presented vertically.



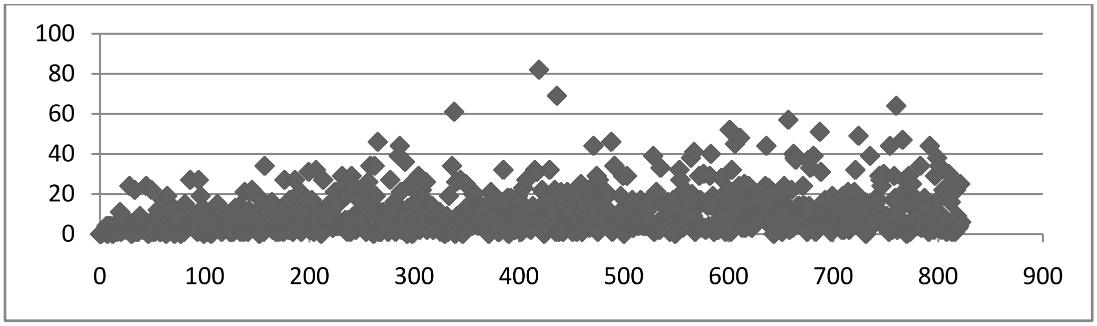
Graph 1: For n=1000 the highest value of m is 24. Here, $\frac{m}{n} = \frac{24}{1000} = .024$ **.**



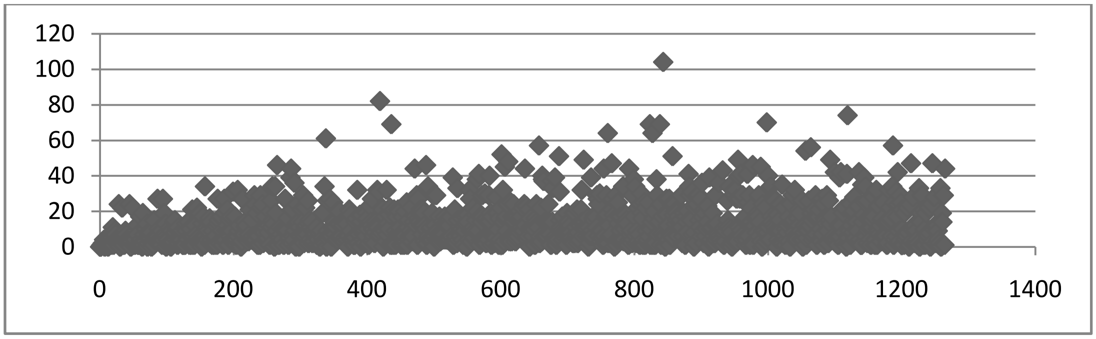
Graph 2: For n=10000 the highest value of m is 34. Here, $\frac{m}{n} = \frac{34}{10000} = .0034$ **.**



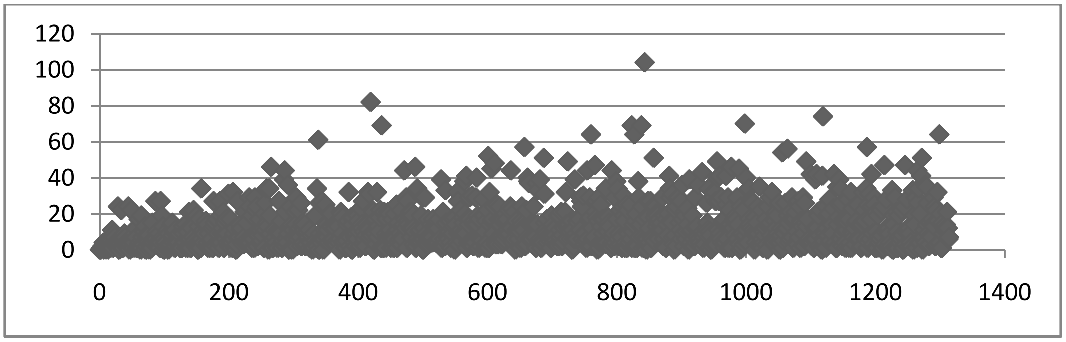
Graph 3: For n=30000 the highest value of m is 82. Here, $\frac{m}{n} = \frac{82}{30000} = .00273$ **.**



Graph 4: For n=60000 the highest value of m is82. Here, $\frac{m}{n} = \frac{82}{60000} = .00137$.



Graph 5: For n=100000 the highest value of m is 104. Here, $\frac{m}{n} = \frac{104}{100000} = .00104$



Graph 6: For n=105000 the highest value of m is 104. Here, $\frac{m}{n} = \frac{104}{105000} = .00099$

From the graph, we see that with the increasing values of *n,* the ratios between m and n decreaseand the differences increase.

CHAPTER 4

APPLICATIONS OF PRIMES IN CRYPTOGRAPHY

The study of numbers, especially prime numbers, has got a huge fascination among the mathematicians from all over the world since ancient times to till date. Since public key cryptography (PKC) is based on prime factorization of whole numbers, we frequently can use prime numbers.

4.1 Applications of prime numbers

The followings are few applications of primes:

i) Finding the factors of a large composite number is difficult. So we find factors of large number, which are prime numbers, called prime factorization. Public key cryptography (PKC) is based on prime factorization of whole numbers.

ii) Applying prime factorization algorithm, quantum computers can efficiently decompose a large number into two prime numbers faster than classical computers.

iii) Prime factorization is a key pair generator. RSA (Rivest-Shamir-Adleman) is a good example of practical use of primes which involves a public key and a private key. The public key that is used to encrypt messages can be known to everyone. Messages encrypted using the public key can only be decrypted with the private key.

iv) Cyber security involves protecting data such as intellectual property, financial data, personal information, or other types of data across networks that are at a very high risk of unauthorized access or exposure. Prime numbers protect us from cybercrime through the RSA encryption system.

v) In coding theory, random number generators, error correcting codes, and hashes often involve primes either directly or indirectly.

vi) In cryptographic applications, elliptic curves over a finite field,has the property that the group order is prime or nearly prime.

4.1.1 Applications of Twin Primes

Twin prime is a pair of primes where both the members of that pair are also primes. So, all the applications for primes are also applicable for twin primes. Further research can be carried outto find more general applications of twin primes.

4.2 Cryptography

Cryptography plays a major role in cyber security. This section will enlighten in cryptography.

4.2.1 Cryptography Goals

By using cryptography many goals can be achieved. These goals can be either all achieved at the same time in one application, or only one of them.

These goals are:

1. **Confidentiality**: It is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.
2. **Authentication:** It is the process of providing the identity that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don‟t have personal knowledge of their identities.
3. **Data Integrity:** It ensures that the received messages have not been changed in any way from its original form. The data may get modified by an unauthorized entity intentionally or accidentally. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.
4. **Non-Repudiation**: It is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.
5. **Access Control:** It is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources. If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access [38].

4.2.2 Types of Cryptography Methods

There are three types cryptography method.

1. Symmetric Cryptography
2. Asymmetric Cryptography
3. Hybrid Cryptography

4.3 Public-Key cryptography

Public-Key cryptography is a form of cryptosystem in which encryption and decryption are performed using the different keys- one a public key and another a private key. These keys are mathematically related although knowledge of one key does not allows someone to easily determine the other key. The sender A uses the public key of receiver B (or some set of rules) to encrypt the plaintext message M and sends the ciphertext C to the receiver. The receiver applies own private key (or rule set) to decrypt the cipher text C and recover the plaintext message M. Because pair of keys is required, this approach is also called asymmetric cryptography. Asymmetric encryption can be used for confidentiality, authentication, or both [36].

Public-key cryptography is used interchangeably with asymmetric cryptography; they both denote exactly the same thing and are used synonymously. Symmetric cryptography has been used for at least 400 years. Public-key cryptography, on the other hand, is quite new. It was publicly introduced by Whitfield Diffie, Martin Hellman and Ralph Merkle in 1976. Much more recently, in 1997 British documents which were declassified revealed that the researchers James Ellis, Clifford Cocks and Graham Williamson from the Uk‟s Government Communications Headquarters (GCHQ) discovered and realized the principle of public-key cryptography few years earlier, in 1972. However, it is still being debated whether the government office fully recognized the far-reaching consequences of public key cryptography for commercial security applications [37].

4.4 Diffie-Hellman Key Exchange

A simple public-key algorithm is Diffie-Hellman key exchange. This protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established. D-H is used for secret-key key exchange only, and not for authentication or digital signatures.

4.4.1 Illustration of Diffie-Hellman Key Exchange

To illustrate Diffie-Hellmen Key Exchange Cryptography ([1], [39]) consider two persons: one is A and another is B. The procedure is as following:

1. A and B together chooses a big prime number p and a number g such that $1 < g < p$.
2. A secretly chooses an integer a.
3. B secretly chooses an integer b.
4. A computes $g^a (mod\ p)$ and tells B the resulting number.
5. B computes $g^b (mod\ p)$ and tells A.
6. The shared secret key is
$$s \equiv (g^a)^b = (g^b)^a = g^{ab} (mod\ p)$$
Which both A and B can compute.

Example

To simplify the above Diffie-Hellmen Key Exchange Cryptography

Let, $p = 89,\ g = 7,\ a = 35,\ b = 65$.

Then A computes $g^a (mod\ p) = 7^{35} (mod\ 89)$. Here,$b^1 = 7,\ b^2 = 49,\ b^3 = 76,\ b^4 = 87,$ $b^8 = 4,\ b^{16} = 16,\ b^{32} = 78, b^{35} = 54$.

Hence A tells B $g^a \equiv 54(mod\ 89)$.

Similarly, B computes $g^b (mod\ p) = 7^{65} (mod\ 89)$or $g^b \equiv 46(mod\ 89)$.

Finally, $s \equiv (g^a)^b \equiv (g^b)^a \equiv 5\ (mod\ 89)$, which can be computed by both A and B.

So A sends $g^a(modp)$ to B. B can interprets and decrypts it operating $g^{ab}(modp)$. And when B sends $g^b(modp)$ to A, A can interprets and decrypts it operating$g^{ab}(modp)$.

The main drawbacks of the Diffie-Hellmen Key exchange is it can be decrypted and changed by third parties.

4.5 RSA Cryptosystem

The first, and still most common, public key cryptography implementation, named for the three MIT mathematicians, who developed it – Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number$n$, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. RSA has three phases: Key Generation, Encryption, and Decryption.The Diffie-Hellman key exchange has drawbacks. In the other hand, the RSA public-key cryptosystem of Rivest, Shamir, and Adleman is more flexible in some ways.

4.5.1 How RSA Works

The fundamental idea behind RSA is to try to construct a trap-door or one-way function on a set X. This is an invertible function

$$E: X \to X$$

such that it is easy for A to compute E^{-1}, but extremely difficult for anybody else to do so.
Here is how A makes a one-way function E on the set of integers $modulo\ n$.

1. A picks two large primes p and q, and lets $n = pq$.
2. It is then easy for A to compute
$$\varphi(n) = \varphi(p).\varphi(q) = (p-1)(q-1).$$
3. A next chooses a random integer e with
$$1 < e < \varphi(n)\ and\ \gcd(e, \varphi(n)) = 1\ .$$
4. A find a solution $x = d$ to the equation
$$ex \equiv 1\ (mod\ \varphi(n)).$$
5. Finally, A defines a function $E: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by
$$E(x) = x^e \in \mathbb{Z}/n\mathbb{Z}.$$

Note that anybody can compute E fairly quickly using the repeated squaring algorithm. A‟s public key is the pair of integers (n, e), which is just enough information for people to easily compute$E$. A knows a number d such that $ed \equiv 1(mod\varphi(n))$, so, as we will see, he/she can quickly compute E^{-1}.

To send a message, proceed as follows. Encode your message, in some way, as sequence of numbers $modulo\ n$.

$$m_1, \dots, m_r \in \mathbb{Z}/n\mathbb{Z}\,,$$

then send

$$E(m_1), \dots, E(m_r)$$

to A.(Recall that $E(m) = m^e$ for $m \in \mathbb{Z}/n\mathbb{Z}$.)

When A receives $E(m_i)$, he/she finds each m_i by using that $E^{-1}(m) = m^d$.

4.5.2 Proposition (Decryption Key)

Let n be an integer that is a product of distinct primes and let $d, e \in N$ be such that$(p-1)|(de-1)$ for each prime $p|n$. Then $a^{de} \equiv a(mod\ n)$ for all $a \in \mathbb{Z}$.

Thus to decrypt $E(m_i)$ A computes

$$E(m_i)^d = (m_i^e)^d = m_i$$

4.5.3 Encoding a Phrase in a Number

In order to use the RSA cryptosystem to encrypt messages, it is necessary to encode them as a sequence of numbers of size less than $n = pq$. We now describe a simple way to do this. Note that in any actual deployed implementation, it is crucial that one adds extra random characters at the beginning of each block of messages, so that the same plain text encodes differently each time. This helps thwart chosen plain text attacks.

Suppose s is a sequence of capital letters and spaces, and that s does not begins with space. We encode s as a number in base 27 as follows: a single space corresponds to 0, the letter A to $1, B$ to $2, \dots, Z$ to 26. Thus "$PRIME\ NUMBERS$" is a number written in base 27.

$$\begin{aligned} PRIME\ NUMBERS \leftrightarrow\ & 27^{12}.16 + 27^{11}.18 + 27^{10}.9 + 27^{9}.13 + 27^{8}.5 + 27^{7}.0 + 27^{6}.14 \\ & + 27^{5}.21 + 27^{4}.13 + 27^{3}.2 + 27^{2}.5 + 27^{1}.18 + 19 \\ & = 2401514164751985936 + 100063090197999414 \\ & \quad +1853020188851841 + 99132767304831 + 1412147682405 \\ & \quad +5423886846 + 301327047 + 6908733 + 39366 + 3645 + 4 + 19 \\ & = 2503530825785990569 \end{aligned}$$

To recover the letters from decimal number, repeatedly divide by 27 and read off the letter corresponding to each remainders.

$$\begin{array}{rcll} 2503530825785990569 & = & 92723363917999650.27 + 19 & "S" \\ 92723363917999650 & = & 3434198663629616.27 + 18 & "R" \\ 3434198663629616 & = & 127192543097393.27 + 5 & "E" \end{array}$$

$$\begin{array}{rrc}
127192543097393 = & 4710834929533.27 + 2 & "B" \\
4710834929533 = & 174475367760.27 + 13 & "M" \\
174475367760 = & 6462050657.27 + 21 & "U" \\
6462050657 = & 239335209.27 + 14 & "N" \\
239335209 = & 8864267.27 + 0 & "Space" \\
8864267 = & 328306.27 + 5 & "E" \\
328306 = & 12159.27 + 13 & "M" \\
12159 = & 450.27 + 9 & "I" \\
450 = & 16.27 + 18 & "R" \\
16 = & 0.27 + 16 & "P"
\end{array}$$

If $27^k \leq n$, then any sequence of k letters can be encoded as above, using a positive integer $\leq n$. Thus if we can encrypt integers of size at most n, then we must break our message up into blocks of size at most $\log_{27}(n)$.

4.5.4 Some Complete Examples

To make the arithmetic easier to follow, we use small prime numbers p and q and encrypt the single letter "P" using the RSA cryptosystem. First, we compute the parameters of an RSA cryptosystem.

1. Choose p and q: Let $p = 13, q = 11$, so $n = pq = 143$.
2. Compute $\varphi(n)$:
$$\varphi(n) = \varphi(p.q) = \varphi(p).\varphi(q) = (p-1)(q-1)$$
$$= pq - p - q + 1 = 143 - 13 - 11 + 1 = 120.$$
3. Randomly choose an $e < 120$ such that $\gcd(e, \varphi(n)) = 1$: We choose $e = 77$.
4. Solve
$$77x \equiv 1(mod\ 120).$$

To solve this we will use Gcd algorithm to find x, y such that $77x + 120y = 1$:

$$120 = 1.77 + 43$$
$$77 = 1.43 + 34$$
$$43 = 1.34 + 9$$
$$34 = 3.9 + 7$$
$$9 = 1.7 + 2$$
$$7 = 3.2 + 1$$

Then,

$$43 = -1.77 + 120$$
$$34 = 2.77 - 120$$
$$9 = -3.77 + 2.120$$
$$7 = 11.77 - 7.120$$
$$2 = -14.77 + 9.120$$
$$1 = 53.77 - 34.120$$

Using the GCD algorithm, we find that $d = 53$which solves the equation.

We have thus computed the parameters of an RSA public key cryptosystem.

The public key is $(143, 77)$, so the encryption function is

$$E(x) = x^{77},$$

And the decryption function is

$$D(x) = x^{53}.$$

Next, we encrypt the letter "P". It is encoded as the number 16, since P is the $16th$ letter of the alphabet. We have
$E(16) = 16^{77} = 113 \in \mathbb{Z}/143\mathbb{Z}$.
To decrypt, we compute E^{-1}:
$E^{-1}(113) = 113^{53} = 16 \in \mathbb{Z}/143\mathbb{Z}$.

4.5.5 Attacking RSA

Suppose the public key of A is (n, e) and his/her decryption key is d, so $ed \equiv 1(mod\ \varphi(n))$. If somehow we can compute the factorization $n = pq$ and can compute $\varphi(n) = (p-1)(q-1)$ then we can compute d. Thus, if we can factor n then we can break the corresponding RSA public-key cryptosystem.

CHAPTER 5

CONCLUSION

In this paper, *Theorem 3.1*shows the summation of two primes of an even integer greater than 6 where one of the primes could be one of a twin prime in between n and $2n$ or in between 3 and n or 3. From which we can deduce the *Lemma 3.2*which is a more precise form of *Theorem 3.1* and states that, there is at least one twin prime in between nand $2n$, when $2\mathrm{n} > 12$. We have verified both of them for any n by using programming code in programming language Python. We can easily verify those for 6 to 7 digits. For time and space complexity of program it takes a long time to verify those for large number of digits.

Here we have also given two propositions. We have seen that, by using *Proposition-1* we can find out few prime summations of two consecutive even integers if the prime summation of one is known and where one prime is one of a twin prime. *Proposition-2* finds out the equality of two primes from the middle of the integer (which is the summation of those two primes).

At last we have seen that the distance between two consecutive twin primes can be represent in the form $6m + 4$, where $m = 0,1,2,3, \dots$ and it was verified by a program run by Python programming language.

5.1 Future Scope

Study on prime number shows that in number theory prime numbers achieved a certain place. Twin primes are arranged in a certain manner. Further study on twin prime may evolve many unknown matter of number theory.

REFERENCES

[1] Stein, W., *Elementary Number Theory: Primes, Congruences and Secrets*, Springer, 2017.

[2] Kuhl, H. K., *Prime Numbers-Things Long-Known and Things New-Found*, Germany, Eckhard Bonder, Pressath, 2019.

[3] Rezgui, H., Conjecture Of Twin Primes (Still Unsolved Problem in Number Theory) An Expository Essay, *Surveys in Mathematics and its Applications*, Vol 12, pp. 229-252, 2017.

[4] Sondow, J. , "Ramanujan Primes and Bertrand‛‛s Postulate", The American Mathematical Monthly, *Mathematical Association of America*, Vol. 116(7), pp. 630-635, 2009.

[5] Silva, T. O. e, Herzog, S., Pardi, S., "Empirical Verification of the Even Goldbach Conjecture and Computation of Prime Gaps up to 4•10^18", Mathematics of Computation, *American Mathematical Society*, Vol. 83(288), pp. 2033-2060, 2014.

[6] Cai, Y., "On Chen‛‛s theorem (II)", Journal of Number Theory, *Elsevier*, Vol. 128(5), pp. 1336-1357, 2008.

[7] Gunasekara, A. R. C. D. V., Jayathilake, A. A. C. A., Perera, A. A. I., "Survey On Prime Numbers", Elixir International Journal, *Elixir Appl. Math.,* Vol. 88, pp. 36296-36301, 2015.

[8] Jhang, Y., "Bounded Gaps Between Primes", Annals Of Mathematics, *Ann. of Math. (2),* Vol. 179(3), pp.1121-1174, 2014.

[9] Murty, M. R., "New developments on the twin prime problem and generalizations", Hardy-Ramanujan Journal, *Hardy-Ramanujan Society*, Vol. 37, pp. 13-19, 2014.

[10] Maynard, J., "Bounded Gaps Between Primes", Annals Of Mathematics, *Annals of Mathematics*, Vol. 181, pp.383-413, 2015.

[11] Yue, Z., "A proof on the conjecture of twin primes", International Journal of Applied Mathematics and Theoretical Physics, *SciencePG*, Vol. 5(3), pp. 82-84, 2019.

[12] Baoshan, Z., "Researches On The Twin Prime Problem", Mathematics, *General Mathematics*, pp. 16,Arxiv:1405.2490. 2014.

[13] Kuhlman, D., *A Python Book: Beginning Python, Advanced Python and Python Exercises*, Platypus Global Media, 2011.

[14] Nicely, T., “Enumeration To 10^4 Of The Twin Primes And Brun‟s Constant.” *Virginia J. Sci.*, Vol. 46, pp. 195-204, 1996.

[15] Meher, J., Murty, M. R., “Ramanujan‟s Proof of Bertrand‟s Postulate”, The American Mathematical Monthly, *Mathematical Association of America,* Vol. 120(7), pp.650-653, 2013.

[16] Guy, R.K., *Unsolved Problems In Number Theory, 3rd edition*. New York, Springer, 2004.

[17] Anton, H., Bivens, I., Davis, S., *Calculus: Early Transcendentals, 10th Edition*, Hoboken, New Jersey, John Wiley and Sons, Inc., 2012.

[18] Mazur, B., Stein, W., Prime *Number And The Riemann Hypothesis*. Cambridge University Press, 2016.

[19] Wijesuriya H. H. K. G., “Proof of Twin Prime Conjecture”, Global Journal of Pure and Applied Mathematics, *Research India Publications*, Vol. 15(5), pp. 615-622, 2019.

[20] Hefferon, J., *Elementary Number Theory, A Revision By Jim Hefferon, St. Michael’s College.* (Notes By W. Edwin Clark, University Of South Florida, 2002), 2003.

[21] Nazardonyavi, S., *Some History About Twin Prime Conjecture*. Cornell University, arXiv:1205.0774v1 [math.HO], 2012.

[22] Arenstorf, R. F., “There Are Infinitely Many Prime Twins”, 2004. Http://Arxiv.Org/Abs/Math/0405509v1, Posted On May 26, 2004; Withdrawn on June 9, 2004.

[23] Carella, N. A., *Primes Counting Methods: Twin Primes*, Cornell University, 2012.

[24] Ruiz, S. M., Ariff, A., “Basic Characteristic of Twin Primes and it‟s Generalization”, *Smarandache Notions Journal Archive*, Vol. 14(1), 2004.

[25] Iverson, K. E., *A Programming Language*, New York , John Wiley Inc., 1962.

[26] Knuth, D. E., *The Art of Computer Programming II: Seminumerical Algorithms, Third Edition.* Massachusetts, Addison Wesley, Reading, 1998.

[27] Bradley, C. J., “The Location of Twin Primes”, *The mathematical Gazette*, Vol. 66(442), pp. 292-294, 1983.

[28] Estermann, T., “On Goldbach's Problem: Proof that Almost All Even Positive Integers are Sums of Two Primes”, London Mathematical Society, *Proc. London*, Vol. s2-44(1), pp. 307-314, 1938.

[29] Ross, P.M., “On Chen‟s Theorem that Each Large Even Number Has the Form $\mathrm{P}_1 + \mathrm{P}_2 \mathrm{Or} \mathrm{P}_1 + \mathrm{P}_2 \mathrm{P}_3$”, *Journal of the London Mathematical Society,* Vol. e S2-10(4), Pp.500-506, 1975.

[30] Kumar, V., “Prime Number Generation and Factor Elimination”, 2014. Arxiv:1411.3356v1 [Math.GM].

[31] Goldstein, L. J., “A History of the Prime Number Theorem”, The American Mathematical Monthly, *Mathematical Association of American*, Vol. 80(6), pp. 599-615, 1973.

[32] Desai, T., “Application of Prime Numbers in Computer Science and the Algorithms Used to Test the Primility of a Number”, International Journal of Science and Research, *IJSR*, Vol. 4(9), pp. 132-135, 2013.

[33] Aparajita, Rana, A., “Steneography- “The Art of Hiding Information” A comparison from Cryptography”, International Journal of Innovative Research in Science, Engineering and Technology, *IJIRSET*, Vol. 2(5), pp. 1308-1312, 2003.

[34] Stallings, W., “*Cryptography and Network Security Principles and Practice*”, New York, Pearson Education, Inc., 2011.

[35] Singh, P., Shende, P., “Symmetric Key Cryptography: Current Trends”, International Journal of Computer Science and Information Technology, *IJCSMC*, Vol. 3(12), pp. 410-415, 2014.

[36] Kumar, S. N., “Review on Network Security and Cryptography”, International Transaction of Electrical and Computer Engineer‟s System, *Science and education Publishing*, Vol. 3(1), pp. 1-11, 2015.

[37] Paar, C., Pelzl, J., *Understanding Cryptography*. Verlag Berlin, Heidelberg, Springer, 2010.

[38] Kumari, S., “A Research Paper on Cryptography Encryption and Compression Techniques”, International Journal of Engineering and Computer Science, *IJECS,* Vol. 6(4), pp. 20915-20919, 2017.

[39] Schneier, B., *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth)*, John Wiley & Sons, Inc., 1996.