Hexile Sieve Analysis of Natural Numbers with Zero and Prime-Counting Fuction

by

Adnan Khaliq

A dissertation submitted in partial fulfillment of the requirements
for the degree of Master of Philosophy in Mathematics

Supervised by

Dr. Matloob Anwar

Department of Mathematics, School of Natural Sciences
National University of Sciences and Technology
Islamabad, Pakistan

23 October 2013

Abstract

We present a sieve for analyzing composite and the prime numbers using equivalence classes based on the modulo 6 return value as applied to the natural numbers. Five characteristics of this Hexile sieve are brushed up. The first aspect is that it narrows the search for primes to one-third. The second feature is that we can obtain from the equivalence class formulae, a property of its diophantine equations to distinguish between primes and composites resulting from multiplication of these primes. Thirdly, we ascribe a non-random occurrence to not only the composites in the two equivalence classes but by default and as a consequence: non-randomness of occurrence to the resident primes from these diophantine formulations. Fourthly, we develop a theoretical basis for sieving primes. In the last, we discuss about the diophantine equations that allow another route to a prime counting function.

Acknowledgement

My thanks goes first to Almighty Allah, Who gives power to the weak and helps the helpless, The most Gracious and Merciful.

I would like to thank my supervisor, Assistant Professor at School of Natural Sciences (SNS), Dr. Matloob Anwar, for his many valuable suggestions, his support, guidance and encouragement throughout my thesis and research work.

I also wish to express my appreciation to the principal of SNS, National University of Sciences and Technology, Islamabad, Dr. Azad A. Siddiqui for his valuable support and efforts for the students of his department.

I am also thankful to all the faculty members, especially Dr. Rashid Farooq, Dr. Muhammad Imran from SNS-NUST, Dr. Quanita Kiran from SEECS-NUST and Dr. Tayyab Kamran from Department of Mathematics, Quaid-i-Azam University Islamabad for their kind attention and encouragement.

My thanks also go to all of my friends. I cannot name all of them but some are, (at SNS) Ali, Afzal, Lt. Afzal, Hashir, Irfan, Sheraz, Shoaib, Tauseef and Yasir for making my time memorable.

(Friend names are alphabetically arranged;)

Adnan khaliq

Contents

Chapter 1

Prime and Composite Numbers

1.1 Prime Numbers

A natural number (i.e. 1, 2, 3, 4, etc.) is called a prime number or simply prime if it has just two positive divisors, 1 and the number itself [5].

2 is a prime because 2 has only positive divisors by 1 and 2. 3 is also prime: the only natural numbers dividing 3 are 1 and 3. However, 4 is not a prime, since 2 is another number dividing 4 without remainder in addition to 1 and 4. Any even number greater than 2 is not prime because by definition, any even number n, greater than 2 has at least three distinct positive divisors, namely 1, 2, and n. This implies that n is not prime. Consequently, the term odd prime is related to any prime greater than 2. Similarly, all prime numbers greater than 5 when written in the usual decimal system have the last digit 1, 3, 7, or 9, because all the even numbers are divisible by 2 and numbers ending in 0 or 5 are divisible by 5.

If n is a prime, then n is only divided by 1 and n without remainder. Therefore, we can also restate the condition of being a prime as: a number n greater than 1 is a prime number if it can not be divided by any of $2, 3, 4, ..., n - 1$ without remainder. However another way to state the same is: a number n greater than 1 is prime number if there do not exist any two greater than 1 integers a and b such that $n = a.b$.

List of all less than 1000 primes is.

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
53	59	61	67	71	73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173	179	181	191	193	197
199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359	367	373	379
383	389	397	401	409	419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541	547	557	563	569	571
577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743	751	757	761
769	773	787	797	809	811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941	947	953	967	971	977
983	991	997												

We can divide roughly, the theory of primes into main four inquiries:

(i) How many prime numbers are there?

(ii) How one can recognize them?

(iii) How one can create them?

(iv) How are prime numbers distributed between the natural numbers?

Theorem 1.1.1. *There are boundlessly many primes. It can also be stated as: the prime numbers 2, 3, 5, 7, 11, ... never end.*

Above theorem is cited to, in honor of the ancient Greek mathematician Euclid as "*Euclid's theorem*", since the first known proof for this theorem is assigned to him. Many more proofs about infiniteness of primes are known, including an analytical proof by Euler, Goldbach's proof based on Fermat numbers [16], using general topology Furstenberg's proof [1] and elegant proof of Kummer [13]. In mathematics, the Riemann hypothesis, suggested by Bernhard Riemann (1859), is a conjecture that the real part of all the nontrivial zeros of the Riemann zeta function is 1/2. In addition to the Riemann hypothesis, many more conjectures relating about prime numbers have been posed. Often having an elementary formulation, many of these conjectures have resisted a proof for decades: all four of problems of Landau from 1912 are even unsolved. One of them is conjecture of Goldbach, which asserts that every greater than 2 even integer n can be represented as a sum of two prime numbers. As of February 2011, this conjecture has been proved for all numbers up to $n = 2 \times 10^{17}$ [15]. Weaker arguments than this have been proven, for example Vinogradov's theorem states that "every sufficiently large odd integer can be written as a sum of three primes". Chen's theorem states that "every sufficiently large even number can be expressed as the sum of a prime and a semiprime, the product of two primes". Also, "any even integer can be written as the sum of six primes [12]". The branch of number theory examining such questions is called additive number theory.

In number theory, the asymptotic distribution of the primes is given by the prime number theorem (PNT). The prime number theorem (PNT) gives a general description of how the prime numbers are distributed between the natural numbers. It formalizes the intuitive thought that prime numbers become less common as they become bigger. In mathematics, the function which is used to count the number of prime numbers less than or equal to some real number n is called prime-counting function [3]. It is denoted by $\pi(n)$ (this does not relate to the number π). Following graph shows the values of $\pi(n)$ for first 60 non-negative integers.

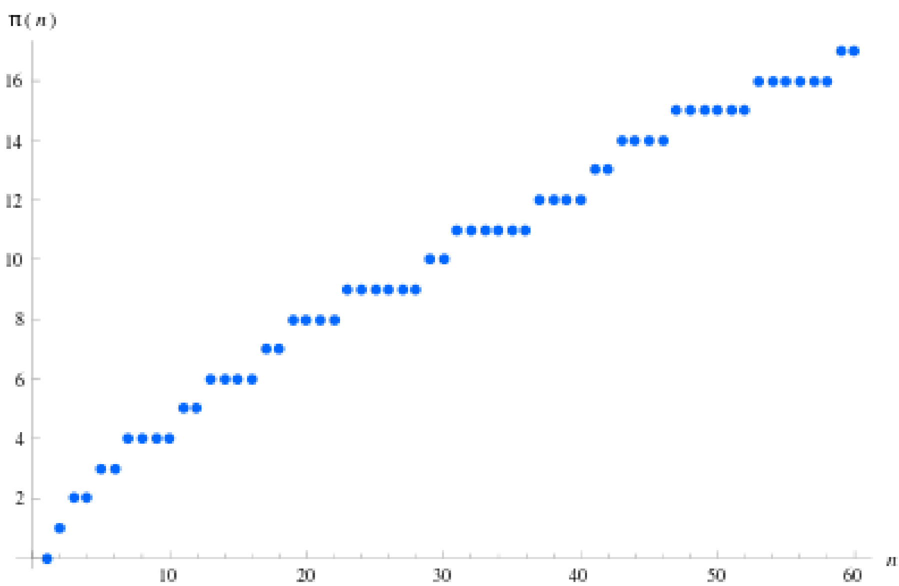

Figure 1.1: The Value of $\pi(n)$ for First 60 Integers

The growth rate of prime-counting function is of great interest in number theory. At the end of the 18th century, it was conjectured by Gauss and Legendre to be approximately:

$$\pi(n) = \frac{n}{\ln n}. \tag{1.1}$$

In the sense that

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1.$$

The above statement is called prime number theorem. Jacques Hadamard and Charles de la Valle Poussin proved the prime number theorem in 1896 first time independently, using properties of the Riemann zeta function given by Riemann in 1859.

There are many interesting facts about prime numbers, some of them are: 1 is not a prime because there must be exactly two divisors of a prime number, 1 and number itself but 1 has only one divisor which is 1 itself. There is only one even prime number “2”and it is the smallest prime number. The scientists have interest in prime numbers, especially in larger ones. Larger prime numbers are used as keys to send secret messages in codes. Such codes are difficult to break because they are not easy to find. There is no formula to find the sequence of prime numbers. The table below shows an indication of ”how many prime numbers are there” and their % in all numbers.

Range from 0 to	Number of primes	% of primes
10	4	40%
100	25	25%
1000	168	16.8%
10000	1229	12.3%
100000	9592	9.6%
1000000	78498	7.8%
10000000	664579	6.6%
100000000	5761455	5.8%
1000000000	50847534	5.1%
10000000000	455052511	4.6%

Table 1.1: Number of primes from 0 to 10000000000 and their % among the numbers

The prime numbers constitute at the same time one of the most basic and one of the most confusing concepts in the whole mathematics. They are, according to the fundamental theorem of arithmetic, the “atoms”or “building blocks”of the integers and have been studied ever since mankind started studying mathematics itself. Indeed, even today, you would be hardly pressed to find an elementary number theory book or course that does not mention them at the beginning; Euclid’s proof about the infinity of primes is among the very first proofs, any young mathematician encounters. At the same time, the primes are at the heart of many of modern mathematics’ hardest and most puzzling problems, from the famous Goldbach and Twin Prime conjectures to the Riemann Hypothesis, widely considered one of the most important unsolved problems of the whole mathematics. Although they are among the “purest”of mathematical objects, their theory has applications in areas of cryptography and computer science. We think to know them well yet they constantly surprise us with their properties and behavior. The whole theory of prime numbers is filled with such conflicting truths and indeed our very attitudes towards them have ranged from adoration (as was the case of the Pythagoreans) to confusion (as is echoed by Euler's quote, even though few in the history of mathematics have been as acquainted with them as he was).

1.1.1 Historical Background

The prime numbers have a deep history. The ancient Egyptians were known as earliest civilization who know about prime numbers. There aren't many strong evidence that they absolutely knew about prime numbers, Only the surviving records show that they had some knowledge. The earliest civilization that has a surviving record of prime numbers come from the Greeks. Euclid's Elements, a mathematical writing that includes 13 books composed by Euclid in 300BC, included important theorems about primes. Euclid was able to solve how to create a perfect number (a positive integer which is equal to the sum of of its positive divisors), using Mersen prime. After the Greeks, there is a huge gap in prime numbers until the 17th century, because nothing really happened in the development of prime numbers.

In 1640, Pierre de Fermat conjectured that all the integers of the form $2^{2^n} + 1$ are prime, and he did not provide any proof. His theory was only true until $n = 5$ because $2^{2^5} + 1 = 4294967297$ is a composite number. In the 19th century, Gauss and Legendre theorized that as n moves to infinity, the number of primes up to n is approximately equal to n/lnn . In 1859, Riemann wrote a paper on the zeta function, which eventually let to Hadamard proving the prime number theorem in 1896.

Until 1970, prime numbers are thought to be pretty useless in the real world, and can only be used in theoretical mathematics. In 1970, the public-key cryptography, a system requiring two separate keys to open, was invented. Prime numbers were the basic building blocks for the public-key cryptography's first algorithms. Since 1951, the largest prime numbers were founded by the computers. However, there are a lot of interests to find even greater prime numbers. The "Great Internet Mersenne Prime Search"and other 3rd party organizations are trying to find bigger prime numbers for the past 15 years. Interest in prime numbers is still high, and they are yet to be fully understood by mathematicians today.

1.2 Composite Numbers

A natural number that can be divided by a natural number without leaving any remainder other than 1 and itself is called a *composite number*. In other words any positive integer greater than one is called a composite number if it is not a prime number [11].

For example, since $6 = 1 \times 6 = 2 \times 3$.
It means 2 and 3 can divide 6, so 6 is composite.
Also $15 = 15 \times 1 = 5 \times 3$.
Which shows that 3 and 5 are divisors of 15, so 15 is composite.
Let $n > 0$ be an integer, if there exist integers a greater than 1 and integer b less than $n$such that $n = ab$, then n is a composite integer. For example, the integer 14 can be factored as 2×7, so 14 is a composite number. But, the integers 2 and 3 are not composite numbers because each of them can be divided only by 1 and the number itself.
The integer 1 is a unit; it is neither composite nor prime [6]. All the even numbers can be divided by 2 and so all greater than 2 even numbers are composite numbers. All numbers that are divisible by 5 end in 5. Therefore all numbers which are greater than 5 and end with 5 are composite numbers. The list of first 100 composite numbers is

4	6	8	9	10	12	14	15	16	18	20	21	22	24	25
26	27	28	30	32	33	34	35	36	38	39	40	42	44	45
46	48	49	50	51	52	54	55	56	57	58	60	62	63	64
65	66	68	69	70	72	74	75	76	77	78	80	81	82	84
85	86	87	88	90	91	92	93	94	95	96	98	99	100	102
104	105	106	108	110	111	112	114	115	116	117	118	119	120	121
122	123	124	125	126	128	129	130	132	133					

Theorem 1.2.1 (Fundamental Theorem of Arithmetics)**.** *Every composite number can be represented as the product of two or more primes (not need to be distinct); moreover, this representation is unique up to the order of the components.*

Proof. □

Every greater than 1 positive integer n can be represented in just one way as a product of prime powers:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

where $p_1 < p_2 < ... < p_k$ are prime numbers and the α_i denote positive integers. This representation is known as *canonical representation* of n.
For example $333 = 3^2 \times 37$, $2000 = 2^4 \times 5^3$, $715 = 5 \times 11 \times 13$ etc. The table given below prime factorization of first twenty composite numbers.

Composite Number	Prime Factorization	Composite Number	Prime Factorization
4	2^2	20	$2^2 \times 5$
6	2×3	21	3×7
8	2^3	22	2×11
9	3^2	24	$2^3 \times 3$
10	2×5	25	5^2
12	$2^2 \times 3$	26	2×13
14	2×7	27	3^3
15	3×5	28	$2^2 \times 7$
16	2^4	30	$2 \times 3 \times 5$
18	2×3^2	32	2^5

Table 1.2: Prime factorization of first twenty composite numbers

1.2.1 Types of Composite Numbers

By counting the number of prime factors, we can classify the composite numbers. A composite number is called a semiprime or 2-almost prime if it has only two prime factors, the factors need not to be distinct, so squares of primes are included. A composite is called sphenic number if it has three distinct prime factors. It is necessary to differentiate between composite numbers with an even number of distinct prime factors and those with an odd number of distinct prime factors in some applications.

A composite number is called a powerful number if all the prime factors of number are repeated. If all the prime factors are non-repeated, then it is called squarefree (1 and all prime numbers are squarefree). We can classify composite numbers by counting the number of divisors also. There exist at least three divisors for any composite number. If a number n has more divisors than any x less than n, then it is called highly composite number. So the first two such numbers are 1 and 2.

1.3 Arithmetic Progression

If the common difference $(a_n - a_{n-1})$ between any two consecutive terms of a sequence of numbers is constant then it is called an arithmetic progression $(A.P)$ or an arithmetic sequence .

For example 7, 15, 23, 31, 39, . . . is an arithmetic sequence with common difference of 8.

If a_1 is the initial term of an arithmetic progression and d is the common difference between any two consecutive terms, then the nth term of arithmetic progression is denoted by a_n and is given by

$$a_n = a_1 + (n-1)d, \tag{1.2}$$

and generally, we can write for $m \leq n$

$$a_n = a_m + (n-m)d.$$

The behavior of an arithmetic progression depends upon the common difference d. If the common difference d is:

- Greater than 0, the members (terms) will tend towards positive infinity.
- Less than 0, the members (terms) will tend towards negative infinity.

Finding the number of terms of an $A.P$ less than or equal to any given number

Let an $A.P$ and a number be given. We have to find number of terms of $A.P$ less than or equal to that given number. Let C be a given number and suppose a_1 is the first term of arithmetic progression and d is the common difference between any two consecutive terms. Let number of term of a_n be n such that

$$a_n \leq C.$$

Using equation (1.2), we can write

$$\begin{aligned} a_1 + (n-1)d &\leq C \\ n &\leq \frac{C - a_1 + d}{d}. \end{aligned}$$

Let k be the number of term of a_k such that a_k is the largest term which is less than C. Then we can write

$$k = Floor\left[\frac{C - a_1 + d}{d}\right].$$

Where "$Floor[\cdot]$"denotes the floor function.
The above process can be explained by using following example.

Example 1.3.1. *Let 2, 6, 10, 14, $\cdots$ be an arithmetic progression. Then*

$$a_1 = 2,$$

and

$$d = 4.$$

Suppose we have to find the total number of terms of above arithmetic progression less or equal to $C = 155$. *Let* n *be the number of term of* a_n *such that*

$$a_n \leq 155.$$

Using equation (1.2), *we can write*

$$a_1 + (n-1)d \leq C.$$

By putting values, we get

$$\begin{aligned} 2 + (n-1)4 &\leq 155 \\ n &\leq \frac{157}{4}. \end{aligned}$$

Let k *be the number of term of* a_k *such that* a_k *is the largest term which is less than* $C = 155$. *Then we can write*

$$k = Floor\left[\frac{157}{4}\right] = 39.$$

Hence number of terms of A.P 2, 6, 10, 14, $\cdots$ *which are less than or equal to 155 is 39.*

Chapter 2

Sieve Methods

Sieve method, or the method of sieves, can mean

1. in mathematics and computer science, a simple method for finding prime numbers e.g. the sieve of Eratosthenes;

    - in number theory, any of a variety of methods studied in sieve theory.
    - in combinatorics, the set of methods dealt with in sieve theory or more specifically, the inclusion-exclusion principle.

2. in statistics, and particularly in econometrics, the use of sieve estimators.

The history of sieve methods is very long and productive. The sieve of Eratosthenes (around 3rd century B.C.) was a tool to produce prime numbers. later on it is used by Legendre in his study of the prime counting function $\pi(x)$. After the initiating work of Viggo Brun, sieve methods flourished and became a topic of intense investigation. Using his formulation of the sieve Brun proved, that the sum

$$\sum_{p,\ p+2 \text{ both prime}} \frac{1}{p}$$

converges. This was the first result of its kind, relating the *Twin-prime* problem. A slew of sieve methods were grew over the years. Upper bound sieve of Selberg, Rosser's sieve, the Asymptotic sieve, the Large sieve to name a few. Using these sieves, many beautiful results have been proved. The Brun-Titchmarsh theorem and the very powerful result of Bombieri are two important examples. Chen's theorem [4] that "there are infinitely many primes p such that $p + 2$ is a product of at most two primes", is another proof of the power of sieve methods. The Brun sieve, the Selberg sieve and the large sieve are included in the modern sieves. One of the basic aims of sieve theory was to attempt to prove conjectures in number theory such as the Twin-Prime conjecture. As the basic broad purposes of sieve theory are still largely unachieved, there have been some partial achievements, particularly in combination with other number theoretic tools.

The methods can be quite powerful of sieve theory, but they appear to be limited by an obstacle known as the *parity problem*, which roughly talking asserts that sieve theory methods have extreme difficulty in distinguishing between numbers with an even number of prime factors and numbers with an odd number of prime factors. This parity problem is not very well understood yet. Compared with other methods in number theory, sieve theory is relatively elementary, in the sense that it does not necessarily require advanced concepts from either analytic number theory or algebraic number theory. However, the more advanced sieves can get still very complex and delicate (particularly when mixed with other mysterious techniques in number theory). Entire textbooks have been devoted to this one subfield of number theory; a classic example is (Halberstam & Richert 1974) [8] and a more advanced text is (Iwaniec & Friedlander 2010) [10].

Sieve methods have important applications even in applied fields of number theory such as Algorithmic Number Theory, and Cryptography. Many direct applications are there, for example finding all the prime numbers under a certain bound, or producing numbers free of large prime factors. There are also indirect applications, for example the running time of various factoring algorithms based directly on the distribution of smooth numbers in short intervals. The so called *undeniable signature schemes* involve primes of the form $2p + 1$ such that p is also a prime number. Sieve methods can give valuable hints about these distributions and hence allow us to control the running times of such algorithms.

2.1 Sieve of Primes

In a 1975 lecture, D. Zagier commented [7]:

"There are two facts about the distribution of prime numbers of which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts. The first is that, despite their simple definition and role as the building blocks of the natural numbers, the prime numbers grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will come out. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision".

A prime number sieve or sieve of prime is a quick type of algorithm for searching primes. There are lots of prime sieves. The simple sieve of Eratosthenes, the quick but more complicated Atkin sieve and the several wheel sieves are most common. A prime sieve works by producing a list of all integers up to a wanted limit and increasingly removing composite numbers (which it directly produce) until only prime numbers are left. This is the most effective way to find a large range of primes; however, to find individual prime numbers, more efficient is to apply direct primality tests .

2.2 Sieve of Eratosthenes

Eratosthenes (276-194 B.C.) was the third librarian of the well known library in Alexandria and an great scholar all around. He is known for his measurement of the circumference of the Earth, estimates of the distances to the moon and the sun, and, in mathematics, for giving of an algorithm for gathering prime numbers. The algorithm is known as the Sieve of Eratosthenes.

To find all prime numbers below a given number N, write all integers from 1 to N in order. 1 is not a prime number and is crossed out right away. The algorithm proceed sequentially in steps. On every step, find the first number not yet crossed, mark it as prime and cross out all of its remaining multiples. Repeat this step while the least available number does not exceed the square root of N.

The above process to find all the prime numbers less than or equal to a given integer N by using sieve of Eratosthenes can be explained by following steps:

1. Create a list of consecutive integers from 1 to N: $(1, 2, 3, 4, ..., N)$.
2. Cross out 1 as it is not prime.
3. Initially, let p equal 2, the first prime number.
4. Starting from p, count up in increments of p and mark each of these numbers greater than p itself in the list. These will be $2p$, $3p$, $4p$, etc.; multiples of p: note that some of them may have been marked already.
5. Find the first number greater than p in the list that is not marked. Stop, if there was no such number. Otherwise, let p equal to this number (which is the next prime) now, and repeat from step 3.

When the algorithm ends, all the numbers are prime in the list that are not marked. The main thought here is that every value for p is prime, because we have marked already all the multiples of the numbers less than p. As a refinement, it is enough to mark the numbers in step 3 starting from p^2, as all the smaller multiples of p will have already been marked at that point. This means that the algorithm is allowed to terminate in step 4 when p^2 is greater than N [9]. Another refinement is to initially list odd numbers only, (3, 5, ..., N), and count up using an increment of $2p$ in step 3, thus marking only odd multiples of p greater than p itself. This actually appears in the original algorithm [9]. This can be generalized with wheel factorization, forming the initial list only from numbers coprime with the first few primes and not just from odds, i.e. numbers coprime with 2 [14].

For example, for first 50 natural numbers, we can find prime numbers using Eratosthenes sieve as follows:

Example 2.2.1. ***Step-i*** *cross out 1; it is not prime.*

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Step-ii *leaving 2, cross out multiples of 2.*

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~

Step-iii *leaving 3, cross out multiples of 3.*

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

Step-iv *leaving 5, cross out multiples of 5.*

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

Step-v *leaving 7, cross out multiples of 7.*

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

The remaining uncrossed numbers {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, *43, 47}* are prime numbers less than 50.*

Generally, the sieve of Eratosthenes is considered the easiest sieve to implement, but it is not the fastest.

2.3 Sieve of Euler

Euler commented in [7] "Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the mind will never penetrate".

The ancient Sieve of Eratosthenes that creats the list of prime numbers is ineffective in the sense that some composite numbers are marked out more than one time; for example, 21 is marked out by both 3 and 7. The outstanding Swiss mathematician Leonhard Euler formed a sieve that strikes out each composite number exactly one time, at the cost of some additional paper work. The process of Euler sieve can be explained by following steps:

1. Make a list of numbers from 2, as large as you wish; call the maximum number n.
2. Extract the first number from the list, make a new list in which each element of the original list, including the first, is multiplied by the extracted first number.
3. "Subtract"the new list from the original, keeping in an output list only those numbers in the original list that do not appear in the new list.
4. Output the first number from the list, which is prime, and repeat the second, third and fourth steps on the reduced list excluding its first element, continuing until the input list is exhausted.

Example 2.3.1. *Sieve of Euler for* $n = 30$ *can be explained as:*

- *Start with the list 2, 3, 4, 5, . . . , 30.*
- *Extract first number 2 from the list and make a new list 4, 6, 8, 10, . . . , 60.*
- *Subtracting the new list from the old gives the list 2, 3, 5, 7, 9, . . . , 29.*
- *Now 2 is prime and the process repeats on the list 3, 5, 7, 9, . . . , 29.*
- *At the next step extract 3 and make a new list 9, 15, 21, 27, . . . , 87, subtracting gives the list 3, 5, 7, 11, 13, . . . , 29, now 2 and 3 are prime and the process repeats on the list 5, 7, 11, 13, . . . , 29.*

- *Likewise for the primes 5 and 7, and since* $7 \times 7 > 30$*, the process stops, with the remaining list 11, 13, 17, 19, 23, 29.*
- *So the complete list of primes less than 30 is 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.*

We can increase the speed of the Sieve of Euler by taking only odd numbers, by ending once the first item is greater than the square root of n in the list, and by calculating the new list in the second step only as far as n.

2.4 Wheel Sieve

Wheel factorization is a graphical method for manually doing a preliminary to the Sieve of Eratosthenes that separates primes from composite numbers. Write the natural numbers around circles initially. Prime numbers in the innermost circle have their multiples in the other circles in similar positions as themselves, forming spokes of primes and their multiples. Multiples of the prime numbers in the innermost circle form spokes of composite numbers in the outer circles.

The algorithm to find out the primes using Wheel sieve method is as follows:

1. Find the first few prime numbers. They are known or can be found quickly using Sieve of Eratosthenes.
2. Multiply the prime numbers together to give the result n.
3. Write 1 to n in a circle. This will be the inner-most circle.
4. Taking x to be the number of circles written so far, continue to write $xn + 1$ to $xn + n$ in another circle around the inner-most circle, such that $xn + 1$ is in the same position as $(x - 1)n + 1$.
5. Repeat step 4 until the largest number to be tested for primality.
6. Strike off the number 1.
7. Strike off the spokes of prime numbers (found in step 1) with its multiples without striking off the numbers in the inner-most circle.
8. Strike off the spokes of all multiples of prime numbers found in step 1.
9. The remaining numbers in the wheel contain mostly prime numbers. Use other methods such as Sieve of Eratosthenes to remove the remaining non-primes.

Example 2.4.1. *Wheel Factorization with* $n = 2 \times 3 = 6$ *can be explained as:*

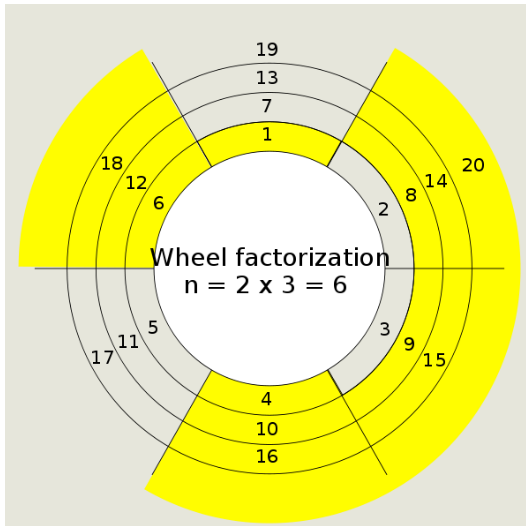

Figure 2.1: Wheel factorization with $n = 2 \times 3 = 6$

- *Start with prime numbers 2 and 3. Since* $2 \times 3 = 6$*, so* $n = 6$*.*
- *Write 1 to n=6 in a circle. This will be the inner-most circle.*
- *For 1st circle around the inner most circle, taking x=1.*
- *Because* $xn + 1 = 1.6 + 1 = 7$ *and* $xn + n = 1.6 + 6 = 12$*. Therefore write 7 to 12 in the 2nd rim of wheel so that 7 is aligned with 1.*
- *Repeat this step for x=2, 3, 4, ... and so on. We will have the circles around the inner most circle as shown in the figure 2.1.*
- *Strike off 1.*
- *Strike off spokes {8, 14, 20, ...} of prime number 2 and spokes {9, 15, 21, ...} of prime number 3 of first step without striking off the numbers 2 and 3.*
- *Strike off multiples {4, 6} of 2 and 3 in the inner-most circle.*
- *Strike off spokes of 4 and 6 in the outer circles.*
- *The remaining numbers in the wheel are mostly prime numbers. Other methods such as Sieve of Eratosthenes can be used to remove the remaining non-primes.*

2.5 Sieve of Atkins

Arthur Oliver Lonsdale Atkin (1925 - 2008), was a British mathematician who published under the name A. O. L. Atkin.

During World War II, as an undergraduate student, Atkin worked at Bletchley Park cracking German codes. He obtained his Ph.D. in 1952 from the University of Cambridge. Here he was one of John Littlewood's research students. He worked at the Atlas Computer Laboratory at Chilton during 1964-1970, computing modular functions. He was Professor of mathematics in the last days of his life at the University of Illinois at Chicago.

Atkin, along with Noam Elkies, extended Schoof's algorithm to produce the Schoof-Elkies-Atkin algorithm. Together with Daniel J. Bernstein, he formulated the sieve of Atkin.

In mathematics, the sieve of Atkin is a quick, modern algorithm for obtaining all prime numbers up to an assigned integer. It is an optimized version of the great sieve of Eratosthenes which does some initial work and then marks off multiples of the square of each prime, instead of multiples of the prime itself. It was invented in 2004 by A. O. L. Atkin and Daniel J. Bernstein [2].

Algorithm

In the algorithm of Sieve of Atkin:

- All remainders are modulo-sixty remainders (divide the number by sixty and return the remainder).
- All the number are positive including x and y.
- Flipping an entry in the sieve list means to change the marking (prime or non-prime) to the opposite marking.

1. Create a results list, filled with 2, 3, and 5.
2. Create a sieve list with an entry for each positive integer; all entries of this list should initially be marked non-prime (composite).
3. For each entry number n in the sieve list, with modulo-sixty remainder r :
   - If r is 1, 13, 17, 29, 37, 41, 49, or 53, flip the entry for each possible solution to $4x^2 + y^2 = n$.
   - If r is 7, 19, 31, or 43, flip the entry for each possible solution to $3x^2+y^2 = n$.

- If r is 11, 23, 47, or 59, flip the entry for each possible solution to $3x^2 - y^2 = n$ when $x > y$.
- If r is something else, ignore it completely.

4. Start with the lowest number in the sieve list.
5. Take the next number in the sieve list still marked prime.
6. Include the number in the results list.
7. Square the number and mark all multiples of that square as non-prime (composite).
8. Repeat steps five through eight.

- This results in numbers with an odd number of solutions to the corresponding equation being prime, and an even number being non-prime.

The algorithm completely ignores any numbers divisible by two, three, or five. All numbers with an even modulo 60 remainder are divisible by two and not prime. All numbers with modulo 60 remainder divisible by three are also divisible by three and not prime. All numbers with modulo 60 remainder divisible by five are divisible by five and not prime. All these remainders are ignored.
All numbers with modulo 60 remainder 1, 13, 17, 29, 37, 41, 49, or 53 have a modulo-four remainder of 1. These numbers are prime if and only if the number of solutions to $4x^2 + y^2 = n$ is odd and the number is square-free [2].
All numbers with modulo 60 remainder 7, 19, 31, or 43 have a modulo-six remainder of 1. These numbers are prime if and only if the number of solutions to $3x^2 + y^2 = n$ is odd and the number is square-free [2].
All numbers with modulo 60 remainder 11, 23, 47, or 59 have a modulo-twelve remainder of 11. These numbers are prime if and only if the number of solutions to $3x^2 - y^2 = n$ is odd and the number is square-free [2].
None of the potential primes are divisible by 2, 3, or 5, so they can't be divisible by their squares. This is why square-free checks do not include 2^2, 3^2, and 5^2.
Once this preprocessing is complete, the actual sieving is performed by running through the sieve starting at 7. For each true element of the array, mark all multiples of the square of the element as false (regardless of their current setting). The remaining true elements are prime.

Chapter 3

Hexile Sieving of $\mathbb{N} \cup \{0\}$ using modulo 6

3.1 Introduction

We can arrange $\mathbb{N} \cup \{0\}$ (set of natural numbers with zero) into six equivalence classes on the basis of their modulo 6 return values as shown in the table 3.1.

Hexile Integer Level : n	$\mathbb{H}^0$	$\mathbb{H}^1$	$\mathbb{H}^2$	$\mathbb{H}^3$	$\mathbb{H}^4$	$\mathbb{H}^5$
0	0	1	2	3	4	5
1	6	7	8	9	10	11
2	12	13	14	15	16	17
3	18	19	20	21	22	23
4	24	25	26	27	28	29
5	30	31	32	33	34	35
6	36	37	38	39	40	41
7	42	43	44	45	46	47
8	48	49	50	51	52	53
9	54	55	56	57	58	59
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Table 3.1: Hexile equivalence class sieving of $\mathbb{N} \cup \{0\}$

3.2 Analysis of Equivalence Classes

In the table 3.1 six equivalence classes are named as "Hexile Integer Classes"and denoted as $\mathbb{H}^k$=$\{x|x = (6 \times n) + k\}$; $k \in \{0, 1, 2, 3, 4, 5\}$. So in set builder notation, we can define six equivalence classes as

$$\begin{aligned}
\mathbb{H}^0 &= \{0, 6, 12, 18, \cdots\} = \{x|x = (6 \times n) + 0\}, && (3.1)\\
\mathbb{H}^1 &= \{1, 7, 13, 19, \cdots\} = \{x|x = (6 \times n) + 1\}, && (3.2)\\
\mathbb{H}^2 &= \{2, 8, 14, 20, \cdots\} = \{x|x = (6 \times n) + 2\}, && (3.3)\\
\mathbb{H}^3 &= \{3, 9, 15, 21, \cdots\} = \{x|x = (6 \times n) + 3\}, && (3.4)\\
\mathbb{H}^4 &= \{4, 10, 16, 22, \cdots\} = \{x|x = (6 \times n) + 4\}, && (3.5)\\
\mathbb{H}^5 &= \{5, 11, 17, 23, \cdots\} = \{x|x = (6 \times n) + 5\}. && (3.6)
\end{aligned}$$

From the table 3.1, we can see that $\mathbb{H}^0$, $\mathbb{H}^2$, $\mathbb{H}^4$ contains all even numbers and except 2 in $\mathbb{H}^2$, they are all those composites which are multiples of 2. We can also see that $\mathbb{H}^3$ contains only one prime element which is 3 and all the other elements are those composites which are multiples of 3.

So we have only $\mathbb{H}^1$ and $\mathbb{H}^5$ as candidates for the domiciled sub-set partitioning of primes in $\mathbb{N} \cup \{0\}$. In these two HICs (Hexile Integer Classes), we can find all the prime numbers greater than 3, as well as the composites which are themselves product of these primes.

Hence in either of $\mathbb{H}^1$ or $\mathbb{H}^5$, prime numbers greater than or equal to 5 can be found.

3.3 Analysis of Composites of $\mathbb{H}^1$ and $\mathbb{H}^5$

In this section, we will discuss the nature of composites of $\mathbb{H}^1$ and $\mathbb{H}^5$.

3.3.1 Multiplication of Two Numbers from $\mathbb{H}^1$

Let p_1 and q_1 be two numbers in $\mathbb{H}^1$ with formulations

$$p_1 = (6 \times m) + 1,$$

and

$$q_1 = (6 \times n) + 1,$$

where m and n are Hexile Integer Level of p_1 and q_1 respectively. Let c^{11} be the composite resulting from the multiplication of p_1 and q_1. Then

$$\begin{aligned}
c^{11} &= p_1 \times q_1\\
c^{11} &= [(6 \times m) + 1] \times [(6 \times n) + 1]\\
c^{11} &= (36 \times m \times n) + (6 \times m) + (6 \times n) + 1. && (3.7)
\end{aligned}$$

If we apply modulo 6 to the result of equation (3.7), we have a remainder 1. It implies that composite c^{11} is an element of $\mathbb{H}^1$.

3.3.2 Multiplication of Two Numbers from $\mathbb{H}^5$

Let p_5 and q_5 be two numbers in $\mathbb{H}^5$ with formulations

$$p_5 = (6 \times m) + 5,$$

and

$$q_5 = (6 \times n) + 5,$$

where m and n are Hexile Integer Level of p_5 and q_5 respectively. Let c^{55} be the composite resulting from the multiplication of p_5 and q_5. Then

$$\begin{aligned} c^{55} &= p_5 \times q_5 \\ c^{55} &= [(6 \times m) + 5] \times [(6 \times n) + 5] \\ c^{55} &= (36 \times m \times n) + (30 \times m) + (30 \times n) + 25. \end{aligned} \tag{3.8}$$

If we apply modulo 6 to the result of equation (3.8), we have a remainder 1. It implies that composite c^{55} is an element of $\mathbb{H}^1$.

3.3.3 Multiplication of One Number from $\mathbb{H}^1$ and Other from $\mathbb{H}^5$

Let p_1 be a number in $\mathbb{H}^1$ with formulation

$$p_1 = (6 \times m) + 1,$$

where m is Hexile Integer Level of p_1.

let q_5 be a number in $\mathbb{H}^5$ with formulation

$$q_5 = (6 \times n) + 5,$$

where n is Hexile Integer Level of q_5.

Let c^{15} be the composite resulting from the multiplication of p_1 and q_5. Then

$$\begin{aligned} c^{15} &= p_1 \times q_5 \\ c^{15} &= [(6 \times m) + 1] \times [(6 \times n) + 5] \\ c^{15} &= (36 \times m \times n) + (30 \times m) + (6 \times n) + 5. \end{aligned} \tag{3.9}$$

If we apply modulo 6 to the result of equation (3.9), we have a remainder 5. It implies that composite c^{15} is an element of $\mathbb{H}^5$.

3.3.4 Possibility of $\mathbb{H}^1$ and $\mathbb{H}^5$ Composites Arising from Multiplication of Other HIC Elements

From the table 3.1, it is clear that all the elements of $\mathbb{H}^0$, $\mathbb{H}^2$ and $\mathbb{H}^4$ are even numbers and all the elements of $\mathbb{H}^1$ and $\mathbb{H}^5$ are odd numbers. Since multiplication of an even number with an odd or even number gives an even number, so multiplication of elements of $\mathbb{H}^0$, $\mathbb{H}^2$ and $\mathbb{H}^4$ cannot possibly give rise to $\mathbb{H}^1$ and $\mathbb{H}^5$ composites.
Only a sole possibility of an element of $\mathbb{H}^3$ left whose multiplication can give rise to a composite in $\mathbb{H}^1$ and $\mathbb{H}^5$. Let r_3 be an element of $\mathbb{H}^3$ with formulation

$$r_3 = (6 \times d) + 3,$$

where d is Hexile Integer Level of r_3.
Now we need to examine the end result of multiplying r_3 with an element of $\mathbb{H}^1$, $\mathbb{H}^3$ and $\mathbb{H}^5$.
Let $p_1 \in \mathbb{H}^1$ and $q_5 \in \mathbb{H}^5$ with formulations

$$\begin{aligned} p_1 &= (6 \times m) + 1, \\ q_5 &= (6 \times n) + 5, \end{aligned}$$

where m and n are Hexile Integer Level of p_1 and q_5 respectively.
Table 3.2 given below, shows the results of the multiplications of an element $r_3 \in \mathbb{H}^3$ with $r_3 \in \mathbb{H}^3$, $p_1 \in \mathbb{H}^1$ and $p_5 \in \mathbb{H}^5$.

The results of table 3.2 show that an element of $\mathbb{H}^3$ will not result in a $\mathbb{H}^1$ or $\mathbb{H}^5$ composite through multiplication. So the composites in $\mathbb{H}^1$ and $\mathbb{H}^5$ are found indigenous with primes from which they are the product through multiplication.

	r_3=$(6 \times d) + 3$	modulo 6 results
r_3	c^{33}=$(36 \times d^2) + (36 \times d) + 9$	3
p_1	$c^{13} = (36 \times d \times m) + (18 \times m) + (6 \times d) + 3$	3
q_5	$c^{53} = (36 \times d \times n) + (30 \times d) + (18 \times n) + 15$	3

Table 3.2: Multiplication results of an element of $\mathbb{H}^3$ with an element of $\mathbb{H}^1$, $\mathbb{H}^3$ and $\mathbb{H}^5$

3.4 Formulation of Composites using Hexile Level of their Component Primes

Our investigation will now take us to the inner place of the formulaic expression of composites. For this purpose, we define a more liable term "Nucleus of a Natural Number".

Definition 3.4.1. We define the *nucleus value* of a natural number, as the quotient obtained when number is divided by 6.

It is clear from the definition of nucleus value that Hexile Level of a natural number can also be referred as the nucleus value, which was initially referenced as the row numbers in the Hexile Sieve table 3.1.
Applying the above definition 3.4.1 to the three formulations of composites of $\mathbb{H}^1$ and $\mathbb{H}^5$ given in the equations (3.7), (3.8) and (3.9), we obtain the following three formulations for *nuclei* values as shown in table 3.3.

Composite Formulae	Nucleus Formulae
$c^{11} = (36 \times m \times n) + (6 \times m) + (6 \times n) + 1$	$(6 \times m \times n) + m + n$
$c^{55} = (36 \times m \times n) + (30 \times m) + (30 \times n) + 25$	$(6 \times m \times n) + (5 \times m) + (5 \times n) + 4$
$c^{15} = (36 \times m \times n) + (30 \times m) + (6 \times n) + 5$	$(6 \times m \times n) + (5 \times m) + n$

Table 3.3: Formulations of nucleus values of $\mathbb{H}^1$ and $\mathbb{H}^5$ composites

For any element of $\mathbb{H}^1$ and $\mathbb{H}^5$, the results of table 3.3 can be used as preliminary investigative formulating-decomposition tool.
So if modulo 6 returned value is 1 for any given positive integer c and its *nucleus* value is Q, then we can ascribe to it as a composite one of the following two formulations of equations (3.10) and (3.11) given below.

$$Q = (6 \times m \times n) + m + n, \tag{3.10}$$

or

$$Q = (6 \times m \times n) + (5 \times m) + (5 \times n) + 4. \tag{3.11}$$

Also if modulo 6 returned value is 5 for a given natural number c and its *nucleus* value is Q, we can ascribe to it as a composite of the following formulation of equation (3.12) given below:

$$Q = (6 \times m \times n) + (5 \times m) + n, \tag{3.12}$$

where m and n are Hexile levels of the two constituent integers presumed to be primes in the composite element of $\mathbb{H}^1$ and $\mathbb{H}^5$ as symbolized by the variable c.

3.5 Composite Linear Diophantine Equations

We investigated in the previous section 3.4, three diophantine equations for the composites in $\mathbb{H}^1$ and $\mathbb{H}^5$. For the ease of writing, we designate equations (3.10),

(3.11) and (3.12) as *Composite Linear Diophantine Equation*(s) or *colide*(s) for short.
Specifically we will reference a colide-11 to the equation (3.10) given below:

$$Q = (6 \times m \times n) + m + n.$$

Also a colide-55, we will reference to the equation (3.11) given below:

$$Q = (6 \times m \times n) + (5 \times m) + (5 \times n) + 4,$$

where m and n are the HI-levels of the constituent primes/composites and Q being computable *nucleus* value.
And a colide-15 we will refer to by equation (3.12) given below:

$$Q = (6 \times m \times n) + (5 \times m) + n,$$

where m and n are the HI-levels of the constituent primes/composites and Q being computable *nucleus* value.
The importance of these three colides is that *they have no integer solutions for the primes.* Else if they possibly do, by contradiction they are composite as we can derive back m and n which will be HI-levels of its two multiplicand integers.

3.6 Sequencing of Nuclei Values for $\mathbb{H}^1$ and $\mathbb{H}^5$ Composites

Using colide-11, colide-55 and colide-15, as defined in the pervious sections 3.5, we will attempt to examine the sequence of *nucleus* values of composites in $\mathbb{H}^1$ and $\mathbb{H}^5$.

3.6.1 Sequencing of Nuclei Values for Colide-11 Composites

Recalling a colide-11, given by equation

$$Q = (6 \times m \times n) + m + n.$$

Where m and n are the HI-levels of the constituent primes/composites and Q being computable *nucleus* value.

Definition 3.6.1. We can transmute colide-11 equation into the following function:

$$f_{11}(m, n) = (6 \times m \times n) + m + n. \tag{3.13}$$

This function is taken on ordered integer pair: (m, n) of HI-levels of two constituent primes/composites where $m,\ n \in \mathbb{Z}^+$. This function is named as colide-11 state function, abbreviated to CS-11 function.

Table 3.4 shows the values obtained by applying first 10 positive integers to CS-11 function (3.13).

LEVEL : (m)	1	2	3	4	5	6	7	8	9	10
LEVEL : (n)										
1	**8**	15	22	29	36	43	50	57	64	71
2	15	**28**	41	54	67	80	93	106	119	132
3	22	41	**60**	79	98	117	136	155	174	193
4	29	54	79	**104**	129	154	179	204	229	254
5	36	67	98	129	**160**	191	222	253	284	315
6	43	80	117	154	191	**288**	265	302	339	376
7	50	93	136	179	222	265	**308**	351	394	437
8	57	106	155	204	253	302	351	**400**	449	498
9	64	119	174	229	284	339	394	449	**504**	559
10	71	132	193	254	315	376	437	498	559	**620**

Table 3.4: The resulting 10×10 - symmetric matrix of colide-11 values obtained on applying the CS-11 function to the various combination-pairs of the first 10 positive integers excluding zero.

The resulting tabulation of values in the table (3.4) is a symmetric matrix, showing the predictable sequencing of *nucleus* values of colide-11 composites. The reason of symmetry is commutative mutual emplacement of m and n variables within the CS-11 function. It is also clear from the table (3.4) that colide-11 HI-levels are producing a sequence which is predictable and non-random in nature.

3.6.2 Sequencing of Nuclei Values for Colide-55 Composites

The equation for colide-55 is is given below:

$$Q = (6 \times m \times n) + (5 \times m) + (5 \times n) + 4.$$

Where m and n are the HI-levels of the constituent primes/composites and Q being computable *nucleus* value.

Definition 3.6.2. We can transmute colide-55 equation into the following function:

$$f_{55}(m, n) = (6 \times m \times n) + (5 \times m) + (5 \times n) + 4. \tag{3.14}$$

This function is taken on ordered integer pair: (m, n) of HI-levels of two constituent primes/composites where $m \geq 0$ and $n \geq 0$ are integers. This function is named as colide-55 state function, abbreviated to CS-55 function.

Table 3.5 shows the results obtained by applying first 10 values to variables m and n of CS-55 function.

LEVEL : (m)	0	1	2	3	4	5	6	7	8	9
LEVEL : (n)										
0	**4**	9	14	19	24	29	34	39	44	49
1	9	**20**	31	42	53	64	75	86	97	108
2	14	31	**48**	65	82	99	116	133	150	167
3	19	42	65	**88**	111	134	157	180	203	226
4	24	53	82	111	**140**	169	198	227	256	285
5	29	64	99	134	169	**204**	239	274	309	344
6	34	75	116	157	198	239	**280**	321	362	403
7	39	86	133	180	227	274	321	**368**	415	462
8	44	97	150	203	256	309	362	415	**468**	521
9	49	108	167	226	285	344	403	462	521	**580**

Table 3.5: Table showing the resulting 10×10 symmetric matrix of colide-55 values obtained on applying the CS-55 function to the various combination-pairs of the first 10 positive integers including zero.

The resulting tabulation of values in table 3.5 is a symmetric matrix with its main diagonal is highlighted bold. Values of table 3.5 shows non-random and predictable sequences of *nucleus* values of colide-55 composites.

3.6.3 Sequencing of Nuclei Values for Colide-15 Composites

The equation for colide-15 is given below:

$$Q = (6 \times m \times n) + (5 \times m) + n.$$

Where m and n are the HI-levels of the constituent primes/composites and Q being computable *nucleus* value.

Definition 3.6.3. We can transmute colide-15 equation into the following function:

$$f_{15}(m, n) = (6 \times m \times n) + (5 \times m) + n. \quad (3.15)$$

This function is taken on ordered integer pair: (m, n) of HI-levels of two constituent primes/composites where $m > 0$ and $n \geq 0$ are integers. This function is named as colide-15 state function, abbreviated to CS-15 function.

Table 3.6 shows the results obtained by applying first 10 values to variables m and n of CS-15 function.

LEVEL : (m)	1	2	3	4	5	6	7	8	9	10
LEVEL : (n)										
0	5	10	15	20	25	30	35	40	45	50
1	12	23	34	45	56	67	78	89	100	111
2	19	36	53	70	87	104	121	138	155	172
3	26	49	72	95	118	141	164	187	210	233
4	33	62	91	120	149	178	207	236	265	294
5	40	75	110	145	180	215	250	285	320	355
6	47	88	129	170	211	252	293	334	375	416
7	54	101	148	195	242	289	336	383	430	477
8	61	114	167	220	273	326	379	432	485	538
9	68	127	186	245	304	363	422	481	540	599

Table 3.6: The resultant 8×8 - matrix table, showing the colide-15 values obtained on applying the CS-15 function to various combination-pairs of the first 10 values to variables m and n of CS-15 function

In the table 3.6, the resulting tabulation of values shows predictable arithmetic sequences of *nuclues* values of colide-15 composites. Hence *nucleus* values of composites of CS-15 function form sequences which are predictable and non-random in nature.

3.6.4 Conclusion to Sequencing of Nuclei Values for $\mathbb{H}^1$ and $\mathbb{H}^5$ Elements

From the Tables of values of CS-11 and CS-55 functions, we can see that colide-11 and colide-55 composites which populate $\mathbb{H}^1$ occur in a non-random sequence. This shows that we can logically deduce: that the primes which are the only other elements of $\mathbb{H}^1$, occur in a non-random fashion in the vacant Hexile levels not occupied by colide-11 and colide-55 composites.
Also from the table of values of CS-15 function, we can see that colide-15 composites, which populate $\mathbb{H}^5$ composites occur in non-random sequence. Also from the results of section 3.3.3, we proved that $\mathbb{H}^5$ consists of only colide-15 composites. This means that we can logically deduce: that primes which are the only other elements found in $\mathbb{H}^5$, also occur in a non-random fashion in the vacant Hexile levels not occupied by the colide-15 composites.

Finally, we can conclude that we have crudely established the rhythm and harmonics in the symphony of prime and composite integers.

Chapter 4

Counting of Primes

In this chapter, we will give some basic theorems for prime counting function. In the first section, we will give the theorems to find number of terms of the tables of values of CS-11 function, CS-55 function and CS-15 function. These theorems can be useful in counting the number of composites in $\mathbb{H}^1$ and $\mathbb{H}^5$ less than any given positive integer and in constructing prime counting function on the basis of Hexile sieve analysis. In the second section, we will give working rules to find total number of integers less than any given positive integer in the two classes $\mathbb{H}^1$ and $\mathbb{H}^5$. In the final section, conclusions to above given theorems and some basic ideas about prime counting function are discussed.

4.1 Theorems to Find Number of Composites in $\mathbb{H}^1$ and $\mathbb{H}^5$

In the pervious chapter, we have shown that CS-11 function and CS-55 function populate $\mathbb{H}^1$ composites and CS-15 function populate $\mathbb{H}^5$ composites. Now we will give some theorems for counting the number of terms in the tables of values of CS-11 function, CS-55 function and CS-15 function.

4.1.1 Theorem to Find Number of Terms in the Table of Values of CS-11 Function

Theorem 4.1.1. *Let x be a given positive integer and Q be the nucleus value of x. If the approximate number of non-repeated terms in the table of values of CS-11 function less than or equal to Q is denoted by $\mathbb{K}^{11}_Q$. Then*

$$\mathbb{K}^{11}_Q = \sum_i Floor\left[\frac{Q-i}{6i+1} - (i-1)\right], \tag{4.1}$$

where $i \geq 1$ can be found by

$$i = Floor\left[\frac{2+\sqrt{2(3Q+5)}}{6}\right],$$

and "Floor[·]"denotes the floor function.

Proof. From the equation (3.13), formula for CS-11 function is

$$f_{11}(m,n) = (6 \times m \times n) + m + n,$$

where m and n are the Hexile levels of two constituent primes/composites in $\mathbb{H}^1$. Table shows the results of CS-11 function for first 10 values of m and n.

LEVEL : (m)	1	2	3	4	5	6	7	8	9	10
LEVEL : (n)										
1	**8**	15	22	29	36	43	50	57	64	71
2	15	**28**	41	54	67	80	93	106	119	132
3	22	41	**60**	79	98	117	136	155	174	193
4	29	54	79	**104**	129	154	179	204	229	254
5	36	67	98	129	**160**	191	222	253	284	315
6	43	80	117	154	191	**288**	265	302	339	376
7	50	93	136	179	222	265	**308**	351	394	437
8	57	106	155	204	253	302	351	**400**	449	498
9	64	119	174	229	284	339	394	449	**504**	559
10	71	132	193	254	315	376	437	498	559	**620**

From the above table, we can see that
(i) It is a symmetric matrix.
(ii) Each row/column forms an arithmetic progression.
Let x be a given positive integer and let Q be the *nucleus* value of x.
We have to find total number of terms of the table which are less than or equal to Q.
Let j_1^{11} be the number of term of T_1^{11} term in arithmetic progression of first row of the table such that

$$\begin{aligned} T_1^{11} &\leq Q, \\ \implies a_1 + (j_1^{11} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of first row

$$\begin{aligned} 8 + (j_1^{11} - 1)7 &\leq Q, \\ 8 + 7j_1^{11} - 7 &\leq Q, \\ 7j_1^{11} + 1 &\leq Q, \\ j_1^{11} &\leq \frac{Q-1}{7}. \end{aligned}$$

Let k_1^{11} be the number of term of the greatest term in the arithmetic progression of first row which is less than or equal to Q, then

$$k_1^{11} = Floor\left[\frac{Q-1}{7}\right]. \tag{4.2}$$

Let j_2^{11} be the number of term of T_2^{11} term in arithmetic progression of second row of the table such that

$$\begin{aligned} T_2^{11} &\leq Q, \\ \Longrightarrow a_1 + (j_2^{11} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of second row, we have

$$\begin{aligned} 15 + (j_2^{11} - 1)13 &\leq Q, \\ 15 + 13j_2^{11} - 13 &\leq Q, \\ 13j_2^{11} + 2 &\leq Q, \\ j_2^{11} &\leq \frac{Q-2}{13}. \end{aligned}$$

Let k_2^{11} be the number of term of the greatest term in arithmetic progression (starts after first repeated term) of second row which is less than or equal to Q, then

$$k_2^{11} = Floor\left[\frac{Q-2}{13} - 1\right]. \tag{4.3}$$

Here 1 is subtracted because of symmetric property of table, second row contains 1 element of first row.
Let j_3^{11} be the number of term of T_3^{11} term in arithmetic progression of third row of the table such that

$$\begin{aligned} T_3^{11} &\leq Q, \\ \Longrightarrow a_1 + (j_3^{11} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of third row

$$\begin{aligned}
22+(j_3^{11}-1)19 &\leq Q,\\
22+19j_3^{11}-19 &\leq Q,\\
19j_3^{11}+3 &\leq Q,\\
j_3^{11} &\leq \frac{Q-3}{19}.
\end{aligned}$$

Let k_3^{11} be the number of term of the greatest term in arithmetic progression (starts after first 2 repeated terms) of third row which is less than or equal to Q, then

$$k_3^{11} = Floor\left[\frac{Q-3}{19}-2\right]. \tag{4.4}$$

Here 2 is subtracted because of symmetric property of table, third row contains two elements of second row.
From equations (4.2), (4.3) and (4.4), we can write the values of k_4^{11} (number of term of greatest term which is less than or equal to Q in the arithmetic progression of forth row starts after first 3 repeated terms), k_5^{11} (number of term of greatest term which is less than or equal to Q in the arithmetic progression of fifth row starts after first 4 repeated terms) and so on as

$$k_4^{11} = Floor\left[\frac{Q-4}{25}-3\right], \tag{4.5}$$

and

$$k_5^{11} = Floor\left[\frac{Q-5}{31}-4\right], \tag{4.6}$$

and so on.
So the total approximate number of non-repeated terms in the table of CS-11 function less than or equal to Q is

$$\begin{aligned}
\mathbb{K}_Q^{11} &= k_1^{11}+k_2^{11}+k_3^{11}+k_4^{11}+\dots\\
&= Floor\left[\frac{Q-1}{7}\right]+Floor\left[\frac{Q-2}{13}-1\right]+Floor\left[\frac{Q-3}{19}-2\right]+Floor\left[\frac{Q-4}{25}-3\right]+\dots\\
&= \sum_i Floor\left[\frac{Q-i}{6i+1}-(i-1)\right].
\end{aligned}$$

Where value of i can be found such that

$$\begin{aligned}
\frac{Q-i}{6i+1}-(i-1) &= 0,\\
Q-i-6i^2-i+6i+1 &= 0,\\
6i^2-4i-(Q+1) &= 0,
\end{aligned}$$

using quadratic formula

$$i = \frac{2 \pm \sqrt{2(3Q+5)}}{6}.$$

Using mathematical induction, it can be easily proved that

$$2 < \sqrt{2(3Q+5)},$$

so

$$i = \frac{2 - \sqrt{2(3Q+5)}}{6},$$

can be neglected and because i is a term number so

$$i = Floor\left[\frac{2 + \sqrt{2(3Q+5)}}{6}\right].$$

Hence the approximate number of non-repeated terms less than or equal to Q in the table of CS-11 function is

$$\mathbb{K}_Q^{11} = \sum_i Floor\left[\frac{Q-i}{6i+1} - (i-1)\right],$$

where

$$i = Floor\left[\frac{2 + \sqrt{2(3Q+5)}}{6}\right].$$

□

4.1.2 Theorem to Find Number of Terms in the Table of Values of CS-55 Function

Theorem 4.1.2. *Let x be a given positive integer and Q be the nucleus value of x. If the approximate number of non-repeated terms in the table of values of CS-55 function less than or equal to Q is denoted by $\mathbb{K}_Q^{55}$. Then*

$$\mathbb{K}_Q^{55} = \sum_i Floor\left[\frac{Q+i}{6i-1} - (i-1)\right], \tag{4.7}$$

where $i \geq 1$ can be found by

$$i = Floor\left[\frac{4 + \sqrt{2(3Q+5)}}{6}\right],$$

and "Floor$[\cdot]$"denotes the floor function.

Proof. From the equation (3.14), formula for CS-55 function is

$$f_{55}(m,n) = (6 \times m \times n) + (5 \times m) + (5 \times n) + 4,$$

where m and n are the Hexile levels of two constituent primes/composites in $\mathbb{H}^5$. Table shows the results of CS-55 function for first 10 values of m and n.

LEVEL : (m)	0	1	2	3	4	5	6	7	8	9
LEVEL : (n)										
0	**4**	9	14	19	24	29	34	39	44	49
1	9	**20**	31	42	53	64	75	86	97	108
2	14	31	**48**	65	82	99	116	133	150	167
3	19	42	65	**88**	111	134	157	180	203	226
4	24	53	82	111	**140**	169	198	227	256	285
5	29	64	99	134	169	**204**	239	274	309	344
6	34	75	116	157	198	239	**280**	321	362	403
7	39	86	133	180	227	274	321	**368**	415	462
8	44	97	150	203	256	309	362	415	**468**	521
9	49	108	167	226	285	344	403	462	521	**580**

From the above table, we can see that

(i) It is a symmetric matrix.

(ii) Each row/column forms an arithmetic progression.

Let x be a given positive integer and let Q be the *nucleus* value of x.

First we will find total number of terms of the table which are less than or equal to Q.

Let j_1^{55} be the number of term of T_1^{55} term in arithmetic progression of first row of the table such that

$$\begin{aligned} T_1^{55} &\leq Q, \\ \implies a_1 + (j_1^{55} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of first row

$$\begin{aligned} 4 + (j_1^{55} - 1)5 &\leq Q, \\ 4 + 5j_1^{55} - 5 &\leq Q, \\ 5j_1^{55} - 1 &\leq Q, \\ j_1^{55} &\leq \frac{Q+1}{5}. \end{aligned}$$

Let k_1^{55} be the number of term of the greatest term in the arithmetic progression of first row which is less than or equal to Q, then

$$k_1^{55} = Floor\left[\frac{Q+1}{5}\right]. \tag{4.8}$$

Let j_2^{55} be the number of term of T_2^{55} term in arithmetic progression of second row of the table such that

$$\begin{aligned} T_2^{55} &\leq Q, \\ \Longrightarrow a_1 + (j_2^{55} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of second row, we get

$$\begin{aligned} 9 + (j_2^{55} - 1)11 &\leq Q, \\ 9 + 11j_2^{55} - 11 &\leq Q, \\ 11j_2^{55} - 2 &\leq Q, \\ j_2^{55} &\leq \frac{Q+2}{11}. \end{aligned}$$

Let k_2^{55} be the number of term of the greatest term in arithmetic progression (starts after first 1 repeated term) of second row which is less than or equal to Q, then

$$k_2^{55} = Floor\left[\frac{Q+2}{11} - 1\right]. \tag{4.9}$$

Here 1 is subtracted because of symmetric property of table, second row contains one element of first row.
Let j_3^{55} be the number of term of T_3^{55} term in arithmetic progression of third row of the table such that

$$\begin{aligned} T_3^{55} &\leq Q, \\ \Longrightarrow a_1 + (j_3^{55} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of third row, we get

$$\begin{aligned} 14 + (j_3^{55} - 1)17 &\leq Q, \\ 14 + 17j_3^{55} - 17 &\leq Q, \\ 17j_3^{55} - 3 &\leq Q, \\ j_3^{55} &\leq \frac{Q+3}{17}. \end{aligned}$$

Let k_3^{55} be the number of term of the greatest term in arithmetic progression (starts after first 2 repeated terms) of third row which is less than or equal to Q, then

$$k_3^{55} = Floor\left[\frac{Q+3}{17} - 2\right]. \tag{4.10}$$

Here 2 is subtracted because of symmetric property of table, third row contains two elements of second row.
From equations (4.8), (4.9) and (4.10), we can write the values of k_4^{55} (number of term of greatest term which is less than or equal to Q in the arithmetic progression of forth row starts after first 3 repeated terms), k_5^{55} (number of term of greatest term which is less than or equal to Q in the arithmetic progression of fifth row starts after first 4 repeated terms) and so on as

$$k_4^{55} = Floor\left[\frac{Q+4}{23} - 3\right], \tag{4.11}$$

and

$$k_5^{55} = Floor\left[\frac{Q+5}{29} - 4\right], \tag{4.12}$$

and so on.
So the approximate number of non-repeated terms of the table of CS-55 function less than or equal to Q is

$$\begin{aligned}
\mathbb{K}_Q^{55} &= k_1^{55} + k_2^{55} + k_3^{55} + k_4^{55} + \dots \\
&= Floor\left[\frac{Q+1}{5}\right] + Floor\left[\frac{Q+2}{11} - 1\right] + Floor\left[\frac{Q+3}{17} - 2\right] + Floor\left[\frac{Q+4}{23} - 3\right] + \dots \\
&= \sum_i Floor\left[\frac{Q+i}{6i-1} - (i-1)\right].
\end{aligned}$$

Where value of i can be found such that

$$\begin{aligned}
\frac{Q+i}{6i-1} - (i-1) &= 0, \\
Q + i - 6i^2 + i + 6i - 1 &= 0, \\
6i^2 - 8i - (Q-1) &= 0.
\end{aligned}$$

Using quadratic formula

$$i = \frac{4 \pm \sqrt{2(3Q+5)}}{6}.$$

Using mathematical induction, it can be easily proved that

$$4 \quad \leq \quad \sqrt{2(3Q+5)},$$

so

$$i \quad = \quad \frac{4-\sqrt{2(3Q+5)}}{6},$$

can be neglected and because i is a term number so

$$i \quad = \quad Floor\left[\frac{4+\sqrt{2(3Q+5)}}{6}\right].$$

Hence the approximate number of non-repeated terms less than or equal to Q in table of CS-55 function is

$$\mathbb{K}_Q^{55} \quad = \quad \sum_i Floor\left[\frac{Q+i}{6i-1} - (i-1)\right],$$

where

$$i \quad = \quad Floor\left[\frac{4+\sqrt{2(3Q+5)}}{6}\right].$$

□

4.1.3 Theorem to Find Number of Terms in the Table of Values of CS-15 Function

Theorem 4.1.3. *Let x be a given positive integer and Q be the nucleus value of x. If the approximate number of non-repeated terms in the table of values of CS-15 function less than or equal to Q is denoted by $\mathbb{K}_Q^{15}$. Then*

$$\mathbb{K}_Q^{15} \quad = \quad Floor\left[\frac{Q}{5}\right] + \sum_i Floor\left[\frac{Q-i}{6i+5}\right], \qquad (4.13)$$

where "Floor$[\cdot]$"denotes the floor function and $i \geq 1$ can be found by using

$$i \quad = \quad Ceiling\left[\frac{Q-5}{7}\right],$$

where "Ceiling$[\cdot]$"denotes the ceiling function.

Proof. From the equation (3.15), formula for CS-15 function is

$$f_{15}(m,n) = (6 \times m \times n) + (5 \times m) + n,$$

where m and n are the Hexile levels of two constituent primes/composites in $\mathbb{H}^1$ and $\mathbb{H}^5$ respectively.
Table shows the results of CS-15 function for first 10 values of m and n.

LEVEL : (m)	1	2	3	4	5	6	7	8	9	10
LEVEL : (n)										
0	5	10	15	20	25	30	35	40	45	50
1	12	23	34	45	56	67	78	89	100	111
2	19	36	53	70	87	104	121	138	155	172
3	26	49	72	95	118	141	164	187	210	233
4	33	62	91	120	149	178	207	236	265	294
5	40	75	110	145	180	215	250	285	320	355
6	47	88	129	170	211	252	293	334	375	416
7	54	101	148	195	242	289	336	383	430	477
8	61	114	167	220	273	326	379	432	485	538
9	68	127	186	245	304	363	422	481	540	599

From the above table, we can see that
(i) It is a non-symmetric matrix.
(ii) Each row/column forms an arithmetic progression.
Let x be a given positive integer and let Q be the *nucleus* value of x.
First we will find total number of terms of the table which are less than or equal to Q.
Let j_1^{15} be the number of term of T_1^{15} term in arithmetic progression of first row of the table such that

$$\begin{aligned} T_1^{15} &\leq Q, \\ \Longrightarrow a_1 + (j_1^{15} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of first row

$$\begin{aligned} 5 + (j_1^{15} - 1)5 &\leq Q, \\ 5 + 5j_1^{15} - 5 &\leq Q, \\ 5j_1^{15} &\leq Q, \\ j_1^{15} &\leq \frac{Q}{5}. \end{aligned}$$

Let k_1^{15} be the number of term of the greatest term in the arithmetic progression of first row which is less than or equal to Q, then

$$k_1^{15} = Floor\left[\frac{Q}{5}\right]. \tag{4.14}$$

Let j_2^{15} be the number of term of T_2^{15} term in arithmetic progression of second row of the table such that

$$\begin{aligned} T_2^{15} &\leq Q, \\ \Longrightarrow a_1 + (j_2^{15} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of second row

$$\begin{aligned} 12 + (j_2^{15} - 1)11 &\leq Q, \\ 12 + 11j_2^{15} - 11 &\leq Q, \\ 11j_2^{15} + 1 &\leq Q, \\ j_2^{15} &\leq \frac{Q-1}{11}. \end{aligned}$$

Let k_2^{15} be the number of term of the greatest term in arithmetic progression of second row which is less than or equal to Q, then

$$k_2^{15} = Floor\left[\frac{Q-1}{11}\right]. \tag{4.15}$$

Let j_3^{15} be the number of term of T_3^{15} term in arithmetic progression of third row of the table such that

$$\begin{aligned} T_3^{15} &\leq Q, \\ \Longrightarrow a_1 + (j_3^{15} - 1)d &\leq Q, \end{aligned}$$

by putting values from arithmetic progression of third row

$$\begin{aligned} 19 + (j_3^{15} - 1)17 &\leq Q, \\ 19 + 17j_3^{15} - 17 &\leq Q, \\ 17j_3^{15} + 2 &\leq Q, \\ j_3^{15} &\leq \frac{Q-2}{17}. \end{aligned}$$

Let k_3^{15} be the number of term of the greatest term in arithmetic progression of third row which is less than or equal to Q, then

$$k_3^{15} = Floor\left[\frac{Q-2}{17}\right]. \tag{4.16}$$

From equations (4.15) and (4.16), we can write the values of k_4^{15} (number of term of greatest term which is less than or equal to Q in the arithmetic progression of forth row), k_5^{15} (number of term of greatest term which is less than or equal to Q in the arithmetic progression of fifth row) and so on as

$$k_4^{15} = Floor\left[\frac{Q-3}{23}\right], \tag{4.17}$$

and

$$k_5^{15} = Floor\left[\frac{Q-4}{29}\right], \tag{4.18}$$

and so on.
So the approximate number of non-repeated terms of table of CS-15 function less than or equal to Q is

$$\begin{aligned}
\mathbb{K}_Q^{15} &= k_1^{15} + k_2^{15} + k_3^{15} + k_4^{15} + \cdots \\
&= Floor\left[\frac{Q}{5}\right] + Floor\left[\frac{Q-1}{11}\right] + Floor\left[\frac{Q-2}{17}\right] + Floor\left[\frac{Q-3}{23}\right] + \cdots \\
&= Floor\left[\frac{Q}{5}\right] + \sum_i Floor\left[\frac{Q-i}{6i+5}\right].
\end{aligned}$$

Where value of i can be found such that

$$\begin{aligned}
0 \le Q - i &\le 6i + 5, \\
\Rightarrow Q - i &\le 6i + 5, \\
\Rightarrow i &\ge \frac{Q-5}{7}.
\end{aligned}$$

So the smallest value of i which is greater than above value is

$$i = Ceiling\left[\frac{Q-5}{7}\right].$$

Hence approximate number of non-repeated terms less than or equal to Q in table of CS-15 function is

$$\mathbb{K}_Q^{15} = Floor\left[\frac{Q}{5}\right] + \sum_i Floor\left[\frac{Q-i}{6i+5}\right],$$

where

$$i = Ceiling\left[\frac{Q-5}{7}\right].$$

□

4.2 Working Rules to Find Total Number of Integers in $\mathbb{H}^1$ and $\mathbb{H}^5$

Now our final stage is to find total number of integers in $\mathbb{H}^1$ and $\mathbb{H}^5$ less than any given integer in order to find number of primes less than that given integer. For this, working rules are given below.
Let x be a given integer. We have to find total number of integers in $\mathbb{H}^1$ and $\mathbb{H}^5$ less than or equal to x. Let Q be the nucleus value of x and r be the modulo 6 remainder. Suppose total number of integer less than or equal to x in $\mathbb{H}^1$ and $\mathbb{H}^5$ is denoted by $\eta_{15}(x)$, then by using table 3.1, we have following cases for the value of $\eta_{15}(x)$.

Case 1:

If $r = 0$ i.e. $r \in \mathbb{H}^0$, then

$$\eta_{15}(x) = 2Q. \tag{4.19}$$

Case 2:

If $r = \{1, 2, 3, 4\}$ i.e. $r \in \mathbb{H}^i$, for some $i \in \{1, 2, 3, 4\}$ then

$$\eta_{15}(x) = 2Q + 1. \tag{4.20}$$

Case 3:

If $r = 5$ i.e. $r \in \mathbb{H}^5$, then

$$\eta_{15}(x) = 2Q + 2. \tag{4.21}$$

4.3 Conclusions to Theorems and Prime Counting Function

Since terms in the table of CS-11 function are the *nucleus* values of composites of $\mathbb{H}^1$ populated by CS-11 function, therefore the theorem 4.1.1 of $\mathbb{K}_Q^{11}$ can be used in the formula to find total number of composites in $\mathbb{H}^1$ populated by CS-11 function.

Also, since terms in the table of CS-55 function are the *nucleus* values of composites of $\mathbb{H}^1$ populated by CS-55 function, therefore the theorem 4.1.2 of $\mathbb{K}_Q^{55}$ can be used in the formula to find total number of composites in $\mathbb{H}^1$ populated by CS-55 function. Similarly terms in the table of CS-15 function are the *nucleus* values of composites of $\mathbb{H}^5$ populated by CS-15 function, therefore the theorem 4.1.3 of $mathbbK_Q^{15}$ can be used in the formula to find total number of composites in $\mathbb{H}^5$ populated by CS-15 function.
Now the value of $\pi(x)$ (number of primes less than or equal to x) can be found after subtraction of total number of composites less than or equal to x in $\mathbb{H}^1$ and $\mathbb{H}^5$ from the value of $\eta_{15}(x)$ (total number of integers less than or equal to x in $\mathbb{H}^1$ and $\mathbb{H}^5$). In the final answer 2 is added because only two primes 2 and 3 are not included in $\mathbb{H}^1$ and $\mathbb{H}^5$ primes.

4.4 Conclusions and Future Work

The main objective of work was attempt to reduce the search of primes and to give a basis to an algorithm for prime counting function. A simple explanation is given for critical mysteries surrounding primes and composites. Hopefully this discussion is a stimulus and starting point to solve other key areas of conjectures and interest in Number Theory.

In this thesis we were just able to give some theorems regarding prime counting function. We invite the readers to investigate the followings:

- to find mutual intersection of tables of values of CS-11 function, CS-55 function and CS-15 function.
- to construct an algorithms for prime counting functions using ideas given in this thesis and comparison with other existing algorithms.

Bibliography

[1] Aigner, Martin, Ziegler, Gnter M., *Proofs from The Book*, Berlin, New York: Springer-Verlag (1998).

[2] A.O.L. Atkin, D.J. Bernstein, *Prime sieves using binary quadratic forms*, Math. Comp., **73** (2004), 1023–1030.

[3] Bach, Eric, Shallit, Jeffrey, *Algorithmic Number Theory*, MIT Press, (1996).

[4] Chen J., On the representation of a large even integer as the sum of a prime and the product of at most two primes, *Sci. Sinica*, **16** (1973) 157-176.

[5] Dudley, Underwood, *Elementary number theory (2nd ed.)*, W. H. Freeman and Co (1978).

[6] Fraleigh, B. John, *A First Course In Abstract Algebra*, Addison-Wesley, (1976).

[7] H.J. Gamma, *Exploring Euler's Constant*, Princeton, NJ: Princeton University Press, (2003).

[8] H. Halberstam, H.E. Richert, *Sieve Methods*, Academic Press (1974).

[9] R. Horsley, F.R.S. Samuel., The Sieve of Eratosthenes. Being an account of his method of finding all the Prime Numbers, *Philosophical Transactions*, **62** (1772) 327–347.

[10] H. Iwaniec, J. Friedlander, *Opera de cribro*, AMS, (2010).

[11] Pettofrezzo, J. Anthony, Byrkit, R. Donald, *Elements of Number Theory*, Englewood Cliffs: Prentice Hall, (1970).

[12] O. Ramaré, On snirel'man's constant, *Annali della Scuola Normale Superiore di Pisa, Classe di Scienze*, **22** (1995), 645–706.

[13] P. Ribenboim, *The Little Book of Bigger Primes*, Springer-Verlag, (2004).

[14] C. Runciman, Functional Pearl: Lazy wheel sieves and spirals of primes, *Journal of Functional Programming*, **7** (1997) 219–225.

[15] T.O. Silva, S. Herzog, S. Pardi, Empirical verification of the even Goldbach conjecture, and computation of prime gaps, up to 410^18, to appear in *Mathematics of Computation*, (2013).

[16] Letter in Latin from Goldbach to Euler, July 1730.($http : //www.math.dartmouth.edu/\ euler/correspondence/letters/OO0722.pdf$)