On the representation of even numbers as the sum and difference of two primes and the representation of odd numbers as the sum of an odd prime and an even semiprime and the distribution of primes in short intervals

Shan-Guang Tan
Zhejiang University, Hangzhou, 310027, China
tanshanguang@163.com

Abstract 1. The representation of even numbers as the sum of two odd primes and the distribution of primes in short intervals were investigated in this paper. A main theorem was proved. It states: There exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the even number $2n$ can be represented as the sum of two odd primes where one is smaller than $\sqrt{2n}$ and another is greater than $2n - \sqrt{2n}$.

The proof of the main theorem is based on the fundamental theorem of arithmetic and the theory of linear algebra. Its key ideas are as follows (1) For every number $n$ greater than a positive number $n_0$, let $Q_r = \{q_1, q_2, \ldots, q_r\}$ be a group of odd primes smaller than $\sqrt{2n}$ and $\gcd(q_i, n) = 1$ for any $q_i \in Q_r$. Then the even number $2n$ can be represented as the sum of an odd prime $q_i \in Q_r$ and an odd number $d_i = 2n - q_i$. (2) If all the odd numbers $d_i$ are composite, then a group of linear algebraic equations can be formed and with the solutions $q_i \in Q_r$. (3) When a contradiction between the expectation and the actual results of the solutions is obtained, the main theorem will be proved.

It has been found that $n_0 = 31, 637$. Based on the main theorem and by verifying for $n \leq n_0$, it was proved that for every number $n$ greater than 1, there are always at least one pair of primes $p$ and $q$ which are symmetrical about the number $n$ so that even numbers greater than 2 can be expressed as the sum of two primes. Hence, Goldbach’s conjecture was proved.

Also based on the main theorem, some theorems of the distribution of primes in short intervals were proved. By these theorems, the Legendre’s conjecture, the Oppermann’s conjecture, the Hanssner’s conjecture, the Brocard’s conjecture, the Andrica’s conjecture, the Sierpinski’s conjecture and the Sierpinski’s conjecture of triangular numbers were proved and the Mills’ constant can be determined.

2. The representation of odd numbers as the sum of an odd prime and an even semiprime, and the distribution of primes in short intervals were investigated in this paper. A main theorem was proved. It states: There exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the odd number $2n + 1$ can be represented as the sum of an odd prime $p$ and an even semiprime $2q$ where $q$ is an odd prime smaller than $\sqrt{2n}$ and $p$ is greater than $2n + 1 - 2\sqrt{2n}$.

The proof of the main theorem is based on the fundamental theorem of arithmetic and the theory of linear algebra. Its key ideas are as follows (1) For every number $n$ greater than a positive number $n_0$, let $Q_r = \{q_1, q_2, \ldots, q_r\}$ be a group of odd primes smaller than $\sqrt{2n}$ and $\gcd(q_i, 2n + 1) = 1$ for any $q_i \in Q_r$. Then the odd number $2n + 1$ can be represented as the sum of an even semiprime $2q_i$ and an
odd number \( d_i = 2n + 1 - 2q_i \), where \( q_i \in Q_r \). (2) If all the odd numbers \( d_i \) are composite, then a group of linear algebraic equations can be formed and with the solutions \( q_i \in Q_r \). (3) When a contradiction between the expectation and the actual results of the solutions is obtained, the main theorem will be proved.

It has been found that \( n_0 = 19,875 \). Based on the main theorem and by verifying for \( n \leq n_0 \), it was proved that for every number \( n \) greater than 2, there are always at least one pair of primes \( p \) and \( q \) so that all odd integers greater than 5 can be represented as the sum of an odd prime and an even semiprime. Therefore, Lemoine’s conjecture was proved.

Also based on the main theorem, some theorems of the distribution of primes in short intervals were given out and proved. By these theorems, the Legendre’s conjecture and the Andrica’s conjecture were proved and the Mills’ constant can be determined.

3. It was proved in this paper that:

(1) Let \( R_2(x) \) denote the number of odd prime pairs \( p \) and \( x - p \) for \( 3 \leq p \leq x/2 \). Then for large even numbers \( x \), a positive number \( N \) always exists such that the inequalities

\[
R_2^*(x, N) \leq R_2(x) < R_2^*(x, N + 1)
\]

hold where

\[
R_2^*(x, N) = \alpha_2 \frac{x}{\log x} \sum_{n=1}^{N} \frac{n!}{\log^n x},
\]

and \( R_2(x) \) is asymptotically equal to

\[
R_2(x) = \alpha_2 Li_2(x) + O(\sqrt{x \log x})
\]

where \( \alpha_2 \) is a positive constant dependent of \( x (mod \ 6) \).

(2) Let \( R_3(x) \) denote the number of odd prime pairs \( p \) and \( x - 2p \) for \( 3 \leq p \leq (x-3)/2 \). Then for large odd numbers \( x \), a positive number \( N \) always exists such that the inequalities

\[
R_3^*(x, N) \leq R_3(x) < R_3^*(x, N + 1)
\]

hold where

\[
R_3^*(x, N) = \alpha_3 \frac{x}{\log x} \sum_{n=1}^{N} \frac{n!}{\log^n x},
\]

and \( R_3(x) \) is asymptotically equal to

\[
R_3(x) = \alpha_3 Li_2(x) + O(\sqrt{x \log x})
\]

where \( \alpha_3 \) is a positive constant dependent of \( x (mod \ 6) \).

4. It is proved in this paper that for every number \( i \) greater than 1, there is asymptotically

\[
p_{i+1} - p_i = O(\log^2 p_i)
\]

and

\[
\lim \sup_{n \to \infty} \frac{p_{i+1} - p_i}{\log^2 p_i} = 1
\]

where \( p_i \) is the \( i^{th} \) prime number.

5. The representation of even numbers as the difference of two consecutive primes investigated in this paper. A basic theorem was proved. It states: Every even number is the difference of two consecutive primes in infinitely many ways.

To prove the basic theorem, we proved that:
(1) At least an even number is the difference of two consecutive primes in infinitely many ways.
(2) Let \(2m_1\) denote the smallest difference of two consecutive primes in infinitely many ways, then any other difference of two consecutive primes in infinitely many ways should be the multiple of \(2m_1\).
(3) The smallest difference of two consecutive primes in infinitely many ways should be equal to 2.
(4) For \(k = 1, 2, \ldots\), every even number \(2k\) is the difference of two consecutive primes in infinitely many ways.

Based on the basic theorem, it was proved that:
(1) There are infinitely many twin primes \(p\) and \(p + 2\).
(2) There are infinitely many cousin primes \(p\) and \(p + 4\).
(3) There are infinitely many sexy primes \(p\) and \(p + 6\).
(4) There are infinitely many pairs of consecutive primes \(p\) and \(p + 2k\) for \(k = 1, 2, \ldots\).

6. Let \(\pi_{2k}(x)\) be the number of odd prime pairs \(p\) and \(p + 2k\) such that \(p \leq x\) and \(1 \leq k \leq \sqrt{x}\). It was proved that:
(1) For large numbers \(x\), the number \(\pi_{2k}(x)\) satisfies
\[
\pi_{2k}^*(x, N) \leq \pi_{2k}(x) < \pi_{2k}^*(x, N + 1)
\]
where \(N\) is a positive number and
\[
\pi_{2k}^*(x, N) = a_{2k} \frac{x}{\log^2 x} \sum_{n=2}^{N} \frac{n!}{\log^{n-1} x}
\]
where \(a_{2k}\) is a positive constant dependent of the number \(k\).
(2) A pair of positive numbers \(x\) and \(N\) always exist such that the number \(\pi_{2k}(x)\) satisfies
\[
\pi_{2k}(x) - \pi_{2k}^*(x, N) < a_{2k}(x \log x)^{1/2}.
\]
(3) For large numbers \(x\), \(\pi_{2k}(x)\) is asymptotically equal to
\[
\pi_{2k}(x) = a_{2k} \text{Li}_2(x) + O(\sqrt{x \log x}).
\]

7. The generalization of Eisenstein’s criterion of irreducible polynomials over the field \(Q\) of rational numbers was investigated in this paper. Firstly, if a polynomial
\[
F(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in Z[X]
\]
can not be written as
\[
F(Y) = a_{k \cdot d} Y^k + a_{(k-1) \cdot d} Y^{k-1} + \cdots + a_d Y + a_0 \in Z[Y]
\]
by defining \(Y = X^d\) where \(k \cdot d = n\), \(k\) and \(d\) are positive integers greater than 1, then \(F(X)\) can be called a fundamental polynomial. Secondly, theorems were proved and state:
(1) For any number \(n\) and a fundamental polynomial \(F(X)\), if there exist a prime \(p\) and a positive number \(r\) such that \(2 \nmid r\) or \(2 \nmid n\), \(r < n\), \(p \nmid a_n\), \(p^r | a_i (i = 0, 1, \ldots, n - 1)\) and \(p^{r+1} | a_0\), then \(F(X)\) is irreducible over the field \(Q[X]\) of rational numbers.
(2) For any number \(n\), a polynomial \(F(X)\) is irreducible over the field \(Q[X]\) of rational numbers if and only if all of its fundamental polynomials are irreducible over the field \(Q[X]\) of rational numbers.

To prove the first theorem, a main assumption that a fundamental polynomial \(F(X) = g(X) h(X)\) and some definitions are made. Then for all different cases, reductions to absurdity are derived so
that the assumption that the fundamental polynomial $F(X) = g(X)h(X)$ is proved false. Hence the theorem holds.

8. Problems on irreducible polynomials were investigated in this paper. Some theorems were proved as follows

(1) For a polynomial $f_n(X) \in \mathbb{Z}(X)$ and

$$f_n(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

where a prime $p | a_n$, if $f_{n-1}(X)$ is irreducible over $\mathbb{Q}(X)$ and $\bar{f}_{n-1}(X) = f_{n-1}(X)$ where $\bar{f}_{n-1}(X) \equiv f_{n-1}(X) \pmod{p}$, then $f_n(X)$ is irreducible over $\mathbb{Q}(X)$.

(2) For any positive integer $n$, the polynomial

$$s_n(x) = 1 + \sum_{k=1}^{n} p_{k+1}x^k = 1 + p_2x + p_3x^2 + \cdots + p_{n+1}x^n$$

is irreducible over the field $\mathbb{Q}$ of rational numbers. Moreover, $s_n(x)$ is reducible modulo an odd prime $p$ if and only if $n = kp-1$ or $n = kp-2$, where $k$ is a positive integer greater than 1.

(3) For any positive integer $n$, the polynomial

$$s_n(x) = \sum_{m=0}^{n} (m+1)x^m = 1 + 2x + 3x^2 + \cdots + (n+1)x^n$$

is irreducible over the field $\mathbb{Q}$ of rational numbers. Moreover, $s_n(x)$ is reducible modulo any prime not greater than $p_m$ if and only if $n = \kappa(p_m#) - 1$ or $n = \kappa(p_m#) - 2$, where $\kappa$ is a positive integer, $p_m$ is the $m^{th}$ prime and $p_m# = p_1p_2\cdots p_m$. Furthermore $s_n(x)$ is reducible modulo any prime if and only if $n = \kappa(p_m#) - 1$ or $n = \kappa(p_m#) - 2$ when $m \to \infty$ such that $n \to \infty$.

Keywords number theory, distribution of primes, Goldbach’s conjecture, Lemoine’s conjecture, Legendre’s conjecture, Oppermann’s conjecture, Brocard’s conjecture, Andrica’s conjecture, Cramér’s conjecture, Polignac’s conjecture, Eisenstein’s criterion, irreducible polynomial

MR(2010) Subject Classification 11A41, 11C08, 12E05

Part I

On the representation of even numbers as the sum of two primes and the distribution of primes in short intervals

Abstract The representation of even numbers as the sum of two odd primes and the distribution of primes in short intervals were investigated in this paper. A main theorem was proved. It states: There
exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the even number $2n$ can be represented as the sum of two odd primes where one is smaller than $\sqrt{2n}$ and another is greater than $2n - \sqrt{2n}$.

The proof of the main theorem is based on the fundamental theorem of arithmetic and the theory of linear algebra. Its key ideas are as follows (1) For every number $n$ greater than a positive number $n_0$, let $Q_r = \{q_1, q_2, \cdots, q_r\}$ be a group of odd primes smaller than $\sqrt{2n}$ and $gcd(q_i, n) = 1$ for any $q_i \in Q_r$. Then the even number $2n$ can be represented as the sum of an odd prime $q_i \in Q_r$ and an odd number $d_i = 2n - q_i$. (2) If all the odd numbers $d_i$ are composite, then a group of linear algebraic equations can be formed and with the solutions $q_i \in Q_r$. (3) When a contradiction between the expectation and the actual results of the solutions is obtained, the main theorem will be proved.

It has been found that $n_0 = 31,637$. Based on the main theorem and by verifying for $n \leq n_0$, it was proved that for every number $n$ greater than 1, there are always at least one pair of primes $p$ and $q$ which are symmetrical about the number $n$ so that even numbers greater than 2 can be expressed as the sum of two primes. Hence, Goldbach’s conjecture was proved.

Also based on the main theorem, some theorems of the distribution of primes in short intervals were proved. By these theorems, the Legendre’s conjecture, the Oppermann’s conjecture, the Hanssner’s conjecture, the Brocard’s conjecture, the Andrica’s conjecture, the Sierpinski’s conjecture and the Sierpinski’s conjecture of triangular numbers were proved and the Mills’ constant can be determined.

**Keywords**  number theory, distribution of primes, Goldbach’s conjecture, Legendre’s conjecture, Oppermann’s conjecture, Brocard’s conjecture, Andrica’s conjecture

### 1 Introduction

1.1 Goldbach’s conjecture

The well known Goldbach’s conjecture is one of Landau’s problems (1912). It states: Every even number greater than 2 can be expressed as the sum of two primes [1-9].

Since Goldbach’s conjecture is very difficult to be solved and up to now is unsolved, many people believe that it is an isolated problem. For example, it seems completely different from and not related to Legendre’s conjecture [10-11] which is another one of Landau’s problems.

But it is proved in this paper that Goldbach’s conjecture is not an isolated problem. There are relationships between Goldbach’s conjecture and the distribution of primes in short intervals.

Since the method used in this paper is different from what normally used in the analytic number theory, the results of analytic number theory on Goldbach’s conjecture are not used and mentioned here.

1.2 Main theorem and the key ideas of its proof

The representation of even numbers as the sum of two odd primes and the distribution of primes in short intervals were investigated in this paper. A main theorem was proved. It states: There exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the even number $2n$ can be represented as the sum of two odd primes where one is smaller than $\sqrt{2n}$ and another is greater than $2n - \sqrt{2n}$.

The proof of the main theorem is based on the fundamental theorem of arithmetic and the theory of linear algebra. Its key ideas are as follows (1) For every number $n$ greater than a positive number $n_0$, let $Q_r = \{q_1, q_2, \cdots, q_r\}$ be a group of odd primes smaller than $\sqrt{2n}$ and $gcd(q_i, n) = 1$ for any $q_i \in Q_r$. Then the even number
2n can be represented as the sum of an odd prime $q_i \in Q_r$ and an odd number $d_i = 2n - q_i$.

(2) If all the odd numbers $d_i$ are composite, then every $d_i$ can be represented as the product of an odd number and an odd prime $q_j \in Q_r$, such that $d_i = a_{i,j} q_j$ where $q_j \neq q_i$. Thus a group of linear algebraic equations can be formed and with the solutions $q_i \in Q_r$.

(3) By using the analysis of a matrix equation and proving three lemmas on solutions of the matrix equation, it can be proved that at least one of the solutions is not equal to its corresponding expected solution $q_i \in Q_r$ when $n \to \infty$, and there exists a finite positive number $n_0$ such that the actual solutions to the group of linear algebraic equations are not equal to $q_i \in Q_r$ when $n > n_0$.

(4) This contradiction shows that the assumption ”all the odd numbers $d_i$ are composite” is false. When $n > n_0$, at least one odd number $d_i$ is not composite but an odd prime greater than $2n - \sqrt{2n}$. Therefore the main theorem is proved.

The assertion in the main theorem has been verified for $2n = N \leq 6.5 \times 10^{16}$. It has been found that $n_0 = 31,637$.

Based on the main theorem for $n > n_0$ and by verifying for $n \leq n_0$, it was proved that for every number $n$ greater than 1, there are always at least one pair of primes $p_i$ and $q_i$ which are symmetrical about the number $n$ so that even numbers greater than 2 can be expressed as the sum of two primes. Hence, Goldbach’s conjecture was proved.

1.3 Distribution of primes in short intervals

Based on the main theorem, some theorems of the distribution of primes in short intervals were proved.

1. It was proved that for every positive number $m$ there is always one prime between $m^2$ and $(m + 1)^2$. Thus the Legendre’s conjecture[10-11] was proved.

2. It was proved that for every positive number $m$ there are always two primes between $m^2$ and $(m + 1)^2$. One is between $m^2$ and $m(m + 1)$, and another is between $m(m + 1)$ and $(m + 1)^2$. Thus the Oppermann’s conjecture[19] was proved.

3. It was proved that for every positive number $m$ there are always three primes between $m^3$ and $(m + 1)^3$. The first one is between $m^3$ and $m^2(m + 1)$, and the second one is between $m^2(m + 1)$ and $m(m + 1)^2$, and the third one is between $m(m + 1)^2$ and $(m + 1)^3$. So, the theorem can be used to determine the Mills’ constant[17].

4. It was proved that for every positive number $m$ there are always $k$ primes between $m^k$ and $(m + 1)^k$ where $k$ is a positive integer greater than 1. For $i = 1, 2, \cdots, k$, there is always one prime between $m^{k-i+1}(m + 1)^{i-1}$ and $m^{k-i}(m + 1)^i$.

5. It was proved that there are at least two primes between $p_i^2$ and $p_i p_{i+1}$, and there are also at least two primes between $p_i p_{i+1}$ and $p_{i+1}^2$, for $i > 1$, where $p_i$ is the $i^{th}$ prime. Thus the Hanssner’s conjecture[8] was proved.

6. It was proved that there are at least four primes between $p_i^2$ and $p_{i+1}^2$, for $i > 1$, where $p_i$ is the $i^{th}$ prime. Thus the Brocard’s conjecture[20] was proved.

7. It was proved that for every positive number $m$ there are always four primes between $m^3$ and $(m + 1)^3$. Thus the theorem can be used to determine the Mills’ constant[17].

8. It was proved that for every positive number $m \geq a^k - 1$ where $a$ and $k$ are integers greater than 1, if there are at least $S_k$ primes between $m^k$ and $(m + 1)^k$, then there are always
$S_{k+1}$ primes between $m^{k+1}$ and $(m+1)^{k+1}$ where $S_{k+1} = aS_k$.

9. It was proved that there is always a prime between $m - m^\theta$ and $m$ where $\theta = 1/2$ and $m$ is a positive number greater than a positive number $2n_0$.

10. It was proved that there is always a prime between $m$ and $m + m^\theta$ where $\theta = 1/2$ and $m$ is a positive number greater than a positive number $2n_0$.

11. It was proved that the inequality $\sqrt{p_{i+1}} - \sqrt{p_i} < 1$ holds for all $i > 0$, where $p_i$ is the $i^{th}$ prime. Thus the Andrica’s conjecture[18] was proved.

12. It was proved that there is always one prime between $km$ and $(k+1)m$ where $m$ is a positive number greater than a positive number $2n_0$.

13. It was proved that if the numbers $1, 2, 3, \cdots, m^2$ with $m > 1$ are arranged in $m$ rows each containing $m$ numbers, then each row contains at least one prime. Thus the Sierpinski’s conjecture[8] was proved.

14. It was proved that between any two triangular numbers, there is at least one prime. Thus the Sierpinski’s conjecture of triangular numbers[8] was proved.

2 Definitions

2.1 Sets of primes

Let $n$ denote a positive number greater than or equal to $2^3$, an even number $N = 2n$ and $P$ denote a set of all odd primes smaller than or equal to the number $n$ where

$$P = \{p_2, p_3, \cdots, p_l\}, 3 = p_2 < p_3 < \cdots < p_l \leq n. \quad (2.1)$$

By the fundamental theorem of arithmetic, a positive number $n \geq 2^3$ can be written as one of three expressions as follows

$$n = 2^\alpha,$$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}, \quad 2 \leq i_1 < i_2 < \cdots < i_s \leq l, \quad (2.2)$$

$$n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}, \quad 2 \leq i_1 < i_2 < \cdots < i_s < l,$$

where $p_{ij} \in P$, $\alpha$ and $\alpha_j$ are positive integers for $j = 1, 2, \cdots, s$.

Then, let $P_s$ and $Q$ denote two subsets of $P$ where

$$P_s = \{\} = \phi \subset P \quad \text{for } n = 2^\alpha, \quad (2.3)$$

$$P_s = \{p_{i_1}, p_{i_2}, \cdots, p_{i_s}\} \subset P \quad \text{for } n \neq 2^\alpha,$$

and

$$Q = P \setminus P_s = \{q_1, q_2, \cdots, q_m\} \subset P, \quad (2.4)$$

$$3 \leq q_1 < q_2 < \cdots < q_m < n.$$

Let take the first $r$ elements of $Q$ to form a prime set $Q_r$, that is

$$Q_r = \{q_1, q_2, \cdots, q_r\} \subset Q \quad (2.5)$$

where for $n > 15$ the number $r$ is determined by the inequalities

$$q_r < \sqrt{2n} < q_{r+1}.$$

Hence the number $r$ is dependent on the number $n$. Generally speaking, the number $r$ is increased when the number $n$ is increased.
For example, when \( n = 2^4 \), there are \( 5 < \sqrt{2n} = \sqrt{32} < 7 \) so that there is \( r = 2 \); when \( n = 2^5 \) there are \( 7 < \sqrt{2n} = 8 < 11 \) so that there is \( r = 3; \cdots \); and when \( n = 2 \times 3 \times 5 \) there are \( 7 < \sqrt{2n} = \sqrt{60} < 11 \) or when \( n = 2^2 \times 3 \times 5 \) there are \( 7 < \sqrt{2n} = \sqrt{240} < 17 \), so that there is \( r = 1 \); when \( n = 2^3 \times 3 \times 5 \) there are \( 13 < \sqrt{2n} = \sqrt{240} < 17 \), so that there is \( r = 3; \cdots \).

Let \( a_{\text{min}} \) be a real and consider the following equation

\[
a_{\text{min}}q_r + q_{r+1} = 2n.
\]

Since \((\sqrt{2n}/4)^3 > n\) for \( n > 2^9 \), there are at most two primes which are divisors of the number \( n \) in the region \((q_r, q_{r+1})\). Then by Chebyshev-Bertrand theorem the inequality \( q_{r+1} < 8q_r \) holds. Hence we have

\[
a_{\text{min}} = \frac{2n - q_{r+1}}{q_r} > \frac{2n - 8q_r}{q_r} > \sqrt{2n} - 8. \tag{2.6}
\]

2.2 Linear algebraic equations

Let make a main assumption.

**Definition 2.1** (Main assumption)  *At least one even number greater than 4 can not be expressed as the sum of two odd primes.*

According to the main assumption \((2.1)\) and by using the prime set \( Q \), take \( q_i \in Q \) and let an odd number \( d_i = 2n - q_i \) for \( i = 1, 2, \cdots, m \). Then all the odd numbers \( d_i \) for \( i = 1, 2, \cdots, m \) should be composite.

By the fundamental theorem of arithmetic, for \( i = 1, 2, \cdots, m \), we can write

\[
d_i = q_{i,1}^{\alpha_{i,1}}q_{i,2}^{\alpha_{i,2}}\cdots q_{i,m_i}^{\alpha_{i,m_i}} \tag{2.7}
\]

where \( m_i \) is the sum of different prime factors of \( d_i \) and \( \alpha_{i,1}, \alpha_{i,2}, \cdots, \alpha_{i,m_i} \) are positive integers. Since \( \gcd(d_i, n) = 1 \), there are \( q_{i,k} \in Q \) for \( k = 1, 2, \cdots, m_i \).

For \( i = 1, 2, \cdots, m \) and \( 1 \leq j_i \leq r \), when \( q_{j_i} \in Q \) is equal to \( q_{i,k} \) which is a divisor of \( d_i \), let denote

\[
a_{i,j_i} = d_i/q_{j_i} = q_{i,1}^{\alpha_{i,1}}q_{i,2}^{\alpha_{i,2}}\cdots q_{i,k}^{\alpha_{i,k}}\cdots q_{i,m_i}^{\alpha_{i,m_i}}. \tag{2.8}
\]

Since \( q_i \leq q_r \) for \( 1 \leq i \leq r \) and \( q_{j_i} \leq q_r < q_{r+1} \) for \( 1 \leq j_i \leq r \), then for \( i = 1, 2, \cdots, r \) there are

\[
a_{i,j_i} - a_{\text{min}} = \frac{2n - q_i}{q_{j_i}} - a_{\text{min}} \geq \frac{2n - q_r}{q_r} - \frac{2n - q_{r+1}}{q_r} = \frac{q_{r+1} - q_r}{q_r} > 0
\]

so that there are \( a_{i,j_i} > a_{\text{min}} \) for \( i = 1, 2, \cdots, r \) and \( 1 \leq j_i \leq r \).

Hence, we can form a group of equalities as follows

\[
q_i + a_{i,j_i}; q_{j_i} = 2n \text{ for } i = 1, 2, \cdots, m \text{ and } 1 \leq j_i \leq r \tag{2.9}
\]

where \( q_i \) is not a divisor of \( n \) then \( q_i \neq q_{j_i} \).

Take the first \( r \) equalities in **Equality (2.9)** and let \( x_i = q_i \in Q_r \) for \( i = 1, 2, \cdots, r \). Then there are

\[
x_i + a_{i,j_i}; x_{j_i} = 2n \text{ for } i = 1, 2, \cdots, r \text{ and } 1 \leq j_i \leq r
\]

and the solutions to this group of linear algebraic equations should be \( x_i = q_i \in Q_r \) for \( i = 1, 2, \cdots, r \).

Thus we have the following definition of a matrix equation.
**Definition 2.2** (Linear algebraic equations) Based on the main assumption \((2.1)\) and by using the prime set \(Q_r\) and expressions \((2.7)-(2.9)\), let define a group of linear algebraic equations in the matrix form

\[
A x = b
\]  

(2.10)

then the solutions to this group of linear algebraic equations should be \(x_i = q_i \in Q_r\) for \(i = 1, 2, \cdots, r\) where

\[
A = \begin{bmatrix}
1 & 0 & \cdots & a_{1,j_1} & \cdots & 0 \\
0 & 1 & \cdots & a_{2,j_2} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_{r,j_r} & \cdots & 1
\end{bmatrix}, \quad b = 2n \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{bmatrix}
\]

where all diagonal elements \(a_{i,i}\) for \(i = 1, 2, \cdots, r\) are equal to 1 and there is just one non-diagonal and non-zero element \(a_{i,j_i}\) in each row of the matrix \(A\). For \(i = 1, 2, \cdots, r\), \(1 \leq j_i \leq r\) and \(j_i \neq i\), \(a_{i,j_i}\) is an odd number greater than 1 and satisfies \(a_{i,j_i} > a_{\text{min}}\) and \(\gcd(a_{i,j_i}, n) = 1\), and \(q_i \in Q_r\) is neither a divisor of \(a_{i,j_i}\) nor \(a_{i,j_i}\) is an even number.

It is easy to prove that if \(|\det(A)| = 1\) then all solutions of Equation \((2.10)\) will be composite. Thus it contradicts the fact that all solutions of Equation \((2.10)\) should be primes smaller than \(\sqrt{2n}\). Therefore there should be \(|\det(A)| \neq 1\). In fact, by the theory of linear algebra, \(|\det(A)|\) is an even number.

Since \(|\det(A)| \geq 2\), there is \(\det(A) \neq 0\). Therefore let \(A^{-1}\) and \(B\) denote the inverse and adjoint matrix of \(A\), respectively.

By exchanging its rows and columns, the matrix \(A\) in Definition \((2.2)\) can be written as one of three forms of a matrix \(\tilde{A}\) according to the value of \(|\det(A)|\).

The first form of \(\tilde{A}\) is

\[
\tilde{A} = \begin{bmatrix}
1 & 0 & 0 & \cdots & 0 & a_{1,\bar{r}} \\
a_{2,1} & 1 & 0 & \cdots & 0 & 0 \\
0 & a_{3,2} & 1 & \cdots & 0 & 0 \\
0 & 0 & a_{4,3} & \ddots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & a_{\bar{r},\bar{r}-1} & 1
\end{bmatrix}
\]  

(2.11)

where \(\text{rank}(\tilde{A}) = \bar{r}\) with \(\bar{r} = r\); all diagonal elements \(a_{i,i}\) are equal to 1; and there is just one non-diagonal and non-zero element \(a_{i,i-1}\) in each row of the matrix \(\tilde{A}\) with \(i - 1 \equiv \bar{r}, 1, \cdots, \bar{r}-1 (mod \ \bar{r})\) for \(i = 1, 2, \cdots, \bar{r}\).
The second form of \( \bar{A} \) is
\[
\bar{A} = \begin{bmatrix}
\mathbf{A}_s & 0 & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots \\
0 & \ddots & \ddots & 1 \\
\vdots & \ddots & \ddots & \ddots \\
0 & 0 & \ddots & 0 \\
\mathbf{A}_r & \mathbf{A}_{r+1} & \cdots & 1
\end{bmatrix}
\] (2.12)
where \( \mathbf{A}_s \) is a sub-matrix of \( \mathbf{A} \) with \( \text{rank}(\mathbf{A}_s) = s \) and similar to Form (2.11); all diagonal elements \( a_{i,i} \) are equal to 1; and there is just one non-diagonal and non-zero element \( a_{i,j} \) in each row of the matrix \( \bar{A} \) with \( j_i < i \) for rows \( i = s + 1, s + 2, \ldots, r \). Thus, we can only investigate the first form of \( \bar{A} \) with \( \bar{r} = s < r \).

The third form of \( \bar{A} \) is
\[
\bar{A} = \begin{bmatrix}
\mathbf{A}_1 & 0 & 0 & 0 \\
0 & \mathbf{A}_2 & 0 & 0 \\
0 & 0 & \ddots & 0 \\
0 & 0 & 0 & \mathbf{A}_m
\end{bmatrix}
\]
where any one of \( \mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_m \) is a sub-matrix of \( \mathbf{A} \) and similar to Form (2.11) or (2.12). Thus, we can only investigate the first form of \( \bar{A} \) with \( \bar{r} = r < r \).

Thus, by exchanging its rows and columns, the matrix \( A \) or at least one of its sub-matrixes can be written as a matrix \( \bar{A} \) in Form (2.11) with \( \bar{r} \leq r \).

Hence, without loss of generality, let consider solutions of Equation (2.10) with a matrix \( \bar{A} \) in Form (2.11).

3 Lemmas of linear algebraic equations

3.1 Solutions of linear algebraic equations

**Lemma 3.1** For a matrix \( \bar{A} \) in Form (2.11), solutions to Equation (2.10) are
\[
x_i = \frac{2n}{1 + \sum_{j=1}^{\bar{r}-1} c_{i,j}} \ldots, i = 1, 2, \ldots, \bar{r}
\] (3.1)
where \( i - 1 \equiv \bar{r}, 1, \ldots, \bar{r} - 1 (\text{mod } \bar{r}) \) for \( i = 1, 2, \ldots, \bar{r} \),
\[
a_1 = a_{2,1}, a_2 = a_{3,2}, \ldots, a_{\bar{r}} = a_{1,\bar{r}}
\] (3.2)
and
\[
c_{i,i} = a_i b_{i,i} = a_i, \quad i = 1, 2, \ldots, \bar{r},
\]
\[
c_{i,j} = a_i b_{i,j} = (-1)^{i+j+\bar{r}} \prod_{k=1}^{i} a_k, \quad j < i = 2, 3, \ldots, \bar{r},
\]
\[
c_{i,j} = a_i b_{i,j} = (-1)^{i+j+\bar{r}} \prod_{k=1}^{\bar{r}} a_k \prod_{k=j}^{\bar{r}} a_k, \quad i < j = 2, 3, \ldots, \bar{r},
\] (3.3)
where \( b_{i,j} \) are elements of \( \bar{B} \) which is the adjoint matrix of \( \bar{A} \).

**Proof** For a matrix \( \bar{A} \) in Form (2.11), we obtain
\[
det(\bar{A}) = 1 + (-1)^{\bar{r}+1} a_1 a_2 \cdots a_{\bar{r}-1} a_{\bar{r}}
\] (3.4)
where \( a_1, a_2, \ldots, a_{\bar{r}} \) are defined by Expression (3.2), and

\[
\hat{B} = \begin{bmatrix}
1 & b_{1,2} & \cdots & b_{1,\bar{r}} \\
b_{2,1} & 1 & \cdots & b_{2,\bar{r}} \\
\vdots & \vdots & \ddots & \vdots \\
b_{\bar{r},1} & b_{\bar{r},2} & \cdots & 1
\end{bmatrix}
\]  

(3.5)

where

\[
b_{i,i} = 1, \quad i = 1, 2, \ldots, \bar{r},
\]

\[
b_{i,j} = (-1)^{i+j} \prod_{k=j}^{i-1} a_k, \quad j < i = 2, 3, \ldots, \bar{r},
\]

\[
b_{i,j} = (-1)^{i+j+\bar{r}} \prod_{k=j}^{i-1} a_k \prod_{k=j}^{\bar{r}} a_k, \quad i < j = 2, 3, \ldots, \bar{r}.
\]  

(3.6)

According to Expression (3.6) and for \( \bar{r} + 1 \equiv 1(\text{mod } \bar{r}) \), we have

\[
\max\{|b_{i,j}|: j = 1, 2, \ldots, \bar{r}\} = |b_{i,i+1}|, i = 1, 2, \ldots, \bar{r}
\]

and

\[
b_{i,i+1} = (-1)^{i+1} \prod_{k=i+1}^{\bar{r}} a_k,
\]

\[
b_{i,i} = (-1)^{i+j} \prod_{k=j}^{i} a_k, \quad j = 1, 2, \ldots, \bar{r} - 1, j < i,
\]

\[
b_{i,i} = (-1)^{i+j} \prod_{k=j}^{\bar{r}-1} a_k \prod_{k=j+1}^{i} a_k, \quad j = 1, 2, \ldots, \bar{r} - 1, i < j,
\]

\[
b_{i,i} = (-1)^{i+j} \prod_{k=j+1}^{\bar{r}} a_k, \quad j = 2, 3, \ldots, \bar{r}.
\]

Thus, solutions to Equation (2.10) should be

\[
x_i = 2n \frac{\sum_{j=1}^{\bar{r}} b_{i,j}}{1 + (-1)^{i+1} a_1 a_2 \cdots a_{\bar{r}}}, i = 1, 2, \ldots, \bar{r}.
\]  

(3.7)

The ratio of \( x_i \) to \( x_k \) in Solution (3.7) is

\[
\frac{x_i}{x_k} = \frac{\sum_{j=1}^{\bar{r}} b_{i,j}}{\sum_{j=1}^{\bar{r}} b_{k,j}}, i, k = 1, 2, \ldots, \bar{r}.
\]  

(3.8)

According to Expression (3.6) and for \( \bar{r} + 1 \equiv 1(\text{mod } \bar{r}) \), we have

\[
\max\{|c_{i,j}|: j = 1, 2, \ldots, \bar{r}\} = |c_{i,i+1}| = \prod_{k=1}^{\bar{r}} a_k, i = 1, 2, \ldots, \bar{r},
\]

\[
\frac{c_{i,j}}{c_{i,i+1}} = (-1)^{i+j+\bar{r}} \prod_{k=j}^{i} a_k, \quad j = 1, 2, \ldots, \bar{r} - 1, j < i,
\]

\[
\frac{c_{i,j}}{c_{i,i+1}} = (-1)^{i+j+\bar{r}} \prod_{k=j}^{\bar{r}-1} a_k \prod_{k=j+1}^{i} a_k, \quad j = 1, 2, \ldots, \bar{r} - 1, i < j,
\]

\[
\frac{c_{i,j}}{c_{i,i+1}} = (-1)^{i+j+\bar{r}} \prod_{k=j+1}^{\bar{r}} a_k, \quad j = 2, 3, \ldots, \bar{r},
\]

and

\[
\sum_{j=1}^{\bar{r}} \frac{c_{i,j}}{c_{i,i+1}} = 1 - \frac{1}{a_{i+1}} + \frac{1}{a_{i+1}a_{i+2}} - \cdots + (-1)^{i-1} \frac{1}{\prod_{j=i}^{\bar{r}-1} a_{i+j}}
\]  

(3.10)

(3.11)

where \( i = 1, 2, \ldots, \bar{r} \) and \( i + j \equiv 1, 2, \ldots, \bar{r}(\text{mod } \bar{r}) \) for \( i + j = 1, 2, \ldots, \bar{r} \).

Thus, solutions to Equation (2.10) can be written as

\[
x_i = \frac{2n}{a_i} \frac{\sum_{j=1}^{\bar{r}} c_{i,j}}{1 + (-1)^{i+1} a_1 a_2 \cdots a_{\bar{r}}}, i = 1, 2, \ldots, \bar{r}.
\]  

(3.12)
The ratio of \( x_i \) to \( x_k \) in Solution (3.12) can be written as
\[
\frac{x_i}{x_k} = \frac{a_k}{a_i} \frac{\sum_{j=1}^{\bar{r}} c_{i,j}}{\sum_{j=1}^{\bar{r}} c_{k,j}}, \quad i, k = 1, 2, \ldots, \bar{r}.
\] (3.13)

By using Expression (3.13) and substituting
\[
x_\bar{r} = \frac{a_1}{a_\bar{r}} \frac{\sum_{j=1}^{\bar{r}} c_{\bar{r},j} x_1}{\sum_{j=1}^{\bar{r}} c_{1,j}}
\]
into the first equation of the group of linear algebraic equations (2.10) with a matrix \( \bar{A} \) in Form (2.11), we obtain
\[
(1 + a_1 \frac{\sum_{j=1}^{\bar{r}} c_{\bar{r},j}}{\sum_{j=1}^{\bar{r}} c_{1,j}}) x_1 = 2n.
\]

Hence, in the same way, solutions to Equation (2.10) can be written as
\[
x_i = \frac{2n}{1 + a_i \frac{\sum_{j=1}^{\bar{r}} c_{i,j-1}}{\sum_{j=1}^{\bar{r}} c_{i,j}}}, \quad i = 1, 2, \ldots, \bar{r}.
\] (3.14)

The proof of the lemma is completed.

### 3.2 Analysis of solutions of linear algebraic equations

**Lemma 3.2**  By Definition (2.2), at least one of \( x_i \) for \( i = 1, 2, \ldots, \bar{r} \) in solutions to Equation (2.10) is not equal to its corresponding expected solution \( q_i \in Q_r \) when \( n \to \infty \).

**Proof**  Based on Lemma 3.1, let consider Solution 3.1.

When \( n \to \infty \), since \( a_i > a_{\min} > \sqrt{2n} - 8 \) for \( i = 1, 2, \ldots, \bar{r} \), there are
\[
\lim_{n \to \infty} \sqrt{2n} - 8, \lim_{n \to \infty} \frac{1}{a_{\min}} = 0 \quad \text{and} \quad \lim_{n \to \infty} \frac{1}{a_i} = 0 \quad \text{for} \quad i = 1, 2, \ldots, \bar{r}.
\]

Then according to expressions (3.9-3.11) there are
\[
1 = \lim_{n \to \infty} \left( 1 - \frac{1}{a_{i+1}} \right) \leq \lim_{n \to \infty} \sum_{j=1}^{\bar{r}} \frac{c_{i,j}}{c_{i,i+1}} \leq \lim_{n \to \infty} \left( 1 - \frac{1}{a_{i+1}} + \frac{1}{a_{i+1}a_{i+2}} \right) = 1
\]
for \( i = 1, 2, \ldots, \bar{r} \) so that we obtain
\[
\lim_{n \to \infty} \frac{\sum_{j=1}^{\bar{r}} c_{i,j}}{\sum_{j=1}^{\bar{r}} c_{k,j}} = \lim_{n \to \infty} \frac{c_{i,i+1}}{c_{k,k+1}} \lim_{n \to \infty} \frac{\sum_{j=1}^{\bar{r}} c_{i,j}}{\sum_{j=1}^{\bar{r}} c_{k,j}} = 1
\] (3.15)

where \( i, k = 1, 2, \ldots, \bar{r} \).

Thus, according to expressions (3.1), when \( n \to \infty \), we have
\[
\lim_{n \to \infty} x_i = \lim_{n \to \infty} \frac{2n}{1 + a_i} \quad \text{for} \quad i = 1, 2, \ldots, \bar{r}.
\] (3.16)

In Expression (3.16) for \( i = 1, 2, \ldots, \bar{r} \), the limit of \( x_i \) always exists and is with a finite value or an infinite value. Since \( 2n \) and \( 1 + a_i \) are integers, the value of \( \frac{2n}{1 + a_i} \) is always a rational. If \( x_i \) is an integer, then there must be \( x_i | n \) so that \( x_i \) is not an element of \( Q_r \) and contradicts the fact that there should be \( x_i \in Q_r \) and \( \gcd(x_i, n) = 1 \). Thus whether \( x_i \) is an integer or not an integer, and the value of the limit of \( x_i \) in Expression (3.16) for \( i = 1, 2, \ldots, \bar{r} \) is finite or infinite, \( x_i \) is not equal to its corresponding expected solution \( q_i \in Q_r \).
Hence, when $n \to \infty$, no group of primes $q_i$ for $i = 1, 2, \cdots, r$ can satisfy Equation (2.10) and at least one of $x_i$ for $i = 1, 2, \cdots, r$ in solutions to Equation (2.10) is not equal to its corresponding expected solution $q_i \in Q_r$.

The proof of the lemma is completed.

**Lemma 3.3** By Definition (2.2), when $x_i$ is the solution to Equation (2.10) and its corresponding expected solution is the prime $q_i$ for $i = 1, 2, \cdots, r$, then at least one inequality $|x_i - q_i| > 0$ always holds for any big positive number $n$ greater than a positive number $n_0$ where

$$n_0 = \max\{n|q_i - q_j = 0 \text{ for } i = 1, 2, \cdots, r\}.$$

**Proof** Based on Lemma (3.1), let consider values $\varepsilon_i = |x_i - q_i|$ for $i = 1, 2, \cdots, r$ and $\varepsilon_n = \max\{\varepsilon_i| i = 1, 2, \cdots, r\}$.

Since by Lemma (3.2) there is

$$\lim_{n \to \infty} x_i \neq \lim_{n \to \infty} q_i \text{ or } \lim_{n \to \infty} |x_i - q_i| \neq 0,$$

then we obtain

$$\lim_{n \to \infty} \varepsilon_i = \lim_{n \to \infty} |x_i - q_i| > 0 \text{ and } \varepsilon_n = \lim_{n \to \infty} \varepsilon_n > 0.$$

Thus for any given small positive value $\varepsilon$ smaller than $\varepsilon_n$, a big positive number $n_\varepsilon$ can always be found to obtain at least one inequality $|x_i - q_i| \geq \varepsilon$ for any big positive number $n$ not smaller than the big positive number $n_\varepsilon$.

Therefore only small values of $n$ can satisfy equations $x_i - q_i = 0$ for $i = 1, 2, \cdots, r$. Then let define a positive number

$$n_0 = \max\{n|x_i - q_i = 0 \text{ for } i = 1, 2, \cdots, r\}.$$

Thus for any given small positive value $\varepsilon$ smaller than $\varepsilon_n$, a big positive number $n_\varepsilon$ can always be found to obtain at least one inequality $|x_i - q_i| \geq \varepsilon$ for $n \geq n_\varepsilon > n_0$.

The proof of the lemma is completed.

4 Theorems of primes

4.1 Main theorem

**Theorem 4.1** (Main theorem) There exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the even number $2n$ can be represented as the sum of two odd primes where one is smaller than $\sqrt{2n}$ and another is greater than $2n - \sqrt{2n}$.

**Proof** Let consider any number $n$ greater than a positive number $n_0$. According to the definitions in Sec. (2) and by using the prime set $P$, take $p_i \in P$ and let an odd number $c_i = 2n - p_i$ for $i = 2, 3, \cdots, l$, then we can form a group of equalities as follows

$$p_i + c_i = 2n \text{ for } i = 2, 3, \cdots, l.$$  (4.1)

When $p_i$ is a divisor of $n$ where $2 \leq i \leq l$, $c_i$ must be a composite number with a divisor $p_i$ or equal to $p_i$, then the corresponding $i^{th}$ equation can be removed from the group of equations (4.1).
Hence, by using the prime set \( Q \), take \( q_i \in Q \) and let an odd number \( d_i = 2n - q_i \) for \( i = 1, 2, \ldots, m \), then we can form a group of equalities as follows

\[
q_i + d_i = 2n \text{ for } i = 1, 2, \ldots, m. \tag{4.2}
\]

For \( n > n_0 > 15 \), there is \( q_1 < \sqrt{2n} \). Since \( q_i \) is an odd prime then \( \gcd(d_i, n) = 1 \). Meanwhile \( q_i \) is neither a divisor of \( d_i \) nor a divisor of \( n \).

Let assume that every odd number \( d_i \) contains prime factors smaller than \( \sqrt{2n} \) or can be expressed as the product of primes smaller than \( n \), that is, assume that all the odd numbers \( d_i \) are composite. Thus, by using expressions (2.7)[2.9] and taking the first \( r \) equalities in Equality (2.9), we can let 

\[
x_i = q_i \in Q_r \text{ for } i = 1, 2, \ldots, r
\]

and form a group of linear algebraic equations

\[
x_i + a_{i,j}x_j = 2n \text{ for } i = 1, 2, \ldots, r. \tag{4.3}
\]

or in the matrix form as Equation (2.10). By Definition (2.2) \( \det(A) \neq 0 \).

When all the odd numbers \( d_i \) for \( i = 1, 2, \ldots, r \) are composite, Equation (2.10) can be solved and solutions to Equation (2.10) should satisfy

\[
x_i = q_i \text{ for } i = 1, 2, \ldots, r. \tag{4.4}
\]

According to Equation (4.4), let define a set of numbers

\[
S = \{ n | n > 15 \text{ and } x_i - q_i = 0 \text{ for } i = 1, 2, \ldots, r \}.
\]

Then let \( n_0 \) and \( s_0 \) denote the maximum value and number of elements of the set \( S \), respectively. By the assumption that all the odd numbers \( d_i \) for \( i = 1, 2, \ldots, m \) are composite for every number \( n \), the numbers \( n_0 \) and \( s_0 \) should be infinite so that the number set \( S \) should be an infinite set.

Now, let investigate solutions to equations (4.3) or (2.10) to verify the assumption that all the odd numbers \( d_i \) for \( i = 1, 2, \ldots, m \) are composite.

When \( \text{rank}(A) = r = 1 \), since \( q_1 \) is not a divisor of \( d_1 \) and \( q_1 < \sqrt{2n} < q_2 \), \( d_1 \) must be a prime greater than \( 2n - \sqrt{2n} \).

Then, since \( |\det(A)| \neq 1 \), by lemmas (3.1) and (3.2) for the positive number \( n \to \infty \) or by lemmas (3.1) and (3.3) for any big positive number \( n_0 < n \to \infty \), it can be proved that the numbers \( n_0 \) and \( s_0 \) are finite so that the number set \( S \) is a finite set, and at least one of \( x_i \) for \( i = 1, 2, \ldots, r \) in solutions to Equation (2.10) is not equal to its corresponding expected solution \( q_i \in Q_r \). Hence, solutions \( x_i \) can not satisfy Equation (4.4) and at least one of \( d_i \) for \( i = 1, 2, \ldots, r \) is a prime greater than \( 2n - \sqrt{2n} \).

In the investigation of solutions of a group of linear algebraic equations (4.3), reductions to absurdity are derived and the assumption that all the odd numbers \( d_i \) for \( i = 1, 2, \ldots, m \) are composite, is proved false. Hence, it is proved that for every number \( n \) greater than \( n_0 \) at least one odd number \( d_i \) where \( 1 \leq i \leq r \), does not contain any prime factor smaller than \( \sqrt{2n} \) and must be an odd prime greater than \( 2n - \sqrt{2n} \).

This completes the proof of the theorem.

For small values of numbers \( n \) greater than 3, the assertion in the theorem has been verified for \( 2n = N \leq 6.5 \times 10^{10} \) and some higher small ranges up to \( 4.0 \times 10^{12} \) by the author. It has been found that \( n_0 = 31,637 \) and \( s_0 = 67 \). Some values of the number \( n \in S \) are \( n = 4, 6, 9, 12, 15, 19, 49, 61, 63, 64, 110, \ldots \).
4.2 Representation of even numbers

**Theorem 4.2**  For every number $n$ greater than 1, there are at least one pair of primes $p$ and $q$ which are symmetrical about the number $n$ and satisfy

$$p = n + x \quad \text{and} \quad q = n - x$$

(4.5)

where $x$ is a non-negative integer and $x = (p - q)/2$.

**Proof**  Let consider any number $n$ greater than 1.

For $n \leq n_0$ where $n_0$ is a positive number, we can easily find pairs of primes $p \geq n$ and $q \leq n$ satisfying

$$p = n + x \quad \text{and} \quad q = n - x \quad \text{where} \quad x = (p - q)/2.$$ 

Actually for small values of numbers $n$ greater than 3, the assertion in the theorem has been verified for $2n = N \leq 1.609 \times 10^{18}$ and some higher small ranges up to $4 \times 10^{18}$ by T. Oliveira e Silva[1].

For $n > n_0$, by Theorem (4.1), we can find at least one pair of primes $q < n$ and $p = 2n - q$ satisfying

$$p = n + x \quad \text{and} \quad q = n - x \quad \text{where} \quad x = (p - q)/2.$$ 

This completes the proof of the theorem.

**Theorem 4.3**  Every even number greater than 2 can be expressed as the sum of two primes.

**Proof**  Consider any even number $N = 2n$ greater than 2. By Theorem (4.2), for every number $n$ greater than 1, there are always at least one pair of primes $p$ and $q$ satisfying

$$p = n + x \quad \text{and} \quad q = n - x.$$ 

Thus, for every even number $N = 2n$ greater than 2, we have

$$N = 2n = p + q,$$

that is, every even number $N > 2$ can be expressed as the sum of two primes.

This completes the proof of the theorem and the Goldbach’s conjecture is proved.

4.3 Distribution of primes in short intervals

**Theorem 4.4**  For every positive number $m$ there is always one prime $p$ between $m^2$ and $(m + 1)^2$.

**Proof**  For $1 \leq m \leq \sqrt{2n_0}$ where $n_0$ is a positive number we can easily verify the truth of the theorem. The smallest primes between $m^2$ and $(m + 1)^2$ for $m = 1, 2, \cdots$ are $2, 5, \cdots$. Let consider any number $m$ greater than $\sqrt{2n_0}$.

Let a number $n$ satisfy

$$m^2 \leq 2n - \sqrt{2n} \quad \text{and} \quad m(m + 1) \leq 2n \leq (m + 1)^2,$$

then we have

$$n > n_0 \quad \text{and} \quad m < \sqrt{2n} \leq m + 1.$$ 

By Theorem (4.1), we can find at least one pair of primes

$$q < \sqrt{2n} \quad \text{and} \quad p = 2n - q > 2n - \sqrt{2n} \quad \text{when} \quad n > n_0.$$
Then, there must be
\[ q \leq m \text{ and } m^2 < p < 2n \leq (m + 1)^2. \]

The last inequality shows that there is one prime \( p \) between \( m^2 \) and \( (m + 1)^2 \).

This completes the proof of the theorem and the Legendre’s conjecture is proved.

**Theorem 4.5** For every positive number \( m \) there are always two primes between \( m^2 \) and \( (m + 1)^2 \). One is between \( m^2 \) and \( m(m + 1) \), and another is between \( m(m + 1) \) and \( (m + 1)^2 \).

**Proof** For \( 1 \leq m \leq \sqrt{2n_0} \) where \( n_0 \) is a positive number we can easily verify the truth of the theorem. The primes between \( m^2 \) and \( (m + 1)^2 \) for \( m = 1, 2, \ldots \) are \{2, 3\}, \{5, 7\}, \ldots. Let consider any number \( m \) greater than \( \sqrt{2n_0} \).

Firstly let a number \( n = \frac{m(m + 1)}{2} \), so we have
\[ n > n_0 \text{ and } m < \sqrt{2n} < m + 1. \]

By Theorem 4.1, we can find at least one pair of primes
\[ q < \sqrt{2n} \text{ and } p = 2n - q > 2n - \sqrt{2n} \text{ when } n > n_0. \]

Since \( q \) and \( p \) are integers, there must be
\[ q \leq m \text{ and } p = 2n - q \geq 2n - m \geq m(m + 1) - m = m^2. \]

Since \( p \) is a prime, then there must be
\[ q \leq m \text{ and } m^2 < p < 2n \leq (m + 1). \]

The last inequality shows that there is a prime \( p \) between \( m^2 \) and \( m(m + 1) \).

Secondly let the number \( n \) satisfy
\[ m(m + 2) \leq 2n \leq (m + 1)^2, \]
so we have
\[ n > n_0 \text{ and } m < \sqrt{2n} \leq m + 1. \]

By Theorem 4.1, we can find at least one pair of primes
\[ q < \sqrt{2n} \text{ and } p = 2n - q > 2n - \sqrt{2n} \text{ when } n > n_0. \]

Since \( q \) and \( p \) are integers, there must be
\[ q \leq m \text{ and } p = 2n - q \geq 2n - m \geq m(m + 2) - m = m(m + 1). \]

Since \( p \) is a prime, then there must be
\[ q \leq m \text{ and } m(m + 1) < p < 2n \leq (m + 1)^2. \]

The last inequality shows that there is a prime \( p \) between \( m(m + 1) \) and \( (m + 1)^2 \).

Thus, for every positive number \( m \) there are two primes between \( m^2 \) and \( (m + 1)^2 \). One is between \( m^2 \) and \( m(m + 1) \), and another is between \( m(m + 1) \) and \( (m + 1)^2 \).

This completes the proof of the theorem and the Oppermann’s conjecture is proved.

**Theorem 4.6** For every positive number \( m \) there are always three primes between \( m^3 \) and \( (m + 1)^3 \). The first one is between \( m^3 \) and \( m^2(m + 1) \), and the second one is between \( m^2(m + 1) \) and \( m(m + 1)^2 \), and the third one is between \( m(m + 1)^2 \) and \( (m + 1)^3 \).
Proof For $1 \leq m \leq \sqrt[3]{2n_0}$ where $n_0$ is a positive number we can easily verify the truth of the theorem. The primes between $m^3$ and $(m + 1)^3$ for $m = 1, 2, \cdots$ are $\{2, 3, 5\}$, $\{11, 13, 19\}$, $\cdots$.

Let consider any number $m$ greater than $\sqrt[3]{2n_0}$.

Firstly let a number $n = m^2(m + 1)/2$, so we have $n > n_0$ and

$$2n - \sqrt{2n} = m^2(m + 1) - m\sqrt{m + 1} > m^3.$$ 

By Theorem (4.1), we can find at least one pair of primes

$q < \sqrt{2n}$ and $p = 2n - q > 2n - \sqrt{2n}$ when $n > n_0$.

Therefore, we have

$$q \leq m\sqrt{m + 1} \text{ and } m^3 < p < 2n = m^2(m + 1).$$

The inequalities show that there is a prime $p$ between $m^3$ and $m^2(m + 1)$.

Secondly let the number $n = m(m + 1)^2/2$, so we have $n > n_0$ and

$$2n - \sqrt{2n} = m(m + 1)^2 - \sqrt{m(m + 1)} > m^2(m + 1).$$

By Theorem (4.1), we can find at least one pair of primes

$q < \sqrt{2n}$ and $p = 2n - q > 2n - \sqrt{2n}$ when $n > n_0$.

Therefore, we have

$$q \leq \sqrt{m(m + 1)} \text{ and } m^2(m + 1) < p < 2n = m(m + 1)^2.$$ 

The inequalities show that there is a prime $p$ between $m^2(m + 1)$ and $m(m + 1)^2$.

Thirdly let the number $n$ satisfy

$$m(m + 1)^2 + m(m + 2) \leq 2n \leq (m + 1)^3,$$ 

so we have $n > n_0$ and

$$2n - \sqrt{2n} \geq m(m + 1)^2 + m(m + 2) - \sqrt{m + 1}(m + 1) > m(m + 1)^2.$$ 

By Theorem (4.1), we can find at least one pair of primes

$q < \sqrt{2n}$ and $p = 2n - q > 2n - \sqrt{2n}$ when $n > n_0$.

Therefore, we have

$$q \leq \sqrt{m + 1}(m + 1) \text{ and } m(m + 1)^2 < p < 2n \leq (m + 1)^3.$$ 

The inequalities show that there is a prime $p$ between $m(m + 1)^2$ and $(m + 1)^3$.

Thus, for every positive number $m$ there are always three primes between $m^3$ and $(m + 1)^3$.

This completes the proof of the theorem.

Theorem 4.7 For every positive number $m$ there are always $k$ primes between $m^k$ and $(m + 1)^k$ where $k$ is a positive integer greater than 1. For $i = 1, 2, \cdots, k$, there is always one prime between $m^{k-i+1}(m + 1)^{i-1}$ and $m^{k-i}(m + 1)^i$. 
Theorem 4.9

Since \( p \) is a composite number, then there are always two primes between \( p \) and \( k \).

For \( k > 2 \) and \( i = 1,2,\ldots,k \), let the number \( n = m^{k-i}(m+1)^i/2 \), since
\[
m^{(k-i)/2} > (m+1)^{1-i/2} \text{ for } k > 2
\]
then we have
\[
m^{k-i}(m+1)^{i-1} - m^{(k-i)/2}(m+1)^{i/2} > 0
\]
and
\[
2n - \sqrt{2n} = m^{k-i}(m+1)^i - m^{(k-i)/2}(m+1)^{i/2} > m^{k-i+1}(m+1)^{i-1}.
\]

By Theorem (4.1), we can find at least one pair of primes
\[
q < \sqrt{2n} \text{ and } p = 2n - q > 2n - \sqrt{2n} \text{ when } n > n_0.
\]

Therefore, we have
\[
q \leq m^{(k-i)/2}(m+1)^{i/2} \text{ and } m^{k-i+1}(m+1)^{i-1} < p < 2n = m^{k-i}(m+1)^i.
\]
The last inequality shows that there is a prime \( p \) between \( m^{k-i+1}(m+1)^{i-1} \) and \( m^{k-i}(m+1)^i \).

Thus, for every positive number \( m \) there are \( k \) primes between \( m^k \) and \( (m+1)^k \). For \( i = 1,2,\ldots,k \), there is one prime between \( m^{k-i+1}(m+1)^{i-1} \) and \( m^{k-i}(m+1)^i \).

This completes the proof of the theorem.

Theorem 4.8

There are at least two primes between \( p_i^2 \) and \( p_i p_{i+1} \), and there are also at least two primes between \( p_i p_{i+1} \) and \( p_{i+1}^2 \), for \( i > 1 \), where \( p_i \) is the \( i \)th prime.

Proof

Since \( p_{i+1} > p_i + 2 \) and \( p_i \leq p_{i+1} - 2 \), we have
\[
p_i p_{i+1} \geq p_i(p_i + 2) = p_i^2 + 2p_i = (p_i + 1)^2 - 1
\]
and
\[
p_i p_{i+1} \leq (p_i + 2)p_{i+1} = p_{i+1}^2 - 2p_{i+1} = (p_{i+1} - 1)^2 - 1.
\]

By Theorem (4.5), there are always two primes between \( p_i^2 \) and \( (p_i + 1)^2 \). Since \( p_i(p_i + 2) \) is a composite number, then there are always two primes between \( p_i^2 \) and \( p_i p_{i+1} \).

Also by Theorem (4.5), there are always two primes between \( (p_{i+1} - 1)^2 \) and \( p_{i+1}^2 \). Since \( (p_{i+1} - 2)p_{i+1} \) is a composite number, then there are always two primes between \( p_i p_{i+1} \) and \( p_{i+1}^2 \).

This completes the proof of the theorem and the Hanssner’s conjecture is proved.

Theorem 4.9

There are at least four primes between \( p_i^2 \) and \( p_{i+1}^2 \), for \( i > 1 \), where \( p_i \) is the \( i \)th prime.

Proof

Since \( p_i < p_{i+1} < p_{i+1} \), there is a square \( (p_{i} + 1)^2 \) between \( p_i^2 \) and \( p_{i+1}^2 \).

By Theorem (4.5), there are always two primes between \( p_i^2 \) and \( (p_{i} + 1)^2 \), and also there are always two primes between \( (p_{i} + 1)^2 \) and \( p_{i+1}^2 \). Thus, there are always at least four primes between \( p_i^2 \) and \( p_{i+1}^2 \).

This completes the proof of the theorem and the Brocard’s conjecture is proved.
Theorem 4.10  For every positive number \( m \) there are always four primes between \( m^3 \) and \((m + 1)^3\).

Proof  For \( 1 \leq m \leq \sqrt[3]{2n_0} \) we can easily verify the truth of the theorem. The primes between \( m^3 \) and \((m + 1)^3\) for \( m = 1, 2, \cdots \) are \( \{2, 3, 5, 7\}, \{11, 13, 19, 23\}, \cdots \). Let consider any number \( m \) greater than \( \sqrt[3]{2n_0} \).

Since for any number \( m \) greater than 5, there is always a number \( s \) satisfying \( m^{3/2} \leq s \leq (m + 1)^{3/2} - 2 \). Then there are \( m^3 \leq s^2 \) and \( (s + 2)^2 \leq (m + 1)^3 \).

By Theorem 4.11, there are always two primes between \( s^2 \) and \((s + 1)^2\), and also there are always two primes between \((s + 1)^2 \) and \((s + 2)^2\). Thus, there are always at least four primes between \( m^3 \) and \((m + 1)^3\).

This completes the proof of the theorem.

Theorem 4.11  For every positive number \( m \geq a^k - 1 \) where \( a \) and \( k \) are integers greater than 1, if there are at least \( S_k \) primes between \( m^k \) and \((m + 1)^k\), then there are always \( S_{k+1} \) primes between \( m^{k+1} \) and \((m + 1)^{k+1} \) where \( S_k = aS_{k+1} \).

Proof  For any number \( m \geq a^k - 1 \), there is always a number \( s \) satisfying \( m^{1+1/k} \leq s \leq (m + 1)^{1+1/k} - a \). Then there are \( m^{k+1} \leq s^k \) and \((s + a)^k \leq (m + 1)^{k+1} \).

Since there are at least \( S_k \) primes between \( s^k \) and \((s + 1)^k\) for \( s \geq m \geq a^k - 1 \), then there are also at least \( S_k \) primes between \((s + i)^k \) and \((s + i + 1)^k\) for \( i = 1, 2, \cdots, a - 1 \). Thus, there are always \( S_{k+1} \) primes between \( m^{k+1} \) and \((m + 1)^{k+1} \) where \( S_k = aS_{k+1} \).

This completes the proof of the theorem.

Theorem 4.12  There is always a prime \( p \) between \( m - m^\theta \) and \( m \) where \( \theta = 1/2 \) and \( m \) is a positive number greater than a positive number \( 2n_0 \).

Proof  Let consider any positive number \( m \) greater than \( 2n_0 \).

Let a number \( n = (m + 1)/2 \). Then for \( m > 2n_0 \) we have \( n > n_0 \). By Theorem 4.1, we can find at least one pair of primes

\[
q < \sqrt{2n} \quad \text{and} \quad p = 2n - q > 2n - \sqrt{2n} \quad \text{when} \quad n > n_0.
\]

Since \( 1 + \sqrt{2n - 1} > \sqrt{2n} \) and the prime \( q \geq 3 \), we have

\[
2n - 1 - \sqrt{2n - 1} < 2n - \sqrt{2n} < p < 2n - 1.
\]

Firstly for \( m = 2n - 1 \) let \( m - m^\theta = 2n - 1 - \sqrt{2n - 1} = m - \sqrt{m} \), so we have \( \theta = 1/2 \) and \( q < m^\theta \) and \( m - m^\theta < p < m \).

The last inequality shows that there is a prime \( p \) between \( m - m^\theta \) and \( m \) where \( \theta = 1/2 \) and \( m \) is an odd number greater than \( m_0 \).

Secondly for \( m = 2n \) let \( m - m^\theta = 2n - \sqrt{2n} = m - \sqrt{m} \), so we have \( \theta = 1/2 \) and \( q < m^\theta \) and \( m - m^\theta < p < m \).

The last inequality shows that there is a prime \( p \) between \( m - m^\theta \) and \( m \) where \( \theta = 1/2 \) and \( m \) is an even number greater than \( m_0 \).

This completes the proof of the theorem.
Theorem 4.13 There is always a prime $p$ between $m$ and $m + m^\theta$ where $\theta = 1/2$ and $m$ is a positive number greater than a positive number $2n_0$.

Proof Let consider any positive number $m$ greater than $2n_0$.

Let a number $n$ satisfy

$$m \leq 2n - \sqrt{2n} < m + 1,$$

then we have $n > n_0$ for $m > 2n_0$ and

$$\sqrt{m + 1/4 + 1/2} \leq \sqrt{2n} < \sqrt{m + 5/4 + 1/2}$$

and

$$\sqrt{m + 1/4 + m + 1/2} \leq 2n < \sqrt{m + 5/4 + m + 3/2}.$$

Let consider the equation

$$2n = m + m^\theta + f(m, x, y) - \sqrt{m} \text{ where } f(m, x, y) = \sqrt{m + x + y}. \quad (4.6)$$

When $f(m, 1/4, 1/2)$ is substituted into Equation (4.6), we obtain

$$m^\theta \geq \sqrt{m} \text{ and } \theta \geq 1/2$$

and when $f(m, 5/4, 3/2)$ is substituted into Equation (4.6), we obtain

$$m^\theta < \sqrt{m} \text{ and } \theta < 1/2.$$

Therefore, we can always find a suitable value of $f(m, x, y)$ to get

$$m^\theta = \sqrt{m} \text{ and } \theta = 1/2.$$

By Theorem (4.1), we can find at least one pair of primes

$$q < \sqrt{2n} \text{ and } p = 2n - q > 2n - \sqrt{2n} \text{ when } n > n_0.$$

Since any odd prime $q$ is greater than 2, then $p \leq 2n - 3$. For $1/4 \leq x \leq 5/4$ and $1/2 \leq y \leq 3/2$, since $f(m, x, y) - \sqrt{m} \leq 2$, the values of $\theta$ are in a small neighborhood of $1/2$, and the values of $m + m^\theta$ are in the region $[2n - 2, 2n]$ and are greater than the upper bound of the prime $p$, that is, $p \leq 2n - 3$. Hence we have

$$m < p < m + m^\theta < 2n.$$

The inequality shows that there is a prime $p$ between $m$ and $m + m^\theta$ where $\theta = 1/2$ and $m$ is a positive number greater than $n_0$.

This completes the proof of the theorem.

Theorem 4.14 The inequality $\sqrt{p_i+1} - \sqrt{p_i} < 1$ holds for all $i > 0$, where $p_i$ is the $i^{th}$ prime.

Proof For $1 \leq i \leq k$ where $p_k \geq 2n_0$ we can easily verify the truth of the theorem. Let consider any positive number $i$ greater than $k$.

The inequality $\sqrt{p_{i+1}} - \sqrt{p_i} < 1$ can be written as

$$g_i = p_{i+1} - p_i < 2\sqrt{p_i} + 1.$$

Let a number $n = (p_{i+1} + 1)/2$, so we have $n > n_0$ where $n_0$ is a positive number.
By Theorem (4.1), we can find at least one pair of primes
\[ q < \sqrt{2n} \text{ and } p = 2n - q > 2n - \sqrt{2n} \text{ when } n > n_0. \]

Since \( p_i \geq p \), then we obtain
\[ g_i = p_{i+1} - p_i < 2n - p < \sqrt{2n} = \sqrt{p_{i+1} + 1} \]
\[ < \sqrt{p_{i+1}} + 1 < \sqrt{2p_i + 1}. \]

Also by Theorem (4.13), let a number \( m = p_i \) greater than \( 2n_0 \), so there is always a prime \( p \) between \( p_i \) and \( p_i + \sqrt{p_i} \). Therefore we obtain
\[ g_i = p_{i+1} - p_i < \sqrt{p_i}. \]

Therefore we have
\[ g_i = p_{i+1} - p_i < 2\sqrt{p_i} + 1 \text{ and } \sqrt{p_{i+1}} - \sqrt{p_i} < 1. \]

This completes the proof of the theorem and the Andrica’s conjecture is proved.

**Theorem 4.15** There is always one prime \( p \) between \( km \) and \((k+1)m\) where \( m \) is a positive number greater than 1 and \( 1 \leq k < m \).

**Proof** For \( 2 \leq m \leq n_0 \) where \( n_0 \) is a positive number we can easily verify the truth of the theorem. Let consider any positive number \( m \) greater than \( n_0 \).

Since \( m = (k+1)m - km \geq \sqrt{(k+1)m} \) for \( 1 \leq k < m \), we can find a number \( n \) satisfying \( km \leq 2n - \sqrt{2n} \) and \( 2n \leq (k+1)m \). Then for \( 1 \leq k < m \) and \( m > n_0 \) we have \( n > n_0 \) and
\[ m = (k+1)m - km \geq 2n - (2n - \sqrt{2n}) = \sqrt{2n} \text{ or } m \geq \sqrt{2n}. \]

By Theorem (4.1), we can find at least one pair of primes
\[ q < \sqrt{2n} \text{ and } p = 2n - q > 2n - \sqrt{2n} \text{ when } n > n_0. \]

Therefore, we obtain
\[ q < \sqrt{2n} \leq m \text{ and } km \leq 2n - \sqrt{2n} < p < 2n \leq (k+1)m. \]

The last inequality shows that there is a prime \( p \) between \( km \) and \((k+1)m\).

This completes the proof of the theorem.

**Theorem 4.16** If the numbers \( 1, 2, 3, \ldots, m^2 \) with \( m > 1 \) are arranged in \( m \) rows each containing \( m \) numbers:

\[
\begin{array}{cccc}
1, & 2, & 3, & \cdots, m \\
\times 1, & m + 2, & m + 3, & \cdots, 2m \\
2m + 1, & 2m + 2, & 2m + 3, & \cdots, 3m \\
\times \cdots, & \cdots, & \cdots, & \cdots, \cdots, \\
(m - 1)m + 1, & (m - 1)m + 2, & (m - 1)m + 3, & \cdots, m^2 \\
\end{array}
\]

then each row contains at least one prime.
Proof The first row of Table (4.7) contains of course \((m > 1)\) prime 2.

By Theorem (4.15) for a positive number \(k\) smaller than \(m\), there is always one prime between \(km\) and \((k + 1)m\), which means that the \((k + 1)\)th row of Table (4.7) contains at least one prime.

Thus, each row of Table (4.7) contains at least one prime.

This completes the proof of the theorem and the Sierpinski’s conjecture is proved.

**Theorem 4.17** Between any two triangular numbers, there is at least one prime. Namely, if we arrange natural numbers in rows in such a manner that in the \(m\)th row we put \(m\) consecutive natural numbers, i.e. if we form the table

\[
\begin{align*}
1 \\
2, & \quad 3 \\
4, & \quad 5, \quad 6 \\
7, & \quad 8, \quad 9, \quad 10 \\
11, & \quad 12, \quad 13, \quad 14, \quad 15 \\
\cdots & \quad \cdots & \quad \cdots & \quad \cdots & \quad \cdots
\end{align*}
\]

(4.8)

then each but the first of its rows contains at least one prime.

Proof For \(2 \leq m \leq \sqrt{2n_0}\) where \(n_0\) is a positive number we can easily verify the truth of the theorem. The smallest primes in the \(m\)th row of Table (4.8) for \(m = 2, 3, \ldots\) are 2, 5, \ldots. Let consider any number \(m\) greater than \(\sqrt{2n_0}\).

Since the \((m - 1)\)th and \(m\)th triangular numbers are \((m - 1)m/2\) and \(m(m + 1)/2\), respectively, the difference of the \(m\)th and \((m - 1)\)th triangular numbers is

\[
m = m(m + 1)/2 - (m - 1)m/2 > \sqrt{m(m + 1)/2}.
\]

Then, we can find a number \(n\) satisfying \((m - 1)m/2 \leq 2n - \sqrt{2n}\) and \(2n \leq m(m + 1)/2\) for \(m > k\) we have \(n > n_0\) and

\[
m = m(m + 1)/2 - (m - 1)m/2 \geq 2n - (2n - \sqrt{2n}) = \sqrt{2n} \text{ or } m > \sqrt{2n}.
\]

By Theorem (4.1), we can find at least one pair of primes

\[
q < \sqrt{2n} \text{ and } p = 2n - q > 2n - \sqrt{2n} \text{ when } n > n_0.
\]

Then, we have

\[
q < \sqrt{2n} < m \text{ and } (m - 1)m/2 < p < 2n \leq m(m + 1)/2.
\]

The last inequality shows that there is one prime \(p\) between \((m - 1)m/2\) and \(m(m + 1)/2\), i.e. between any two triangular numbers, there is at least one prime.

This completes the proof of the theorem and the Sierpinski’s conjecture of triangular numbers is proved.

References
[1] Wapedia - Wiki, Goldbach’s conjecture.
[2] Weisstein, Eric W., Goldbach Conjecture. MathWorld.
Part II

On the representation of odd numbers as the sum of an odd prime and an even semiprime and the distribution of primes in short intervals

Abstract. The representation of odd numbers as the sum of an odd prime and an even semiprime, and the distribution of primes in short intervals were investigated in this paper. A main theorem was proved. It states: There exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the odd number $2n + 1$ can be represented as the sum of an odd prime $p$ and an even semiprime $2q$ where $q$ is an odd prime smaller than $\sqrt{2n}$ and $p$ is greater than $2n + 1 - 2\sqrt{2n}$.

The proof of the main theorem is based on the fundamental theorem of arithmetic and the theory of linear algebra. Its key ideas are as follows (1) For every number $n$ greater than a positive number $n_0$, let $Q_r = \{q_1, q_2, \ldots, q_r\}$ be a group of odd primes smaller than $\sqrt{2n}$ and $gcd(q_i, 2n + 1) = 1$ for any...
Then the odd number $2n + 1$ can be represented as the sum of an even semiprime $2q_i$ and an odd number $d_i = 2n + 1 - 2q_i$ where $q_i \in Q_r$. (2) If all the odd numbers $d_i$ are composite, then a group of linear algebraic equations can be formed and with the solutions $q_i \in Q_r$. (3) When a contradiction between the expectation and the actual results of the solutions is obtained, the main theorem will be proved.

It has been found that $n_0 = 19,875$. Based on the main theorem and by verifying for $n \leq n_0$, it was proved that for every number $n$ greater than 2, there are always at least one pair of primes $p$ and $q$ so that all odd integers greater than 5 can be represented as the sum of an odd prime and an even semiprime. Therefore, Lemoine’s conjecture was proved.

Also based on the main theorem, some theorems of the distribution of primes in short intervals were given out and proved. By these theorems, the Legendre’s conjecture and the Andrica’s conjecture were proved and the Mills’ constant can be determined.

**Keywords** number theory, distribution of primes, Lemoine’s conjecture, Legendre’s conjecture, Andrica’s conjecture

### 5 Introduction

#### 5.1 Lemoine’s conjecture

Lemoine’s conjecture, also known as Levy’s conjecture, states that all odd integers greater than 5 can be represented as the sum of an odd prime and an even semiprime[1-9].

The Lemoine’s conjecture is similar to but stronger than Goldbach’s weak conjecture. Since it is difficult to be solved and up to now is unsolved, many people believe that it is an isolated problem. For example, it seems completely different from and no relation to Legendre’s conjecture which is one of Landau’s problems (1912).

But it is proved in this paper that Lemoine’s conjecture is not an isolated problem. There are relationships between Lemoine’s conjecture and the distribution of primes in short intervals.

Since the method used in this paper is different from what normally used in the analytic number theory, the results of analytic number theory on Lemoine’s conjecture are not used and mentioned here.

#### 5.2 Main theorem and the key ideas of its proof

The representation of odd numbers as the sum of an odd prime and an even semiprime and the distribution of primes in short intervals were investigated in this paper. A main theorem was proved. It states: There exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the odd number $2n + 1$ can be represented as the sum of an odd prime $p$ and an even semiprime $2q$ where $q$ is an odd prime smaller than $\sqrt{2n}$ and $p$ is greater than $2n + 1 - 2\sqrt{2n}$.

The proof of the main theorem is based on the fundamental theorem of arithmetic and the theory of linear algebra, and its key ideas are as follows

(1) For every number $n$ greater than a positive number $n_0$, let $Q_r = \{q_1, q_2, \ldots, q_r\}$ be a group of odd primes smaller than $\sqrt{2n}$ and $gcd(q_i, 2n + 1) = 1$ for any $q_i \in Q_r$. Then the odd number $2n + 1$ can be represented as the sum of an even semiprime $2q_i$ and an odd number $d_i = 2n + 1 - 2q_i$ where $q_i \in Q_r$.

(2) If all the odd numbers $d_i$ are composite, then every $d_i$ can be represented as the product of an odd number and an odd prime $q_j \in Q_r$ such that $d_i = a_i \cdot q_j$ where $q_j \neq q_i$. Thus a group
of linear algebraic equations can be formed and with the solutions \( q_i \in Q_r \).

(3) By using the analysis of a matrix equation and proving three lemmas on solutions of the matrix equation, it can be proved that at least one of the solutions is not equal to its corresponding expected solution \( q_i \in Q_r \) when \( n \to \infty \), and there exists a finite positive number \( n_0 \) such that the actual solutions to the group of linear algebraic equations are not equal to \( q_i \in Q_r \) when \( n > n_0 \).

(4) This contradiction shows that the assumption ”all the odd numbers \( d_i \) are composite” is false. When \( n > n_0 \), at least one odd number \( d_i \) is not composite but an odd prime greater than \( 2n + 1 - 2\sqrt{2n} \). Therefore the main theorem is proved.

The assertion in the main theorem has been verified for \( 2n + 1 = N \leq 6.5 \times 10^{10} \). It has been found that \( n_0 = 19,875 \).

Based on the main theorem for \( n > n_0 \) and by verifying for \( n \leq n_0 \), it was proved that for every number \( n \) greater than 2, there are always at least one pair of primes \( p \) and \( q \) so that all odd integers greater than 5 can be represented as the sum of an odd prime and an even semiprime. Hence, Lemoine’s conjecture was proved.

5.3 Distribution of primes in short intervals

Based on the main theorem, some theorems of the distribution of primes in short intervals were proved.

1. It was proved that for every positive number \( m \) there is always a prime between \( m^2 \) and \( (m + 1)^2 \). Thus the Legendre’s conjecture[10-11] was proved.

2. It was proved that for every positive number \( m \) there are always three primes between \( m^3 \) and \( (m + 1)^3 \). The first one is between \( m^3 \) and \( m^2(m + 1) \), and the second one is between \( m^2(m + 1) \) and \( m(m + 1)^2 \), and the third one is between \( m(m + 1)^2 \) and \( (m + 1)^3 \). So, the theorem can be used to determine the Mills’ constant[15].

3. It was proved that there is always a prime between \( m - 2m^\theta \) and \( m \) where \( \theta = 1/2 \) and \( m \) is a positive number greater than a positive number \( 2n_0 \).

4. It was proved that there is always a prime between \( m \) and \( m + 2m^\theta \) where \( \theta = 1/2 \) and \( m \) is a positive number greater than a positive number \( 2n_0 \).

5. It was proved that the inequality \( \sqrt{p_{i+1}} - \sqrt{p_i} < 1 \) holds for all \( i > 0 \), where \( p_i \) is the \( i^{th} \) prime. Thus the Andrica’s conjecture[16] was proved.

6 Definitions

6.1 Sets of primes

Let \( n \) denote a positive number greater than or equal to \( 2^3 \), an odd number \( N = 2n + 1 \) and \( P \) denote a set of all odd primes smaller than the number \( n \) where

\[
P = \{p_2, p_3, \ldots, p_t\}, \quad 3 = p_2 < p_3 < \cdots < p_t < n.
\]

By the fundamental theorem of arithmetic, a positive number \( N = 2n + 1 \) can be written as

\[
N = 2n + 1 = p_{i_1}^{\alpha_{i_1}}p_{i_2}^{\alpha_{i_2}}\cdots p_{i_s}^{\alpha_{i_s}}p_{i_{s+1}}^{\alpha_{i_{s+1}}}p_{i_{s+2}}^{\alpha_{i_{s+2}}}\cdots p_{i_l}^{\alpha_{i_l}}
\]

for \( 2 \leq i_1 < i_2 < \cdots < i_s < i_{s+1} < i_{s+2} < \cdots < i_t \leq l \) where \( p_{i_j} \leq n < p_{i_{j+1}} \), \( p_{i_j} \in P \) for \( j = 1, 2, \cdots, s \), all \( \alpha_{i_j} \) are positive integers for \( j = 1, 2, \cdots, t \).
Then, let $P_s$ and $Q$ denote two subsets of $P$ where

$$P_s = \{\} = \phi \subset P \quad \text{for } s = 0,$$

$$P_s = \{p_{i_1}, p_{i_2}, \ldots, p_{i_s}\} \subset P \quad \text{for } s > 0$$

and

$$Q = P \setminus P_s = \{q_1, q_2, \ldots, q_m\} \subset P,$$

$$3 \leq q_1 < q_2 < \cdots < q_m < n.$$

Let take the first $r$ elements of $Q$ to form a prime set $Q_r$, that is

$$Q_r = \{q_1, q_2, \ldots, q_r\} \subset Q$$

where for $2n + 1 > 15$ the number $r$ is determined by the inequalities

$$q_r < \sqrt{2n} < q_{r+1}.$$

Hence the number $r$ is dependent on the number $n$. Generally speaking, the number $r$ is increased when the number $n$ is increased.

For example, when $n = 2^3$ there are $3 < \sqrt{2n} = 4 < 5$ so that there is $r = 1$; when $n = 2^4$ there are $5 < \sqrt{2n} = \sqrt{32} < 7$ so that there is $r = 2$; \ldots; and when $2n + 1 = 3^3$ there are $5 < \sqrt{2n} = \sqrt{26} < 7$, so that there is $r = 1$; when $2n + 1 = 3^4$ there are $7 < \sqrt{2n} = \sqrt{80} < 11$ so that there is $r = 2$; \ldots.

Let $a_{min}$ be a real and consider the following equation

$$a_{min}q_r + 2q_{r+1} = 2n + 1.$$

Since $(\sqrt{2n}/4)^3 > 2n$ for $n > 2^{11}$, there are at most two primes which are divisors of the number $2n + 1$ in the region $(q_r, q_{r+1})$. Then by Chebyshev-Bertrand theorem the inequality $q_{r+1} < 8q_r$ holds. Hence we have

$$a_{min} = \frac{2n + 1 - 2q_{r+1}}{q_r} > \frac{2n + 1 - 16q_r}{q_r} > \sqrt{2n} - 16. \quad (6.6)$$

### 6.2 Linear algebraic equations

Let make a main assumption.

**Definition 6.1** (Main assumption) *At least one odd number greater than 5 can not be expressed as the sum of an odd prime and an even semiprime.*

By using the prime set $Q$, take $q_i \in Q$ and let an odd number $d_i = 2n + 1 - 2q_i$ for $i = 1, 2, \ldots, m$. Then all the odd numbers $d_i$ for $i = 1, 2, \ldots, m$ should be composite numbers according to the main assumption [6.1].

By the fundamental theorem of arithmetic, for $i = 1, 2, \ldots, m$, we can write

$$d_i = q_{i,1}^{\alpha_{i,1},1} q_{i,2}^{\alpha_{i,2}} \cdots q_{i,m_i}^{\alpha_{i,m_i}} \quad (6.7)$$

where $m_i$ is the sum of different prime factors of $d_i$ and $\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,m_i}$ are positive integers. Since $\gcd(d_i, 2n+1) = 1$, there are $q_{i,k} \in Q_r$ for $k = 1, 2, \ldots, m_i$.

For $i = 1, 2, \ldots, m$ and $1 \leq j_i \leq r$, when $q_{j_i} \in Q_r$ is equal to $q_{i,k}$ which is a divisor of $d_i$, let denote

$$a_{i,j_i} = d_i/q_{j_i} = q_{i,1}^{\alpha_{i,1},1} q_{i,2}^{\alpha_{i,2},1} \cdots q_{i,k-1}^{\alpha_{i,k-1},1} q_{i,m_i}^{\alpha_{i,m_i}}. \quad (6.8)$$
Since \( q_i \leq q_r \) for \( 1 \leq i \leq r \) and \( q_{j_i} \leq q_r < q_{r+1} \) for \( 1 \leq j_i \leq r \), then for \( i = 1, 2, \cdots, r \) there are
\[
a_{i,j_i} - a_{\text{min}} = \frac{2n + 1 - 2q_i}{q_r} - a_{\text{min}} \\
\geq \frac{2n + 1 - 2q_r}{q_r} - \frac{2n + 1 - 2q_{r+1}}{q_r} = 2q_{r+1} - q_r > 0,
\]
so that there are \( a_{i,j_i} > a_{\text{min}} \) for \( i = 1, 2, \cdots, r \) and \( 1 \leq j_i \leq r \).

Hence, we can form a group of equalities as follows
\[
2q_i + a_{i,j_i}q_{j_i} = 2n + 1 \quad \text{for} \quad i = 1, 2, \cdots, m \quad \text{and} \quad 1 \leq j_i \leq r \quad \text{(6.9)}
\]
where since \( q_i \) is not a divisor of the number \( 2n + 1 \) then \( q_i \neq q_{j_i} \).

Take the first \( r \) equalities in Equality (6.9) and let \( x_i = q_i \in Q_r \) for \( i = 1, 2, \cdots, r \). Then there are
\[
2x_i + a_{i,j_i}x_{j_i} = 2n + 1 \quad \text{for} \quad i = 1, 2, \cdots, r \quad \text{and} \quad 1 \leq j_i \leq r
\]
and the solutions to this group of linear algebraic equations should be \( x_i = q_i \in Q_r \) for \( i = 1, 2, \cdots, r \).

Thus we have the following definition of a matrix equation.

**Definition 6.2** (Linear algebraic equations) Based on the main assumption (6.1) and by using the prime set \( Q_r \) and expressions (6.7)(6.9), let define a group of linear algebraic equations in the matrix form
\[
Ax = b
\]
then the solutions to this group of linear algebraic equations should be \( x_i = q_i \in Q_r \) for \( i = 1, 2, \cdots, r \) where
\[
A = \begin{bmatrix}
2 & 0 & \cdots & a_{1,j_1} & \cdots & 0 \\
0 & 2 & \cdots & a_{2,j_2} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_{r,j_r} & \cdots & 2
\end{bmatrix},
\]
\[
b = (2n + 1) \begin{bmatrix} 1 \\
1 \\
\vdots \\
1 \end{bmatrix},
\]
\[
x = \begin{bmatrix} x_1 \\
x_2 \\
\vdots \\
x_r \end{bmatrix}
\]
where all diagonal elements \( a_{i,i} \) for \( i = 1, 2, \cdots, r \) are equal to 2 and there is just one non-diagonal and non-zero element \( a_{i,j_i} \) in each row of the matrix \( A \). For \( i = 1, 2, \cdots, r, 1 \leq j_i \leq r \) and \( j_i \neq i, a_{i,j_i} \) is an odd number greater than 1 and satisfies \( a_{i,j_i} > a_{\text{min}} \) and \( \gcd(a_{i,j_i}, 2n+1) = 1 \), and \( q_i \in Q_r \) is neither a divisor of \( a_{i,j_i} \) nor a divisor of \( 2n + 1 \).

It is easy to prove that if \( |\det(A)| = 1 \) then all solutions of Equation (6.10) will be composite. Thus it contradicts the fact that all solutions of Equation (6.10) should be primes smaller than \( \sqrt{2n} \). Therefore there should be \( |\det(A)| \neq 1 \).

It is also easy to prove that if \( |\det(A)| = 2^r \) then all solutions of Equation (6.10) will not be primes smaller than \( \sqrt{2n} \). Thus it contradicts the fact that all solutions of Equation (6.10) should be primes smaller than \( \sqrt{2n} \). Therefore there should be \( |\det(A)| \neq 2^r \).

Since \( |\det(A)| \geq 1 \), there is \( \det(A) \neq 0 \). Therefore let \( A^{-1} \) and \( B \) denote the inverse and adjoint matrix of \( A \), respectively.

By exchanging its rows and columns, the matrix \( A \) in Definition (6.2) can be written as one of three forms of a matrix \( \bar{A} \) according to the value of \( |\det(A)| \).
The first form of \( \bar{A} \) is

\[
\bar{A} = \begin{bmatrix}
2 & 0 & 0 & \cdots & 0 & a_{1,\bar{r}} \\
a_{2,1} & 2 & 0 & \cdots & 0 & 0 \\
0 & a_{3,2} & 2 & \cdots & 0 & 0 \\
0 & 0 & a_{4,3} & \ddots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & a_{\bar{r},\bar{r}-1} & 2
\end{bmatrix}
\]

(6.11)

where \( \text{rank}(\bar{A}) = \bar{r} \) with \( \bar{r} = r \); all diagonal elements \( a_{i,i} \) are equal to 2; and there is just one non-diagonal and non-zero element \( a_{i,i-1} \) in each row of the matrix \( \bar{A} \) with \( i-1 \equiv \bar{r}, 1, \cdots, \bar{r}-1 (\text{mod } \bar{r}) \) for \( i = 1, 2, \cdots, \bar{r} \).

The second form of \( \bar{A} \) is

\[
\bar{A} = \begin{bmatrix}
A_s & 0 & 0 & 0 & 0 \\
\cdots & a_{s+1,j+s+1} & \cdots & 2 & 0 & 0 \\
\cdots & a_{s+2,j+s+2} & \cdots & 2 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & 0 \\
\cdots & a_{r,j_r} & \cdots & \cdots & 2
\end{bmatrix}
\]

(6.12)

where \( A_s \) is a sub-matrix of \( A \) with \( \text{rank}(A_s) = s \) and similar to Form (6.11); all diagonal elements \( a_{i,i} \) are equal to 2; and there is just one non-diagonal and non-zero element \( a_{i,j_i} \) in each row of the matrix \( \bar{A} \) with \( j_i < i \) for rows \( i = s + 1, s + 2, \cdots, r \). Thus, we can only investigate the first form of \( \bar{A} \) with \( \bar{r} = s < r \).

The third form of \( \bar{A} \) is

\[
\bar{A} = \begin{bmatrix}
A_1 & 0 & 0 & 0 \\
0 & A_2 & 0 & 0 \\
0 & 0 & \ddots & 0 \\
0 & 0 & 0 & A_m
\end{bmatrix}
\]

where any one of \( A_1, A_2, \cdots, A_m \) is a sub-matrix of \( A \) and similar to Form (6.11) or (6.12). Thus, we can only investigate the first form of \( \bar{A} \) with \( \bar{r} < r \).

Thus, by exchanging its rows and columns, the matrix \( A \) or at least one of its sub-matrixes can be written as a matrix \( \bar{A} \) in Form (6.11) with \( \bar{r} \leq r \).

Hence, without loss of generality, let consider solutions of Equation (6.10) with a matrix \( \bar{A} \) in Form (6.11).

7 Lemmas of linear algebraic equations

7.1 Solutions of linear algebraic equations

**Lemma 7.1** For a matrix \( \bar{A} \) in Form (6.11), solutions to Equation (6.10) are

\[
x_i = \frac{2n+1}{2 + a_1^2 \sum_{j=1}^{r-1} c_{r-1,j} \sum_{j=1}^r c_{i,j}}, \quad i = 1, 2, \cdots, \bar{r}
\]

(7.1)
where \( i - 1 \equiv r, 1, \ldots, \bar{r} - 1 (\mod \bar{r}) \) for \( i = 1, 2, \ldots, \bar{r} \),

\[
a_1 = a_{2,1}, a_2 = a_{3,2}, \ldots, a_{\bar{r}} = a_{1,\bar{r}} \quad (7.2)
\]

and

\[
c_{i,j} = a_i b_{i,j} = a_i 2^{\bar{r} - 1}, \quad i = 1, 2, \ldots, \bar{r},
\]

\[
c_{i,j} = a_i b_{i,j} = (-1)^{i+j} 2^{\bar{r} - j - 1} \prod_{k=1}^{i} a_k, \quad j < i = 2, 3, \ldots, \bar{r}, \quad (7.3)
\]

\[
c_{i,j} = a_i b_{i,j} = (-1)^{i+j+\bar{r}} 2^{\bar{r} - i - 1} \prod_{k=1}^{i} a_k \prod_{k=j}^{\bar{r}} a_k, \quad i < j = 2, 3, \ldots, \bar{r},
\]

where \( b_{i,j} \) are elements of \( B \) which is the adjoint matrix of \( A \).

**Proof**

For a matrix \( A \) in Form (6.11), we obtain

\[
det(A) = 2^\bar{r} + (-1)^{\bar{r}+1} a_1 a_2 \cdots a_{\bar{r}-1} a_{\bar{r}} \quad (7.4)
\]

where \( a_1, a_2, \ldots, a_{\bar{r}} \) are defined by Expression (7.2), and

\[
\bar{B} = \begin{bmatrix}
2^{\bar{r} - 1} & b_{1,2} & \cdots & b_{1,\bar{r}} \\
& b_{2,1} & 2^{\bar{r} - 1} & \cdots & b_{2,\bar{r}} \\
& & \ddots & \ddots & \ddots \\
& & & b_{\bar{r},1} & b_{\bar{r},2} & \cdots & 2^{\bar{r} - 1}
\end{bmatrix} \quad (7.5)
\]

where

\[
b_{i,j} = 2^{\bar{r} - 1}, \quad i = 1, 2, \ldots, \bar{r},
\]

\[
b_{i,j} = (-1)^{i+j} 2^{\bar{r} - j - 1} \prod_{k=1}^{i} a_k, \quad j < i = 2, 3, \ldots, \bar{r}, \quad (7.6)
\]

\[
b_{i,j} = (-1)^{i+j+\bar{r}} 2^{\bar{r} - i - 1} \prod_{k=1}^{i} a_k \prod_{k=j}^{\bar{r}} a_k, \quad i < j = 2, 3, \ldots, \bar{r}.
\]

According to Expression (7.6) and for \( \bar{r} + 1 \equiv 1 (\mod \bar{r}) \), we have

\[
\max \{|b_{i,j}| : j = 1, 2, \ldots, \bar{r}\} = |b_{i,i+1}|, \quad i = 1, 2, \ldots, \bar{r}
\]

and

\[
\frac{b_{i,i+1}}{b_{i+1,i+1}} = (-1)^{i+j+\bar{r}} \frac{2^{\bar{r} - j - 1}}{\prod_{k=j}^{\bar{r}} a_k}, \quad i = 1, 2, \ldots, \bar{r} - 1, j > i,
\]

\[
\frac{b_{i,j}}{b_{i+1,j}} = (-1)^{i+j+\bar{r}} \frac{2^{\bar{r} - j - 1}}{\prod_{k=j}^{\bar{r}} a_k}, \quad i = 1, 2, \ldots, \bar{r} - 1, j \leq i,
\]

\[
\frac{b_{i+1,j}}{b_{i+1,i+1}} = (-1)^{i+j+\bar{r}} \frac{2^{\bar{r} - j - 1}}{\prod_{k=i}^{\bar{r}} a_k}, \quad j = 2, 3, \ldots, \bar{r}.
\]

Thus, solutions to Equation (6.10) should be

\[
x_i = \frac{2n + 1}{2^\bar{r} + (-1)^{\bar{r}+1} a_1 a_2 \cdots a_{\bar{r}}}, \quad i = 1, 2, \ldots, \bar{r} \quad (7.7)
\]

The ratio of \( x_i \) to \( x_k \) in Solution (7.7) is

\[
\frac{x_i}{x_k} = \frac{\sum_{j=1}^{\bar{r}} b_{i,j}}{\sum_{j=1}^{\bar{r}} b_{k,j}}, \quad i, k = 1, 2, \ldots, \bar{r}. \quad (7.8)
\]

According to Expression (7.3) and for \( \bar{r} + 1 \equiv 1 (\mod \bar{r}) \), we have

\[
\max \{|c_{i,j}| : j = 1, 2, \ldots, \bar{r}\} = |c_{i,i+1}| = \prod_{k=1}^{\bar{r}} a_k, \quad i = 1, 2, \ldots, \bar{r}, \quad (7.9)
\]
Lemma 7.2 Analysis of solutions of linear algebraic equations

Proof Based on Lemma (7.1), let consider solutions (7.1).

By using Expression (7.13) and substituting \( x \) in Solution (7.12) can be written as

\[
\sum_{j=1}^{\bar{r}} \frac{c_{i,j}}{c_{i,i+1}} = 1 - \frac{2}{a_{i+1}} + \frac{2^2}{a_{i+1}a_{i+2}} - \cdots + (-1)^{\bar{r}-1} \frac{2^{\bar{r}-1}}{\prod_{j=1}^{\bar{r}-1} a_{i+j}}
\]

(7.11)

where \( i = 1, 2, \ldots, \bar{r} \) and \( i + j \equiv 1, 2, \ldots, \bar{r}(\text{mod } \bar{r}) \) for \( i + j = 1, 2, \ldots \).

Thus, solutions to Equation (6.10) can be written as

\[
x_i = \frac{2n + 1}{a_i} \cdot \frac{\sum_{j=1}^{\bar{r}} c_{i,j}}{2^\bar{r} + (-1)^{\bar{r}+1} a_1 a_2 \cdots a_{\bar{r}}} \cdot x_1, \quad i = 1, 2, \ldots, \bar{r}.
\]

(7.12)

The ratio of \( x_i \) to \( x_k \) in Solution (7.12) can be written as

\[
\frac{x_i}{x_k} = \frac{a_k}{a_i} \cdot \frac{\sum_{j=1}^{\bar{r}} c_{i,j}}{\sum_{j=1}^{\bar{r}} c_{k,j}} \cdot x_1, \quad i, k = 1, 2, \ldots, \bar{r}.
\]

(7.13)

By using Expression (7.13) and substituting

\[
x_{\bar{r}} = \frac{a_1}{a_{\bar{r}}} \cdot \frac{\sum_{j=1}^{\bar{r}} c_{\bar{r},j}}{\sum_{j=1}^{\bar{r}} c_{1,j}} \cdot x_1
\]

into the first equation of the group of linear algebraic equations (6.10) with a matrix \( \hat{A} \) in Form (6.11), we obtain

\[
(2 + a_i \sum_{j=1}^r \frac{c_{r,j}}{c_{1,j}}) x_1 = 2n + 1.
\]

Hence, in the same way, solutions to Equation (6.10) can be written as

\[
x_i = \frac{2n + 1}{2 + a_i \sum_{j=1}^{\bar{r}} \frac{c_{i,j}}{c_{i,i+1}}} x_1, \quad i = 1, 2, \ldots, \bar{r}.
\]

(7.14)

The proof of the lemma is completed.

7.2 Analysis of solutions of linear algebraic equations

Lemma 7.2 By Definition (6.2), at least one of \( x_i \) for \( i = 1, 2, \ldots, r \) in solutions to Equation (6.10) is not equal to its corresponding expected solution \( q_i \in Q_r \) when \( n \to \infty \).

Proof Based on Lemma (7.1), let consider solutions (7.1).

When \( n \to \infty \), since \( a_i > a_{\min} > \sqrt{2n} - 16 \) for \( i = 1, 2, \ldots, \bar{r} \), there are

\[
\lim_{n \to \infty} \sqrt{2n} - 16 \to \infty, \quad \lim_{n \to \infty} \frac{1}{a_{\min}} = 0 \quad \text{and} \quad \lim_{n \to \infty} \frac{1}{a_i} = 0 \quad \text{for} \quad i = 1, 2, \ldots, \bar{r}.
\]

Then according to expressions (6.9) (7.11) there are

\[
1 = \lim_{n \to \infty} (1 - \frac{2}{a_{i+1}}) \leq \lim_{n \to \infty} \sum_{j=1}^{\bar{r}} \frac{c_{i,j}}{c_{i,i+1}} \leq \lim_{n \to \infty} (1 - \frac{2}{a_{i+1}} + \frac{2^2}{a_{i+1}a_{i+2}}) = 1
\]

for \( i = 1, 2, \ldots, \bar{r} \) so that we obtain

\[
\lim_{n \to \infty} \sum_{j=1}^{\bar{r}} \frac{c_{i,j}}{c_{k,j}} = \lim_{n \to \infty} \frac{c_{i,i+1}}{c_{k,k+1}} \lim_{n \to \infty} \sum_{j=1}^{\bar{r}} \frac{c_{i,j}}{c_{k,j}} = 1
\]

(7.15)
where $i, k = 1, 2, \cdots, \bar{r}$.

Thus, according to expressions (7.1), when $n \to \infty$, we have

$$\lim_{n \to \infty} x_i = \lim_{n \to \infty} \frac{2n + 1}{2 + a_i} \quad \text{for } i = 1, 2, \cdots, \bar{r}. \quad (7.16)$$

In Expression (7.10) for $i = 1, 2, \cdots, \bar{r}$, the limit of $x_i$ always exists and is with a finite value or an infinite value. Since $2n + 1$ and $2 + a_i$ are integers, the value of $\frac{2n + 1}{2 + a_i}$ is always a rational. If $x_i$ is an integer, then there must be $x_i|2n + 1$ so that $x_i$ is not an element of $Q_r$ and contradicts the fact that there should be $x_i \in Q_r$ and $gcd(x_i, 2n + 1) = 1$. Thus whether $x_i$ is an integer or not an integer, and the value of the limit of $x_i$ in Expression (7.16) for $i = 1, 2, \cdots, \bar{r}$ is finite or infinite, $x_i$ is not equal to its corresponding expected solution $q_i \in Q_r$.

Hence, when $n \to \infty$, no group of primes $q_i$ for $i = 1, 2, \cdots, r$ can satisfy Equation (6.10) and at least one of $x_i$ for $i = 1, 2, \cdots, r$ in solutions to Equation (6.10) is not equal to its corresponding expected solution $q_i \in Q_r$.

The proof of the lemma is completed.

**Lemma 7.3** By Definition (6.2), when $x_i$ is the solution to Equation (6.10) and its corresponding expected solution is the prime $q_i$ for $i = 1, 2, \cdots, r$, then at least one inequality $|x_i - q_i| > 0$ always holds for any big positive number $n$ greater than a positive number $n_0$ where

$$n_0 = \max\{n|x_i - q_i = 0 \quad \text{for } i = 1, 2, \cdots, r\}.$$

**Proof** Based on Lemma (7.1), let consider values $\varepsilon_i = |x_i - q_i|$ for $i = 1, 2, \cdots, r$ and $\varepsilon_n = \max\{\varepsilon_i|i = 1, 2, \cdots, r\}$.

Since by Lemma (7.2) there is

$$\lim_{n \to \infty} x_i \neq \lim_{n \to \infty} q_i \text{ or } \lim_{n \to \infty} |x_i - q_i| \neq 0,$$

then we obtain

$$\lim_{n \to \infty} \varepsilon_i = \lim_{n \to \infty} |x_i - q_i| > 0 \quad \text{and } \varepsilon_{\infty} = \lim_{n \to \infty} \varepsilon_n > 0.$$

Thus for any given small positive value $\varepsilon$ smaller than $\varepsilon_{\infty}$, a big positive number $n_{\varepsilon}$ can always be found to obtain at least one inequality $|x_i - q_i| \geq \varepsilon$ for any big positive number $n$ not smaller than the big positive number $n_{\varepsilon}$.

Therefore only small values of $n$ can satisfy equations $x_i - q_i = 0$ for $i = 1, 2, \cdots, r$. Then let define a positive number

$$n_0 = \max\{n|x_i - q_i = 0 \quad \text{for } i = 1, 2, \cdots, r\}.$$

Thus for any given small positive value $\varepsilon$ smaller than $\varepsilon_{\infty}$, a big positive number $n_{\varepsilon}$ can always be found to obtain at least one inequality $|x_i - q_i| \geq \varepsilon$ for $n \geq n_{\varepsilon} > n_0$.

The proof of the lemma is completed.

8 Theorems of primes

8.1 Main theorem

**Theorem 8.1** (Main theorem) There exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the odd number $2n + 1$ can be represented as the sum of an odd prime $p$ and an even semiprime $2q$ where $q$ is an odd prime smaller than $\sqrt{2n}$ and $p$ is greater than $2n + 1 - 2\sqrt{2n}$. 
Proof Let consider any number $n$ greater than a finite positive number $n_0$. According to the definitions in Sec. (6) and by using the prime set $P$, take $p_i \in P$ and let an odd number $c_i = 2n + 1 - 2p_i$ for $i = 2, 3, \cdots, l$, then we can form a group of equalities as follows

$$2p_i + c_i = 2n + 1 \text{ for } i = 2, 3, \cdots, l. \quad (8.1)$$

When $p_i$ is a divisor of $2n + 1$ where $2 \leq i \leq l$, $c_i$ must be a composite number with a divisor $p_i$ or equal to $p_i$, then the corresponding $i^{th}$ equation can be removed from the group of equations (8.1).

Hence, by using the prime set $Q$, take $q_i \in Q$ and let an odd number $d_i = 2n + 1 - 2q_i$ for $i = 1, 2, \cdots, m$, then we can form a group of equalities as follows

$$2q_i + d_i = 2n + 1 \text{ for } i = 1, 2, \cdots, m. \quad (8.2)$$

For $n > n_0 > 15$, there is $q_1 < \sqrt{2n}$. Since $q_i$ is an odd prime then $gcd(d_i, 2n + 1) = 1$. Meanwhile $q_i$ is neither a divisor of $d_i$ nor a divisor of $2n + 1$.

Let assume that every odd number $d_i$ contains prime factors smaller than $\sqrt{2n}$ or can be expressed as the product of primes smaller than $n$, that is, assume that all the odd numbers $d_i$ are composite. Thus, by using expressions (6.1)(6.9) and taking the first $r$ equalities in Equality (6.9), we can let $x_i = q_i \in Q_r$ for $i = 1, 2, \cdots, r$ and form a group of linear algebraic equations

$$2x_i + a_{i,j}x_j = 2n + 1 \text{ for } i = 1, 2, \cdots, r. \quad (8.3)$$

or in the matrix form as Equation (6.10). By Definition (6.2) $det(A) \neq 0$.

When all the odd numbers $d_i$ for $i = 1, 2, \cdots, r$ are composite, Equation (6.10) can be solved and solutions to Equation (6.10) should satisfy

$$x_i = q_i \text{ for } i = 1, 2, \cdots, r. \quad (8.4)$$

According to Equation (8.4), let define a set of numbers

$$S = \{n|n > 15 \text{ and } x_i - q_i = 0 \text{ for } i = 1, 2, \cdots, r\}.$$ 

Then let $n_0$ and $s_0$ denote the maximum value and number of elements of the set $S$, respectively. By the assumption that all the odd numbers $d_i$ for $i = 1, 2, \cdots, m$ are composite for every number $n$, the numbers $n_0$ and $s_0$ should be infinite so that the number set $S$ should be an infinite set.

Now, let investigate solutions to equations (8.3) or (6.10) to verify the assumption that all the odd numbers $d_i$ for $i = 1, 2, \cdots, m$ are composite.

When $rank(A) = r = 1$, since $q_1$ is not a divisor of $d_1$ and $q_1 < \sqrt{2n} < q_2$, $d_1$ must be a prime greater than $2n + 1 - 2\sqrt{2n}$.

Then, since $|det(A)| \neq 2^r$, by lemmas (7.1) and (7.2) for the positive number $n \to \infty$ or by lemmas (7.1) and (7.3) for any big positive number $n$ satisfying $n_0 < n < \infty$, it can be proved that the numbers $n_0$ and $s_0$ are finite so that the number set $S$ is a finite set, and at least one of $x_i$ for $i = 1, 2, \cdots, r$ in solutions to Equation (6.10) is not equal to its corresponding expected solution $q_i \in Q_r$. Hence, solutions $x_i$ can not satisfy Equation (8.4) and at least one of $d_i$ for $i = 1, 2, \cdots, r$ is a prime greater than $2n + 1 - 2\sqrt{2n}$.

In the investigation of solutions of a group of linear algebraic equations (8.3), reductions to absurdity are derived and the assumption that all the odd numbers $d_i$ for $i = 1, 2, \cdots, m$ are
composite, is proved false. Hence, it is proved that for every number \( n \) greater than \( n_0 \), there is at least one odd number \( d_i \) where \( 1 \leq i \leq r \), which does not contain any prime factor smaller than \( \sqrt{2n} \) and must be a prime greater than \( 2n + 1 - 2\sqrt{2n} \).

This completes the proof of the theorem.

For small values of numbers \( n \) greater than 3, the assertion in the theorem has been verified for \( 2n + 1 = N \leq 6.5 \times 10^{10} \) and some higher small ranges up to \( 4.0 \times 10^{12} \) by the author. It has been found that \( n_0 = 19,875 \) and \( s_0 = 47 \). Some values of the number \( n \in S \) are \( n = 4, 7, 10, 15, 22, 45, 50, 52, 69, 113, 115, \cdots \).

8.2 Representation of odd numbers

**Theorem 8.2** All odd integers greater than 5 can be represented as the sum of an odd prime and an even semiprime.

**Proof** Let put the theorem algebraically, \( 2n + 1 = p + 2q \) always has a solution in primes \( p \) and \( q \) for \( n > 2 \).

For \( n \leq n_0 \) where \( n_0 \) is a positive number, we can easily find pairs of primes \( p \) and \( q \) satisfying

\[
2n + 1 = p + 2q.
\]

Actually, for small values of numbers \( n \) greater than 2, the assertion in the theorem has been verified for \( 2n + 1 = N \leq 10^9 \) by Corbitt[3].

For \( n > n_0 \), by Theorem (8.1), we can find at least one pair of primes \( q < \sqrt{2n} \) and \( p = 2n + 1 - 2q \) satisfying

\[
2n + 1 = p + 2q.
\]

This completes the proof of the theorem and the Lemoine’s conjecture is proved.

8.3 Distribution of primes in short intervals

**Theorem 8.3** For every positive number \( m \) there is always a prime \( p \) between \( m^2 \) and \( (m + 1)^2 \).

**Proof** For \( 1 \leq m \leq \sqrt{2n_0} \) where \( n_0 \) is a positive number we can easily verify the truth of the theorem. The smallest primes between \( m^2 \) and \( (m + 1)^2 \) for \( m = 1, 2, \cdots \) are 2, 5, \cdots . Let consider any number \( m \) greater than \( \sqrt{2n_0} \).

Let a number \( n \) satisfy \( 2n - 1 \leq (m + 1)^2 \leq 2n \), so we have

\[
n > n_0 \text{ and } m \leq \sqrt{2n} - 1.
\]

By Theorem (8.1), we can find at least one pair of primes

\[
q < \sqrt{2n} \text{ and } p = 2n + 1 - 2q > 2n + 1 - 2\sqrt{2n} = (\sqrt{2n} - 1)^2 \text{ when } n > n_0.
\]

Therefore, there must be

\[
m^2 < p < 2n - 1 \leq (m + 1)^2.
\]

The inequality shows that there is always a prime \( p \) between \( m^2 \) and \( (m + 1)^2 \).

This completes the proof of the theorem and the Legendre’s conjecture is proved.

**Theorem 8.4** For every positive number \( m \) there are always three primes between \( m^3 \) and \( (m + 1)^3 \). The first one is between \( m^3 \) and \( m^2(m + 1) \), and the second one is between \( m^2(m + 1) \) and \( m(m + 1)^2 \), and the third one is between \( m(m + 1)^2 \) and \( (m + 1)^3 \).
Proof  For $1 \leq m \leq \sqrt[3]{2n_0}$ where $n_0$ is a positive number we can easily verify the truth of the theorem. The primes between $m^3$ and $(m + 1)^3$ for $m = 1, 2, \cdots$ are $\{2, 3, 5\}, \{11, 13, 19\}, \cdots$.

Let consider any number $m$ greater than $\sqrt[3]{2n_0}$.

Firstly let a number $n = m^2 (m + 1)/2$, so we have $n > n_0$ and

$$2n - 2\sqrt{2n} = m^2 (m + 1) - 2m \sqrt{m + 1} > m^3.$$ 

By Theorem (5.1), we can find at least one pair of primes

$$q < \sqrt{2n} \quad \text{and} \quad p = 2n + 1 - 2q > 2n + 1 - 2\sqrt{2n} \quad \text{when} \quad n > n_0.$$ 

Therefore, we have

$$q \leq m \sqrt{m + 1} \quad \text{and} \quad m^3 < p < 2n = m^2 (m + 1).$$

The inequalities show that there is a prime $p$ between $m^3$ and $m^2 (m + 1)$.

Secondly let the number $n = m (m + 1)^2/2$, so we have $n > n_0$ and

$$2n - 2\sqrt{2n} = m (m + 1)^2 - 2\sqrt{m (m + 1)} > m^2 (m + 1).$$ 

By Theorem (5.1), we can find at least one pair of primes

$$q < \sqrt{2n} \quad \text{and} \quad p = 2n + 1 - 2q > 2n + 1 - 2\sqrt{2n} \quad \text{when} \quad n > n_0.$$ 

Therefore, we have

$$q \leq \sqrt{m + 1} (m + 1) \quad \text{and} \quad m^2 (m + 1) < p < 2n = m (m + 1)^2.$$ 

The inequalities show that there is a prime $p$ between $m^2 (m + 1)$ and $m (m + 1)^2$.

Thirdly let the number $n$ satisfy

$$m (m + 1)^2 + m (m + 2) \leq 2n \leq (m + 1)^3,$$

so we have $n > n_0$ and

$$2n - 2\sqrt{2n} \geq m (m + 1)^2 + m(m + 2) - 2\sqrt{m + 1}(m + 1) > m (m + 1)^2.$$ 

By Theorem (5.1), we can find at least one pair of primes

$$q < \sqrt{2n} \quad \text{and} \quad p = 2n + 1 - 2q > 2n + 1 - 2\sqrt{2n} \quad \text{when} \quad n > n_0.$$ 

Therefore, we have

$$q \leq \sqrt{m + 1} (m + 1) \quad \text{and} \quad m (m + 1)^2 < p < 2n \leq (m + 1)^3.$$ 

The inequalities show that there is a prime $p$ between $m (m + 1)^2$ and $(m + 1)^3$.

Thus, for every positive number $m$ there are always three primes between $m^3$ and $(m + 1)^3$.

The first one is between $m^3$ and $m^2 (m + 1)$, and the second one is between $m^2 (m + 1)$ and $m (m + 1)^2$, and the third one is between $m (m + 1)^2$ and $(m + 1)^3$.

This completes the proof of the theorem.

**Theorem 8.5**  There is always a prime $p$ between $m - 2m^0$ and $m$ where $\theta = 1/2$ and $m$ is a positive number greater than a positive number $2n_0$.  

Let consider any positive number $m$ greater than $2n_0$.

Let a number $n = (m + 1)/2$. Then for $m > 2n_0$ we have $n > n_0$. By Theorem (8.1), we can find at least one pair of primes

$$q < \sqrt{2n} \text{ and } p = 2n + 1 - 2q > 2n + 1 - 2\sqrt{2n} \text{ when } n > n_0.$$  

Since $1 + 2\sqrt{2n} - 1 > 2\sqrt{2n}$ and the prime $q \geq 3$, we have

$$2n - 1 - 2\sqrt{2n} - 1 < 2n - 2\sqrt{2n} < p < 2n - 1.$$  

Firstly for $m = 2n - 1$ let $m - 2m^\theta = 2n - 1 - 2\sqrt{2n} - 1 = m - 2\sqrt{m}$, so we have $\theta = 1/2$ and

$$q < m^\theta \text{ and } m - 2m^\theta < p < m.$$  

The last inequality shows that there is a prime $p$ between $m - 2m^\theta$ and $m$ where $\theta = 1/2$ and $m$ is an odd number greater than $2n_0$.

Secondly for $m = 2n$ let $m - 2m^\theta = 2n - 2\sqrt{2n} = m - 2\sqrt{m}$, so we have $\theta = 1/2$ and

$$q < m^\theta \text{ and } m - 2m^\theta < p < m.$$  

The last inequality shows that there is a prime $p$ between $m - 2m^\theta$ and $m$ where $\theta = 1/2$ and $m$ is an even number greater than $2n_0$.

This completes the proof of the theorem.

**Theorem 8.6** There is always a prime $p$ between $m$ and $m + 2m^\theta$ where $\theta = 1/2$ and $m$ is a positive number greater than a positive number $2n_0$.

**Proof** Let consider any positive number $m$ greater than $2n_0$.

Let a number $n$ satisfy

$$m \leq 2n + 1 - 2\sqrt{2n} < m + 1,$$

so we have $n > n_0$ for $m > 2n_0$ and

$$\sqrt{m} + 1 \leq \sqrt{2n} < \sqrt{m + 1} + 1$$

and

$$m + 2(\sqrt{m} + 1) \leq 2n + 1 < m + 2(\sqrt{m + 1} + 1).$$

Let consider the equation

$$2n + 1 = m + 2m^\theta + 2f(m, x) - 2\sqrt{m} \text{ where } f(m, x) = \sqrt{m} + x + 1. \quad (8.5)$$

When $f(m, 0)$ is substituted into Equation (8.5), we obtain

$$m^\theta \geq \sqrt{m} \text{ and } \theta \geq 1/2$$

and when $f(m, 1)$ is substituted into Equation (8.5), we obtain

$$m^\theta < \sqrt{m} \text{ and } \theta < 1/2.$$  

Therefore, we can always find a suitable value of $f(m, x)$ to get

$$m^\theta = \sqrt{m} \text{ and } \theta = 1/2.$$
By Theorem (8.1), we can find at least one pair of primes
\[ q < \sqrt{2n} \text{ and } p = 2n + 1 - 2q > 2n + 1 - 2\sqrt{2n} \text{ when } n > n_0. \]

Since any odd prime \( q \) is greater than 2, then \( p \leq 2n - 2 \). For \( 0 \leq x \leq 1 \), since \( f(m, x) - \sqrt{m} < 3/2 \), the values of \( \theta \) are in a small neighborhood of \( 1/2 \), and the values of \( m + 2m \theta \) are in the open interval \((2n - 2, 2n + 1)\) and are greater than the upper bound of the prime \( p \), that is, \( p \leq 2n - 2 \). Hence we have
\[ m < p < m + 2m \theta < 2n + 1. \]

The inequality shows that there is a prime \( p \) between \( m \) and \( m + 2m \theta \) where \( \theta = 1/2 \) and \( m \) is a positive number greater than \( n_0 \).

This completes the proof of the theorem.

**Theorem 8.7** The inequality \( \sqrt{p_{i+1}} - \sqrt{p_i} < 1 \) holds for all \( i > 0 \), where \( p_i \) is the \( i \)th prime.

**Proof** For \( 1 \leq i \leq k \) where \( p_k \geq 2n_0 \) we can easily verify the truth of the theorem. Let consider any positive number \( i \) greater than \( k \).

The inequality \( \sqrt{p_{i+1}} - \sqrt{p_i} < 1 \) can be written as
\[ g_i = p_{i+1} - p_i < 2\sqrt{p_i} + 1. \]

By Theorem (8.1), let a number \( m = p_i \), so there is always a prime \( p \) between \( p_i \) and \( p_i + 2\sqrt{p_i} \). Therefore we obtain
\[ g_i = p_{i+1} - p_i < 2\sqrt{p_i}. \]

Thus we have
\[ g_i = p_{i+1} - p_i < 2\sqrt{p_i} + 1 \text{ and } \sqrt{p_{i+1}} - \sqrt{p_i} < 1. \]

This completes the proof of the theorem and the Andrica’s conjecture is proved.

**References**

[1] Wapedia - Wiki, Lemoine’s conjecture.
[2] Weisstein, Eric W., Levy’s Conjecture. MathWorld.
[3] D. Corbit, Conjecture on Odd Numbers. sci.math posting. Nov 19, 1999. [http://groups-beta.google.com/group/sci.math/msg/539c96e47e4ed582?hl=en](http://groups-beta.google.com/group/sci.math/msg/539c96e47e4ed582?hl=en)
[4] L. Hodges, A Lesser-Known Goldbach Conjecture. Math. Mag. 66, 45-47, 1993.
[5] H. Levy, On Goldbach’s Conjecture. Math. Gaz. 47, 274, 1963.
[6] N. J. A. Sloane, Sequence A046927 in The On-Line Encyclopedia of Integer Sequences.
[7] John O. Kiltinen and Peter B. Young, Goldbach, Lemoine, and a Know/Don’t Know Problem. Mathematics Magazine, Vol. 58, No. 4 (Sep., 1985), pp. 195C203 [http://www.jstor.org/stable/2689513?seq=7](http://www.jstor.org/stable/2689513?seq=7)
[8] W. Sierpinski, Elementary Theory of Numbers. Hafner, New York, 1964(2nd edition, North-Holland, Amsterdam,1988).
[9] Richard K. Guy, Unsolved Problems in Number Theory. New York: Springer-Verlag 2004: C1
[10] Wapedia - Wiki, Legendre’s conjecture.
[11] Weisstein, Eric W., Legendre’s conjecture. MathWorld.
[12] J. R. Chen, On the Distribution of Almost Primes in an Interval. Sci. Sinica 18, 611-627, 1975.
[13] P. Ribenboim, The New Book of Prime Number Records. 3rd ed. New York: Springer-Verlag, pp. 132-134 and 206-208, 1996.
[14] H. Iwaniec and J. Pintz, Primes in Short Intervals. Monatsh. f. Math. 98, 115-143, 1984.
[15] W. H. Mills, A Prime-Representing Function. Bull. Amer. Math. Soc. 53, 604, 1947.
Part III

On the number of Goldbach numbers and the number of Lemoine numbers

Abstract  It was proved in this paper that:
(1) Let \( R_2(x) \) denote the number of odd prime pairs \( p \) and \( x - p \) for \( 3 \leq p \leq x/2 \). Then for large even numbers \( x \), a positive number \( N \) always exists such that the inequalities

\[
R^*_2(x, N) \leq R_2(x) < R^*_2(x, N + 1)
\]

hold where

\[
R^*_2(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x},
\]

and \( R_2(x) \) is asymptotically equal to

\[
R_2(x) = \alpha_x Li_2(x) + O(\sqrt{x \log x})
\]

where \( \alpha_x \) is a positive constant dependent of \( x (\text{mod} \ 6) \).

(2) Let \( R_3(x) \) denote the number of odd prime pairs \( p \) and \( x - 2p \) for \( 3 \leq p \leq (x - 3)/2 \). Then for large odd numbers \( x \), a positive number \( N \) always exists such that the inequalities

\[
R^*_3(x, N) \leq R_3(x) < R^*_3(x, N + 1)
\]

hold where

\[
R^*_3(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x},
\]

and \( R_3(x) \) is asymptotically equal to

\[
R_3(x) = \alpha_x Li_2(x) + O(\sqrt{x \log x})
\]

where \( \alpha_x \) is a positive constant dependent of \( x (\text{mod} \ 6) \).

Keywords  Goldbach number, Lemoine number

9 Introduction

9.1 Goldbach’s conjecture and Lemoine’s conjecture

Goldbach’s conjecture states: Every even number greater than 2 is a Goldbach number, a number that can be expressed as the sum of two primes[1-3].

Lemoine’s conjecture, also known as Levy’s conjecture, states that all odd integers greater than 5 can be represented as the sum of an odd prime and an even semiprime[3-6].
Let $x$ be an even number greater than a positive even number $x_0$, $R_2(x)$ be the number of prime pair $p$ and $x - p$ such that $p \leq x$. Hardy and Littlewood (1923) conjectured that $R_2(x)$ is asymptotically equal to

$$R_2(2n) \sim 2\Pi_{2n}Li_2(2n), \Pi_{2n} = \Pi_2 \prod_{q|n} \frac{q - 1}{q - 2} \text{ and } Li_2(x) = \int_2^x \frac{dt}{\log^2 t}$$

where $\Pi_2$ is known as the twin primes constant and $\Pi_2 = 0.660161816 \cdots$, $\Pi_{2n}$ is a function of $2n$, and $\sim$ means that the quotient of two expressions tends to $1$ as $x$ approaches infinity.

9.2 Works in this paper

The number of odd composite numbers in an odd number set was investigated in this paper. A basic theorem was proved, which states: For an odd number set $D$, let $\sigma$ denote the number of odd composite numbers $d \in D$, then the inequalities

$$\sigma \leq C_1(x)x - C_2(x)\pi(\sqrt{x})\sqrt{x} \leq C_3(x)x$$

always hold formally where $C_3(x)x$ is the number of elements of the odd number set $D$.

The proof of the basic theorem is based on the analysis of composite numbers in an odd number set. Based on the basic theorem, it was proved that:

1. Let $R_2(x)$ denote the number of odd prime pairs $p$ and $x - p$ for $3 \leq p \leq x/2$. Then for large even numbers $x$, a positive number $N$ always exists such that the inequalities

$$R_2^*(x, N) \leq R_2(x) < R_2^*(x, N + 1)$$

hold where

$$R_2^*(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x},$$

and $R_2(x)$ is asymptotically equal to

$$R_2(x) = \alpha_x Li_2(x) + O(\sqrt{x \log x})$$

where $\alpha_x$ is a positive constant dependent of $x(\text{mod } 6)$.

2. Let $R_3(x)$ denote the number of odd prime pairs $p$ and $x - 2p$ for $3 \leq p \leq (x - 3)/2$. Then for large odd numbers $x$, a positive number $N$ always exists such that the inequalities

$$R_3^*(x, N) \leq R_3(x) < R_3^*(x, N + 1)$$

hold where

$$R_3^*(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x},$$

and $R_3(x)$ is asymptotically equal to

$$R_3(x) = \alpha_x Li_2(x) + O(\sqrt{x \log x})$$

where $\alpha_x$ is a positive constant dependent of $x(\text{mod } 6)$. 


10 Definitions

10.1 Sets of primes

For any number $x$, let $\pi(\sqrt{x}) = n$ and $\pi(x) = n + r$. Then let denote a set of primes by $P$ where

$$P = \{p_i | i = 1, 2, \cdots, n + r\}$$

(10.1)

and

$$2 = p_1 < p_2 < \cdots < p_n \leq \sqrt{x} < p_{n+1} < p_{n+2} < \cdots < p_{n+r} \leq x.$$  

Let $P_n$ denote a subset of $P$ where

$$P_n = \{p_i | i = 2, 3, \cdots, n\} \subset P.$$  

(10.2)

Let $Q_u$ and $Q_v$ denote subsets of $P$ where

$$Q_u = \{q_i | q_i \in P, q_i = 6m_i + 1, i = 1, 2, \cdots, r_u\}$$

(10.3)

and

$$Q_v = \{q_i | q_i \in P, q_i = 6m_i - 1, i = 1, 2, \cdots, r_v\}$$

(10.4)

where $r_u$ and $r_v$ are numbers of elements of odd prime sets $Q_u$ and $Q_v$, respectively.

10.2 Sets of odd numbers

Let $D_u$ and $D_v$ denote subsets of odd numbers where

$$D_u = \{d_i | d_i = 6m_i + 1, i = 1, 2, \cdots, r_u\}$$

(10.5)

and

$$D_v = \{d_i | d_i = 6m_i - 1, i = 1, 2, \cdots, r_v\}$$

(10.6)

where $r_u$ and $r_v$ are numbers of elements of odd number sets $D_u$ and $D_v$, respectively.

Let $D$ denote $D_u$ or $D_v$, or $D_u \cup D_v$, that is

$$D = D_u \text{ or } D = D_v \text{ or } D = D_u \cup D_v.$$  

(10.7)

Let $D_j$ for $j = 1, 2, \cdots, n$ denote odd composite number sets where

$$D_j = \{d | d \in D, \max\{q | q \in P_n, q|d\} = p_j\} \subset D$$

(10.8)

such that $D_i \cap D_j = \phi$ for $i, j = 1, 2, \cdots, n$ and $i \neq j$. Hence any odd composite number $d \in D$ can be uniquely classified into an odd composite number set $D_j$. Let denote

$$D_{12} = D_1 \cup D_2 \cup D_3 \cup \cdots \cup D(n)$$

then there is $D_{12} \subseteq D$. If $D_{12} \neq D$ or the number of elements of $D_{12}$ is smaller than the number of elements of $D$, then some odd numbers $d \in D$ must be primes.

11 Estimation theorem of composite numbers

In this section for any big number $x$ we will investigate odd composite numbers $d \in D$ based on the prime set $P_n$ and odd composite number sets $D_j$ for $j = 1, 2, \cdots, n$. 

Lemma 11.1. As defined in Sec. (10) for $1 \leq j \leq n$, let $\sigma_j$ denote the number of elements of $D_j$, then $\sigma_j$ can be formally estimated by inequalities as

$$\sigma_j \leq \begin{cases} C_{1,j}(x) - C_{2,j}(x) \sqrt{x} & \text{for } 1 \leq j \leq j_n \\ C_{1,j}(x) + C_{2,j}(x) \sqrt{x} & \text{for } j_n < j \leq n \end{cases}$$

where $C_{1,j}(x)$ and $C_{2,j}(x)$ are non-negative and dependent of the variable $x$, and $j_n$ is a positive integer dependent of $n$.

Proof. First, since $p_1 = 2$ and any $d \in D$ is an odd number, then there is $gcd(p_1, d) = 1$ such that $D_1 = \phi$. Hence there is $\sigma_1 = 0$ such that there are $C_{1,1}(x) = 0$ and $C_{2,1}(x) = 0$.

Second, since $p_2 = 3$ is not a prime divisor of any $d \in D$, then there is $gcd(p_2, d) = 1$ such that $D_2 = \phi$. Hence there is $\sigma_2 = 0$ such that there are $C_{1,2}(x) = 0$ and $C_{2,2}(x) = 0$.

Third, since any $d \in D_3$ can be written as $d = mp_3$ where $m$ is a positive integer satisfying $\sqrt{x}/p_3 < m \leq \lfloor x/p_3 \rfloor$, then $\sigma_3$ can be formally estimated by an inequality as

$$\sigma_3 \leq C_{1,3}(x) - C_{2,3}(x) \sqrt{x}$$

where $C_{1,3}(x)$ and $C_{2,3}(x)$ are positive and dependent of the variable $x$.

Fourth, since any $d \in D_n$ can be written as $d = mp_n$ where $m$ is a positive integer satisfying $2 \leq m \leq \lfloor x/p_n \rfloor$, then $\sigma_n$ can be formally estimated by an inequality as

$$\sigma_n \leq C_{2,n}(x) \sqrt{x}$$

where $C_{2,n}(x)$ is positive and dependent of the variable $x$ or

$$\sigma_n \leq C_{1,n}(x) + C_{2,n}(x) \sqrt{x}$$

where $C_{1,n}(x) = 0$ and $C_{2,n}(x)$ is positive and dependent of the variable $x$.

Finally, since we have

$$\sigma_3 \leq C_{1,3}(x) - C_{2,3}(x) \sqrt{x} \quad \text{and} \quad \sigma_n \leq C_{1,n}(x) + C_{2,n}(x) \sqrt{x},$$

then there is always a number $j_n$ where $3 \leq j_n < n$ such that $\sigma_j$ can be formally estimated by inequalities as

$$\sigma_j \leq \begin{cases} C_{1,j}(x) - C_{2,j}(x) \sqrt{x} & \text{for } 3 \leq j \leq j_n \\ C_{1,j}(x) + C_{2,j}(x) \sqrt{x} & \text{for } j_n < j \leq n \end{cases}$$

where $C_{1,j}(x)$ is non-negative and $C_{2,j}(x)$ is positive, both are dependent of the variable $x$, and $j_n$ is a positive integer dependent of $n$.

The proof of the lemma is completed.

Theorem 11.2 (Estimation theorem). For an odd number set $D$ defined in Sec. (10), let $\sigma$ denote the number of odd composite numbers $d \in D$, then the inequalities

$$\sigma \leq C_1(x) - C_2(x) \pi(\sqrt{x}) \sqrt{x} \leq C_d(x)$$

(11.1)

always hold formally where $C_d(x)$ is the number of elements of the odd number set $D$.

Proof. By Lemma (11.1), we have

$$\sigma = \sigma_1 + \sigma_2 + \sigma_3 + \cdots + \sigma_n$$
\[ \leq \sum_{j=1}^{n} C_{1,j}(x)x - \sum_{j=1}^{n} C_{2,j}(x)\sqrt{x} + \sum_{j=j_n+1}^{n} C_{2,j}(x)\sqrt{x} \]
\[ = C_1(x)x - C_2(x)\pi(\sqrt{x})\sqrt{x} \]

where

\[ C_1(x) = \sum_{j=1}^{n} C_{1,j}(x) \text{ and } C_2(x) = \frac{1}{\pi(\sqrt{x})} \left( \sum_{j=1}^{n} C_{2,j}(x) - \sum_{j=j_n+1}^{n} C_{2,j}(x) \right). \]

Since \( C_{1,j}(x)x \equiv C_{2,j}(x)\sqrt{x} \) for \( j = 1, 2, \ldots, n \) corresponds to the number of elements of a composite number set \( D_j \subseteq D \), then there is

\[ D_1 \cup D_2 \cup D_3 \cup \cdots \cup D(n) = D_{\cup} \subseteq D \]

such that \( C_1(x)x - C_2(x)\pi(\sqrt{x})\sqrt{x} \) corresponds to the number of elements of the composite number set \( D_{\cup} \subseteq D \) and the inequalities

\[ \sigma \leq C_1(x)x - C_2(x)\pi(\sqrt{x})\sqrt{x} \leq C_d(x)x \]

always hold formally where \( C_d(x)x \) is the number of elements of the odd number set \( D \).

This completes the proof of the theorem.

12 Theorems of Goldbach numbers

**Theorem 12.1** (Theorem of Goldbach numbers) For any even number \( x \) greater than a positive even number \( x_0 \), let \( R_2(x) \) denote the number of odd prime pairs \( p \) and \( x - p \) for \( 3 \leq p \leq x/2 \), then the inequalities

\[ R_2(x) \geq \alpha_x \frac{x}{\log^2 x} + \beta_x \frac{\pi(\sqrt{x})\sqrt{x}}{2\log^2 x} \geq 1 \] (12.1)

always hold where \( \alpha_x \) and \( \beta_x \) are positive constants dependent of \( x(\text{mod} \ 6) \).

**Proof** Let \( x = 6m_x + r_x \). Then for \( p = 6m + 1 \) we have

\[ x - p = 6m_x + r_x - (6m + 1) = \begin{cases} 6(m_x - m) - 1 & \text{for } r_x = 0 \\ 6(m_x - m) + 1 & \text{for } r_x = 2 \\ 6(m_x - m) + 3 & \text{for } r_x = 4 \end{cases} \]

and for \( p = 6m - 1 \) we have

\[ x - p = 6m_x + r_x - (6m - 1) = \begin{cases} 6(m_x - m) + 1 & \text{for } r_x = 0 \\ 6(m_x - m) + 3 & \text{for } r_x = 2 \\ 6(m_x - m) - 1 & \text{for } r_x = 4. \end{cases} \]

Thus for \( p_i \in P \) and \( i = 2, 3, \ldots, \pi(x/2) \), we can let \( D^* \) denote a set of odd numbers where

\[ D^* = \{ d \mid d = x - p_i, p_i \in P, i = 2, 3, \ldots, \pi(x/2) \}, r_d = \pi(x/2) - 1 \] for \( r_x = 0 \)

\[ \{ d \mid d = x - q_i, q_i \in Q, i = 1, 2, \ldots, r_u \}, r_u \approx r_d/2 \] for \( r_x = 2 \)

\[ \{ d \mid d = x - q_i, q_i \in Q, i = 1, 2, \ldots, r_v \}, r_v \approx r_d/2 \] for \( r_x = 4. \]
Hence $D^*$ is similar to the odd number set $D$ defined in Sec. 10. When we take $D_j$ for $j = 1, 2, \cdots, n$ such that $D_{\cup} \subseteq D^*$, if $D_{\cup} \neq D^*$ then some prime pairs of the form $(p, x - p)$ exist for any even number $x$.

By Theorem 11.2 for $C_d(x) = [\pi(x/2) - 1]/x$, the number of odd composite numbers $d$ is less than or equal to $\sigma$. Then we have
\[
R_2(x) = [\pi(x/2) - 1] - \sigma
\]
\[
\geq C_d(x) x - [C_1(x)x - C_2(x)\pi(\sqrt{x})\sqrt{x}]
\]
\[
= [C_d(x) - C_1(x)]x + C_2(x)\pi(\sqrt{x})\sqrt{x}
\]
\[
= \alpha(x)x + \beta(x)\pi(\sqrt{x})\sqrt{x}/2
\]
and
\[
\rho(x) = \frac{R_2(x)}{x/\log^2 x}
\]
\[
\geq \alpha(x)\log^2 x + \beta(x)\frac{\pi(\sqrt{x})}{\sqrt{x}/\log \sqrt{x}} \log x
\]
\[
\sim \rho^*(x) = \alpha(x)\log^2 x + \beta(x) \log x
\]
where
\[
\alpha(x) = C_d(x) - C_1(x) \text{ and } \beta(x) = 2C_2(x)
\]
are dependent of the even number $x$.

Since $\rho(x)$ can not be negative and $\pi(x)/x$ is stationarily decreased and tends to zero when $x$ is increased such that $R_2(x)/x$ is stationarily decreased and tends to zero when $x$ is increased, thus $\rho(x)$ should be stationarily decreased and tend to a limiting value when $x$ is increased such that $\alpha(x)$ and $\beta(x)$ must be decreased and tend to zero when $x$ is increased.

Shan-Guang Tan (2011) proved that for any even number $x$ greater than 4 there are at least a pair of odd primes $p$ and $x - p$. Thus there must be
\[
0 < \alpha(x) < C_d(x) \text{ and } \lim_{x \to \infty} \alpha(x) = 0
\]
so that $\alpha(x)$ and $\rho(x)$ are always greater than zero for $x < \infty$.

Hence by the form of the function $\rho^*(x)$ we can let
\[
\alpha_x = \alpha(x)\log^2 x \text{ and } \beta_x = \beta(x)\log^2 x
\]
then there is $\alpha_x > 0$ and $\rho^*(x)$ becomes
\[
\rho^*(x) = \alpha_x + \beta_x/\log x.
\]
Since $\alpha_x > 0$ then $\beta_x$ should be greater than zero otherwise $R_2(x)/x$ will be stationarily increased when $x$ is increased. Thus $\alpha_x$ and $\beta_x$ are positive constants.

Hence a positive even number $x_0$ always exists such that when $x > x_0$ the inequalities
\[
R_2(x) \geq \alpha_x \frac{x}{\log^2 x} + \beta_x \frac{\pi(\sqrt{x})\sqrt{x}}{2 \log^2 x} \geq 1
\]
always hold such that at least one $d$ can not be composite and $d = x - p$ must be a prime for $x > x_0$.

This completes the proof of the theorem.
By calculation, there are approximately
\[ \alpha_x = \begin{cases} 2\Pi_2 & \text{for } x \equiv 0 \pmod{6} \\ \Pi_2 & \text{for } x \equiv 2 \pmod{6} \quad \text{and} \quad \beta_x = 2.4\alpha_x \\ \Pi_2 & \text{for } x \equiv 4 \pmod{6} \end{cases} \]
for Goldbach numbers where \( \Pi_2 \) is the twin primes constant such that we can take \( x_0 \geq 10^3 \). Hence we may write
\[ \rho^*(x) = (1 + 2.4/\log x) \ast \left\{ \begin{array}{ll} 2\Pi_2 & \text{for } x \equiv 0 \pmod{6} \\ \Pi_2 & \text{for } x \equiv 2 \pmod{6} \\ \Pi_2 & \text{for } x \equiv 4 \pmod{6} \end{array} \right. \] (12.2)

**Theorem 12.2** (Bounds theorem of Goldbach numbers) 
For any large even number \( x \), let \( R_2(x) \) denote the number of odd prime pairs \( p \) and \( x - p \) for \( 3 \leq p \leq x/2 \). Then a positive number \( N \) always exists such that the inequalities
\[ R_2^*(x, N) \leq R_2(x) < R_2^*(x, N + 1) \] (12.3)
hold where
\[ R_2^*(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log n - 1} \] (12.4)
and
\[ \lim_{x \to \infty} \frac{R_2(x)}{\alpha_x x/ \log^2 x} = 1. \] (12.5)

**Proof** By the proof of Theorem (12.1) we have
\[ \alpha_x \pi(\sqrt{x}) \sim R_2(\sqrt{x}) \log \sqrt{x}, \]
\[ R_2(x) \geq \alpha_x \pi(x) + \beta_x \pi(\sqrt{x}) \sqrt{x}/2 + R_2(\sqrt{x}) \]
\[ \sim \alpha_x \frac{x}{\log^2 x} \left[ 1 + \frac{\beta_x}{\alpha_x} \frac{\pi(\sqrt{x})}{\log x} \right] = \alpha_x \frac{x}{\log^2 x} \eta^*(x) \quad \text{where} \quad \eta(x) = \frac{R_2(x)}{\alpha_x x/ \log^2 x} \]
and
\[ \lim_{x \to \infty} \eta(x) = \lim_{x \to \infty} \eta^*(x) = 1. \]

Then for large numbers \( x \) and \( \beta_x^* = \beta_x/\alpha_x \) we have
\[ \eta(x) = \frac{R_2(x)}{\alpha_x x/ \log^2 x} \geq 1 + \beta_x^* \frac{\eta(\sqrt{x})}{\log x} \] (12.6)

First since there is
\[ \eta(x) \geq 1 \]
then we can set
\[ \eta(x) = 1 + \delta_1(x) \]
and substitute it into Inequality (12.6), thus we have
\[ 1 + \delta_1(x) \geq 1 + \beta_x^* \frac{1 + \delta_1(\sqrt{x})}{\log x} \]
\[ 1 + \beta_x^* \frac{1}{\log x} + \beta_x^* \delta_1(\sqrt{x}) \]

such that we obtain

\[ \delta_1(x) \geq \beta_x^* \frac{1}{\log x} + \beta_x^* \delta_1(\sqrt{x}) \]  

(12.7)

and can set

\[ \delta_1(x) = \frac{2!}{\log x} + \delta_2(x). \]  

(12.8)

Second by substituting \( \delta_1(x) \) into Inequality (12.7), we have

\[ \frac{2!}{\log x} + \delta_2(x) \geq \beta_x^* \frac{1}{\log x} + \beta_x^* \frac{2!}{\log \sqrt{x}} + \delta_2(\sqrt{x}) \]

\[ = \beta_x^* \frac{1}{2 \log x} + \beta_x^* \frac{2}{3 \log^2 x} + \beta_x^* \delta_2(\sqrt{x}) \]

such that we obtain

\[ \delta_2(x) \geq (\beta_x^* \frac{1}{2} - 1) \frac{2!}{\log x} + \beta_x^* \frac{2}{3 \log^2 x} + \beta_x^* \delta_2(\sqrt{x}) \]  

(12.9)

and can set

\[ \delta_2(x) = \frac{3!}{\log^3 x} + \delta_3(x). \]  

(12.10)

Third by substituting \( \delta_2(x) \) into Inequality (12.9), we have

\[ \frac{3!}{\log^2 x} + \delta_3(x) \geq \sum_{m=1}^{\frac{1}{2}} (\beta_x^* \frac{2m! - 1}{m + 1}) \frac{(m + 1)!}{\log^m x} + \beta_x^* \frac{21}{3} \frac{3!}{\log^2 x} + \beta_x^* \frac{2!}{4 \log x} + \beta_x^* \frac{3!/\log^2 \sqrt{x} + \delta_3(\sqrt{x})}{\log x} \]

\[ = \sum_{m=1}^{\frac{1}{2}} (\beta_x^* \frac{2m! - 1}{m + 1}) \frac{(m + 1)!}{\log^m x} + \beta_x^* \frac{21}{3} \frac{3!}{\log^2 x} + \beta_x^* \frac{2}{4} \frac{4!}{\log x} + \beta_x^* \delta_3(\sqrt{x}) \]

such that we obtain

\[ \delta_3(x) \geq \sum_{m=1}^{\frac{1}{2}} (\beta_x^* \frac{2m! - 1}{m + 1}) \frac{(m + 1)!}{\log^m x} + \beta_x^* \frac{22}{4} \frac{4!}{\log^3 x} + \beta_x^* \frac{\delta_3(\sqrt{x})}{\log x} \]  

(12.11)

and can set

\[ \delta_3(x) = \frac{4!}{\log^3 x} + \delta_4(x). \]  

(12.12)

Forth by substituting \( \delta_3(x) \) into Inequality (12.11), we have

\[ \frac{4!}{\log^3 x} + \delta_4(x) \geq \sum_{m=1}^{\frac{1}{2}} (\beta_x^* \frac{2m! - 1}{m + 1}) \frac{(m + 1)!}{\log^m x} + \beta_x^* \frac{22}{4} \frac{4!}{\log^3 x} + \beta_x^* \frac{4!/\log^3 \sqrt{x} + \delta_4(\sqrt{x})}{\log x} \]

\[ = \sum_{m=1}^{\frac{1}{2}} (\beta_x^* \frac{2m! - 1}{m + 1}) \frac{(m + 1)!}{\log^m x} + \beta_x^* \frac{22}{4} \frac{4!}{\log^3 x} + \beta_x^* \frac{23}{5} \frac{5!}{\log^4 x} + \beta_x^* \frac{\delta_4(\sqrt{x})}{\log x} \]

such that we obtain

\[ \delta_4(x) \geq \sum_{m=1}^{\frac{3}{2}} (\beta_x^* \frac{2m! - 1}{m + 1}) \frac{(m + 1)!}{\log^m x} + \beta_x^* \frac{23}{5} \frac{5!}{\log^4 x} + \beta_x^* \frac{\delta_4(\sqrt{x})}{\log x} \]  

(12.13)

and can set

\[ \delta_4(x) = \frac{5!}{\log^4 x} + \delta_5(x). \]  

(12.14)
Fifth by substituting \( \delta_4(x) \) into Inequality \((12.13)\), we have
\[
\frac{5!}{\log^4 x} + \delta_5(x) \geq \sum_{m=1}^{3} (\beta_{m+1} \frac{2^{m-1}}{m+1} - 1) \frac{(m+1)!}{\log^m x} + \beta_{m+1} \frac{2^3}{5} \frac{5!}{\log^5 x} + \beta_{m+1}^* \frac{5!}{\log^4 x} \sqrt{x} + \delta_5(\sqrt{x}) \]
\[
= \sum_{m=1}^{3} (\beta_{m+1} \frac{2^{m-1}}{m+1} - 1) \frac{(m+1)!}{\log^m x} + \beta_{m+1} \frac{2^3}{5} \frac{5!}{\log^5 x} + \beta_{m+1}^* \frac{2^4}{6} \frac{6!}{\log^6 x} + \beta_{m+1}^* \delta_5(\sqrt{x}) \frac{\log x}{\log x}
\]
such that we obtain
\[
\delta_5(x) \geq \sum_{m=1}^{4} (\beta_m \frac{2^{m-1}}{m+1} - 1) \frac{(m+1)!}{\log^m x} + \beta_{m+1} \frac{2^4}{6} \frac{6!}{\log^6 x} + \beta_{m+1}^* \delta_5(\sqrt{x}) \frac{\log x}{\log x}
\]
(12.15)
and can set
\[
\delta_5(x) = \frac{6!}{\log^5 x} + \delta_6(x).
\]
(12.16)
Then by substituting \( \delta_n(x) \) for \( n = 1, 2, 3, 4, 5 \) into the expression of \( \eta(x) \) we obtain
\[
\eta(x) = 1 + \frac{2!}{\log x} + \frac{3!}{\log^2 x} + \frac{4!}{\log^3 x} + \frac{5!}{\log^4 x} + \frac{6!}{\log^5 x} + \delta_6(x) = \sum_{n=1}^{6} \frac{n!}{\log^{n-1} x} + \delta_6(x).
\]
Going on in the same way for \( n = 6, 7, \ldots , N \) we have
\[
\delta_n(x) \geq \sum_{m=1}^{n-1} (\beta_m \frac{2^{m-1}}{m+1} - 1) \frac{(m+1)!}{\log^m x} + \beta_{m+1} \frac{2^{m-1}}{n+1} \frac{(n+1)!}{\log^n x} + \beta_{m+1}^* \delta_n(\sqrt{x}) \frac{\log x}{\log x}
\]
(12.17)
and can set
\[
\delta_n(x) = \frac{(n+1)!}{\log^n x} + \delta_{n+1}(x)
\]
(12.18)
such that we obtain
\[
\eta(x) = \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x} + \delta_N(x).
\]
(12.19)
Since by Equality \((12.18)\) for \( n = 1, 2, \ldots \) the inequality
\[
\delta_n(x) - \delta_{n+1}(x) = \frac{(n+1)!}{\log^n x} > 0
\]
always holds then we have
\[
\delta_1(x) > \delta_2(x) > \delta_3(x) > \cdots > \delta_N(x) > \delta_{N+1}(x) > \cdots
\]
Based on the Stirling’s formula
\[
n! = \sqrt{2\pi n} \left( \frac{n}{e} \right)^n e^{\theta n}, \quad 0 < \theta < 1
\]
for a fixed positive number \( x \), a positive number \( n_c \) always exists such that when \( n \geq n_c \) there are
\[
\frac{n}{e \log x} \geq 1 \quad \text{and} \quad \frac{n!}{\log^n x} > \sqrt{2\pi n} \left( \frac{n}{e \log x} \right)^n \geq \sqrt{2\pi n}.
\]
Then on the right hand side of the Inequality \((12.17)\) there is
\[
\lim_{n \to \infty} \sum_{m=1}^{n-1} (\beta_m \frac{2^{m-1}}{m+1} - 1) \frac{(m+1)!}{\log^m x} \to \infty
\]
Thus there must be
\[ \lim_{n \to \infty} \delta_n(\sqrt{x}) \to -\infty \]
such that there must be
\[ \lim_{n \to \infty} \delta_{n+1}(x) \to -\infty. \]

Hence for any positive number \( x \), a positive number \( N \) always exists such that there are \( \delta_N(x) \geq 0 \) and \( \delta_{N+1}(x) < 0 \). Thus the inequalities
\[ \eta^*(x, N) \leq \eta(x) < \eta^*(x, N + 1) \]
and
\[ R^*_2(x, N) \leq R_2(x) < R^*_2(x, N + 1) \]
hold where
\[ \eta^*(x, N) = \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x} \]
and
\[ R^*_2(x, N) = \alpha_x \frac{x}{\log^2 x} \eta^*(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}. \]

Hence we have
\[ \eta(x) \sim \eta^*(x, N) \]
and
\[ \lim_{x \to \infty} \eta(x) = \lim_{x \to \infty} \eta^*(x, N) = 1. \]

This completes the proof of the theorem.

**Theorem 12.3** (Relation between \( x \) and \( N \)) Let \( \varphi(x, N) = (\log x)/(N + 3/2) \). Then there are approximately
\[ \varphi(x, N) \leq \varphi^*(x) = 5.1 - 5.5 \frac{\log 10}{\log x}. \] (12.20)

**Proof** By the proof of Theorem 12.2, let
\[ \Delta(x, N) = \eta^*(x, N + 1) - \eta^*(x, N) = \frac{(N + 1)!}{\log^{(N+1)} x}. \]

Then we have
\[ \varphi(x, N) = \frac{N + 1}{N + 3/2} \frac{\Delta(x, N - 1)}{\Delta(x, N)}. \]

When \( x \) is increased, since \( \eta^*(x, M) \) for \( M = N - 1, N, N + 1 \) are decreased and tend to 1, then \( \Delta(x, N - 1) \) and \( \Delta(x, N) \) are also decreased and tend to zero. Since \( N + 1 < \log x \) and \( \Delta(x, N) < \Delta(x, N - 1) \), then \( \Delta(x, N)/\Delta(x, N - 1) \) is also decreased and tends to a limiting value when \( x \) is increased. Thus \( \varphi(x, N) \) should be increased and tend to a limiting value when \( x \) is increased.

Without loss of generality we can assume that \( \varphi(x, N) \) satisfies
\[ \varphi(x, N) \leq \varphi^*(x) \text{ and } \varphi^*(x) = \alpha - \beta/\log x \]
where \( \alpha \) and \( \beta \) are positive constants.
By calculation $\alpha$ and $\beta$ are approximately equal to 5.1 and $5.5 \log 10$, respectively. Then there are approximately
\[ \varphi(x, N) \leq \varphi^*(x) = 5.1 - 5.5 \frac{\log 10}{\log x} \]
and
\[ \lim_{N \to \infty} \varphi(x, N) \leq \lim_{N \to \infty} \varphi^*(x) = 5.1. \]
This completes the proof of the theorem.

**Theorem 12.4** (Upper bound theorem of Goldbach number gaps) For any small positive value $\epsilon(x)$, a pair of positive numbers $x$ and $N$ always exist such that the bounds gap of prime numbers
\[ g(x, N) = R_2^*(x, N + 1) - R_2^*(x, N) \leq \epsilon(x) \frac{\alpha_x x}{\log^2 x} \]  
(12.21)
and for any positive number $x$, $R_2(x)$ satisfies
\[ R_2(x) - R_2^*(x, N) < g(x, N) \leq \epsilon(x) \frac{\alpha_x x}{\log^2 x} \]  
(12.22)
where $\alpha_x$ is a positive constant dependent of the number $k$,
\[ R_2^*(x, N) \leq R_2(x) < R_2^*(x, N + 1) \]
and
\[ R_2^*(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}. \]
Especially $\epsilon(x)$ can be equal to $x^{-1/2} \log^{5/2} x$ such that
\[ g(x, N) \leq \alpha_x (x \log x)^{1/2} \]  
(12.23)
and for any positive number $x$
\[ R_2(x) - R_2^*(x, N) < \alpha_x (x \log x)^{1/2}. \]  
(12.24)

**Proof** By the proof of Theorem (12.2) when $R_2(x)$ satisfies
\[ R_2^*(x, N) \leq R_2(x) < R_2^*(x, N + 1) \]
then there is
\[ \Delta(x, N) = \frac{g(x, N)}{\alpha_x x/\log^2 x} = \eta^*(x, N + 1) - \eta^*(x, N) = \frac{(N + 1)!}{\log^N x}. \]

For any small positive value $\epsilon(x)$, a pair of positive numbers $x$ and $N$ can be determined by Theorem (12.3) and the inequality
\[ \Delta(x, N) \leq \epsilon(x) \text{ or } \frac{(N + 1)!}{\log^N x} \leq \epsilon(x). \]

Thus for any positive number $x$, $R_2(x)$ satisfies
\[ R_2(x) - R_2^*(x, N) < g(x, N) \leq \epsilon(x) \frac{\alpha_x x}{\log^2 x} \]

Based on the Stirling’s formula
\[ n! = \sqrt{2\pi n} \left( \frac{n}{e} \right)^n e^{\frac{1}{2n} + \theta}, 0 < \theta < 1 \]
for \( x \geq 10^5 \) such that \( \log x > e\sqrt{2\pi e} \) there are
\[
(N + 1)! < e\sqrt{2\pi e}(\frac{N + 1}{x})^{N+3/2}
\]
and
\[
\frac{\log^{N+5/2}x}{(N + 1)! \sqrt{x}} > \log x \geq e\sqrt{2\pi e}(\frac{N + 1}{x})^{N+3/2} > (\frac{e \log x}{N + 3/2})^{N+3/2}.
\]
Since a pair of positive numbers \( x \) and \( N \) always exists, let
\[
\varphi(x, N) = (\log x)/(N + 3/2).
\]
Then we have
\[
\log \varphi(x, N) = (\log x)/(N + 3/2).
\]
Since the inequality
\[
1 + \log \varphi(x, N) - \varphi(x, N)/2 > 0
\]
holds for \( \varphi(x, N) \leq 5.3566938 \), thus by Theorem (12.3) the inequality \( \varphi(x, N) \leq 5.1 \) holds or let \( \varphi(x, N) \leq 5.3566938 \) for calculation of \( R_2^*(x, N) \) such that we obtain
\[
\log \varphi(x, N) = (\log x)/(N + 3/2).
\]
This completes the proof of the theorem.

**Theorem 12.5 (Goldbach number theorem)** For large numbers \( x \), \( R_2(x) \) is asymptotically equal to
\[
R_2(x) = \alpha_x \log x + O(\sqrt{x \log x}) \quad \text{where} \quad \log x = \int_2^x \frac{dt}{\log^2 t}. \tag{12.25}
\]

**Proof** Note that \( \log^2 t \) has the asymptotic expansion about \( \infty \) of
\[
\log x = \int_2^x \frac{dt}{\log^2 t} = li_2(x) - li_2(2) \sim li_2(x) \tag{12.26}
\]
where
\[
li_2(x) = \sum_{n=1}^{\infty} \frac{n! x}{\log^{n+1} x} = \frac{x}{\log^2 x} \sum_{n=1}^{\infty} \frac{n!}{\log^{n+1} x}.
\]
By the proof of Theorem (12.4) for any positive number \( x \), a positive number \( N \) always exists such that \( R_2(x) \) satisfies
\[
R_2(x) - R_2^*(x, N) < g(x, N) \leq \alpha_x (x \log x)^{1/2}.
\]
Hence when positive numbers \( N \to \infty \) and \( x \to \infty \), we have
\[
|R_2(x) - \alpha_x li_2(x)| = |R_2(x) - \lim_{N \to \infty} R_2^*(x, N)|
\]
\[< \lim_{N \to \infty} g(x, N) \leq \alpha_x (x \log x)^{1/2}
\]
so that we obtain
\[
R_2(x) = \alpha_x Li_2(x) + O(\sqrt{x \log x}).
\]
This completes the proof of the theorem.

13 Theorems of Lemoine numbers

Theorem 13.1 (Theorem of Lemoine numbers) For any odd number \( x \) greater than a positive odd number \( x_0 \), let \( R_3(x) \) denote the number of odd prime pairs \( p \) and \( x - 2p \) for \( 3 \leq p \leq (x - 3)/2 \), then the inequalities
\[
R_3(x) \geq \alpha_x \frac{x}{\log^2 x} + \beta_x \frac{\pi(\sqrt{x}) \sqrt{x}}{2 \log^2 x} \geq 1
\]  (13.1)
always hold where \( \alpha_x \) and \( \beta_x \) are positive constants dependent of \( x \mod 6 \).

Proof Let \( x = 6m_x + r_x + 1 \). Then for \( p = 6m + 1 \) we have
\[
6(m_x - 2m) - 1 \quad \text{for } r_x = 0
\]
\[
x - 2p = 6m_x + r_x - 2(6m + 1) = \begin{cases} 6(m_x - 2m) + 1 & \text{for } r_x = 2 \\ 6(m_x - 2m) + 3 & \text{for } r_x = 4 \end{cases}
\]
and for \( p = 6m - 1 \) we have
\[
6(m_x - 2m + 1) - 3 \quad \text{for } r_x = 0
\]
\[
x - 2p = 6m_x + r_x + 1 - 2(6m - 1) = \begin{cases} 6(m_x - 2m + 1) - 1 & \text{for } r_x = 2 \\ 6(m_x - 2m + 1) + 1 & \text{for } r_x = 4 \end{cases}
\]

Thus for \( p_i \in P \) and \( i = 2, 3, \ldots, \pi(\frac{x}{2}) \), we can let \( D^* \) denote a set of odd numbers where
\[
\{d|d = x - 2p, p_i \in P, i = 2, 3, \ldots, \pi(\frac{x}{2})\}, r_d = \pi(\frac{x-3}{2}) - 1 \quad \text{for } r_x = 2
\]
\[
D^* = \begin{cases} \{d|d = x - 2q, q_i \in Q, i = 1, 2, \ldots, r_u\}, r_u \approx r_d/2 & \text{for } r_x = 4 \\ \{d|d = x - 2q, q_i \in Q, i = 1, 2, \ldots, r_v\}, r_v \approx r_d/2 & \text{for } r_x = 0. \end{cases}
\]

Hence \( D^* \) is similar to the odd number set \( D \) defined in Sec. 10. When we take \( D_j \) for \( j = 1, 2, \ldots, n \) such that \( D_j \subseteq D^* \), if \( D_j \neq D^* \) then some prime pairs of the form \((p, x - 2p)\) exist for any odd number \( x \).

By Theorem (11.2) for \( C_d(x) = [\pi(\frac{x-3}{2}) - 1]/x \), the number of odd composite numbers \( d \) is less than or equal to \( \sigma \). Then we have
\[
R_3(x) = [\pi(\frac{x-3}{2}) - 1] - \sigma
\]
\[
\geq C_d(x)x - [C_1(x)x - C_2(x)\pi(\sqrt{x})\sqrt{x}]
\]
\[
= [C_d(x) - C_1(x)]x + C_2(x)\pi(\sqrt{x})\sqrt{x}
\]
\[
= \alpha(x)x + \beta(x)\pi(\sqrt{x})\sqrt{x}/2
\]
\[ \rho(x) = \frac{R_3(x)}{x/\log^2 x} \]
\[ \geq \alpha(x) \log^2 x + \beta(x) \frac{\pi(\sqrt{x}) \sqrt{x}}{\sqrt{x}/\log \sqrt{x}} \log x \]
\[ \sim \rho^*(x) = \alpha(x) \log^2 x + \beta(x) \log x \]
where
\[ \alpha(x) = C_d(x) - C_1(x) \quad \text{and} \quad \beta(x) = 2C_2(x) \]
are dependent of the even number \( x \).

Since \( \rho(x) \) can not be negative and \( \pi(x)/x \) is stationarily decreased and tends to zero when \( x \) is increased such that \( R_3(x)/x \) is stationarily decreased and tends to zero when \( x \) is increased, thus \( \rho(x) \) should be stationarily decreased and tend to a limiting value when \( x \) is increased such that \( \alpha(x) \) and \( \beta(x) \) must be decreased and tend to zero when \( x \) is increased.

Shan-Guang Tan (2012) proved that for any odd number \( x \) greater than 7 there are at least a pair of odd primes \( p \) and \( x - 2p \). Thus there must be
\[ 0 < \alpha(x) \quad \text{and} \quad \lim_{x \to \infty} \alpha(x) = 0 \]
so that \( \alpha(x) \) and \( \rho(x) \) are always greater than zero for \( x < \infty \).

Hence by the form of the function \( \rho^*(x) \) we can let
\[ \alpha_x = \alpha(x) \log^2 x \quad \text{and} \quad \beta_x = \beta(x) \log^2 x \]
then there is \( \alpha_x > 0 \) and \( \rho^*(x) \) becomes
\[ \rho^*(x) = \alpha_x + \beta_x/\log x. \]

Since \( \alpha_x > 0 \) then \( \beta_x \) should be greater than zero otherwise \( R_3(x)/x \) will be stationarily increased when \( x \) is increased. Thus \( \alpha_x \) and \( \beta_x \) are positive constants.

Hence a positive odd number \( x_0 \) always exists such that when \( x > x_0 \) the inequalities
\[ R_3(x) \geq \alpha_x \frac{x}{\log^2 x} + \beta_x \frac{\pi(\sqrt{x}) \sqrt{x}}{2 \log^2 x} \geq 1 \]
always hold such that at last one \( d \) can not be composite so that \( d = x - 2p \) must be a prime for \( x > x_0 \).

This completes the proof of the theorem.

By calculation, there are approximately
\[ \Pi_2 \quad \text{for} \quad x \equiv 0(\text{mod} \ 6) \]
\[ \alpha_x = \{ \begin{array}{ll} 2\Pi_2 & \text{for} \quad x \equiv 2(\text{mod} \ 6) \quad \text{and} \quad \beta_x = 3.0\alpha_x \\ \Pi_2 & \text{for} \quad x \equiv 4(\text{mod} \ 6) \end{array} \]
for Lemoine numbers where \( \Pi_2 \) is the twin primes constant such that we can take \( x_0 \geq 10^3 + 1 \).

Hence we may write
\[ \rho^*(x) = (1 + 3.0/\log x) \ast \{ \begin{array}{ll} 2\Pi_2 & \text{for} \quad x \equiv 2(\text{mod} \ 6) \\ \Pi_2 & \text{for} \quad x \equiv 4(\text{mod} \ 6) \end{array} \} \quad (13.2) \]
Now, we will give out theorems of prime pair numbers for $R_3(x)$, the number of Lemoine numbers. The proofs of these theorems are similar to that for $R_2(x)$, the number of Goldbach numbers.

**Theorem 13.2** (Bounds theorem of Lemoine numbers) For any large odd number $x$, let $R_3(x)$ denote the number of odd prime pairs $p$ and $x-2p$ for $3 \leq p \leq (x-3)/2$, then a positive number $N$ always exists such that the inequalities

$$R_3^*(x, N) \leq R_3(x) < R_3^*(x, N+1)$$

hold where

$$R_3^*(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}$$

and

$$\lim_{x \to \infty} \frac{r_3(x)}{\alpha_x x/ \log^2 x} = 1.$$

**Theorem 13.3** (Relation between $x$ and $N$) Let $\varphi(x, N) = (\log x)/(N + 3/2)$. Then there are approximately

$$\varphi(x, N) \leq \varphi^*(x) = 5.1 - 5.5 \frac{\log 10}{\log x}.$$

**Theorem 13.4** (Upper bound theorem of Lemoine number gaps) For any small positive value $\epsilon(x)$, a pair of positive numbers $x$ and $N$ always exist such that the bounds gap of prime pair numbers

$$g(x, N) = R_3^*(x, N+1) - R_3^*(x, N) \leq \epsilon(x) \frac{\alpha_x x}{\log^2 x}$$

and for any positive odd number $x$, $R_3(x)$ satisfies

$$R_3(x) - R_3^*(x, N) < g(x, N) \leq \epsilon(x) \frac{\alpha_x x}{\log^2 x}$$

where $\alpha_x$ is a positive constant,

$$R_3(x, N) \leq R_3(x) < R_3^*(x, N+1)$$

and

$$R_3^*(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}.$$

Especially $\epsilon(x)$ can be equal to $x^{-1/2} \log^{5/2} x$ such that

$$g(x, N) \leq \alpha_x (x \log x)^{1/2}$$

and for any positive odd number $x$

$$R_3(x) - R_3^*(x, N) < \alpha_x (x \log x)^{1/2}.$$

**Theorem 13.5** (Lemoine number theorem) For large odd numbers $x$, $R_3(x)$ is asymptotically equal to

$$R_3(x) = \alpha_x \text{Li}_2(x) + O(\sqrt{x \log x})$$

where $\text{Li}_2(x) = \int_2^{x} \frac{dt}{\log^2 t}$. 

$$
Part IV

On the solution of the Cramér’s problem

Abstract It is proved in this paper that for every number $i$ greater than 1, there is asymptotically

$$p_{i+1} - p_i = O(\log^2 p_i)$$

and

$$\limsup_{n \to \infty} \frac{p_{i+1} - p_i}{\log^2 p_i} = 1$$

where $p_i$ is the $i^{th}$ prime number.

Keywords Key words and phrases. number theory, primes, gap of primes, Cramér’s conjecture

14 Introduction

14.1 Cramér’s conjecture

In number theory, Cramér’s conjecture, formulated by the Swedish mathematician Harald Cramér in 1936[2], states that

$$p_{i+1} - p_i = O(\log^2 p_i)$$

and

$$\limsup_{n \to \infty} \frac{p_{i+1} - p_i}{\log^2 p_i} = 1$$

where $p_i$ denotes the $i^{th}$ prime number, $O$ is big $O$ notation, and log is the natural logarithm[1].

14.2 Works in this paper

It is proved in this paper that for every number $i$ greater than 1, there is asymptotically

$$p_{i+1} - p_i = O(\log^2 p_i)$$
and
\[ \limsup_{n \to \infty} \frac{p_{i+1} - p_i}{\log^2 p_i} = 1 \]
where \( p_i \) is the \( i \)th prime number.

Hence, the Cramér’s conjecture was proved.

### 15 Theorems proved

Shan-Guang Tan (2011) proved:

**Theorem 15.1** There exists a finite positive number \( n_0 \) such that for every number \( n \) greater than \( n_0 \), the even number \( 2n \) can be represented as the sum of two odd primes where one is smaller than \( \sqrt{2n} \) and another is greater than \( 2n - \sqrt{2n} \).

Shan-Guang Tan (2013) proved:

**Theorem 15.2** (Bounds theorem of Goldbach numbers) For any large even number \( x \), let \( R_2(x) \) denote the number of odd prime pairs \( p \) and \( x - p \) for \( 3 \leq p \leq x/2 \). Then a positive number \( N \) always exists such that the inequalities
\[ R^*_2(x, N) \leq R_2(x) < R^*_2(x, N + 1) \]
hold where
\[ R^*_2(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x} \]
and \( R_2(x) \) is asymptotically equal to
\[ R_2(x) = \alpha_x Li_2(x) + O(\sqrt{x \log x}) \text{ and } Li_2(x) = \int_2^x \frac{dt}{\log^2 t} \]
where \( \alpha_x \) is a positive constant dependent of \( x \pmod{6} \).

By calculation, there are approximately
\[ 2\Pi_2 = 2 \times 0.660161816 \cdots \text{ for } x \equiv 0(\mod{6}) \]
\[ \alpha_x = \begin{cases} 
\Pi_2 = 0.660161816 \cdots & \text{for } x \equiv 2(\mod{6}) \\
\Pi_2 = 0.660161816 \cdots & \text{for } x \equiv 4(\mod{6}) 
\end{cases} \]
where \( \Pi_2 \) is the twin primes constant.

### 16 Theorem of Cramér’s conjecture

**Theorem 16.1** (Theorem of Cramér’s conjecture) For every number \( i \) greater than 1, there is asymptotically
\[ p_{i+1} - p_i = O(\log^2 p_i) \quad (16.1) \]
and
\[ \limsup_{n \to \infty} \frac{p_{i+1} - p_i}{\log^2 p_i} = 1 \quad (16.2) \]
where \( p_i \) is the \( i \)th prime number, \( O \) is big \( O \) notation, and \( \log \) is the natural logarithm.

**Proof** According to Theorem (15.2), let \( R_2^{log}(x) \) denote the number of odd prime pairs \( p \) and \( x - p \) for \( 3 \leq p \leq \log^2 x \).
Since the number $R_2(x)$ is counted for $3 \leq p \leq x/2$, the average density of $R_2(x)$ satisfies
\[
\frac{R^*_2(x,N)}{x/2} \leq \frac{R_2(x)}{x/2} < \frac{R^*_2(x,N+1)}{x/2}
\]
or
\[
\frac{2\alpha_x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x} \leq \frac{R_2(x)}{x/2} < \frac{2\alpha_x}{\log^2 x} \sum_{n=1}^{N+1} \frac{n!}{\log^{n-1} x}.
\]
Hence $\frac{R_2(x)}{x/2} \log^2 x$ is asymptotically equal to
\[
\frac{R_2(x)}{x/2} \log^2 x = 2\alpha_x = \begin{cases} 4\Pi_2 = 2.640647264 \cdots & \text{for } x \equiv 0(\text{mod } 6) \\ 2\Pi_2 = 1.320323632 \cdots & \text{for } x \equiv 2(\text{mod } 6) \\ 2\Pi_2 = 1.320323632 \cdots & \text{for } x \equiv 4(\text{mod } 6) \end{cases}
\]
Since there are
\[
1 > \frac{\pi(x)}{x} > 0, \lim_{x \to \infty} \frac{\pi(x)}{x} = 0
\]
and
\[
1 > \frac{R_2(x)}{x} > 0, \lim_{x \to \infty} \frac{R_2(x)}{x} = 0,
\]
Thus we have
\[
R^\log_2^2 (x) \geq \frac{R_2(x)}{x/2} \log^2 x > 1.320323632 > 1.
\]
This means that by Theorem (15.2) at least a pair of primes $p$ and $q$ exist such that there are
\[
q < \log^2 x \text{ and } p = x - q > x - \log^2 x.
\]
Now, let $x = p_{i+1} + 1$. Then, since $p \leq p_i$ and $p_{i+1} < 2p_i$, we have
\[
p_{i+1} - p_i < \log^2 x \leq \log^2 (2p_i)
\]
\[
= (\log 2 + \log p_i)^2 = (1 + \frac{\log 2}{\log p_i})^2 \log^2 p_i.
\]
Hence we can obtain
\[
p_{i+1} - p_i = O(\log^2 p_i)
\]
and
\[
\limsup_{n \to \infty} \frac{p_{i+1} - p_i}{\log^2 p_i} = 1.
\]
This completes the proof of the theorem.

References
[1] Wapedia - Wiki, Cramér’s conjecture.
[2] Cramér, Harald, On the order of magnitude of the difference between consecutive prime numbers. Acta Arithmetica 2 (1936): pp. 23-46.
[3] Shanks, Daniel, On Maximal Gaps between Successive Primes. Mathematics of Computation (American Mathematical Society) 18 (88)(1964): 646-651, doi:10.2307/2002951, JSTOR 2002951.
[4] Granville, A., Harald Cramér and the distribution of prime numbers. Scandinavian Actuarial Journal 1(1995): 12-28.
[5] Shan-Guang Tan, On the representation of even numbers as the sum of two odd primes and the distribution of primes in short intervals. (arXiv:1110.3465)
Part V

On the representation of even numbers as the difference of two consecutive primes

Abstract The representation of even numbers as the difference of two consecutive primes investigated in this paper. A basic theorem was proved. It states: Every even number is the difference of two consecutive primes in infinitely many ways.

To prove the basic theorem, we proved that:
1. At least an even number is the difference of two consecutive primes in infinitely many ways.
2. Let $2m_1$ denote the smallest difference of two consecutive primes in infinitely many ways, then any other difference of two consecutive primes in infinitely many ways should be the multiple of $2m_1$.
3. The smallest difference of two consecutive primes in infinitely many ways should be equal to 2.
4. For $k = 1, 2, \cdots$, every even number $2k$ is the difference of two consecutive primes in infinitely many ways.

Based on the basic theorem, it was proved that:
1. There are infinitely many twin primes $p$ and $p + 2$.
2. There are infinitely many cousin primes $p$ and $p + 4$.
3. There are infinitely many sexy primes $p$ and $p + 6$.
4. There are infinitely many pairs of consecutive primes $p$ and $p + 2k$ for $k = 1, 2, \cdots$.

Keywords twin primes, cousin primes, sexy primes, Polignac’s conjecture

17 Introduction

17.1 Twin primes conjecture and Polignac’s conjecture

Twin primes conjecture is one of the oldest unsolved problems in number theory and in all of mathematics. It is also one of Landau’s problems (1912). It states: There are an infinite number of twin primes $p$ and $p + 2[2-3]$.

Polignac’s conjecture was made by Alphonse de Polignac in 1849 and states: For any positive even number $n$, there are infinitely many prime gaps of size $n$. In other words: There are infinitely many cases of two consecutive prime numbers with difference $n$. The conjecture has not been proven or disproved for any value of $n[1]$.

For $n = 2$, it is the twin prime conjecture. For $n = 4$, it says there are infinitely many cousin primes $(p, p + 4)$. For $n = 6$, it says there are infinitely many sexy primes $(p, p + 6)$ with no prime between $p$ and $p + 6$. 

[6] Shan-Guang Tan, *On the number of Goldbach numbers and the number of Lemoine numbers.* arXiv:1110.3465.
17.2 Works in this paper

The representation of even numbers as the difference of two consecutive primes investigated in this paper. A basic theorem was proved. It states: Every even number is the difference of two consecutive primes in infinitely many ways.

To prove the basic theorem, we proved that:

(1) At least an even number is the difference of two consecutive primes in infinitely many ways.

(2) Let $2m_1$ denote the smallest difference of two consecutive primes in infinitely many ways, then any other difference of two consecutive primes in infinitely many ways should be the multiple of $2m_1$.

(3) The smallest difference of two consecutive primes in infinitely many ways should be equal to 2.

(4) For $k = 1, 2, \cdots$, every even number $2k$ is the difference of two consecutive primes in infinitely many ways.

Based on the basic theorem, it was proved that:

(1) There are infinitely many twin primes $p$ and $p + 2$.

(2) There are infinitely many cousin primes $p$ and $p + 4$.

(3) There are infinitely many sexy primes $p$ and $p + 6$.

(4) There are infinitely many pairs of consecutive primes $p$ and $p + 2k$ for $k = 1, 2, \cdots$.

18 Theorems proved

B. Powell (1983) put forward and R. O. Davies (1984) proved:

**Theorem 18.1** For every positive number $M$ there exists an even number $2k$ such that there are at least $M$ pairs of consecutive primes $p$ and $p + 2k$.

Y. Zhang very recently (2013) proved:

**Theorem 18.2**

$$\liminf_{n \to \infty} (p_{n+1} - p_n) < 7 \times 10^7,$$

where $p_n$ is the $n^{th}$ prime.

Shan-Guang Tan (2011) proved:

**Theorem 18.3** There exists a finite positive number $n_0$ such that for every number $n$ greater than $n_0$, the even number $2n$ can be represented as the sum of two odd primes where one is smaller than $\sqrt{2n}$ and another is greater than $2n - \sqrt{2n}$.

Shan-Guang Tan (2013) proved:

**Theorem 18.4** (Bounds theorem of Goldbach numbers) For any large even number $x$, let $R_2(x)$ denote the number of odd prime pairs $p$ and $x - p$ for $3 \leq p \leq x/2$. Then a positive number $N$ always exists such that the inequalities

$$R_2^*(x, N) \leq R_2(x) < R_2^*(x, N + 1)$$

hold where

$$R_2^*(x, N) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}$$

and

$$R_2(x) = \alpha_x \frac{x}{\log^2 x} \sum_{n=1}^{x/2} \frac{n!}{\log^{n-1} x}$$
and $R_2(x)$ is asymptotically equal to

$$R_2(x) = \alpha_x Li_2(x) + O(\sqrt{x \log x}) \text{ and } Li_2(x) = \int_2^x \frac{dt}{\log^2 t}$$

where $\alpha_x$ is a positive constant dependent of $x (\mod 6)$.

Then based on Theorem (18.4), let prove the following theorem.

**Theorem 18.5** For any small positive value $\epsilon$ there exists a finite positive number $n_\epsilon$ such that for every number $n$ not smaller than $n_\epsilon$, the even number $2n$ can be represented as the sum of two odd primes where one is in the region $(n^{1-\epsilon}, n)$ and another is in the region $(n, 2n - n^{1-\epsilon})$.

**Proof** By Theorem (18.4), there is $R_2(x) \geq \alpha_x \frac{x}{\log^2 x}$.

For any small positive value $\epsilon$ let consider

$$R_2(2n) - \pi(n^{1-\epsilon}) > \alpha_{2n} \frac{2n}{\log^2 (2n)} - n^{1-\epsilon}/2$$

$$= n^{1-\epsilon} (\alpha_{2n} \frac{2n^\epsilon}{\log^2 (2n)} - 1/2) \geq 1.$$

Then there exists a number $n_\epsilon$ such that the inequality

$$n_\epsilon^{1-\epsilon} (\alpha_{2n} \frac{2n^\epsilon}{\log^2 (2n)} - 1/2) \geq 1$$

holds and there are at least a pair of primes $p$ and $q$ in the region $(n_\epsilon^{1-\epsilon}, 2n_\epsilon - n_\epsilon^{1-\epsilon})$.

Thus for every number $n$ not smaller than $n_\epsilon$, the even number $2n$ can be represented as the sum of two odd primes where one is in the region $(n^{1-\epsilon}, n)$ and another is in the region $(n, 2n - n^{1-\epsilon})$.

This completes the proof of the theorem.

19 Theorem of twin primes

**Lemma 19.1** At least an even number is the difference of two consecutive primes in infinitely many ways.

**Proof** By Theorem (18.1) when $M \to \infty$, or directly by Theorem (18.2), there exists at least an even number $2k$ such that it is the difference of two consecutive primes in infinitely many ways.

The proof of the lemma is completed.

**Lemma 19.2** Let $2m_1$ denote the smallest difference of two consecutive primes in infinitely many ways, then any other difference of two consecutive primes in infinitely many ways should be the multiple of $2m_1$.

**Proof** By Lemma (19.1), at least an even number is the difference of two consecutive primes in infinitely many ways.

If $m_1 = 1$, then the lemma holds.

Otherwise when any pair of consecutive primes greater than a number $x_0$ is with a difference not smaller than $2m_1$, let take any two pairs of consecutive primes greater than $x_0$. One pair of
consecutive primes are \( p \) and \( p + 2m_1 \). Another pair of consecutive primes are \( q \) and \( q + 2m_1 \). Then let an even number \( N = p + q \).

Now let consider an infinite sequence

\[
N_i = N + 2m_1 * i \text{ for } i = 1, 2, \ldots.
\]

By Theorem (18.3), every even number \( N_i \) can be represented as the sum of two odd primes \( p_i \) and \( q_i \) where \( p_i < \sqrt{N_i} \) and \( q_i > N_i - \sqrt{N_i} \). By Theorem (18.5), every even number \( N_i \) can be represented as the sum of two odd primes \( p_i \) and \( q_i \) where \( p_i \) is in the region \( ((N_i/2)^{1-\epsilon}, N_i/2) \) and \( q_i \) is in the region \( (N_i/2, N_i - (N_i/2)^{1-\epsilon}) \) where the positive value \( \epsilon \) and the even number \( N = p + q \) can be chosen to satisfy the inequality \((N_i/2)^{1-\epsilon} \geq x_0\).

When any other difference of two consecutive primes in infinitely many ways is the multiple of \( 2 \), then the infinitely many equalities \( N_i = p_i + q_i \) can not be satisfied. Thus any other difference of two consecutive primes in infinitely many ways are not multiples of \( 2 \), and there should be at least a difference \( 2j < 2m_1 \) of two consecutive primes in infinitely many ways. It contradicts the fact that \( 2m_1 \) is the smallest difference of two consecutive primes in infinitely many ways.

**Lemma 19.3** The smallest difference of two consecutive primes in infinitely many ways should be equal to 2.

**Proof** By Lemma (19.2), if \( m_1 = 1 \), then the lemma holds. Otherwise when any pair of consecutive primes greater than a number \( x_0 \) is with a difference not smaller than \( 2m_1 \), let take any two pairs of consecutive primes greater than \( x_0 \). One pair of consecutive primes are \( p \) and \( p + 2m_1 \). Another pair of consecutive primes are \( q \) and \( q + 2m_1 \). Then let an even number \( N = p + q \).

For \( j = 1, 2, \ldots, m_1 - 1 \), let consider the infinite sequence

\[
N_{i,j} = N + 2m_1 * i + 2j \text{ for } i = 0, 1, 2, \ldots.
\]

By Theorem (18.3), every even number \( N_{i,j} \) can be represented as the sum of two odd primes \( p_{i,j} \) and \( q_{i,j} \) where \( p_{i,j} < \sqrt{N_{i,j}} \) and \( q_{i,j} > N_{i,j} - \sqrt{N_{i,j}} \). By Theorem (18.5), every even number \( N_{i,j} \) can be represented as the sum of two odd primes \( p_{i,j} \) and \( q_{i,j} \) where \( p_{i,j} \) is in the region \( ((N_{i,j}/2)^{1-\epsilon}, N_{i,j}/2) \) and \( q_{i,j} \) is in the region \( (N_{i,j}/2, N_{i,j} - (N_{i,j}/2)^{1-\epsilon}) \) where the positive value \( \epsilon \) and the even number \( N = p + q \) can be chosen to satisfy the inequality \((N_{i,j}/2)^{1-\epsilon} \geq x_0\).

Thus there are infinitely many equalities \( N_{i,j} = p_{i,j} + q_{i,j} \) and there should be at least a difference \( 2j < 2m_1 \) of two consecutive primes in infinitely many ways. It contradicts the fact that \( 2m_1 \) is the smallest difference of two consecutive primes in infinitely many ways.
A contradiction. Thus there should be $m_1 = 1$ and the smallest difference of two consecutive primes in infinitely many ways should be equal to 2.

The proof of the lemma is completed.

**Theorem 19.4** (Twin primes theorem) *There are an infinite number of twin primes $p$ and $p + 2$.*

**Proof** By Lemma 19.3, the even number 2 is the difference of two consecutive primes in infinitely many ways.

Thus there are an infinite number of twin primes $p$ and $p + 2$.

This completes the proof of the theorem.

20 **Theorem of cousin primes**

**Lemma 20.1** *At least an even number greater than 2 is the difference of two consecutive primes in infinitely many ways.*

**Proof** By Lemma 19.3, the even number 2 is the difference of two consecutive primes in infinitely many ways.

Then let $\Delta_1 = 2$ and take any pair of consecutive primes $q_1$ and $q_1 + 2$, and consider an infinite sequence

$$n_{1,i} = q_1 + i\Delta_1 \text{ for } i = 1, 2, \ldots$$

Thus for $i = j \cdot q_1$, let consider sequences $n_{1,j \cdot q_1} - 2$ and $n_{1,j \cdot q_1} + 2$ where for $j = 1, 2, \ldots$

$$n_{1,j \cdot q_1} - 2 = q_1 + j \cdot q_1 \Delta_1 - 2 = q_1 - 2 + j \cdot 2q_1$$

and

$$n_{1,j \cdot q_1} + 2 = q_1 + j \cdot q_1 \Delta_1 + 2 = q_1 + 2 + j \cdot 2q_1.$$  

Since $gcd(q_1 - 2, 2q_1) = 1$ and $gcd(q_1 + 2, 2q_1) = 1$, then by Dirichlet theorem there are infinite many primes in sequences $n_{1,j \cdot q_1} - 2$ and $n_{1,j \cdot q_1} + 2$.

If there are an infinite number of cousin primes $n_{1,j \cdot q_1} - 2$ and $n_{1,j \cdot q_1} + 2$, then the even number 4 is the difference of two consecutive primes in infinitely many ways. Otherwise at least an even number greater than 4 is the difference of two consecutive primes in infinitely many ways.

Hence at least an even number greater than 2 is the difference of two consecutive primes in infinitely many ways.

The proof of the lemma is completed.

**Lemma 20.2** *The even number 4 is the difference of two consecutive primes in infinitely many ways.*

**Proof** By Lemma 20.1, at least an even number greater than 2 is the difference of two consecutive primes in infinitely many ways.

If the even number 4 is the difference of two consecutive primes in infinitely many ways, then the lemma is true.

Otherwise let the even number $2m_2$ be the smallest difference greater than 2 of two consecutive primes in infinitely many ways. Then by Lemma 22.3 for $m_k = m_1 = 1$ there is
$m_2 = m_1 + 1 = 2$. Hence the even number 4 is the difference of two consecutive primes in infinitely many ways.

The proof of the lemma is completed.

**Theorem 20.3** (Cousin primes theorem) *There are an infinite number of cousin primes $p$ and $p+4$.*

**Proof** By Lemma 20.2 the even number 4 is the difference of two consecutive primes in infinitely many ways.

Thus there are an infinite number of cousin primes $p$ and $p+4$.

This completes the proof of the theorem.

### 21 Theorem of sexy primes

**Lemma 21.1** *At least an even number greater than 4 is the difference of two consecutive primes in infinitely many ways.*

**Proof** By Lemma 19.3 and Lemma 20.2, every even number $2k$ for $k = 1, 2$ is the difference of two consecutive primes in infinitely many ways.

By the proof of Lemma 20.1, let $\Delta_2 = q_1 \Delta_1$ and $q_2 = n_{1,x_1}q_1 - 2$, then take any pair of consecutive primes $q_2$ and $q_2 + 2 \ast 2$, and consider an infinite sequence

$$n_{2,i} = q_2 + i\Delta_2 \text{ for } i = 1, 2, \cdots.$$ 

Thus for $i = j \ast q_2$, let consider sequences $n_{2,j \ast q_2} - 2$ and $n_{2,j \ast q_2} + 2 \ast 2$ where for $j = 1, 2, \cdots$

$$n_{2,j \ast q_2} - 2 = q_2 + j \ast q_2 \Delta_2 - 2 = q_2 - 2 + j \ast 2q_1q_2$$

and

$$n_{2,j \ast q_2} + 2 \ast 2 = q_2 + j \ast q_2 \Delta_2 + 2 \ast 2 = q_2 + 2 \ast 2 + j \ast 2q_1q_2.$$ 

Since $q_2 = n_{1,x_1}q_1 - 2 = q_1(1 + 2x_1) - 2$ such that for $m = 1, 2$

$$\text{gcd}(q_2 - 2, q_m) = 1 \text{ and } \text{gcd}(q_2 + 2 \ast 2, q_m) = 1$$

and

$$\text{gcd}(q_2 - 2, 2q_1q_2) = 1 \text{ and } \text{gcd}(q_2 + 2 \ast 2, 2q_1q_2) = 1,$$

then by Dirichlet theorem there are infinite many primes in sequences $n_{2,j \ast q_2} - 2$ and $n_{2,j \ast q_2} + 2 \ast 2$.

If there are an infinite number of sexy primes $n_{2,j \ast q_2} - 2$ and $n_{2,j \ast q_2} + 2 \ast 2$, then the even number 6 is the difference of two consecutive primes in infinitely many ways. Otherwise at least an even number greater than 6 is the difference of two consecutive primes in infinitely many ways.

Hence at least an even number greater than 4 is the difference of two consecutive primes in infinitely many ways.

This completes the proof of the theorem.

**Lemma 21.2** *The even number 6 is the difference of two consecutive primes in infinitely many ways.*
Proof. By Lemma (21.1), at least an even number greater than 4 is the difference of two consecutive primes in infinitely many ways.

If the even number 6 is the difference of two consecutive primes in infinitely many ways, then the lemma is true.

Otherwise let the even number $2m_3$ be the smallest difference greater than 4 of two consecutive primes in infinitely many ways. Then by Lemma (22.3) for $m_k = m_2 = 2$ there is $m_3 = m_2 + 1 = 3$. Hence the even number 6 is the difference of two consecutive primes in infinitely many ways.

The proof of the lemma is completed.

Theorem 21.3 (Sexy primes theorem) There are an infinite number of sexy primes $p$ and $p + 6$.

Proof. By Lemma (21.2) the even number 6 is the difference of two consecutive primes in infinitely many ways.

Thus there are an infinite number of sexy primes $p$ and $p + 6$.

This completes the proof of the theorem.

22 Theorems of Polignac primes

Lemma 22.1 If every even number $2k$ for $k = 1, 2, \ldots, m_k$ is the difference of two consecutive primes in infinitely many ways, then at least an even number greater than $2m_k$ is the difference of two consecutive primes in infinitely many ways.

Proof. By Lemma (19.3), Lemma (20.2) and Lemma (21.2), every even number $2k$ for $k = 1, 2, 3$ is the difference of two consecutive primes in infinitely many ways.

By the proof of Lemma (21.1), let $\Delta_3 = q_2\Delta_2$ and $q_3 = n_{2,x_2q_2} - 2$, then take any pair of consecutive primes $q_3$ and $q_3 + 2 \ast 3$, and consider an infinite sequence

$$n_{3,i} = q_3 + i\Delta_3 \text{ for } i = 1, 2, \ldots .$$

Thus for $i = j \ast q_3$, let consider sequences $n_{3,j\ast q_3} - 2$ and $n_{3,j\ast q_3} + 2 \ast 3$ where for $j = 1, 2, \ldots$

$$n_{3,j\ast q_3} - 2 = q_3 + j \ast q_3\Delta_3 - 2 = q_3 - 2 + j \ast 2q_1q_2q_3$$

and

$$n_{3,j\ast q_3} + 2 \ast 3 = q_3 + j \ast q_3\Delta_3 + 2 \ast 3 = q_3 + 2 \ast 3 + j \ast 2q_1q_2q_3.$$ 

Since

$$q_3 = n_{2,x_2q_2} - 2$$

$$= q_2 + x_2q_2\Delta_2 - 2 = q_2(1 + x_2\Delta_2) - 2$$

$$= q_1 + 2x_1q_1 + 2x_2q_2q_1 - 2 = q_1(1 + 2x_1 + 2x_2q_2) - 2$$

such that for $m = 1, 2, 3$

$$gcd(q_3 - 2, q_m) = 1 \text{ and } gcd(q_3 + 2 \ast 3, q_m) = 1$$

and

$$gcd(q_3 - 2, 2q_1q_2q_3) = 1 \text{ and } gcd(q_3 + 2 \ast 3, 2q_1q_2q_3) = 1,$$
then by Dirichlet theorem there are infinite many primes in sequences \( n_{3,j+q_3} - 2 \) and \( n_{3,j+q_3} + 2 \times 3 \).

Assume that going on in the same way, every even number \( 2k \) for \( k = 1, 2, \cdots, m_k \) is the difference of two consecutive primes in infinitely many ways. Then let

\[
\Delta_k = q_{k-1} \Delta_{k-1} \quad \text{and} \quad q_k = n_{k-1, x_{k-1} q_{k-1}} - 2,
\]

and take any pair of consecutive primes \( q_k \) and \( q_k + 2k \), and consider an infinite sequence

\[
n_{k,i} = q_k + i \Delta_k \quad \text{for} \quad i = 1, 2, \cdots.
\]

Thus for \( i = j \times q_k \), let consider sequences \( n_{k,j+q_k} - 2 \) and \( n_{k,j+q_k} + 2k \) where for \( j = 1, 2, \cdots \)

\[
n_{k,j+q_k} - 2 = q_k + j \times q_k \Delta_k - 2 = q_k - 2 + j \times 2q_1 q_2 q_3 \cdots q_k
\]

and

\[
n_{k,j+q_k} + 2k = q_k + j \times q_k \Delta_k + 2k = q_k + 2k + j \times 2q_1 q_2 q_3 \cdots q_k.
\]

Since for any positive number \( k \) we can always choose \( q_1 > k \) and there are

\[
q_k = n_{k-1, x_{k-1} q_{k-1}} - 2
= q_{k-1} + x_{k-1} q_{k-1} \Delta_{k-1} - 2
= q_{k-2} + x_{k-2} q_{k-2} \Delta_{k-2} + x_{k-1} q_{k-1} q_{k-2} \Delta_{k-2} - 2
= q_{k-3} + x_{k-3} q_{k-3} \Delta_{k-3} + q_{k-3} \Delta_{k-3} \sum_{m=k-3}^{k-1} x_m \prod_{n=k-2}^{m} q_n - 2
\]

or

\[
q_k = n_{k-1, x_{k-1} q_{k-1}} - 2
= q_{k-1}(1 + x_{k-1} \Delta_{k-1}) - 2
= q_{k-2}(1 + \Delta_{k-2} \sum_{m=k-2}^{k-1} x_m \prod_{n=k-1}^{m} q_n) - 2
= q_{k-3}(1 + \Delta_{k-3} \sum_{m=k-3}^{k-1} x_m \prod_{n=k-2}^{m} q_n) - 2
= \cdots = q_2(1 + \Delta_2 \sum_{m=2}^{k-1} x_m \prod_{n=3}^{m} q_n) - 2
= q_1(1 + \Delta_1 \sum_{m=1}^{k-1} x_m \prod_{n=2}^{m} q_n) - 2
\]
such that for \( m = 1, 2, \cdots, k \)
\[
gcd(q_k - 2, q_m) = 1 \quad \text{and} \quad gcd(q_k + 2k, q_m) = 1
\]
and
\[
gcd(q_k - 2, 2q_1 q_2 q_3 \cdots q_k) = 1 \quad \text{and} \quad gcd(q_k + 2k, 2q_1 q_2 q_3 \cdots q_k) = 1,
\]
then by Dirichlet theorem there are infinite many primes in sequences \( n_{k,j} \) and \( n_{k,j} + 2k \).

If there are an infinite number of two consecutive primes \( n_{k,j} - 2 \) and \( n_{k,j} + 2m_k \), then the even number \( 2(m_k + 1) \) is the difference of two consecutive primes in infinitely many ways. Otherwise at least an even number greater than \( 2(m_k + 1) \) is the difference of two consecutive primes in infinitely many ways.

Hence at least an even number greater than \( 2m_k \) is the difference of two consecutive primes in infinitely many ways.

The proof of the lemma is completed.

**Lemma 22.2** For \( k = 1, 2, \cdots \), every even number \( 2k \) is the difference of two consecutive primes in infinitely many ways.

**Proof** By Lemma (22.1), at least an even number greater than \( 2m_k \) is the difference of two consecutive primes in infinitely many ways.

If the even number \( 2(m_k + 1) \) is the difference of two consecutive primes in infinitely many ways, then the lemma is true.

Otherwise let the even number \( 2m_{k+1} \) be the smallest difference greater than \( 2m_k \) of two consecutive primes in infinitely many ways. Then by Lemma (22.3) there is \( m_{k+1} = m_k + 1 \). Hence the even number \( 2m_{k+1} = 2(m_k + 1) \) is the difference of two consecutive primes in infinitely many ways.

Hence every even number \( 2k \) for \( k = 1, 2, \cdots \) is the difference of two consecutive primes in infinitely many ways.

The proof of the lemma is completed.

**Lemma 22.3** Assume that every even number of \( 2, 4, \cdots, 2m_k \) is the difference of two consecutive primes in infinitely many ways. Then the even number \( 2(m_k + 1) \) is the smallest difference greater than \( 2m_k \) of two consecutive primes in infinitely many ways.

**Proof** If the even number \( 2m_{k+1} = 2(m_k + 1) \) is the smallest difference greater than \( 2m_k \) of two consecutive primes in infinitely many ways, then the lemma holds.

Otherwise when any pair of consecutive primes greater than a number \( x_0 \) is with a difference \( 2m \) which satisfies \( 2m \leq 2m_k \) or \( 2m \geq 2m_{k+1} \), let consider an infinite sequence \( P_{2k} \) of consecutive prime pairs \( p_i \) and \( p_i + 2m_{k+1} \) where \( p_i \) are greater than a positive number \( x_0 \) for \( i = 0, 1, 2, \cdots \).

Now we can form an infinite sequence \( N_i = p_0 + p_i \) for \( i = 1, 2, \cdots \).

Then every even number \( N = N_i + 2j \) or \( N = N_i + 2m_{k+1} - 2j \) for \( i = 1, 2, \cdots \) and \( j = m_k + 1, m_k + 2, \cdots, m_{k+1} - 1 \) can be represented as the sum of two odd primes \( p \) and \( q \) by Theorem (18.3) where \( p < \sqrt{N} \) and \( q > N - \sqrt{N} \) or by Theorem (18.5) where \( p \) is in the region \( (N/2)^{1-\epsilon}, N/2 \) and \( q \) is in the region \( (N/2, N - (N/2)^{1-\epsilon}) \) where the positive value \( \epsilon \) and the even number \( N = p + q \) can be chosen to satisfy the inequality \( (N/2)^{1-\epsilon} \geq x_0 \). And even more
by Theorem (18.4) for \( x = N \) the number of the representations satisfies 
\[
R_2(x) \geq \alpha \left( \frac{\pi(x)}{\log x} \right)
\]
and is asymptotically equal to 
\[
R_2(x) = \alpha \log x + O(\sqrt{x \log x}).
\]
Thus there are infinitely many equalities \( N = p + q \).

Since the infinitely many equalities \( N_i = p + q \) and \( N_i + 2m_{k+1} = p + q \) for \( i = 1, 2, \ldots \) can be satisfied, let \( m_{k+1} = m_k + 1 \) then no number \( j \) exists for \( j = m_k + 1, m_k + 2, \ldots, m_{k+1} - 1 \) such that even numbers \( N = N_i + 2j \) and \( N = N_i + 2m_{k+1} - 2j \) become \( N = N_i \) and \( N = N_i + 2m_{k+1} \) for \( i = 1, 2, \ldots \) respectively, so that the infinitely many equalities \( N = p + q \) can be satisfied. Since the distribution of primes is unique, the smallest difference greater than \( 2m_k \) of two consecutive primes in infinitely many ways must be \( 2(m_k + 1) \).

On the other hand, although some equalities \( N = p + q \) may be satisfied by some pairs of odd primes \( p \) and \( q \) which are in the form of consecutive primes \( p \) and \( p + 2m \) or \( q + 2m \) with a difference \( 2m \) for \( m \leq m_k \) or \( m \geq m_{k+1} \), since the distribution of primes is unique, there should be at least a difference \( 2j \) of two consecutive primes in infinitely many ways where \( m_k < j < m_{k+1} \) to satisfy the infinitely many equalities \( N = p + q \). It contradicts the fact that \( 2m_{k+1} \) is the smallest difference greater than \( 2m_k \) of two consecutive primes in infinitely many ways. Thus there should be \( m_{k+1} = m_k + 1 \) and the smallest difference of two consecutive primes in infinitely many ways should be equal to \( 2(m_k + 1) \).

The proof of the lemma is completed.

**Theorem 22.4** (Primes difference theorem)  
Every even number is the difference of two consecutive primes in infinitely many ways.

*Proof* By Lemma (22.2), the even number \( 2k \) for \( k = 1, 2, \ldots \) is the difference of two consecutive primes in infinitely many ways. Thus every even number is the difference of two consecutive primes in infinitely many ways.

This completes the proof of the theorem.

**Theorem 22.5** (Polignac primes theorem)  
There are infinitely many pairs of consecutive primes \( p \) and \( p + 2k \) for \( k = 1, 2, \ldots \).

*Proof* By Theorem (22.4), the even number \( 2k \) for \( k = 1, 2, \ldots \) is the difference of two consecutive primes in infinitely many ways. Thus there are infinitely many pairs of consecutive primes \( p \) and \( p + 2k \) for \( k = 1, 2, \ldots \).

This completes the proof of the theorem.

**References**

[1] Wapedia - Wiki, Polignac’s conjecture.
[2] Wapedia - Wiki, Twin primes conjecture.
[3] Marek Wolf, On the Twin and Cousin Primes. IFTUWr 909/96, August, 1996.
[4] B. Powell, Problem 6429: Difference between consecutive primes. Amer. Math. Monthly 90(1983), 998.
[5] R. O. Davies, Solution of problem 6429: Difference between consecutive primes. Amer. Math. Monthly 91(1984), 64.
[6] Yitang Zhang, Bounded gaps between primes. Ann. of Math. (2013), to appear.
[7] Shan-Guang Tan, On the representation of even numbers as the sum of two odd primes and the distribution of primes in short intervals. arXiv:1110.3465
[8] Shan-Guang Tan, On the number of Goldbach numbers and the number of Lemoine numbers. arXiv:1110.3465
Part VI

On the number of Polignac primes

Abstract Let $\pi_{2k}(x)$ be the number of odd prime pairs $p$ and $p + 2k$ which may not be consecutive for $k > 2$ such that $p \leq x$ and $1 \leq k \leq \sqrt{x}$. Then it was proved in this paper that:

(1) For large numbers $x$, the inequality

$$\pi_{2k}(x) \geq a_{2k} \frac{x}{\log^2 x} + b_{2k} \frac{x}{\log^3 x}$$

always holds where $a_{2k}$ and $b_{2k}$ are positive constants dependent of the number $k$.

(2) The number $\pi_{2k}(x)$ satisfies

$$\pi^*_{2k}(x, N) \leq \pi_{2k}(x) < \pi^*_{2k}(x, N + 1)$$

where $N$ is a positive number and

$$\pi^*_{2k}(x, N) = a_{2k} \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}.$$  

(3) Let $\varphi(x, N) = (\log x)/(N + 3/2)$. Then there are approximately

$$\varphi(x, N) \leq \varphi^*(x) = 5.1 - 5.5 \frac{\log 10}{\log x}.$$  

(4) For any small positive value $\epsilon(x)$, a pair of positive numbers $x$ and $N$ always exist such that the number $\pi_{2k}(x)$ satisfies

$$\pi_{2k}(x) - \pi^*_{2k}(x, N) < \epsilon(x) \frac{a_{2k}x}{\log^2 x}.$$  

Especially $\epsilon(x)$ can be equal to $x^{-1/2} \log^{5/2} x$ such that for any positive number $x$, the number $\pi_{2k}(x)$ satisfies

$$\pi_{2k}(x) - \pi^*_{2k}(x, N) < a_{2k}(x \log x)^{1/2}.$$  

(5) For large numbers $x$, $\pi_{2k}(x)$ is asymptotically equal to

$$\pi_{2k}(x) = a_{2k} Li_2(x) + O(\sqrt{x \log x}).$$  

Keywords twin primes, Polignac primes
23 Introduction

23.1 Twin primes conjecture and Polignac’s conjecture

Twin primes conjecture is one of the oldest unsolved problems in number theory and in all of mathematics. It is also one of Landau’s problems (1912). It states: There are an infinite number of twin primes \( p \) and \( p + 2 \).

Polignac’s conjecture was made by Alphonse de Polignac in 1849 and states: For any positive even number \( 2n \), there are infinitely many prime gaps of size \( 2n \). In other words: There are infinitely many cases of two consecutive prime numbers with difference \( 2n \). Then the word “Polignac primes” means a pair of odd primes \( p \) and \( p + 2n \). The conjecture has not been proven or disproven for any value of \( 2n \).

For \( n = 1 \), it is the twin prime conjecture. For \( n = 2 \), it says there are infinitely many cousin primes \((p, p + 4)\). For \( n = 3 \), it says there are infinitely many sexy primes \((p, p + 6)\) with no prime between \( p \) and \( p + 6 \).

Let \( \pi_2(x) \) be the number of twin primes \( p \) and \( p + 2 \) such that \( p \leq x \). Hardy and Littlewood (1923) conjectured that \( \pi_2(x) \) is asymptotically equal to

\[
\pi_2(x) \sim 2\Pi_2 Li_2(x).
\]

Let \( \pi_{2n}(x) \) for even \( 2n \) be the number of prime gaps of size \( 2n \) below \( x \).

The first Hardy-Littlewood conjecture says the asymptotic density is of form

\[
\pi_{2n}(x) \sim 2\Pi_{2n} \frac{x}{\ln^2 x} \sim 2\Pi_{2n} Li_2(x).
\]

23.2 Works in this paper

Let \( \pi_{2k}(x) \) be the number of odd prime pairs \( p \) and \( p + 2k \) which may not be consecutive for \( k > 2 \) such that \( p \leq x \) and \( 1 \leq k \leq \sqrt{x} \). Then it was proved in this paper that:

1. For large numbers \( x \), the inequality

\[
\pi_{2k}(x) \geq a_{2k} \frac{x}{\log^2 x} + b_{2k} \frac{x}{\log^3 x}
\]

always holds where \( a_{2k} \) and \( b_{2k} \) are positive constants dependent of the number \( k \).

2. The number \( \pi_{2k}(x) \) satisfies

\[
\pi_{2k}^*(x, N) \leq \pi_{2k}(x) < \pi_{2k}^*(x, N + 1)
\]

where \( N \) is a positive number and

\[
\pi_{2k}^*(x, N) = a_{2k} \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}.
\]

3. Let \( \varphi(x, N) = (\log x)/(N + 3/2) \). Then there are approximately

\[
\varphi(x, N) \leq \varphi^*(x) = 5.1 - 5.5 \frac{\log 10}{\log x}.
\]

4. For any small positive value \( \epsilon(x) \), a pair of positive numbers \( x \) and \( N \) always exist such that the number \( \pi_{2k}(x) \) satisfies

\[
\pi_{2k}(x) - \pi_{2k}^*(x, N) < \epsilon(x) \frac{a_{2k} x}{\log^2 x}.
\]
Especially \(\varepsilon(x)\) can be equal to \(x^{-1/2} \log^{5/2} x\) such that for any positive number \(x\), the number \(\pi_{2k}(x)\) satisfies
\[
\pi_{2k}(x) - \pi_{2k}^*(x, N) < a_{2k}(x \log x)^{1/2}.
\]

(5) For large numbers \(x\), \(\pi_{2k}(x)\) is asymptotically equal to
\[
\pi_{2k}(x) = a_{2k} Li_2(x) + O(\sqrt{x} \log x).
\]

### 24 Definitions

#### 24.1 Sets of primes
For any number \(x\), let \(\pi(\sqrt{x}) = n\) and \(\pi(x) = n + r\). Then let denote a set of primes by \(P\) where
\[
P = \{p_i | i = 1, 2, \ldots, n + r\}
\] (24.1)
and
\[
2 = p_1 < p_2 < \cdots < p_n \leq \sqrt{x} < p_{n+1} < p_{n+2} < \cdots < p_{n+r} \leq x.
\]
Let \(P_n\) denote a subset of \(P\) where
\[
P_n = \{p_i | i = 2, 3, \ldots, n\} \subset P.
\] (24.2)
Let \(Q_u\) and \(Q_v\) denote subsets of \(P\) where
\[
Q_u = \{q_i | q_i \in P, q_i = 6m_i + 1, i = 1, 2, \ldots, r_u\}
\] (24.3)
and
\[
Q_v = \{q_i | q_i \in P, q_i = 6m_i - 1, i = 1, 2, \ldots, r_v\}
\] (24.4)
where \(r_u\) and \(r_v\) are numbers of elements of odd prime sets \(Q_u\) and \(Q_v\), respectively.

#### 24.2 Sets of odd numbers
Let \(D_u\) and \(D_v\) denote subsets of odd numbers where
\[
D_u = \{d_i | d_i = 6m_i + 1, i = 1, 2, \ldots, r_u\}
\] (24.5)
and
\[
D_v = \{d_i | d_i = 6m_i - 1, i = 1, 2, \ldots, r_u\}
\] (24.6)
where \(r_u\) and \(r_v\) are numbers of elements of odd number sets \(D_u\) and \(D_v\), respectively.

Let \(D\) denote \(D_u\) or \(D_v\) or \(D_u \cup D_v\), that is
\[
D = D_u \text{ or } D = D_v \text{ or } D = D_u \cup D_v.
\] (24.7)

Let \(D_j\) for \(j = 1, 2, \ldots, n\) denote odd composite number sets where
\[
D_j = \{d | d \in D, \max\{q | q \in P_n, q | d\} = p_j\} \subset D
\] (24.8)
such that \(D_i \cap D_j = \emptyset\) for \(i, j = 1, 2, \ldots, n\) and \(i \neq j\). Hence any odd composite number \(d \in D\) can be uniquely classified into an odd composite number set \(D_j\). Let denote
\[
D_{\cup} = D_1 \cup D_2 \cup D_3 \cup \cdots \cup D(n)
\]
then there is \(D_{\cup} \subseteq D\). If \(D_{\cup} \neq D\) or the number of elements of \(D_{\cup}\) is smaller than the number of elements of \(D\), then some odd numbers \(d \in D\) must be primes.
25 Theorem of composite numbers
Shan-Guang Tan (2013) proved:

**Theorem 25.1 (Estimation theorem)** For an odd number set $D$ defined in Sec. [24], let $σ$ denote the number of odd composite numbers $d ∈ D$, then the inequalities

$$σ ≤ C_1(x)x − C_2(x)x ≤ C_d(x)x$$  

(25.1)

always hold where $C_d(x)x$ is the number of elements of the odd number set $D$.

26 Theorem of Polignac primes

**Theorem 26.1 (Theorem of Polignac primes)** For every number $x$ greater than a positive number $x_0$, let $π_{2k}(x)$ be the number of pairs of odd primes $p$ and $p + 2k$ which may not be consecutive for $k > 2$ such that $p ≤ x$ and $1 ≤ k ≤ √x$, and let $τ_{2k}(x) = π_{2k}(x) − π_{2k}(√x)$, then for large numbers $x$, the inequalities

$$τ_{2k}(x) ≥ a_{2k} x \frac{x}{\log x} + b_{2k} \frac{π(√x)√x}{2 \log x} ≥ 1$$  

(26.1)

and

$$π_{2k}(x) ≥ a_{2k} x \frac{x}{\log x} + b_{2k} \frac{x}{\log^3 x}$$  

(26.2)

always hold where $a_{2k}$ and $b_{2k}$ are positive constants dependent of the number $k$.

**Proof** Let $2k = 6m_2k + r_{2k}$. Then for $p = 6m + 1$ we have

$$2k + p = 6m_2k + r_{2k} + (6m + 1) = \begin{cases} 6(m_{2k} + m) + 1 & \text{for } r_{2k} = 0 \\ 6(m_{2k} + m) + 3 & \text{for } r_{2k} = 2 \\ 6(m_{2k} + m + 1) − 1 & \text{for } r_{2k} = 4 \end{cases}$$

and for $p = 6m − 1$ we have

$$2k + p = 6m_2k + r_{2k} + (6m − 1) = \begin{cases} 6(m_{2k} + m) − 1 & \text{for } r_{2k} = 0 \\ 6(m_{2k} + m) + 1 & \text{for } r_{2k} = 2 \\ 6(m_{2k} + m) + 3 & \text{for } r_{2k} = 4. \end{cases}$$

Thus for $\min Q_u > √x$ and $\min Q_v > √x$, we can let $D^*$ denote a set of odd numbers where

$$D^* = \begin{cases} \{d_i|d_i = 2k + p_{n+i}, p_{n+i} ∈ P, i = 1, 2, \ldots, r\}, r = π(x) − π(√x) & \text{for } r_{2k} = 0 \\ \{d|d = 2k + q_i, q_i ∈ Q_u, i = 1, 2, \ldots, r_u\}, r_u ≈ r/2 & \text{for } r_{2k} = 2 \\ \{d|d = 2k + q_i, q_i ∈ Q_v, i = 1, 2, \ldots, r_v\}, r_v ≈ r/2 & \text{for } r_{2k} = 4 \end{cases}$$

for $1 ≤ k ≤ √x$. Thus there are

$$d_i ≤ x + 2√x < (√x + 1)^2 \text{ for } i = 1, 2, \ldots, r.$$
By Theorem (25.1) for \( C_d(x) = [\pi(x) - \pi(\sqrt{x})]/x \), the number of odd composite numbers \( d_i \) is at most equal to \( \sigma \). Then we have

\[
\begin{align*}
\tau_{2k}(x) &= [\pi(x) - \pi(\sqrt{x})] - \sigma \\
&\geq C_d(x) x - [C_1(x) x - C_2(x)\pi(\sqrt{x})\sqrt{x}] \\
&= [C_d(x) - C_1(x)] x + C_2(x)\pi(\sqrt{x})\sqrt{x} \\
&= a_{2k}(x) x + b_{2k}(x)\pi(\sqrt{x})\sqrt{x}/2
\end{align*}
\]

and

\[
\rho_{2k}(x) = \frac{\tau_{2k}(x)}{x/\log^2 x}
\]

\[
\geq a_{2k}(x)\log^2 x + b_{2k}(x)\frac{\pi(\sqrt{x})}{\sqrt{x}/\log x}\log x
\]

\[
\sim \rho^*_{2k}(x) = a_{2k}(x)\log^2 x + b_{2k}(x)\log x
\]

where

\[
a_{2k}(x) = C_d(x) - C_1(x) \quad \text{and} \quad b_{2k}(x) = 2C_2(x)
\]

are dependent of the number \( k \) and the variable \( x \).

Since \( \rho_{2k}(x) \) can not be negative and \( \pi(x)/x \) is stationarily decreased and tends to zero when \( x \) is increased such that \( \tau_{2k}(x)/x \) is stationarily decreased and tends to zero when \( x \) is increased, thus \( \rho_{2k}(x) \) should be stationarily decreased and tend to a limiting value when \( x \) is increased such that \( a_{2k}(x) \) and \( b_{2k}(x) \) must be decreased and tend to zero when \( x \) is increased.

Shan-Guang Tan (2013) proved that for any even number \( 2k \) there are infinitely many pairs of consecutive primes \( p \) and \( p + 2k \). Thus there must be

\[0 < a_{2k}(x) < C_d(x) \quad \text{and} \quad \lim_{x \to \infty} a_{2k}(x) = 0\]

so that \( a_{2k}(x) \) and \( \rho_{2k}(x) \) are always greater than zero for \( x < \infty \).

Hence by the form of the function \( \rho^*_{2k}(x) \) we can let

\[a_{2k} = a_{2k}(x)\log^2 x \quad \text{and} \quad b_{2k} = b_{2k}(x)\log^2 x\]

then there is \( a_{2k} > 0 \) and \( \rho^*_{2k}(x) \) becomes

\[
\rho^*_{2k}(x) = a_{2k} + b_{2k}/\log x.
\]

Since \( a_{2k} > 0 \) then \( b_{2k} \) should be greater than zero otherwise \( \tau_{2k}(x)/x \) will be stationarily increased when \( x \) is increased. Thus \( a_{2k} \) and \( b_{2k} \) are positive constants dependent of the number \( k \).

Hence a positive number \( x_0 \) always exists such that for \( x > x_0 \) the inequalities

\[
\tau_{2k}(x) \geq a_{2k} \frac{x}{\log^2 x} + b_{2k} \frac{\pi(\sqrt{x})\sqrt{x}}{2\log^2 x} \geq 1
\]

always hold and at least one \( d_i \) can not be composite so that \( d_i = p_{n+1} + 2k \) must be a prime in the region \( (\sqrt{x}, x + 2k) \) for \( x > x_0 \geq 4 \).

Hence in the region \( (\sqrt{x}, x + 2k) \) where \( x > x_0 \) and \( 1 \leq k \leq \sqrt{x} \), there are always pairs of odd primes \( p \) and \( p + 2k \) which may not be consecutive for \( k > 2 \).
Then for large numbers $x$ we have

$$
\pi_{2k}(x) = \tau_{2k}(x) + \pi_{2k}(\sqrt{x})
$$

$$
\geq a_{2k}(x)x + b_{2k}(x)\pi(\sqrt{x})\sqrt{x}/2 + \pi_{2k}(\sqrt{x})
$$

$$
\sim a_{2k}(x)\frac{x}{\log^2 x} + b_{2k}(x)\frac{x}{\log^3 x}
$$

and

$$
\eta_{2k}(x) = \frac{\pi_{2k}(x)}{a_{2k}/\log^2 x}
$$

$$
\geq a_{2k}(x)\frac{\log^2 x}{a_{2k}} + b_{2k}(x)\frac{\pi(\sqrt{x})\sqrt{x}/\log x}{a_{2k}} + \frac{4}{a_{2k}\sqrt{x}\sqrt{x}/\log^2 x}
$$

$$
\sim \eta_{2k}^*(x) = 1 + \frac{b_{2k}^*}{\log x}
$$

where $b_{2k}^* = b_{2k}/a_{2k}$.

Hence we have

$$
\lim_{x \to \infty} \eta_{2k}(x) = \lim_{x \to \infty} \eta_{2k}^*(x) = 1.
$$

This completes the proof of the theorem.

By calculation, there are approximately

$$
2\Pi_2 = 2\Pi_2 \cdot 2.18 \quad \text{for } k = 1, 2, 4, 8
$$

$$
4\Pi_2 = 4\Pi_2 \cdot 2.18 \quad \text{for } k = 3, 6, 9
$$

$$
a_{2k} = \left\{ \begin{array}{l}
\frac{4}{3}\Pi_2 \quad \text{and } b_{2k} = \left\{ \begin{array}{l}
\frac{4}{3}\Pi_2 \cdot 2.25 \quad \text{for } k = 5

\frac{2}{3}\Pi_2 \cdot 2.25 \quad \text{for } k = 7

\beta_{2k}\Pi_2 \quad \text{for } 10 \leq k \leq 78
\end{array} \right.
\end{array} \right.
$$

where $\Pi_2$ is the twin primes constant, $\alpha_{2k}$ and $\beta_{2k}$ are positive constants. Thus $a_{2k}$ and $b_{2k}$ are positive constants for $1 \leq k \leq 78$.

**Theorem 26.2** (Theorem of the difference of two primes)  
Every even number can be expressed as the difference of infinite pairs of two primes.

**Proof**  
By Theorem (26.1) there are an infinite number of pairs of odd primes $p$ and $p + 2k$ for every even number $2k$.

Thus every even number can be expressed as the difference of infinite pairs of two primes.

This completes the proof of the theorem.

27 Theorems of the number of Polignac primes

In this subsection, we will give out and prove theorems of prime pair numbers for $\pi_{2k}(x)$, the number of Polignac primes.

**Theorem 27.1** (Bounds theorem of prime pair numbers)  
For any positive number $x$, a positive number $N$ always exists such that the inequalities

$$
\pi_{2k}^*(x, N) \leq \pi_{2k}(x) < \pi_{2k}^*(x, N + 1)
$$

hold where

$$
\pi_{2k}^*(x, N) = a_{2k} \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}
$$

(27.1)
and
\[ \lim_{x \to \infty} \frac{\pi_{2k}(x)}{a_{2k}x / \log^2 x} = 1. \] (27.3)

**Proof** By the proof of Theorem (26.1) we have
\[ a_{2k} \pi(\sqrt{x}) \sim \pi_{2k}(\sqrt{x}) \log \sqrt{x}, \]
\[ \pi_{2k}(x) \geq a_{2k}(x) x + b_{2k}(x) \pi(\sqrt{x}) \sqrt{x} / 2 + \pi_{2k}(\sqrt{x}) \]
\[ \sim a_{2k} \frac{x}{\log^2 x} [1 + \frac{b_{2k} \eta_{2k}(\sqrt{x})}{a_{2k} \log x}] \]

and
\[ \lim_{x \to \infty} \eta_{2k}(x) = \lim_{x \to \infty} \eta_{2k}^2(x) = 1. \]

Then for large numbers \( x \) we have
\[ \eta_{2k}(x) = \frac{\pi_{2k}(x)}{a_{2k}x / \log^2 x} \geq 1 + b_{2k}^* \frac{\eta_{2k}(\sqrt{x})}{\log x}. \] (27.4)

First since there is
\[ \eta_{2k}(x) \geq 1 \]
then we can set
\[ \eta_{2k}(x) = 1 + \delta_1(x) \]
and substitute it into Inequality (27.4), thus we have
\[ 1 + \delta_1(x) \geq 1 + b_{2k}^* \frac{1 + \delta_1(\sqrt{x})}{\log x} \]
\[ = 1 + b_{2k}^* \frac{1}{\log x} + b_{2k}^* \frac{\delta_1(\sqrt{x})}{\log x} \]
such that we obtain
\[ \delta_1(x) \geq b_{2k}^* \frac{1}{\log x} + b_{2k}^* \frac{\delta_1(\sqrt{x})}{\log x} \] (27.5)
and can set
\[ \delta_1(x) = \frac{2!}{\log x} + \delta_2(x). \] (27.6)

Second by substituting \( \delta_1(x) \) into Inequality (27.4), we have
\[ \frac{2!}{\log x} + \delta_2(x) \geq b_{2k}^* \frac{1}{\log x} + b_{2k}^* \frac{2!}{\log \sqrt{x} + \delta_2(\sqrt{x})} \]
\[ = b_{2k}^* \frac{1}{2 \log x} + b_{2k}^* \frac{2!}{3 \log^2 x} + b_{2k}^* \frac{\delta_2(\sqrt{x})}{\log x} \]
such that we obtain
\[ \delta_2(x) \geq (b_{2k}^* \frac{1}{2} - 1) \frac{2!}{\log x} + b_{2k}^* \frac{2!}{3 \log^2 x} + b_{2k}^* \frac{\delta_2(\sqrt{x})}{\log x} \] (27.7)
and can set
\[ \delta_2(x) = \frac{3!}{\log^2 x} + \delta_3(x). \] (27.8)
Third by substituting $\delta_2(x)$ into Inequality (27.7), we have
\[
\frac{3!}{\log^2 x} + \delta_3(x) \geq \sum_{m=1}^{1} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^1 3!}{3 \log^2 x} + b_{2k}^* \frac{3!}{\log^3 x} \log x + \frac{\delta_3(\sqrt{x})}{\log x}
\]
\[
= \sum_{m=1}^{1} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^1 2^2 4!}{4 \log^3 x} + b_{2k}^* \frac{3!}{\log^3 x} \log x + b_{2k}^* \delta_3(\sqrt{x}) \log x
\]
such that we obtain
\[
\delta_3(x) \geq \sum_{m=1}^{2} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^2 4!}{4 \log^3 x} + b_{2k}^* \delta_3(\sqrt{x}) \log x
\] (27.9)
and can set
\[
\delta_3(x) = \frac{4!}{\log^2 x}. \quad (27.10)
\]

Forth by substituting $\delta_3(x)$ into Inequality (27.9), we have
\[
\frac{4!}{\log^2 x} + \delta_4(x) \geq \sum_{m=1}^{2} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^2 4!}{4 \log^3 x} + b_{2k}^* \frac{4!}{\log^3 x} \log x + \frac{\delta_4(\sqrt{x})}{\log x}
\]
\[
= \sum_{m=1}^{2} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^2 2^3 5!}{5 \log^4 x} + b_{2k}^* \frac{4!}{\log^3 x} \log x + b_{2k}^* \delta_4(\sqrt{x}) \log x
\]
such that we obtain
\[
\delta_4(x) \geq \sum_{m=1}^{3} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^3 5!}{5 \log^4 x} + b_{2k}^* \delta_4(\sqrt{x}) \log x
\] (27.11)
and can set
\[
\delta_4(x) = \frac{5!}{\log^3 x}. \quad (27.12)
\]

Fifth by substituting $\delta_4(x)$ into Inequality (27.11), we have
\[
\frac{5!}{\log^3 x} + \delta_5(x) \geq \sum_{m=1}^{3} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^3 5!}{5 \log^4 x} + b_{2k}^* \frac{5!}{\log^4 x} \log x + \frac{\delta_5(\sqrt{x})}{\log x}
\]
\[
= \sum_{m=1}^{3} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^3 5!}{5 \log^4 x} + b_{2k}^* \frac{5!}{\log^4 x} \log x + b_{2k}^* \delta_5(\sqrt{x}) \log x
\]
such that we obtain
\[
\delta_5(x) \geq \sum_{m=1}^{4} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^4 6!}{6 \log^5 x} + b_{2k}^* \delta_5(\sqrt{x}) \log x
\] (27.13)
and can set
\[
\delta_5(x) = \frac{6!}{\log^4 x}. \quad (27.14)
\]

Then by substituting $\delta_n(x)$ for $n = 1, 2, 3, 4, 5$ into the expression of $\eta_{2k}(x)$ we obtain
\[
\eta_{2k}(x) = 1 + \frac{2!}{\log x} + \frac{3!}{\log^2 x} + \frac{4!}{\log^3 x} + \frac{5!}{\log^4 x} + \frac{6!}{\log^5 x} + \delta_6(x) = \sum_{n=1}^{6} \frac{n!}{\log^{n-1} x} + \delta_6(x).
\]
Going on in the same way for \( n = 6, 7, \cdots, N \) we have
\[
\delta_n(x) \geq \sum_{m=1}^{n-1} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} + b_{2k}^* \frac{2^{n-1}(n+1)!}{n+1 \log^n x} + b_{2k}^* \delta_n(\sqrt{x}) \tag{27.15}
\]
and can set
\[
\delta_n(x) = \frac{(n+1)!}{\log^n x} + \delta_{n+1}(x) \tag{27.16}
\]
such that we obtain
\[
\eta_{2k}(x) = \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x} + \delta_N(x). \tag{27.17}
\]
Since by Equality (27.16) for \( n = 1, 2, \cdots \) the inequality
\[
\delta_n(x) - \delta_{n+1}(x) = \frac{(n+1)!}{\log^n x} > 0
\]
always holds then we have
\[
\delta_1(x) > \delta_2(x) > \cdots > \delta_N(x) > \delta_{N+1}(x) > \cdots
\]
Based on the Stirling’s formula
\[
n! = \sqrt{2\pi n} \left( \frac{n}{e} \right)^n e^{-\theta n}, 0 < \theta < 1
\]
for a fixed positive number \( x \), a positive number \( n_c \) always exists such that when \( n \geq n_c \) there are
\[
\frac{n}{e \log x} \geq 1 \quad \text{and} \quad \frac{n!}{\log^n x} > \sqrt{2\pi n} \left( \frac{n}{e \log x} \right)^n \geq \sqrt{2\pi n}.
\]
Then on the right hand side of the Inequality (27.15) there is
\[
\lim_{n \to \infty} \sum_{m=1}^{n-1} \left( b_{2k}^* \frac{2m-1}{m+1} - 1 \right) \frac{(m+1)!}{\log^m x} \to \infty.
\]
Thus there must be
\[
\lim_{n \to \infty} \delta_n(\sqrt{x}) \to -\infty
\]
such that there must be
\[
\lim_{n \to \infty} \delta_{n+1}(x) \to -\infty.
\]
Hence for any positive number \( x \), a positive number \( N \) always exists such that there are \( \delta_N(x) \geq 0 \) and \( \delta_{N+1}(x) < 0 \). Thus the inequalities
\[
\eta^*(x, N) \leq \eta_{2k}(x) < \eta^*(x, N+1)
\]
and
\[
\pi^*_2k(x, N) \leq \pi_{2k}(x) < \pi^*_2k(x, N+1)
\]
hold where
\[
\eta^*(x, N) = \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}
\]
and
\[
\pi^*_2k(x, N) = a_{2k} \frac{x}{\log^2 x} \eta^*(x, N) = a_{2k} \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}.
\]
Hence we have

$$\eta_{2k}(x) \sim \eta^*(x, N)$$

and

$$\lim_{x \to \infty} \eta_{2k}(x) = \lim_{x \to \infty} \eta^*(x, N) = 1.$$

This completes the proof of the theorem.

**Theorem 27.2** (Relation between \(x\) and \(N\)) Let \(\varphi(x, N) = (\log x)/(N + 3/2)\). Then there are approximately

$$\varphi(x, N) \leq \varphi^*(x) = 5.1 - 5.5 \frac{\log 10}{\log x}. \quad (27.18)$$

**Proof** By the proof of Theorem (27.1) let

$$\Delta(x, N) = \eta^*(x, N + 1) - \eta^*(x, N) = \frac{(N + 1)!}{\log (N + 1) x}.$$

Then we have

$$\varphi(x, N) = \frac{N + 1}{N + 3/2} \frac{\Delta(x, N - 1)}{\Delta(x, N)}.$$

When \(x\) is increased, since \(\eta^*(x, M)\) for \(M = N - 1, N, N + 1\) are decreased and tend to 1, then \(\Delta(x, N - 1)\) and \(\Delta(x, N)\) are also decreased and tend to zero. Since \(N + 1 < \log x\) and \(\Delta(x, N) < \Delta(x, N - 1)\), then \(\Delta(x, N)/\Delta(x, N - 1)\) is also decreased and tends to a limiting value when \(x\) is increased. Thus \(\varphi(x, N)\) should be increased and tend to a limiting value when \(x\) is increased.

Without loss of generality we can assume that \(\varphi(x, N)\) satisfies

$$\varphi(x, N) \leq \varphi^*(x) \text{ and } \varphi^*(x) = \alpha - \beta/\log x$$

where \(\alpha\) and \(\beta\) are positive constants.

By calculation \(\alpha\) and \(\beta\) are approximately equal to 5.1 and 5.5 log 10, respectively. Then there are approximately

$$\varphi(x, N) \leq \varphi^*(x) = 5.1 - 5.5 \frac{\log 10}{\log x}$$

and

$$\lim_{N \to \infty} \varphi(x, N) \leq \lim_{N \to \infty} \varphi^*(x) = 5.1.$$

This completes the proof of the theorem.

**Theorem 27.3** (Upper bound theorem of prime pair number gaps) For any small positive value \(\epsilon(x)\), a pair of positive numbers \(x\) and \(N\) always exist such that the bounds gap of prime numbers

$$g(x, N) = \pi_{2k}(x, N + 1) - \pi_{2k}^*(x, N) \leq \epsilon(x) \frac{a_{2k} x}{\log^2 x} \quad (27.19)$$

and for any positive number \(x\), \(\pi_{2k}(x)\) satisfies

$$\pi_{2k}(x) - \pi_{2k}^*(x, N) < g(x, N) \leq \epsilon(x) \frac{a_{2k} x}{\log^2 x} \quad (27.20)$$

where \(a_{2k}\) is a positive constant dependent of the number \(k\),

$$\pi_{2k}^*(x, N) \leq \pi_{2k}(x) < \pi_{2k}^*(x, N + 1)$$
and
\[ \pi_{2k}^*(x, N) = a_{2k} \frac{x}{\log^2 x} \sum_{n=1}^{N} \frac{n!}{\log^{n-1} x}. \]

Especially \( \epsilon(x) \) can be equal to \( x^{-1/2} \log^{5/2} x \) such that
\[ g(x, N) \leq a_{2k} (x \log x)^{1/2} \]  
(27.21)
and for any positive number \( x \)
\[ \pi_{2k}(x) - \pi_{2k}^*(x, N) < a_{2k} (x \log x)^{1/2}. \]  
(27.22)

**Proof** By the proof of Theorem (27.1) when \( \pi_{2k}(x) \) satisfies
\[ \pi_{2k}^*(x, N) \leq \pi_{2k}(x) < \pi_{2k}^*(x, N+1) \]
then there is
\[ \Delta(x, N) = \frac{g(x, N)}{a_{2k} x/\log^2 x} = \eta^*(x, N+1) - \eta^*(x, N) = \frac{(N+1)!}{\log^N x}. \]

For any small positive value \( \epsilon(x) \), a pair of positive numbers \( x \) and \( N \) can be determined by Theorem (27.2) and the inequality
\[ \Delta(x, N) \leq \epsilon(x) \text{ or } \frac{(N+1)!}{\log^N x} \leq \epsilon(x). \]

Thus for any positive number \( x \), \( \pi_{2k}(x) \) satisfies
\[ \pi_{2k}(x) - \pi_{2k}^*(x, N) < g(x, N) \leq \epsilon(x) \frac{a_{2k} x}{\log^2 x}. \]

Based on the Stirling’s formula
\[ n! = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{1/12n}, 0 < \theta < 1 \]
for \( x \geq 10^5 \) such that \( \log x > e\sqrt{2\pi e} \) there are
\[ (N+1)! < e\sqrt{2\pi e} \left(\frac{N+1}{e}\right)^{N+3/2} \]
and
\[ \log^{N+5/2} x \frac{x}{(N+1)!} \geq \log x \left(\frac{e \log x}{N+1}\right)^{N+3/2} > \left(\frac{e \log x}{N+3/2}\right)^{N+3/2}. \]

Since a pair of positive numbers \( x \) and \( N \) always exists, let
\[ \phi(x, N) = (\log x)/(N+3/2). \]

Then we have
\[ \log \frac{\log^{N+5/2} x}{(N+1)! \sqrt{x}} > (N + 3/2) \log\left[\frac{e \log x}{N + 3/2}\right] - \frac{1}{2} \log x \]
\[ = (N + 3/2)[1 + \log \phi(x, N) - \phi(x, N)/2]. \]

Since the inequality
\[ 1 + \log \phi(x, N) - \phi(x, N)/2 > 0 \]
holds for \( \varphi(x, N) \leq 5.3566938 \), thus by Theorem (27.2) the inequality \( \varphi(x, N) \leq 5.1 \) holds or let \( \varphi(x, N) \leq 5.3566938 \) for calculation of \( \pi^*_k(x, N) \) such that we obtain

\[
\log^{N+5/2} x > \sqrt{x} \quad \text{and} \quad \frac{(N + 1)!}{\log^N x} < \frac{\log^{5/2} x}{\sqrt{x}}.
\]

When we let \( \epsilon(x) = x^{-1/2} \log^{5/2} x \), a pair of positive numbers \( x \) and \( N \) can be determined by Theorem (27.2) or the inequality \( \varphi(x, N) \leq 5.3566938 \) such that the inequality

\[
\frac{(N + 1)!}{\log^N x} \leq \frac{\log^{5/2} x}{\sqrt{x}}
\]

holds so that for any positive number \( x \), \( \pi_{2k}(x) \) satisfies

\[
\pi_{2k}(x) - \pi^*_k(x, N) < 2k \log x, N \leq \frac{\log^{5/2} x}{\sqrt{x}} a_{2k} x^2 = a_{2k}(x \log x)^{1/2}.
\]

This completes the proof of the theorem.

**Theorem 27.4** (Prime pair number theorem) For large numbers \( x \), \( \pi_{2k}(x) \) is asymptotically equal to

\[
\pi_{2k}(x) = a_{2k} L_2(x) + O(\sqrt{x \log x}) \quad \text{where} \quad L_2(x) = \int_2^x \frac{dt}{\log^2 t} \quad (27.23)
\]

**Proof** Note that \( L_2(x) \) has the asymptotic expansion about \( \infty \) of

\[
L_2(x) = \int_2^x \frac{dt}{\log^2 t} = li_2(x) - li_2(2) \sim li_2(x) \quad (27.24)
\]

where

\[
li_2(x) = \sum_{n=1}^{\infty} \frac{n!x}{\log^{n+1} x} = \frac{x}{\log^2 x} \sum_{n=1}^{\infty} \frac{n!}{\log^{n-1} x}.
\]

By the proof of Theorem (27.3) for any positive number \( x \), a positive number \( N \) always exists such that \( \pi_{2k}(x) \) satisfies

\[
\pi_{2k}(x) - \pi^*_k(x, N) < g(x, N) \leq a_{2k}(x \log x)^{1/2}.
\]

Hence when positive numbers \( N \to \infty \) and \( x \to \infty \), we have

\[
|\pi_{2k}(x) - a_{2k} li_2(x)| = |\pi_{2k}(x) - \lim_{N \to \infty} \pi^*_k(x, N)|
\]

\[
< \lim_{N \to \infty} g(x, N) \leq a_{2k}(x \log x)^{1/2}
\]

so that we obtain

\[
\pi_{2k}(x) = a_{2k} L_2(x) + O(\sqrt{x \log x}).
\]

This completes the proof of the theorem.

**References**

[1] Wapedia - Wiki, Polignac’s conjecture.
[2] Wapedia - Wiki, Twin primes conjecture.
[3] Weisstein, Eric W., Twin primes. MathWorld.
[4] Marek Wolf, On the Twin and Cousin Primes. IFTUWr 909/96, August,1996.
[5] Shan-Guang Tan, On the representation of even numbers as the sum of two odd primes and the distribution of primes in short intervals. [arXiv:1110.3465](http://arxiv.org/abs/1110.3465)
Part VII

On the generalization of Eisenstein’s criterion

Abstract  The generalization of Eisenstein’s criterion of irreducible polynomials over the field $\mathbb{Q}$ of rational numbers was investigated in this paper. Firstly, if a polynomial

$$F(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$$

can not be written as

$$F(Y) = a_{k+d}Y^k + a_{(k-1)d}Y^{k-1} + \cdots + a_dY + a_0 \in \mathbb{Z}[Y]$$

by defining $Y = X^d$ where $k \cdot d = n$, $k$ and $d$ are positive integers greater than 1, then $F(X)$ can be called a fundamental polynomial. Secondly, theorems were proved and state:

1. For any number $n$ and a fundamental polynomial $F(X)$, if there exist a prime $p$ and a positive number $r$ such that $2 \nmid r$ or $2 \mid n, r < n$, $p \nmid a_n, p^r \mid a_i (i = 0, 1, \cdots, n-1)$ and $p^{r+1} \nmid a_0$, then $F(X)$ is irreducible over the field $\mathbb{Q}[X]$ of rational numbers.

2. For any number $n$, a polynomial $F(X)$ is irreducible over the field $\mathbb{Q}[X]$ of rational numbers if and only if all of its fundamental polynomials are irreducible over the field $\mathbb{Q}[X]$ of rational numbers.

To prove the first theorem, a main assumption that a fundamental polynomial $F(X) = g(X)h(X)$ and some definitions are made. Then for all different cases, reductions to absurdity are derived so that the assumption that the fundamental polynomial $F(X) = g(X)h(X)$ is proved false. Hence the theorem holds.

Keywords  algebra, polynomial, irreducible, Eisenstein’s criterion

28 Introduction

Eisenstein’s criterion of irreducible polynomials over the field $\mathbb{Q}$ of rational numbers is well known and important in Algebra and Number theory. It states: For any number $n$, assume

$$F(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X],$$

if there exist a prime $p$, $p \nmid a_n, p|a_i (i = 0, 1, \cdots, n-1)$ and $p^2 \nmid a_0$, then $F(X)$ is irreducible over the field $\mathbb{Q}[X]$ of rational numbers.

If a polynomial $F(X)$ can not be written as

$$F(Y) = a_{k+d}Y^k + a_{(k-1)d}Y^{k-1} + \cdots + a_dY + a_0 \in \mathbb{Z}[Y]$$

...
by defining $Y = X^d$ where $k \cdot d = n$, $k$ and $d$ are positive integers greater than 1, then $F(X)$ can be called a fundamental polynomial.

The generalization of Eisenstein’s criterion of irreducible polynomials over the field $Q$ of rational numbers was investigated and theorems were proved in this paper, which state:

1. For any number $n$, assume a fundamental polynomial

$$F(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in Z[X],$$

if there exist a prime $p$ and a positive number $r$ such that $2 \nmid r$ or $2 \nmid n$, $r < n$, $p \nmid a_n$, $p^r|a_i (i = 0, 1, \cdots, n - 1)$ and $p^{r+1} \nmid a_0$, then $F(X)$ is irreducible over the field $Q[X]$ of rational numbers.

2. For any number $n$, a polynomial $F(X)$ is irreducible over the field $Q[X]$ of rational numbers if and only if all of its fundamental polynomials are irreducible over the field $Q[X]$ of rational numbers.

To prove the first theorem, a main assumption that a fundamental polynomial $F(X) = g(X)h(X)$ and some definitions are made firstly. Then for all different cases, reductions to absurdity are derived so that the assumption that the fundamental polynomial $F(X) = g(X)h(X)$ is proved false. Hence the theorem holds.

29 Definitions

Definition 29.1 (Main assumption) For any number $n$, assume a fundamental polynomial

$$F(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in Z[X]$$

is reducible over the field $Q[X]$ of rational numbers when there exist a prime $p$ and a positive number $r$ such that $p \nmid a_n$, $p^r|a_i (i = 0, 1, \cdots, n - 1)$ and $p^{r+1} \nmid a_0$.

Thus we can write $F(X) = g(X)h(X)$ where

$$g(X) = g_mX^m + g_{m-1}X^{m-1} + \cdots + g_1X + g_0$$

and

$$h(X) = h_lX^l + h_{l-1}X^{l-1} + \cdots + h_1X + h_0$$

are not constants.

Definition 29.2 Based on the main assumption [29.1], let write

$$g_i = \alpha_ip^{\delta_i} \quad \text{for} \ i = 0, 1, \cdots, m,$$

$$h_j = \beta_jp^{\gamma_j} \quad \text{for} \ j = 0, 1, \cdots, l,$$

where $p \nmid \alpha_i$ and $p \nmid \beta_j$.

Let $m_p$ denote the number of elements in a set

$$G_p = \{s_i | s_i > 0, i = 0, 1, \cdots, m_p - 1\}$$

and $l_p$ denote the number of elements in a set

$$H_p = \{r_i | r_i > 0, i = 0, 1, \cdots, l_p - 1\}.$$

Since $p^{r+1} \nmid a_0 = g_0h_0$, let $p^{s_1}g_0$ and $p^{r-s}|h_0$ where $r - s \leq \lfloor r/2 \rfloor \leq s \leq r$. Thus we can write $s_0 = s$ and $r_0 = r - s$. 
Thus by the main assumption (29.1) for \( k = 0, 1, \cdots, n - 1 \), there are

\[
a_k = \sum_{i=i_0}^{k} g_{k-i}h_i = \sum_{i=i_0}^{k} \alpha_{k-i} \beta_i p^{s_{k-i}+r_i},
\]

(29.2)

for \( m \leq l \) where

\[
i_0 = 0 \quad \text{for} \ k = 1, 2, \cdots, m \\
i_0 = k - m \quad \text{for} \ k = m + 1, m + 2, \cdots, l \\
i_0 = k - m + (k - l) \quad \text{for} \ k = l + 1, l + 2, \cdots, n - 1
\]

and

\[
a_k = \sum_{i=i_0}^{k} g_i h_{k-i} = \sum_{i=i_0}^{k} \alpha_i \beta_{k-i} p^{s_i + r_{k-i}},
\]

(29.3)

for \( l \leq m \) where

\[
i_0 = 0 \quad \text{for} \ k = 1, 2, \cdots, l \\
i_0 = k - l \quad \text{for} \ k = l + 1, l + 2, \cdots, m \\
i_0 = k - l + (k - m) \quad \text{for} \ k = m + 1, m + 2, \cdots, n - 1
\]

Definition 29.3 By the main assumption (29.1), Definition (29.2) and Eqs. (29.2-29.3) for \( k = 1, 2, \cdots, n - 1 \), let \( t_{k,i} \) denote the powers of the prime \( p \) in each product as

\[
s_{k-i} + r_i = t_{k,i} \quad \text{for} \ m \leq l,
\]

\[
s_i + r_{k-i} = t_{k,i} \quad \text{for} \ m \geq l
\]

and if the powers of the prime \( p \) in each product are same then let \( t_k \) denote the same powers of the prime \( p \) in each product as

\[
s_{k-i} + r_i = t_{k,i} = t_k \quad \text{for} \ m \leq l,
\]

\[
s_i + r_{k-i} = t_{k,i} = t_k \quad \text{for} \ m \geq l
\]

Let \( e_t \) denote the number of elements of a set

\[E_k = \{ k | t_k \leq r, 1 \leq k \leq n - 1 \}.\]

Let \( n_t \) denote the number of elements of a set

\[N_k = \{ k | k = 1, 2, \cdots, n - 1 \} \setminus E_k.\]

Since \( p^r | g_0h_1 + g_1h_0 \), there should be \( s_0 + r_1 = s_1 + r_0 \). Also if \( s_m + r_{l-1} \neq s_{m-1} + r_l \) then there will be \( p | g_m \) or \( p | h_l \) such that \( p | g_mh_l = a_n \). A contradiction.

Thus there must be \( 2 \leq e_t \leq n - 1 \).

30 Lemmas of fundamental polynomials

Lemma 30.1 There must be \( m_p = m \) and \( l_p = l \) in the main assumption (29.1) and Definition (29.2).
Proof. By the main assumption (29.1) and Definition (29.2), since $p'|a_k(k=0,1,\ldots,n-1)$, by Eqs. (29.2-29.3) for $k=1,2,\ldots,n-1$, there are

$$p'| \sum_{i=0}^{k-1} g_{k-i}h_i \quad \text{for } m \leq l$$

For $k=m_p+l_p$, if $k=m_p+l_p \leq \min\{m,l\}$ then there is

$$p'| \sum_{i=0}^{m-1} g_ih_{k-i} = \sum_{i=0}^{m_p-1} g_ih_{k-i} + g_{m_p}h_{l_p} + \sum_{i=m_p+1}^{k} g_{k-i}h_i$$

else if $m < l$ then there is

$$p'| \sum_{i=0}^{m-1} g_ih_{k-i} = \sum_{i=0}^{m_p-1} g_ih_{k-i} + g_{m_p}h_{l_p} + \sum_{i=m_p+1}^{m-1} g_ih_{k-i}$$

else there is

$$p'| \sum_{i=0}^{l-1} g_ih_{k-i} = \sum_{i=0}^{l_p-1} g_ih_{k-i} + g_{l_p}h_{l_p} + \sum_{i=l_p+1}^{l-1} g_ih_{k-i}$$

Since $p|g_i$ for $i=0,1,2,\ldots,m_p-1$ and $p|h_j$ for $j=0,1,2,\ldots,l_p-1$, thus if $l_p < l$ then there must be $p|g_{m_p}$ until $m_p = m$ so that there are $p|g_m$ and $p|g_mh_l = a_n$. A contradiction.

For instance, when $r = s = 1$ and $p|g_0$, then there must be $l_p = 0$ so that there are $p|g_m$ and $p|g_mh_l = a_n$. Hence $F(X)$ is irreducible over the field $Q[X]$ of rational numbers. This is the Eisenstein’s criterion.

Thus in the assumption that $F(X) = g(X)h(X)$, there must be $m_p = m$ and $l_p = l$.

The proof of the lemma is completed.

Lemma 30.2. By definitions (29.3-29.3), when $e_t = n - 1$, the main assumption (29.1) holds only if $n|r$.

Proof. When $e_t = n - 1$, by Eqs. (29.2-29.3) for $k=1,2,\ldots,n-1$, there are

$$s_{k-i} + r_i = t_k \quad \text{for } m \leq l,$$

$$s_i + r_{k-i} = t_k \quad \text{for } m \geq l.$$ (30.1)

Thus for $k = n - 1$, there are

$$s_{m-1} + r_l = s_m + r_{l-1} = t_{n-1}.$$ (30.1)

If $s_m > 0$ or $r_l > 0$ then there is $p|g_m$ or $p|h_l$ so that there is $p|g_mh_l = a_n$. A contradiction.

When $r_l = s_m = 0$, then by Eqs. (30.1) for $k = n - j$ and $j = 1,2,\ldots,n$, there are

$$s_{n-j-i} + r_i = t_{n-j} \quad \text{for } m \leq l,$$

$$s_i + r_{n-j-i} = t_{n-j} \quad \text{for } m \geq l.$$ (30.1)

Without loss of generality, let consider the case of $m \leq l.$
Lemma 30.3

For \( j = 1, 2, \cdots, n \) there are

\[
\begin{align*}
    s_{m-1} &= r_{t-1} = t_{n-1}, \\
    s_{m-2} &= s_{m-1} + r_{t-1} = r_{t-2} = t_{n-2} = 2t_{n-1}, \\
    s_{m-3} &= s_{m-2} + r_{t-1} = s_{m-1} + r_{t-2} = r_{t-3} = t_{n-3} = 3t_{n-1}, \\
    & \vdots \\
    s_0 &= s_1 + r_{t-1} = \cdots = s_{m-1} + r_{t-m+1} = r_{t-m} = t_{n-m} = t_l = m \cdot t_{n-1}, \\
    s_0 + r_{t-1} &= s_1 + r_{t-2} = \cdots = s_{m-1} + r_{t-m} = r_{t-m-1} = t_{l-1} = (m+1) \cdot t_{n-1}, \\
    & \vdots \\
    s_0 + r_m &= s_1 + r_{m-1} = \cdots = s_{m-1} + r_0 = t_m = l \cdot t_{n-1}, \\
    s_0 + r_{m-1} &= s_1 + r_{m-2} = \cdots = s_{m-2} + r_1 = s_{m-1} + r_0 = t_{m-1} = (l+1) \cdot t_{n-1}, \\
    & \vdots \\
    s_0 + r_2 &= s_1 + r_1 = s_2 + r_0 = t_2 = (n-2) \cdot t_{n-1}, \\
    s_0 + r_1 &= s_1 + r_0 = t_1 = (n-1) \cdot t_{n-1}, \\
    s_0 + r_0 &= t_0 = n \cdot t_{n-1}.
\end{align*}
\]

Hence we have \( n\mid t_0 = r \) so that the main assumption (29.1) holds only if \( n\mid r \).

The proof of the lemma is completed.

Lemma 30.3 By definitions (29.2), (29.3), when \( e_t = 2 \), the main assumption (29.1) holds only if \( r_0 = s_0 \) and \( m = l \) for \( g(X) \) and \( h(X) \).

Proof When \( e_t = 2 \), there are

\[
    s_{m-1} + r_t = s_m + r_{t-1} = t_{n-1} \quad \text{and} \quad s_1 + r_0 = s_0 + r_1 = t_1.
\]

If \( s_m > 0 \) or \( r_1 > 0 \) then there is \( p\mid g_m \) or \( p\mid h_t \) so that there is \( p\mid g_m h_t = a_n \). A contradiction.

Without loss of generality, let consider the case of \( m \leq l \) and denote \( s_i = \lambda \cdot t_{n-1} \).

(1) Case of \( \lambda = 1 \).

(1.1) Let consider the case of all \( s_i = t_{n-1} \) for \( i < m \).

Similar to the proof of Lemma (30.2), when \( r_t = s_m = 0 \), there are

\[
\begin{align*}
    s_{m-1} &= r_{t-1} = t_{n-1}, \\
    s_{m-2} &= r_{t-2} = t_{n-1} < s_{m-1} + r_{t-1} = 2t_{n-1}, \\
    s_{m-3} &= r_{t-3} = t_{n-1} < s_{m-2} + r_{t-1} = s_{m-1} + r_{t-2} = 2t_{n-1}, \\
    & \vdots \\
    s_1 &= r_{t-m+1} = t_{n-1} < s_2 + r_{t-1} = \cdots = s_{m-1} + r_{t-m+2} = 2t_{n-1}, \\
    s_0 &= r_{t-m} = t_{n-1} < s_1 + r_{t-1} = \cdots = s_{m-1} + r_{t-m+1} = 2t_{n-1}.
\end{align*}
\]

If \( m = l \) then we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

Otherwise there will be \( r_{t-m-1} > 2t_{n-1} \) and \( r_i \geq 2t_{n-1} \) where \( i = 0, 1, \cdots, l - m - 2 \). On the other hand, since \( p\mid \sum_{i=0}^{k} g_{k-i} h_t \) and

\[
    s_0 = r_1 = \cdots = s_m = r_{t-m} = r_{t-m+1} = \cdots = r_{t-1} = t_{n-1},
\]
there should be at least two equalities \( s_{k-i} + r_i = 2t_{n-1} \) for each \( k < l \) where \( i_0 \leq i \leq k \). Therefore, there should be \( s_0 + r_1 = s_1 + r_0 = t_1 = 2t_{n-1} \) so that there are \( r_1 = t_{n-1} \) and \( r_0 = 2t_{n-1} - s_1 \). A contradiction. Thus there should be \( m = l \) so that we have \( s_0 = r_0 \) and 
\[
\begin{align*}
  r_0 + s_1 &= r_1 + s_0 = t_1.
\end{align*}
\]

(1.2) Let consider the case of at least one \( s_j = t_{n-1} \) where \( j < m - 1 \).

Similarly to the case of all \( s_i = t_{n-1} \) for \( i < m \), if \( m = l \) then we have \( s_0 = r_0 \) and 
\[
\begin{align*}
  r_0 + s_1 &= r_1 + s_0 = t_1.
\end{align*}
\]

Otherwise there will be \( r_i \geq 2t_{n-1} \) where \( i = 0, 1, \ldots, l - m - 1 \). On the other hand, since there is \( s_j + r_{j-1} = 2t_{n-1} \), there should be at least two equalities \( s_{k-i} + r_i = 2t_{n-1} \) for each \( k < l + j \) where \( i_0 \leq i \leq k \). Therefore, there should be \( s_0 + r_1 = s_1 + r_0 = t_1 = 2t_{n-1} \) so that there are \( r_1 = t_{n-1} \) and \( r_0 = 2t_{n-1} - s_1 \). A contradiction. Thus there should be \( m = l \) so that we have \( s_0 = r_0 \) and 
\[
\begin{align*}
  r_0 + s_1 &= r_1 + s_0 = t_1.
\end{align*}
\]

(2) Case of \( \lambda = 2 \).

(2.1) Let consider the case of all \( s_j = 2t_{n-1} \) where \( i < m - 1 \).

Similar to the proof of Lemma 30.2, when \( r_1 = s_m = 0 \), there are
\[
\begin{align*}
  s_{m-1} &= r_1 - t_{n-1},
  s_{m-2} &= s_{m-1} + r_{1-1} = 2t_{n-1} - t_{n-1},
  & \cdots
  s_0 &= r_m = 2t_{n-1} - s_1.
\end{align*}
\]

If \( m = l \) then we have \( s_0 = r_0 \) and 
\[
\begin{align*}
  r_0 + s_1 &= r_1 + s_0 = t_1.
\end{align*}
\]

Otherwise there will be \( r_i \geq 3t_{n-1} \) where \( i = 0, 1, \ldots, l - m - 1 \). On the other hand, since 
\[
\begin{align*}
  p^r \sum_{i=0}^k g_{k-i} h_i
\end{align*}
\]
there should be at least two equalities \( s_{k-i} + r_i = 4t_{n-1} \) for each \( k < l \) where \( i_0 \leq i \leq k \). Therefore, there should be \( s_0 + r_1 = s_1 + r_0 = t_1 = 4t_{n-1} \) so that there are \( r_1 = 2t_{n-1} \) and \( r_0 = 4t_{n-1} - s_1 \). A contradiction. Thus there should be \( m = l \) so that we have \( s_0 = r_0 \) and 
\[
\begin{align*}
  r_0 + s_1 &= r_1 + s_0 = t_1.
\end{align*}
\]

(2.2) Let consider the case of at least one \( s_j = 2t_{n-1} \) and all other \( s_i > 2t_{n-1} \) where \( j < m - 2, i < m - 2 \) and \( i \neq j \).

Similarly to the case of all \( s_i = 2t_{n-1} \) for \( i < m - 1 \), if \( m = l \) then we have \( s_0 = r_0 \) and 
\[
\begin{align*}
  r_0 + s_1 &= r_1 + s_0 = t_1.
\end{align*}
\]

Otherwise there will be \( r_i \geq 3t_{n-1} \) where \( i = 0, 1, \ldots, l - m - 1 \). On the other hand, since 
\[
\begin{align*}
  p^r \sum_{i=0}^k g_{k-i} h_i, \text{if } s_j = 2t_{n-1}, \text{ then there should be } r_{l-m+j} = 2t_{n-1} \text{ for } k = l + j.
\end{align*}
\]
there should be at least two equalities \( s_{k-i} + r_i = 4t_{n-1} \) for each \( k < l + j \) where \( i_0 \leq i \leq k \). Therefore, there should be \( s_0 + r_1 = s_1 + r_0 = t_1 = 4t_{n-1} \) so that there are \( r_1 = 2t_{n-1} \) and
representation of numbers and distribution of primes

83

\[ r_0 = 4t_{n-1} - s_1. \] A contradiction. Thus there should be \( m = l \) so that we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1. \)

(3) **Cases of** \( \lambda = 3, 4, \ldots, m - 1. \) Let continue in the same way above to consider the case of all \( s_i = \lambda \ast t_{n-1} \) where \( i < m - \lambda + 1 \) and the case of at least one \( s_j = \lambda \ast t_{n-1} \) where \( j < m - \lambda. \) Then we can get the result that the main assumption (29.1) holds only if \( r_0 = s_0 \) and \( m = l \) for \( g(X) \) and \( h(X). \)

The proof of the lemma is completed.

**Lemma 30.4** By definitions (29.2-29.3), when \( 2 < e_t < n - 1, \) the main assumption (29.1) holds only if \( r_0 = s_0 \) and \( m = l \) for \( g(X) \) and \( h(X). \) or \( r \geq n \ast t_{n-1}. \)

**Proof** When \( 2 < e_t < n - 1, \) if any \( k \in E_k \) except \( k = n - 1 \) is smaller than \( \min \{m, l\}, \) then similar to the proof of Lemma (30.3), the main assumption (29.1) holds only if \( r_0 = s_0 \) and \( m = l \) for \( g(X) \) and \( h(X). \)

Since \( 2 < e_t < n - 1, \) then there is \( n_t > 0, \) so that there is at least one number \( k_m = \max N_k. \) Without loss of generality, let consider the case of \( m \leq l. \)

(I) By the proof of Lemma (30.2), if any \( k \geq \min \{m, l\} \) is in \( E_k, \) then \( s_i \) for \( i = 0, 1, \ldots, m - 1 \) and \( r_j \) for \( j = 0, 1, \ldots, l - 1 \) are determined, so that any \( k < \min \{m, l\} \) will be in \( E_k. \) Thus there should be \( k_m \geq \min \{m, l\}. \)

(II) By the proof of Lemma (30.2), if \( m \leq k_m < l, \) then all \( s_i \) for \( i = 0, 1, \ldots, m - 1 \) are determined. Since all the sum of \( s_i + r_{k_m-i} \) for \( i = 0, 1, \ldots, m - 1 \) are same values, there will be \( s_i + r_{k_m-i} < r_{k_m-m}. \)

Let assume \( k \in E_k \) where \( k = l_0, l_0 + 1, \ldots, n - 1 \) and \( m < l_0 \leq l. \)
Similar to the proofs of lemmas [30.2, 30.3], when \( r_l = s_m = 0 \), there are

\[
\begin{align*}
  s_{m-1} &= r_{l-1} = t_{n-1}, \\
  s_{m-2} &= s_{m-1} + r_{l-1} = r_{l-2} = t_{n-2} = 2t_{n-1}, \\
  s_{m-3} &= s_{m-2} + r_{l-1} = s_{m-1} + r_{l-2} = r_{l-3} = t_{n-3} = 3t_{n-1}, \\
  &\quad \vdots \\
  s_0 &= s_1 + r_{l-1} = \cdots = s_{m-1} + r_{l-m+1} = r_{l-m} = t_{n-m} = t_l = m \cdot t_{n-1}, \\
  s_0 + r_{l-1} &= s_1 + r_{l-2} = \cdots = s_{m-1} + r_{l-m} = r_{l-m-1} = t_{l-1} = (m+1) \cdot t_{n-1}, \\
  &\quad \vdots \\
  s_0 + r_{l_0} &= s_1 + r_{l_0-1} = \cdots = s_{m-1} + r_{l_0-m+1} = r_{l_0-m} = t_{l_0} = (n-l_0) \cdot t_{n-1}, \\
  s_0 + r_{l_0-1} &= s_1 + r_{l_0-2} = \cdots = s_{m-2} + r_{l_0-m+1} = s_{m-1} + r_{l_0-m} \\
  &= (n-l_0+1) \cdot t_{n-1} < r_{l_0-m-1}, \\
  s_0 + r_{l_0-2} &= s_1 + r_{l_0-3} = \cdots = s_{m-2} + r_{l_0-m} = (n-l_0+2) \cdot t_{n-1} \\
  &< s_{m-1} + r_{l_0-m-1}, r_{l_0-m-2} \geq (n-l_0+2) \cdot t_{n-1}, \\
  &\quad \vdots \\
  s_0 + r_{m+1} &= s_1 + r_m = \cdots = s_{2m-l_0+1} + r_{l_0-m} = (l-1) \cdot t_{n-1} \\
  &< s_{2m-l_0+2} + r_{l_0-m-1}, \cdots, r_1 \geq (l-1) \cdot t_{n-1}. \\
  s_0 + r_m &= s_1 + r_{m-1} = \cdots = s_{2m-l_0} + r_{l_0-m} = l \cdot t_{n-1} \\
  &< s_{2m-l_0+1} + r_{l_0-m-1}, \cdots, r_0 \geq l \cdot t_{n-1}. 
\end{align*}
\]

If \( m = l \) then we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

Otherwise since \( s_0 = m \cdot t_{n-1} \) and \( r_0 \geq l \cdot t_{n-1} \), there are

\[
s_0 + r_0 = t_0 = r \geq n \cdot t_{n-1}.
\]

So, the main assumption [29.1] holds only if \( r_0 = s_0 \) and \( m = l \) for \( g(X) \) and \( h(X) \) or \( r \geq n \cdot t_{n-1} \).

(III) By the proof of Lemma [30.2], if \( m \leq l \leq k_m \), then all \( s_i \) for \( i = k_m - l, k_m - l + 1, \ldots, m-1 \) are determined, so that all the sum of \( s_i + r_{k_m-i} \) for \( i = k_m - l + 1, k_m - l + 2, \ldots, m-1 \) are same values.

Let denote \( s_i = \lambda \cdot t_{n-1} \) and assume \( k \in E_k \) where \( k = l + m_0, l + m_0 + 1, \ldots, n - 1 \) and \( 0 < m_0 < m - 1 \).

(1) Case of \( \lambda = 1 \).

(1.1) Let consider the case of all \( s_i = t_{n-1} \) for \( i < m_0 \).
Similar to the proof of Lemma (30.3), when \( r_l = s_m = 0 \), there are

\[
s_{m-1} = r_{l-1} = t_{n-1},
\]

\[
s_{m-2} = s_{m-1} + r_{l-1} = r_{l-2} = t_{n-2} = 2t_{n-1},
\]

\[
s_{m-3} = s_{m-2} + r_{l-1} = s_{m-1} + r_{l-2} = r_{l-3} = t_{n-3} = 3t_{n-1},
\]

\[
\ldots
\]

\[
s_{m_0} = s_{m_0+1} + r_{l-1} = \cdots = s_{m-1} + r_{l+m_0-m+1}
\]

\[
= r_{l+m_0-m} = t_{l+m_0} = (m-m_0)t_{n-1},
\]

\[
s_{m_0-1} = r_{l+m_0-m} = t_{n-1} < s_{m_0} + r_{l-1} = \cdots
\]

\[
= s_{m-1} + r_{l+m_0-m} = (m-m_0+1)t_{n-1},
\]

\[
\ldots
\]

\[
s_1 = r_{l-m+1} = t_{n-1} < s_2 + r_{l-1} = s_{m-1} + r_{l-m+2} \leq \cdots,
\]

\[
s_0 = r_{l-m} = t_{n-1} < s_1 + r_{l-1} = s_{m-1} + r_{l-m+1} \leq \cdots.
\]

If \( m = l \) then we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

Otherwise there will be \( r_{l-m-1} > 2t_{n-1} \) and \( r_i \geq 2t_{n-1} \) where \( i = 0, 1, \ldots, l - m - 2 \). On the other hand, since \( p' \mid \sum_{i=0}^{k} g_{s-i}h_i \) and

\[
s_0 = s_1 = \cdots = s_{m_0-1} = r_{l-m} = r_{l-m+1} = \cdots = r_{l+m_0-m-1} = t_{n-1},
\]

there should be at least two equalities \( s_{k-i} + r_i = 2t_{n-1} \) for each \( k < l \) where \( i_0 \leq i \leq k \). Therefore, there should be \( s_0 + r_1 = s_1 + r_0 = t_1 = 2t_{n-1} \) so that there are \( r_1 = t_{n-1} \) and \( r_0 = 2t_{n-1} - s_1 \). A contradiction. Thus there should be \( m = l \) so that we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 = 2t_{n-1} \).

(1.2) Let consider the case of at least one \( s_j = t_{n-1} \) where \( j < m_0 \).

Similarly to the case of all \( s_i = t_{n-1} \) for \( i < m_0 \), if \( m = l \) then we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

Otherwise there will be \( r_i \geq 2t_{n-1} \) where \( i = 0, 1, \ldots, l - m - 1 \). On the other hand, since there is \( s_j + r_{l-1} = 2t_{n-1} \), there should be at least two equalities \( s_{k-i} + r_i = 2t_{n-1} \) for each \( k < l + j \) where \( i_0 \leq i \leq k \). Therefore, there should be \( s_0 + r_1 = s_1 + r_0 = t_1 = 2t_{n-1} \) so that there are \( r_1 = t_{n-1} \) and \( r_0 = 2t_{n-1} - s_1 \). A contradiction. Thus there should be \( m = l \) so that we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

(2) Case of \( \lambda = 2 \).

(2.1) Let consider the case of all \( s_i = 2t_{n-1} \) where \( i < m - 1 \).
Similar to the proof of Lemma [30.3], when \( r_l = s_m = 0 \), there are
\[
\begin{align*}
s_{m-1} &= r_{l-1} = t_{n-1}, \\
s_{m-2} &= s_{m-1} + r_{l-1} = t_{n-2} = 2t_{n-1}, \\
s_{m-3} &= s_{m-2} + r_{l-1} = s_{m-1} + r_{l-2} = r_{l-3} = t_{n-3} = 3t_{n-1}, \\& 
\vdots \\
s_{m_0} &= s_{m_0+1} + r_{l-1} = \cdots = s_{m-1} + r_{l+m_0-m+1} = r_{l+m_0-m} = t_{l+m_0} = (m-m_0)t_{n-1}, \\
s_{m_0-1} &= r_{l+m_0-m-1} = 2t_{n-1} < s_{m_0} + r_{l-1} = \cdots = s_{m-1} + r_{l+m_0-m} = (m-m_0+1)t_{n-1}, \\& 
\vdots \\
s_1 &= r_{l-m+1} = 2t_{n-1} < s_2 + r_{l-1} = s_{m-1} + r_{l-m+2} \leq \cdots, \\
s_0 &= r_{l-m} = 2t_{n-1} < s_1 + r_{l-1} = s_{m-1} + r_{l-m+1} \leq \cdots.
\end{align*}
\]

If \( m = l \) then we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

Otherwise there will be \( r_i \geq 3t_{n-1} \) where \( i = 0, 1, \cdots, l - m - 1 \). On the other hand, since
\[
p^r \big| \sum_{i=0}^{k} g_{k-i} h_i \big|
\]
there should be at least two equalities \( s_{k-i} + r_i = 4t_{n-1} \) for each \( k < l \) where \( i_0 \leq i \leq k \).
Therefore, there should be \( s_0 + r_1 = s_1 + r_0 = t_1 = 4t_{n-1} \) so that there are \( r_1 = 2t_{n-1} \) and \( r_0 = 4t_{n-1} - s_1 \). A contradiction. Thus there should be \( m = l \) so that we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

(2.2) Let consider the case of at least one \( s_j = 2t_{n-1} \) and all other \( s_i > 2t_{n-1} \) where \( j < m_0, i < m_0 \) and \( i \neq j \).

Similarly to the case of all \( s_i = 2t_{n-1} \) for \( i < m_0 \), if \( m = l \) then we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

Otherwise there will be \( r_i \geq 3t_{n-1} \) where \( i = 0, 1, \cdots, l - m - 1 \). On the other hand, since
\[
p^r \big| \sum_{i=0}^{k} g_{k-i} h_i \big|
\]
there should be \( s_{k-i} + r_i = 4t_{n-1} \) for each \( k < l \) where \( i_0 \leq i \leq k \).
Therefore, there should be \( s_0 + r_1 = s_1 + r_0 = t_1 = 4t_{n-1} \) so that there are \( r_1 = 2t_{n-1} \) and \( r_0 = 4t_{n-1} - s_1 \). A contradiction. Thus there should be \( m = l \) so that we have \( s_0 = r_0 \) and \( r_0 + s_1 = r_1 + s_0 = t_1 \).

(3) Cases of \( \lambda = 3, 4, \cdots, m - 1 \). Let continue in the same way above to consider the case of all \( s_i = \lambda \ast t_{n-1} \) where \( i < \min\{m_0, m - \lambda + 1\} \) and the case of at least one \( s_j = \lambda \ast t_{n-1} \) where \( j < \min\{m_0, m - \lambda\} \). Then we can get the result that the main assumption (29.1) holds only if \( r_0 = s_0 \) and \( m = l \) for \( g(X) \) and \( h(X) \).

The proof of the lemma is completed.

**Lemma 30.5** For any number \( n \) and a polynomial \( F(X) \), if \( F(X) \) is not a binomial, then it is a fundamental polynomial or it can be written as only one fundamental polynomial.
Proof Assume that \( F(X) \) is with \( k + 1 \) terms such that \( F(X) \) can be written as
\[
F(X) = a_{n_k}X^{n_k} + a_{n_{k-1}}X^{n_{k-1}} + \cdots + a_1X + a_0 \in Z[X]
\]
where \( n = n_k > n_{k-1} > \cdots > n_1 \geq 1 \). Thus there should be \( \gcd(n_k, n_{k-1}, \ldots, n_1) = d \).
If \( d = 1 \), then \( F(X) \) is a fundamental polynomial, else \( F(X) \) can be written as only one fundamental polynomial \( F(Y) \) by defining \( Y = X^d \).

The proof of the lemma is completed.

**Lemma 30.6** For any number \( n \) and a binomial \( F(X) \), if \( n \) is prime, then \( F(X) \) is a fundamental polynomial, else \( F(X) \) can be written as more than one fundamental polynomials.

Proof For any number \( n \) and a binomial \( F(X) \), if \( n \) is prime, then \( F(X) \) is a fundamental polynomial since we can not find a factor \( d \) of \( n \) to define \( Y = X^d \) and write \( F(X) \) as a fundamental polynomial
\[
F(Y) = a_{k+d}Y^k + a_{(k-1)d}Y^{k-1} + \cdots + a_dY + a_0 \in Z[Y].
\]

Otherwise, \( F(X) \) can be written as more than one fundamental polynomials
\[
F(Y) = a_{k+d}Y^k + a_{(k-1)d}Y^{k-1} + \cdots + a_dY + a_0 \in Z[Y]
\]
by defining \( Y = X^d \) where \( k \cdot d = n \), \( k \) and \( d \) are positive integers greater than 1.

The proof of the lemma is completed.

### 31 Theorems on irreducible polynomials

**Theorem 31.1** For any number \( n \), assume a fundamental polynomial
\[
F(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in Z[X],
\] (31.1)
if there exist a prime \( p \) and a positive number \( r \) such that \( 2 \not| r \) or \( 2 \not| n \), \( r < n \), \( p \not| a_n \), \( p^i|a_i(i = 0, 1, \ldots, n-1) \) and \( p^{r+1} \not| a_0 \), then \( F(X) \) is irreducible over the field \( Q[X] \) of rational numbers.

Proof By Lemma 30.1, there must be \( m_p = m \) and \( l_p = l \) in the main assumption 29.1 and Definition 29.2.

When \( e_t = n - 1 \), by definitions 29.2 29.3 and Lemma 30.2, the main assumption 29.1 holds only if \( n|r \). But the theorem assumes \( r < n \). A contradiction.

When \( e_t = 2 \), by definitions 29.2 29.3 and Lemma 30.3, the main assumption 29.1 holds only if \( 2|r \) and \( 2|n \). But the theorem assumes \( 2 \not| r \) or \( 2 \not| n \). A contradiction.

When \( 2 < e_t < n - 1 \), by definitions 29.2 29.3 and Lemma 30.4, the main assumption 29.1 holds only if \( 2|r \) and \( 2|n \) or \( r \geq n \cdot t_{n-1} \). But the theorem assumes \( 2 \not| r \) or \( 2 \not| n \), and \( r < n \). A contradiction.

Thus for all different cases of \( e_t \), reductions to absurdity are derived so that the assumption that the fundamental polynomial \( F(X) = g(X)h(X) \) is proved false. Hence the theorem holds.

The proof of the theorem is completed.

**Theorem 31.2** For any number \( n \), assume a fundamental polynomial
\[
F(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in Z[X],
\] (31.2)
if there exist a prime \( p \) and a positive number \( r \) such that \( 2 \nmid r \) or \( 2 \nmid n, \ r < n, \ p \nmid a_0, \ p^r \nmid a_i(i = 1, 2, \cdots, n) \) and \( p^{r+1} \nmid a_n \), then \( F(X) \) is irreducible over the field \( \mathbb{Q}[X] \) of rational numbers.

**Proof**  
Let denote \( \bar{a}_i = a_{n-i} \) for \( i = 0, 1, \cdots, n \). Then there are \( p \nmid \bar{a}_n, \ p^r \nmid \bar{a}_i(i = 0, 1, \cdots, n-1) \) and \( p^{r+1} \nmid a_0 \).

Similar to the proof of Theorem 31.1 by assuming \( F(X) = g(X)h(X) \) and using \( \bar{g}_i = g_{m-i} \) for \( i = 0, 1, \cdots, m \) and \( \bar{h}_i = h_{l-i} \) for \( i = 0, 1, \cdots, l \), for all different cases of numbers \( n \) and \( r \), reductions to absurdity that there will be \( p|\bar{g}_m \) or \( p|\bar{h}_l \) so that \( p|\bar{g}_m\bar{h}_l = \bar{a}_n \), are derived so that the assumption that the fundamental polynomial \( F(X) = g(X)h(X) \) is proved false. Hence the theorem holds.

The proof of the theorem is completed.

**Theorem 31.3**  
For any number \( n \), a polynomial \( F(X) \) is irreducible over the field \( \mathbb{Q}[X] \) of rational numbers if and only if all of its fundamental polynomials are irreducible over the field \( \mathbb{Q}[X] \) of rational numbers.

**Proof**  
Firstly, if a polynomial \( F(X) \) is with one fundamental polynomial \( F(Y) \) reducible over the field \( \mathbb{Q}[X] \) of rational numbers, then there should be \( F(Y) = g(Y)h(Y) \). Since \( Y = X^d \), then we have

\[
F(X^d) = g(X^d)h(X^d) \quad \text{or} \quad F(X) = g(X)h(X),
\]

so that \( F(X) \) is reducible over the field \( \mathbb{Q}[X] \) of rational numbers. Thus \( F(X) \) is irreducible over the field \( \mathbb{Q}[X] \) of rational numbers only if all of its fundamental polynomials are irreducible over the field \( \mathbb{Q}[X] \) of rational numbers.

Secondly, if a polynomial \( F(X) \) is reducible over the field \( \mathbb{Q}[X] \) of rational numbers, then there should be \( F(X) = g(X)h(X) \). If \( F(X) \) can be written as any fundamental polynomial \( F(Y) \), then there should be \( F(Y) = g(Y)h(Y) \) also. Thus when all fundamental polynomials of a polynomial \( F(X) \) are irreducible over the field \( \mathbb{Q}[X] \) of rational numbers, \( F(X) \) is also irreducible over the field \( \mathbb{Q}[X] \) of rational numbers.

The proof of the theorem is completed.

32 Generalization of Eisenstein’s criterion

For any number \( n \), assume a fundamental polynomial

\[
F(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X].
\]

Then Eisenstein’s criterion states: For any number \( n \) and a polynomial \( F(X) \), if there exist a prime \( p \), \( p \nmid a_n, \ p|a_i(i = 0, 1, \cdots, n-1) \) and \( p^2 \nmid a_0 \), then \( F(X) \) is irreducible over the field \( \mathbb{Q}[X] \) of rational numbers.

And Theorem 31.1 states: For any number \( n \) and a fundamental polynomial \( F(X) \), if there exist a prime \( p \) and a positive number \( r \) such that \( 2 \nmid r \) or \( 2 \nmid n, \ r < n, \ p \nmid a_n, \ p^r \nmid a_i(i = 0, 1, \cdots, n-1) \) and \( p^{r+1} \nmid a_0 \), then \( F(X) \) is irreducible over the field \( \mathbb{Q}[X] \) of rational numbers.

By comparing Eisenstein’s criterion and Theorem 31.1, we know that

(1) When \( r = 1 \), Theorem 31.1 becomes Eisenstein’s criterion;
(2) Eisenstein’s criterion can only handle such polynomials $F(X)$ that $p^2 \nmid a_0$ or $r = 1$;
(3) By lemmas 30.5–30.6, theorems 31.1–31.3 can handle polynomials $F(X)$ not only when $r = 1$ but also when $1 < r < n$ for any number $n$.

Hence, theorems 31.1–31.3 are the generalization of Eisenstein’s criterion of irreducible polynomials over the field $\mathbb{Q}$ of rational numbers.

For example, Eisenstein’s criterion can not handle the following polynomials
\begin{align*}
F(X) &= X^3 + p^2, \\
F(X) &= X^3 + p^2(X^2 + X + 1) \\
F(X) &= \left\{ \right. \\
& \quad X^4 + p^3(X^3 + X^2 + X + 1) \\
& \quad \cdots \\
& \quad X^n + p^{n-1}(X^{n-1} + \cdots + X + 1)
\end{align*}

and
\begin{align*}
F(X) &= X^n + p^r(X^{n-1} + \cdots + X + 1)
\end{align*}

where $p$ is a prime and $1 < r < n$ when $2 \nmid r$ or $2 \nmid n$.

But these polynomials can be handled by theorems 31.1–31.3 and determined irreducible over the field $\mathbb{Q}[X]$ of rational numbers.

References
[1] Wapedia - Wiki, Eisenstein’s criterion.
[2] Hua Loo-Keng, Introduction to Number Theory. Berlin Heidelberg New York, Springer-Verlag 1982.

Part VIII
On some irreducible polynomials

Abstract Problems on irreducible polynomials were investigated in this paper. Some theorems were proved as follows
(1) For a polynomial $f_n(X) \in \mathbb{Z}(X)$ and
\begin{align*}
f_n(X) &= a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0
\end{align*}
where a prime $p|a_n$, if $f_n-1(X)$ is irreducible over $\mathbb{Q}(X)$ and $f_n-1(X) \equiv f_n-1(X) \pmod{p}$, then $f_n(X)$ is irreducible over $\mathbb{Q}(X)$.
(2) For any positive integer $n$, the polynomial
\begin{align*}
s_n(x) &= 1 + \sum_{k=1}^{n} p_kx^k = 1 + p_2x + p_3x^2 + \cdots + p_{n+1}x^n
\end{align*}
is irreducible over the field $\mathbb{Q}$ of rational numbers.
(3) For any positive integer $n$, the polynomial
\begin{align*}
s_n(x) &= \sum_{m=0}^{n} (m+1)x^m = 1 + 2x + 3x^2 + \cdots + (n+1)x^n
\end{align*}
is irreducible over the field $Q$ of rational numbers. Moreover, $s_n(x)$ is reducible modulo an odd prime $p$ if and only if $n = kp - 1$ or $n = kp - 2$, where $k$ is a positive integer greater than 1.

(4) For any positive integer $n$, the polynomial

$$s_n(x) = \sum_{m=0}^{n} (m+1)x^m = 1 + 2x + 3x^2 + \cdots + (n+1)x^n$$

is irreducible over the field $Q$ of rational numbers. Moreover, $s_n(x)$ is reducible modulo any prime not greater than $p_m$ if and only if $n = \kappa(p_m#) - 1$ or $n = \kappa(p_m#) - 2$, where $\kappa$ is a positive integer, $p_m$ is the $m^{th}$ prime and $p_m#$ is $p_1p_2\cdots p_m$. Furthermore $s_n(x)$ is reducible modulo any prime if and only if $n = \kappa(p_m#) - 1$ or $n = \kappa(p_m#) - 2$ when $m \to \infty$ such that $n \to \infty$.

Keywords algebra, polynomial, irreducible

33 Introduction

33.1 Conjectures of irreducible polynomials

Zhi-Wei Sun (2013) conjectured:

1. For any positive integer $n$, the polynomial

$$s_n(x) = \sum_{k=1}^{n} p_{k+1}x^k = 1 + p_2x + p_3x^2 + \cdots + p_{n+1}x^n$$

$$= 1 + 3x + 5x^2 + 7x^3 + \cdots + p_{n+1}x^n,$$

is irreducible over the field $Q$ of rational numbers.

2. For any positive integer $n$, the polynomial

$$s_n(x) = \sum_{m=0}^{n} (m+1)x^m = 1 + 2x + 3x^2 + \cdots + (n+1)x^n$$

is irreducible over the field $Q$ of rational numbers. Moreover, $s_n(x)$ is reducible modulo any prime if and only if $n$ has the form $8k(k+1)$, where $k$ is a positive integer.

33.2 Proved theorem

**Theorem 33.1** For $f(X) \in Z(X)$ and

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X^1 + a_0,$$  \hspace{1cm} (33.1)

if there exists a prime $p \nmid a_n$ and $f(X)$ is irreducible modulo the prime $p$, then $f(X)$ is irreducible over $Z(X)$.

33.3 Works in this paper

Problems on irreducible polynomials were investigated in this paper. Some theorems were proved as follows

**Theorem 33.2** (Basic theorem) For a polynomial $f_n(X) \in Z(X)$ and

$$f_n(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X^1 + a_0$$  \hspace{1cm} (33.2)

where a prime $p|a_n$, if $f_{n-1}(X)$ is irreducible over $Q(X)$ and $f_{n-1}(X) = f_{n-1}(X)$ where $f_{n-1}(X) \equiv f_{n-1}(X)(\text{mod } p)$, then $f_n(X)$ is irreducible over $Q(X)$.
Theorem 33.3  For a polynomial \( f_n(X) \in \mathbb{Z}(X) \) and

\[
    f_n(X) = a_nX^n - a_{n-1}X^{n-1} + \cdots + (-1)^{n-1}a_1X^1 + (-1)^na_0
\]  (33.3)

where a prime \( p | a_n \), if \( f_{n-1}(X) \) is irreducible over \( \mathbb{Q}(X) \) and \( \bar{f}_{n-1}(X) = f_{n-1}(X) \) where \( \bar{f}_{n-1}(X) \equiv f_{n-1}(X) \pmod{p} \), then \( f_n(X) \) is irreducible over \( \mathbb{Q}(X) \).

Theorem 33.4 (Theorem of Conjecture 1)  For any positive integer \( n \), the polynomial

\[
    s_n(x) = 1 + \sum_{k=1}^{n} p_{k+1}x^k = 1 + p_2x + p_3x^2 + \cdots + p_{n+1}x^n
\]  (33.4)

is irreducible over the field \( \mathbb{Q} \) of rational numbers.

Theorem 33.5  For any positive integer \( n \), the polynomial

\[
    s_n(x) = \sum_{k=1}^{n} (-1)^{n-k}p_kx^{k-1} = p_nx^{n-1} - p_{n-1}x^{n-2} + \cdots + (-1)^{n-1}p_1
\]  (33.5)

is irreducible over the field \( \mathbb{Q} \) of rational numbers.

Theorem 33.6  For any positive integer \( n \), the polynomial

\[
    s_n(x) = \sum_{m=0}^{n} (m+1)x^m = 1 + 2x + 3x^2 + \cdots + (n+1)x^n
\]  (33.6)

is irreducible over the field \( \mathbb{Q} \) of rational numbers. Moreover, \( s_n(x) \) is reducible modulo an odd prime \( p \) if and only if \( n = kp - 1 \) or \( n = kp - 2 \), where \( k \) is a positive integer greater than 1.

Theorem 33.7  For any positive integer \( n \), the polynomial

\[
    s_n(x) = \sum_{m=0}^{n} (m+1)x^m = 1 + 2x + 3x^2 + \cdots + (n+1)x^n
\]  (33.7)

is irreducible over the field \( \mathbb{Q} \) of rational numbers. Moreover, \( s_n(x) \) is reducible modulo any prime not greater than \( p_m \) if and only if \( n = \kappa(p_m\#) - 1 \) or \( n = \kappa(p_m\#) - 2 \), where \( \kappa \) is a positive integer, \( p_m \) is the \( m^{th} \) prime and \( p_m\# = p_1p_2\cdots p_m \). Furthermore \( s_n(x) \) is reducible modulo any prime if and only if \( n = \kappa(p_m\#) - 1 \) or \( n = \kappa(p_m\#) - 2 \) when \( m \to \infty \) such that \( n \to \infty \).

34  Proof of Theorem

Proof  Assume \( f_n(X) = (\alpha pX^m + g(X))h(X) \) and denote

\[
    \bar{f}_n(X) \equiv f_n(X) \pmod{p}, \\
    \bar{f}_{n-1}(X) \equiv f_{n-1}(X) \pmod{p}, \\
    \bar{g}(X) \equiv \alpha pX^m + g(X) \pmod{p}, \\
    \bar{h}(X) \equiv h(X) \pmod{p}.
\]

Since \( f_{n-1}(X) = f_n(X) - a_nX^n \), there are

\[
    \bar{f}_{n-1}(X) = \bar{f}_n(X) = \bar{g}(X)\bar{h}(X).
\]

If \( f_{n-1}(X) \) is irreducible over \( \mathbb{Q}(X) \) and \( \bar{f}_{n-1}(X) = f_{n-1}(X) \), then there must be

\[
    m = 1, \bar{g}(X) = 1 \text{ and } \bar{h}(X) = \bar{f}_{n-1}(X) = f_{n-1}(X),
\]
so that there will be
\[ f_n(X) = (apX^m + g(X))h(X) = (apX + 1)f_{n-1}(X). \]

But it is impossible that all the corresponding coefficients of \( X^i \) for \( i = 0, 1, \cdots, n \) on both hand sides of the equation are equal to each other so that there is \( f_n(X) \neq (apX^m + g(X))h(X) \). Thus \( f_n(X) \) is irreducible over \( Q(X) \).

This completes the proof of the theorem.

35 Proof of Theorem (33.3)

**Proof** Assume \( f_n(X) = (apX^m + g(X))h(X) \) and denote
\[
\begin{align*}
\bar{f}_n(X) &\equiv f_n(X) \pmod{p}, \\
\bar{f}_{n-1}(X) &\equiv f_{n-1}(X) \pmod{p}, \\
\bar{g}(X) &\equiv apX^m + g(X) \pmod{p}, \\
\bar{h}(X) &\equiv h(X) \pmod{p}.
\end{align*}
\]
Since \( f_{n-1}(X) = a_nX^n - f_n(X) \), there are
\[ \bar{f}_{n-1}(X) = -\bar{f}_n(X) = -\bar{g}(X)\bar{h}(X). \]
If \( f_{n-1}(X) \) is irreducible over \( Q(X) \) and \( \bar{f}_{n-1}(X) = f_{n-1}(X) \), then there must be
\[ m = 1, \bar{g}(X) = -1 \quad \text{and} \quad \bar{h}(X) = \bar{f}_{n-1}(X) = f_{n-1}(X), \]
so that there will be
\[ f_n(X) = (apX^m + g(X))h(X) = (apX + 1)f_{n-1}(X) \]

But it is impossible that all the corresponding coefficients of \( X^i \) for \( i = 0, 1, \cdots, n-1 \) on both hand sides of the equation are equal to each other so that there is \( f_n(X) \neq (apX^m + g(X))h(X) \). Thus \( f_n(X) \) is irreducible over \( Q(X) \).

This completes the proof of the theorem.

36 Proof of Theorem (33.4)

**Proof** Let denote \( \bar{s}_{n-1}(x) \equiv s_{n-1}(x) \pmod{p_{n+1}} \).
First for \( n = 2 \), the polynomial \( s_1(x) = 1 + 3x \) is irreducible over \( Q(X) \) and \( \bar{s}_1(x) = s_1(x) \), then by Theorem (33.2) the polynomial \( s_2(x) \) is irreducible over \( Q(x) \).

Second, assume the polynomial \( s_{n-1}(x) \) is irreducible over \( Q(X) \), then there is \( \bar{s}_{n-1}(x) = s_{n-1}(x) \) since \( n < p_{n+1} \) and \( p_{i+1} < p_{n+1} \) for \( i = 1, 2, \cdots, n-1 \), thus by Theorem (33.2) the polynomial \( s_{n}(x) \) is irreducible over \( Q(x) \).

This completes the proof of the theorem.

37 Proof of Theorem (33.5)

**Proof** Let denote \( \bar{s}_{n-1}(x) \equiv s_{n-1}(x) \pmod{p_n} \).
First for \( n = 3 \), the polynomial \( s_2(x) = 3x - 2 \) is irreducible over \( Q(X) \) and \( \bar{s}_2(x) = s_2(x) \), then by Theorem (33.3) the polynomial \( s_3(x) \) is irreducible over \( Q(x) \).
Second, assume the polynomial $s_{n-1}(x)$ is irreducible over $Q(X)$, then there is $s_{n-1}(x) = s_{n-1}(x)$ since $n < p_n$ and $p_i < p_n$ for $i = 1, 2, \ldots, n - 1$, thus by Theorem (33.3) the polynomial $s_n(x)$ is irreducible over $Q(x)$.

This completes the proof of the theorem.

38 Proof of Theorem (33.6)

38.1 Proof of $s_n(x)$ reducible modulo an odd prime over $Q(x)$

Proof

(1) Sufficient conditions.

Firstly for an odd prime $p$, if $n = kp - 1$, where $k$ is a positive integer greater than 1, then we can write

$$s_n(x) = \sum_{m=0}^{n} (m+1)x^m = \sum_{m=0}^{kp-1} (m+1)x^m$$

$$= \sum_{m=0}^{p-1} (m+1)x^m + x^p \sum_{m=0}^{p-1} (p+m+1)x^m + \cdots + x^{(k-1)p} \sum_{m=0}^{p-1} ((k-1)p+m+1)x^m$$

$$= \sum_{i=0}^{k-1} x^p \sum_{m=0}^{p-1} (ip+m+1)x^m,$$

so that since $x^p \equiv x^{(mod\ p)}$ we obtain

$$s_n(x) = \sum_{m=0}^{n} (m+1)x^m \equiv \sum_{i=0}^{k-1} x^i \sum_{m=0}^{p-2} (m+1)x^m (mod\ p).$$

Secondly for an odd prime $p$, if $n = kp - 2$, where $k$ is a positive integer greater than 1, then we can write

$$s_n(x) = \sum_{m=0}^{n} (m+1)x^m$$

$$= \sum_{m=0}^{kp-2} (m+1)x^m = \sum_{m=0}^{kp-1} (m+1)x^m - kpx^{kp-1}$$

$$= \sum_{m=0}^{p-1} (m+1)x^m + x^p \sum_{m=0}^{p-1} (p+m+1)x^m + \cdots + x^{(k-1)p} \sum_{m=0}^{p-1} ((k-1)p+m+1)x^m - kpx^{kp-1}$$

$$= \sum_{i=0}^{k-1} x^p \sum_{m=0}^{p-1} (ip+m+1)x^m - kpx^{kp-1},$$

so that since $x^p \equiv x^{(mod\ p)}$ we obtain

$$s_n(x) = \sum_{m=0}^{n} (m+1)x^m \equiv \sum_{i=0}^{k-1} x^i \sum_{m=0}^{p-2} (m+1)x^m (mod\ p).$$

Hence when $n = kp - 1$ or $n = kp - 2$, where $k$ is a positive integer greater than 1, the polynomial $s_n(x)$ is reducible modulo an odd prime $p$ over the field $Q$ of rational numbers.

(2) Necessary conditions.
When \( s_n(x) \) is reducible modulo an odd prime \( p \) over the field \( Q \) of rational numbers then let write

\[
 s_n(x) = \sum_{m=0}^{n} (m+1)x^m \equiv \sum_{i=0}^{k-1} x^i \sum_{m=0}^{p-2} (m+1)x^m \pmod{p}
\]

where polynomials \( 1 + 2x + 3x^2 + \cdots + (p-1)x^{p-2} \) is irreducible over the field \( Q \) of rational numbers by the Eisenstein’s criterion[3].

Since \( x^p \equiv x \pmod{p} \) and

\[
 \sum_{i=0}^{p-1} (ip + m + 1)x^m = \sum_{m=0}^{p-2} (m+1)x^m \pmod{p}
\]

for \( i = 0, 1, 2, \cdots \) such that there are

\[
 \sum_{i=0}^{k-1} x^i \equiv \sum_{i=0}^{k-1} x^{ip} \pmod{p},
\]

and

\[
 \sum_{i=0}^{k-1} x^i \sum_{m=0}^{p-2} (m+1)x^m \equiv \sum_{i=0}^{k-1} x^{ip} \sum_{m=0}^{p-1} (ip + m + 1)x^m \pmod{p}
\]

or

\[
 \sum_{i=0}^{k-1} \sum_{m=0}^{p-2} (m+1)x^m \equiv \sum_{i=0}^{k-1} x^{ip} \sum_{m=0}^{p-1} (ip + m + 1)x^m - kpx^{kp-1} \pmod{p},
\]

then we obtain

\[
 s_n(x) = \sum_{m=0}^{n} (m+1)x^m
\]

\[
 = \sum_{i=0}^{k-1} x^{ip} \sum_{m=0}^{p-1} (ip + m + 1)x^m = \sum_{m=0}^{kp-1} (m+1)x^m
\]

or

\[
 s_n(x) = \sum_{m=0}^{n} (m+1)x^m
\]

\[
 = \sum_{i=0}^{k-1} x^{ip} \sum_{m=0}^{p-1} (ip + m + 1)x^m - kpx^{kp-1} = \sum_{m=0}^{kp-2} (m+1)x^m.
\]

Thus there should be \( n = kp - 1 \) or \( n = kp - 2 \).

Hence when the polynomial \( s_n(x) \) is reducible modulo an odd prime \( p \) over the field \( Q \) of rational numbers, there must be \( n = kp - 1 \) or \( n = kp - 2 \), where \( k \) is a positive integer greater than 1.

This completes the proof of the theorem for \( s_n(x) \) reducible modulo an odd prime over \( Q(x) \).
38.2 Proof of \( s_n(x) \) irreducible over \( Q(x) \)

**Proof**

First, when \( n = kp - 1 \) or \( n = kp - 2 \) for an odd prime \( p \), assume \( s_n(x) = g(x)h(x) \) and denote

\[
g(x) \equiv g(x) \pmod{p} \quad \text{and} \quad h(x) \equiv h(x) \pmod{p}.
\]

Then there are

\[
g(x) = \sum_{i=0}^{k-1} x^i \quad \text{and} \quad h(x) = \sum_{j=0}^{p-2} (j+1)x^j,
\]

so that since

\[\begin{align*}
x^p & \equiv x \pmod{p} , \quad a_ip + 1 \equiv 1 \pmod{p} \quad \text{and} \quad b_jp + j + 1 \equiv j + 1 \pmod{p} \\
& \text{for } i = 0, 1, 2, \cdots \text{ and } j = 0, 1, 2, \cdots ,
\end{align*}\]

then there are

\[
g(x) = \sum_{i=0}^{k-1} (a_ip + 1)x^{ip} \quad \text{and} \quad h(x) = \sum_{j=0}^{p-2} (b_jp + j + 1)x^j + b_{p-1}px^{p-1}.
\]

Thus by \( s_n(x) = g(x)h(x) \) there should be

\[
s_n(x) = \sum_{m=0}^{n} (m+1)x^m = 1 + 2x + 3x^2 + \cdots + (n+1)x^n
\]

\[
= \sum_{i=0}^{k-1} (a_ip + 1)x^{ip} \left( \sum_{j=0}^{p-2} (b_jp + j + 1)x^j + b_{p-1}px^{p-1} \right) - a_kpx^{kp-1}
\]

\[
= \sum_{i=0}^{k-1} (ip + 1)x^{ip} \sum_{j=0}^{p-1} (j+1)x^j - a_kpx^{kp-1}
\]

where by comparing the corresponding coefficients of \( x^j \) for \( j = 0, 1, \cdots , p - 1 \), \( x^{ip} \) for \( i = 0, 1, \cdots , k - 1 \) and \( x^{kp-1} \) on both hand sides of the equation, there must be \( b_j = 0 \) for \( j = 0, 1, \cdots , p - 2 \), \( b_{p-1} = 1 \), \( a_i = i \) for \( i = 0, 1, \cdots , k - 1 \), and \( a_k = (k-1)(p-1) \) for \( n = kp - 1 \) or \( a_k = kp - p + 1 \) for \( n = kp - 2 \).

But it is impossible that all the corresponding coefficients of \( x^m \) for \( m = 0, 1, \cdots , n \) on both hand sides of the equation are equal to each other so that there is \( s_n(x) \neq g(x)h(x) \). Thus \( s_n(x) \) is irreducible over the field \( Q \) of rational numbers.

Second, for an odd prime \( p \), when \( n \neq kp - 1 \) and \( n \neq kp - 2 \), since the polynomial \( s_n(x) \) is irreducible modulo the prime \( p \) and \( a_n = n + 1 \neq kp \) such that \( p \nmid a_n \), then by Theorem \ref{33.1}, the polynomial \( s_n(x) \) is irreducible over the field \( Q \) of rational numbers.

Hence for any positive number \( n \) the polynomial \( s_n(x) \) is irreducible over the field \( Q \) of rational numbers.

This completes the proof of the theorem for \( s_n(x) \) irreducible over \( Q(x) \).

For \( n = kp - 1 \), let \( k = p \) and denote \( p = 2m + 1 \), then there are

\[
n = kp - 1 = p^2 - 1 = (p - 1)(p + 1) = 4m(m + 1).
\]

For \( n = kp - 2 \), let \( k = 2p \) and denote \( p = 2m + 1 \), then there are

\[
n = kp - 2 = 2p^2 - 2 = 2(p - 1)(p + 1) = 8m(m + 1).
\]
39 Proof of Theorem (33.7)  

Proof By Theorem (33.6), the polynomial $s_n(x)$ is irreducible over $Q(x)$ and reducible modulo an odd prime $p$ if and only if $n = kp - 1$ or $n = kp - 2$, where $k$ is a positive integer greater than 1.

First, it is obvious that $s_n(x)$ is reducible modulo the even prime $p_1$.

Second, when $n = \kappa(p_m#) - 1$ or $n = \kappa(p_m#) - 2$, then for any odd prime $p$ not greater than $p_m$ there is $n = kp - 1$ or $n = kp - 2$, where $k = \kappa(p_m#)/p$ is a positive integer greater than 1. Thus $s_n(x)$ is reducible modulo any prime $p$ not greater than $p_m$.

Third, if $s_n(x)$ is reducible modulo any odd prime $p$ not greater than $p_m$, then there must be $n = kp - 1$ or $n = kp - 2$ for any odd prime $p$, where $k$ is a positive integer greater than 1. Thus, there must be $k = \kappa(p_m#)/p$ so that there is $n = \kappa(p_m#) - 1$ or $n = \kappa(p_m#) - 2$.

Hence $s_n(x)$ is reducible modulo any prime not greater than $p_m$ if and only if $n = \kappa(p_m#) - 1$ or $n = \kappa(p_m#) - 2$, and $s_n(x)$ is reducible modulo any prime if and only if $n = \kappa(p_m#) - 1$ or $n = \kappa(p_m#) - 2$ when $m \rightarrow \infty$ such that $n \rightarrow \infty$.

This completes the proof of the theorem.

For $n = \kappa(p_m#) - 2$ and $m > 1$, let $\kappa = (p_m#)/2$ and denote $(p_m#)/2 = 2\gamma + 1$, then there are

$$n = \kappa(p_m#) - 2 = 2(p_m#/2)^2 - 2 = 2(p_m#/2 - 1)(p_m#/2 + 1) = 8\gamma(\gamma + 1).$$

References

[1] Zhi-Wei Sun, Problems on irreducible polynomials. https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;be59d7ed.1303.

[2] Zhi-Wei Sun, Primes of the form $1 + 2 * s + ... + n * s^{n-1}$. https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;445ab6c1.1303.

[3] Hua Loo-Keng, Introduction to Number Theory. Berlin Heidelberg New York, Springer-Verlag 1982.