ISSN 2347-1921

FROM THE EXPRESSION OF PRIME NUMBERS TO GOLDBACH CONJECTURE

Kaifu Song[1], Xue Wang[2]

[1] Yichang, Hubei Province, China East Lake High School

[2] Department of Mathematics in Zhejiang Normal University, China

[1] skf08@sina.com, [2] wangxue2013210@sina.com

Abstract: Operation instead of screening method to solve the congruence equation. Discussion on the expression of prime numbers and its applications; Setting up the residual model to solve the problem of related distribution; The problem of solving the problems about prime pairs of even numbers with the correspondence model of even numbers.

Key words: Screening method; Congruence equation; Residual model; Expression of prime numbers. Distribution of prime numbers; Distribution of twins of prime numbers; Distribution of ten pairs of twins of prime numbers; Distribution of n^2-n+p prime numbers; Correspondence model; Goldbach conjecture.

Academic Discipline And Sub-Disciplines: Elementary Number Theory

NR(2000)：11N05; 11A41; 08B10. **IEIE**:0156:I

Council for Innovative Research

Peer Review Research Publishing System

Journal: JOURNAL OF ADVANCES IN MATHEMATICS

Vol .10, No. 3

www.cirjam.com , editorjam@gmail.com

ISSN 2347-1921

1. The Expression on Prime Numbers

1.1. Introducion

Many problems in the number theory are about prime number. Although the study of prime number has long history, some problems about it are still unsolved. Prime number is a problem-packed part in the number theory as it is hard to demonstrate if any natural number is a prime number or not.

Many people have tried to discover a formula for prime number in use, but at Gaussian times it was acknowledged that there exited no simple formula for prime number, and it is still a hard fact.

Among others, the oldest way to discover a prime number is the screening method from the ancient Greek mathetician Erathosthenes at 2 century B.C. The modern table of prime numbers are based on his idea. The table of prime numbers keep enlarging as the computer sciecne develops. In 2004, Walter Fendt made the table of prime numbers coverіng 10^{12}.

1.2. The Principle of Algorithm

To making a prime table (within the range of N), the first thing we need to do is to make sure that all the prime numbers that are less than or equal to $\sqrt{N}$, and then to rule out the multiples of 2, 3, …, p_r, which are in the range of N. then that we get is a prime table (within the range of N).

Within the range of N, if we rule out the multiples of 2, the rest numbers are the solutions of x≡1 (mod 2).

Within the range of N, if we rule out the multiples of 2 and 3, the rest numbers are the solutions of following equations:

$$\begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 1 \pmod 3 \end{cases} \quad \text{and} \quad \begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 2 \pmod 3. \end{cases}$$

…

As the process above, we use the algorithm, i.e. to solve linear congruence equations, to make a prime table instead of Sieve method.

1.3. Linear Congruence Equations

In linear congruence equations, Chinese reminder theorem (Sunzi theorem) is famous.

Theorem (Chinese reminder theorem) Let m_1, m_2, …, m_n be integer numbers which are mutually prime numbers, $m = m_1 m_2 \ldots m_n$, $m = m_i M_i$ and i=1, 2, …, n, then the solution of congruence equations is:

$$m = m_i M_i \text{ , } i=1, 2, \ldots, n,$$

Here, M_i^{∇} $M_i \equiv 1 \pmod{m_i}$, i=1, 2, …, n.

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ \quad\ldots \\ x\equiv a_n \pmod{m_n} \end{cases}$$

Chinese reminder theorem requests that the modules of equations should be mutually prime numbers, while the following theorem doesn't require that.

Theorem 1.3.1 The sufficient and necessary condition of equations:

$$\begin{cases} x\equiv a \pmod m \\ x\equiv b \pmod n \end{cases} \quad (I)$$

being solvable is : $a+mt \equiv b \pmod n$ or $b+nt \equiv a \pmod m$), $t \in \mathbf{Z}$.

If so, the solution of (I) is: x≡ a+ mt(mod[m, n]) (or x≡ b+ nt(mod[m, n])).

Proof x≡ b≡ a+ mt(mod n)， x≡ a+ mt(mod m). So x≡ a+ mt(mod[m, n]).

x≡ a+ mt(mod[m, n]), we get x≡ a+ mt(mod n).

x≡ b(mod n), so a+ mt≡ b (mod n). □ □

ISSN 2347-1921

Theorem 1.3.2 The sufficient and necessary condition of equations (Ⅱ) being solvable is :

$$a_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[m_1,\ m_2,\ \ldots,\ m_i]\,t_i\equiv b_{i+1}(\mathrm{mod}\,m_{i+1}),\ i=1,2,\ \ldots,n-1.$$

If so, the solution of (Ⅱ)is:

$$x\equiv a_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[m_1,\ m_2,\ \ldots,\ m_{n-1}]\,t_{n-1}(\mathrm{mod}[m_1,\ m_2,\ \ldots,\ m_n]).$$

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ \cdots \\ x\equiv a_n \pmod{m_n} \end{cases} \quad (\text{Ⅱ})$$

Proof According to Theorem 1.3.1, when n=2, the proposition above is true.

Let n=k makes the proposition.

The solution of (II) is:

$$x\equiv a_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[m_1,\ m_2,\ \ldots,m_{k-1}]\,t_{k-1}(\mathrm{mod}[m_1,\ m_2,\ \ldots,\ m_k]).$$

t_{k-1} satisfies the equation

$$a_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[m_1,\ m_2,\ \ldots,\ m_{k-1}]\,t_{k-1}\equiv a_k(\mathrm{mod}\,m_k).$$

When n=k+1

$$\begin{cases} x\equiv a_{k+1}(\mathrm{mod}\,m_{k+1}) \\ x\equiv a_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[m_1,\ m_2,\ \ldots,\ m_{k-1}]\,t_{k-1}(\mathrm{mod}[m_1,\ m_2,\ \ldots,\ m_k]). \end{cases} \quad (\text{✧})$$

According to Theorem 1.3.1, t_k satisfies the equation

$$a_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[m_1,\ m_2,\ \ldots,\ m_i]\,t_i\equiv a_{i+1}(\mathrm{mod}\,m_{i+1}).$$

The solution of (□) is the solution of (II). So the solution of (II) is:

$$x\equiv a_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[m_1,\ m_2,\ \ldots,\ m_k]\,t_k(\mathrm{mod}[m_1,\ m_2,\ \ldots,\ m_{k+1}]).$$

So the proposition n=k+1 is true. □

Example 1.3.1 Get the solution the following equations

$$\begin{cases} x\equiv 1(\mathrm{mod}15) \\ x\equiv -2(\mathrm{mod}12) \\ x\equiv 6(\mathrm{mod}10). \end{cases}$$

Anawer $1+15\,t_1\equiv -2(\mathrm{mod}\ 12)$, $t_1=-1$; $1+15\,t_1+60\,t_2\equiv 6(\mathrm{mod}\ 10)$, $t_2=0$.

So the solution of original equations is $x\equiv 1-15\equiv -14\equiv 46\ (\mathrm{mod}\ 60)$.

Definition 1.3.1 The equations in the same form of (I) and (Ⅲ) are called **opposite equations**. Here,

$$\begin{cases} x\equiv a(\mathrm{mod}\ m) \\ x\equiv b(\mathrm{mod}\ n), \end{cases} \quad (\text{Ⅰ})$$

$$\begin{cases} x\equiv -a(\mathrm{mod}\ m) \\ x\equiv -b(\mathrm{mod}\ n). \end{cases} \quad (\text{Ⅲ})$$

Theorem 1.3.3 The solutions of opposite equations are opposite. (i.e. The solution s are mutually opposite.)

So, if the solution of equations (I) is:$x\equiv a+mt\ (\mathrm{mod}[m,\ n])$, the solution of equation (III) is: $x\equiv -a-mt\ (\mathrm{mod}[m,\ n])$.

ISSN 2347-1921

Proof According to Theorem 1.3.1, the sufficient and necessary conditions of (Ⅰ) and (Ⅲ) being solvable are respectively:

$a+ mt \equiv b \pmod n$ and $-a+ mk \equiv b \pmod n$, so we get $k=-t$.

According to Theorem 1.3.1, the solution of (Ⅲ) is:

$$x \equiv -a+ mk \equiv -a-mt \pmod{[m, n]}. \quad \square$$

For example,

$$\begin{cases} x \equiv 1 \pmod{15} \\ x \equiv -2 \pmod{12} \\ x \equiv 6 \pmod{10}. \end{cases}$$

the solution of equations is:$x \equiv 46 \pmod{60}$. So,

$$\begin{cases} x \equiv -1 \pmod{15} \\ x \equiv 2 \pmod{12} \\ x \equiv -6 \pmod{10}. \end{cases}$$

the solution of equations is:$x \equiv -46 \equiv 14 \pmod{60}$.

Theorem 1.3.4 Let the solutions of the following equations,

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b_1 \pmod n, \end{cases} \quad ①$$

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b_2 \pmod n, \end{cases} \quad ②$$

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b_3 \pmod n. \end{cases} \quad ③$$

are respectively:

$$x \equiv a+ mt_1 \pmod{[m, n]},$$
$$x \equiv a+ mt_2 \pmod{[m, n]},$$
$$x \equiv a+ mt_3 \pmod{[m, n]}.$$

If b_1, b_2, b_3 compose an arithmetic progression, the solutions $a+ mt_1$, $a+ m t_2$, $a+ m t_3$ compose the arithmetic progressions of module [m, n].

Proof According to Theorem 1.3.1, the sufficient and necessary conditions of ①, ②, ③being solvable are respectively:

$$a+ mt_1 \equiv b_1 \pmod n, \quad ④$$
$$a+ mt_2 \equiv b_2 \pmod n, \quad ⑤$$
$$a+ mt_3 \equiv b_3 \pmod n. \quad ⑥$$

From④and⑥,we get $2a+ m(t_1+ t_3) \equiv b_1 + b_3 \equiv 2b_2 \equiv 2a+ 2mt_2 \pmod n$. ⑦

From⑤and⑦, we get $2t_2 \equiv t_1+ t_3 \pmod n$.

Therefore, $2x \equiv 2a+2mt_2 \equiv 2a+2 m(t_1+ t_3) \equiv (a+ mt_1)+(a+ mt_3) \pmod{[m, n]}$. $\square$

1.4. The Solution of Congruence Equations and the Discussion about the Expression on Prime Numbers

ISSN 2347-1921

Lemma 1.4.1 The sufficient and necessary conditions of a_1, a_2, …, a_k being the simplified system of residues of m are:

(i) k=m;

(ii) $a_i \not\equiv a_j \pmod m$, $i \neq j$;

(iii) $(a_i, m)=1$.

Definition 1.4.1 Let A be the simplified system of residues of m. If there exist a_1 and $a_2 \in Z_+$ to make $A= a_1A_1+ a_2A_2$, $a_1A_1+ a_2A_2$ is called **the decomposition** of simplified system of residues A of the Module m.

Here, A_1 and A_2 are respectively the simplified system of residues of m_1 and m_2, and card $(\{A_1\})>1$, card $(\{A_2\})>1$ (card (A) represents the number of group A).

Theorem 1.4.1 Let (m, n)=1,

$$\begin{cases} x \equiv a_i \pmod m \\ x \equiv b_j \pmod n \end{cases} \quad (Ⅳ)$$

If a_i, b_i respectively are simplified system of residues of m and n, the solution of (Ⅳ) $\{ x \mid x \equiv a_i + mt_j \pmod{mn}\}$is the decompostion of module mn,ie. $a_i + mt_j$ is the simplified system of residues on the Module mn.

Proof Because the number of the solutions of (Ⅳ) is card (a_i) card (b_i),

$$(m, n)=1, \varphi(mn)= \varphi(m)\ \varphi(n)= \text{card}(a_i)\text{card}(b_i).$$

On the other hand, is the number of the solutions of (Ⅳ) equals the number of simplified system of residues of mn.

For (m, n)=1, each equations has the unique solution, and because in each equations there is at least an equation different from other equations, each solution of these equations is different. So (Ⅳ) has φ(mn) different solutions on the Module mn.

If $(a_i, m)=1$, $(a_i + mt_j, m)=1$.

$$x \equiv a_i + mt_j \equiv b_j \pmod n \text{ and } (b_j, n)=1,$$

so we can get $(a_i + mt_j, n)=1$.

Therefore, $(a_i + mt_j, mn)=1$.

Accoding to Lemma 1.4.1, the theorem is true. □

Theorem 1.4.2 Let a_i be the simplified system of residues of p_i(i=1,2, …, r), and the number of the solution of Congruence equations $x \equiv a_i \pmod{p_i}$ is μ, so $\mu= \sum_{i=1}^{r}(p_i - 1)$.

(i) If $x \in (1, p_{r+1}^2)$, x is a prime number.

(ii) If $x \geq p_{r+1}^2$, x is a prime number or a composite number without factor p_i.

Proof Because p_i is a prime number and a_i=1, 2, …, p_i—1.

p_i and a_i can compose p_i—1 different equations $x \equiv a_i \pmod{p_i}$.

Take i=1,2, …, r, p_i and a_i can compose $\sum_{i=1}^{r}(p_i - 1)$ groups of equations where there is at least a equation is different from other groups of equations.

$$x \equiv a_i \pmod{p_i},\ i=1, 2, \ldots, r.$$

Between these equations group, there is at least one different equation. And p_1, p_2, …, p_r are mutually prime numbers, so each equation group has the unique solution. And each set of equations concludes at least one equation that is different from other equations, so the solution of each set of equations is different from that of other sets. So equations

ISSN 2347-1921

$x \equiv a_i \pmod{p_i}$, $i=1, 2, \ldots, r$, have $\sum_{i=1}^{r}(p_i - 1)$ solutions.

(i) When $(1, p_{r+1}^2)$, $(x, p_i)=1$, so x is a prime number.

(ii) When $x \geq p_{r+1}^2$, obviously, x is a prime number or a composite number without factor p_i. □

Theorem 1.4.3 (The expression on prime numbers):

If S (x) represents the prime numbers in the the range of x, Then

$$S(p_{r+1}^2)=\{x \mid x \equiv a_i \pmod{p_i}, i=1, 2, \ldots, r, x \in (1, p_{r+1}^2)\} \cup \{p_1, p_2, \ldots, p_r\}.$$

Here, a_i is the simplified system of residues of p_i.

Theorem 1.4.4 If $S(\prod_{i=1}^{r} p_i)$ represents the prime numbers in the the range of $\prod_{i=1}^{r} p_i$, then

$$S(\prod_{i=1}^{r} p_i)=(\complement_{J(x)} f(x)) \cup \{p_1, p_2, \ldots, p_r\}.$$

Here, $J(x)=\{x \mid x \equiv a_i \pmod{p_i}, i=1, 2, \ldots, r, x \in (1, \prod_{i=1}^{r} p_i)\}$,

$$f(x)=\{x \mid x = x_i \cdot x_j, x_i, x_j \in J(x), x_i \neq 1, x_j \neq 1, x_i \cdot x_j \leq \prod_{i=1}^{r} p_i\}.$$

$$\complement_{J(x)} f(x) = \{x \mid x \in J(x), \text{且 } x \notin f(x)\}.$$

The following is a deduction of Theorem 1.4.2.

Theorem 1.4.5 Given that a_i and b_i are respectively the simplified system of residues of m and n, if $(m, n)=1$ and $mn= p_1 p_2 \ldots p_r$, then the number of the solutions of the equations (Ⅴ) is μ. So

$$\mu=\varphi(m)\varphi(n)= \sum_{i=1}^{r}(p_i - 1).$$

(i) If $x \in (1, p_{r+1}^2)$, x is a prime number;

(ii) If $x \geq p_{r+1}^2$, x is a prime number or a composite number without m and n factor.

$$\begin{cases} x \equiv a_i \pmod{m} \\ x \equiv b_i \pmod{n} \end{cases} \quad (Ⅴ)$$

Proof Because p_i is a prime number, $\varphi(p_i)= p_i - 1$, $i=1, 2, \ldots, r$. $mn= p_1 p_2 \ldots p_r$, $(m, n)=1$, so

$$\varphi(mn)= \varphi(m)\varphi(n)= \varphi(p_1)\varphi(p_2) \ldots \varphi(p_r)= \sum_{i=1}^{r}(p_i - 1).$$

There are $\varphi(m)\varphi(n)$ groups of equations, in which there is at least an equation different from the equations of other groups, in the equations(V).

According to Theorem 1.4.2, the proposition is true. □

Theorem 1.4.6 Let $m \in Z_+$ and $m > 2$, if A is the simplified system of residues on the Module m, then

$$\{A\}=\{\pm a_1, \pm a_2, \ldots, \pm a_{\varphi(m)/2}\}.$$

which means, the numbers in {A}are in pairs.

Proof If $a_i \in \{A\}$, according to Theorem 1.4.1, $(m - a_i) \in \{A\}$, $m - a_i$ can be represented as $-a_i$ on the Module m, so $\pm a_i \in \{A\}$. Therefore,

$$\{A\}=\{\pm a_1, \pm a_2, \ldots, \pm a_{\varphi(m)/2}\}.$$ □

ISSN 2347-1921

1.5. Examples of Application

Example 1.5.1 If 2 and 3 are prime numbers, write down the prime numbers within the range of 3^2.

Solution: J (2)={x| x≡1 (mod 2)}.

In the range of 3^2: {x| x≡1 (mod 2)}={1,3,5,7}.

The prime numbers in the range of 3^2: S(3^2)={x| x≡1 (mod 2) within 3^2 is x∈(1, 3^2)}∪{2 }={2,3,5,7}.

Example 1.5.2 2, 3, 5, 7, 11 are prime numbers, figure out the prime numbers within the range of 11^2 .

Solution: According to $J(\prod_{i=1}^{3} p_i)$={x| x≡a_i (mod p_i), i=1, 2, 3}={1, 7, 11, 13, 17, 19, 23, 29}.

The solution of $J(\prod_{i=1}^{4} p_i)$)={x| x≡a_i (mod p_i), i=1, 2, 3, 4} is solution of the following equations:

$$\left\{x \left| \begin{cases} x\equiv 1 \pmod{30} \\ x\equiv 1 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 1 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 1 \pmod{30} \\ x\equiv 2 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 121=11^2 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 1 \pmod{30} \\ x\equiv 3 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 31 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 1 \pmod{30} \\ x\equiv 4 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 151 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 1 \pmod{30} \\ x\equiv 5 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 61 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 1 \pmod{30} \\ x\equiv 6 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 181 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 7 \pmod{30} \\ x\equiv 1 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 127 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 7 \pmod{30} \\ x\equiv 2 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 37 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 7 \pmod{30} \\ x\equiv 3 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 157 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 7 \pmod{30} \\ x\equiv 4 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 67 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 7 \pmod{30} \\ x\equiv 5 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 187=11\times 17 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 7 \pmod{30} \\ x\equiv 6 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 97 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 13 \pmod{30} \\ x\equiv 1 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 43 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 13 \pmod{30} \\ x\equiv 2 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 163 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 13 \pmod{30} \\ x\equiv 3 \pmod 7 \end{cases} \right.\right\} = \{x|\ x\equiv 73 \pmod{210}\};$$

ISSN 2347-1921

$$\left\{x \left| \begin{cases} x\equiv 13 \pmod{30} \\ x\equiv 4 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 193 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 13 \pmod{30} \\ x\equiv 5 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 103 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 13 \pmod{30} \\ x\equiv 6 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 13 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 19 \pmod{30} \\ x\equiv 1 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 169 = 13^2 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 19 \pmod{30} \\ x\equiv 2 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 79 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 19 \pmod{30} \\ x\equiv 3 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 199 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 19 \pmod{30} \\ x\equiv 4 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 109 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 19 \pmod{30} \\ x\equiv 5 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 19 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 19 \pmod{30} \\ x\equiv 6 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 139 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 11 \pmod{30} \\ x\equiv 1 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 71 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 11 \pmod{30} \\ x\equiv 2 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 191 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 11 \pmod{30} \\ x\equiv 3 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 101 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 11 \pmod{30} \\ x\equiv 4 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 11 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 11 \pmod{30} \\ x\equiv 5 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 131 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 11 \pmod{30} \\ x\equiv 6 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 41 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 17 \pmod{30} \\ x\equiv 1 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 197 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 17 \pmod{30} \\ x\equiv 2 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 107 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 17 \pmod{30} \\ x\equiv 3 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 17 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 17 \pmod{30} \\ x\equiv 4 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 137 \pmod{210}\};$$

$$\left\{x \left| \begin{cases} x\equiv 17 \pmod{30} \\ x\equiv 5 \pmod 7 \end{cases} \right.\right\} = \{x \mid x\equiv 47 \pmod{210}\};$$

ISSN 2347-1921

$$\left\{x \left\{\begin{array}{l} x\equiv 17 \pmod{30} \\ x\equiv 6 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 167 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 23 \pmod{30} \\ x\equiv 1 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 113 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 23 \pmod{30} \\ x\equiv 2 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 23 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 23 \pmod{30} \\ x\equiv 3 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 143=11\times 13 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 23 \pmod{30} \\ x\equiv 4 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 53 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 23 \pmod{30} \\ x\equiv 5 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 173 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 23 \pmod{30} \\ x\equiv 6 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 83 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 29 \pmod{30} \\ x\equiv 1 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 29 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 29 \pmod{30} \\ x\equiv 2 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 149 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 29 \pmod{30} \\ x\equiv 3 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 59 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 29 \pmod{30} \\ x\equiv 4 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 179 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 29 \pmod{30} \\ x\equiv 5 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 89 \pmod{210}\};$$

$$\left\{x \left\{\begin{array}{l} x\equiv 29 \pmod{30} \\ x\equiv 6 \pmod 7 \end{array}\right.\right\} = \{x \mid x\equiv 209=11\times 19 \pmod{210}\}.$$

Writing down the solution in the table below:

The simplified system of residues $J(\prod_{i=1}^{4} p_i)$ of $\prod_{i=1}^{4} p_i$

a_i	**1**	29	**7**	23	**11**	19	**13**	17
2k+t	2k+0	2k+0	2k+6	2k+1	2k+3	2k+4	2k+5	2k+2
k	k =0	k =0	k=4	k=3	k=2	k=5	k=1	k=6
0	1	29	7	23	11	19	13	17
1	31	59	37	53	41	49	43	47
2	61	89	67	83	71	79	73	77
3	91	119	97	113	101	109	103	107
4	121	149	127	143	131	139	133	137
5	151	179	157	173	161	169	163	167
6	181	209	187	203	191	199	193	197

ISSN 2347-1921

Note: The trumpet figures are the multiples of 7, rather than the simplified system of residues of $\prod_{i=1}^{4} p_i$.

So $S(11^2)=\{x| x\equiv a_i \pmod{p_i}, i=1, 2,3, 4, x\in(1, 11^2)\}\cup\{ 2, 3, 5, 7\}$

$=\{2,3,5,7,11,13,17,19,23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113\}$.

If $S(\prod_{i=1}^{4} p_4)$ represents the prime numbers within the range of $\prod_{i=1}^{4} p_4$,

$J(\prod_{i=1}^{4} p_4)=\{x| x\equiv a_i \pmod{p_i}, i=1, 2, 3,4 , x\in(1, \prod_{i=1}^{4} p_4)\}=\{11,13,17,19,23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 11^2, 127, 131, 137, 139, 143, 149,151, 157, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199, 209, \}$.

$f(x)=\{x| x= x_i\cdot x_j,\ \ x_i , x_j \in J(x), x_i \neq 1 , x_j \neq 1 , x_i \cdot x_j \leq \prod_{i=1}^{4} p_4 \}=\{11^2, 11\times13, 11\times17, 11\times19, 13^2\}$.

$S(\prod_{i=1}^{4} p_4)=(\bigcup_{J(x)} f(x))\cup\{ p_1,\ p_2,\ p_3,\ p_4\}$

$=\{11,13,17,19,23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149,151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199\}\cup\{ 2, 3, 5, 7\}$

$=\{2, 3, 5, 7, 11,13,17,19,23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149,151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199\}$.

1.6. The Actual Algorithm

It is obviously not an effective way to figure out the reduced residue system of $\prod_{i=1}^{r} p_i$ by solving equations. In fact, if we want to figure out the the prime numbers (or prime number table) within the range of $\prod_{i=1}^{r} p_i$ by using prime numbers expression, we can do as follows:

1) Write a_i, the simplified system $\prod_{i=1}^{r-1} p_i$ of residues of $J(\prod_{i=1}^{r-1} p_i)$.

According to Theorem 1.3.3 , Theorem 1.4.6, and the relationship between a_i and the solution of $-a_i$, in the process of computing, we only need the first $\frac{1}{2}\varphi(\prod_{i=1}^{r-1} p_i)$ digits of $J(\prod_{i=1}^{r-1} p_i)$.

2) Write the solution of equations (Ⅵ):

$$\left\{ x \;\middle|\; \begin{cases} x\equiv a_i \pmod{\prod_{i=1}^{r-1} p_i} \\ x\equiv b_i \pmod{p_r}. \end{cases} \right\} \quad (Ⅵ)$$

p_r is a prime number and b_i =1,2，…，p_r-1 is an arithmetic progression. According to Theorem 1.3.4, the solutions of equation x can make up an arithmetic progression for each a_i, so it's easy to write down the solution of (Ⅵ).

$x\equiv t\prod_{i=1}^{r-1} p_i + a_i \pmod{\prod_{i=1}^{r} p_i}$ (t =0, b_i), rule out the multiples of p_r, then we obtain the solution of (Ⅵ).

3) Write the simplified system of residues $J(\prod_{i=1}^{r} p_i)$ of the Module $\prod_{i=1}^{r} p_i$.

ISSN 2347-1921

According to Theorem 1.4.1, the solution of (Ⅵ) is the simplified system of residues J ($\prod_{i=1}^{r} p_i$) of module $\prod_{i=1}^{r} p_i$.

4) Figure out f(x)={x| x= $x_i \cdot x_j$, x_i , $x_j \in J(x)$, $x_i \neq 1$, $x_j \neq 1$, $x_i \cdot x_j \leq \prod_{i=1}^{r} p_i$ }. Rule out the composite numbers in the range of $\prod_{i=1}^{r} p_i$.

5) According to $S(\prod_{i=1}^{r} p_i)=(\complement_{J(x)} f(x)) \cup \{ p_1, p_2, \ldots, p_r\}$, write dwon the prime numbers (or prime number table)within the range of $\prod_{i=1}^{r} p_i$.

For each equation in (Ⅵ) is independent, the equations (Ⅵ) can be simultaneously solved by many people, so as to improve the process of figuring out the prime numbers.

Example 1.6.1 Get the prime numbers of $\prod_{i=1}^{5} p_i$.

Solution: 1) $\prod_{i=1}^{4} p_i$ =210, J ($\prod_{i=1}^{4} p_i$)={a_i|a_i=1, 11, 13,17,19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 11^2, 127, 131, 137, 139, 143, 149,151, 157, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199, 209}.

According to Theorem 1.3.3, the numbers can only be used are { a_i|a_i=1, 11, 13,17,19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, }.

2) Write the solution of equations (Ⅶ)

$$\left\{ x \left| \begin{cases} x \equiv a_i \pmod{210} \\ x \equiv b_i \pmod{11}. \end{cases} \right. \right\} \qquad (Ⅶ)$$

Accoding to theorem 1.3.3 and theorem 1.3.4, we can get the solution of (Ⅶ). See table 1.6.1, table 1.6.2.

3) Figure out f (x)={x| x= $x_i \cdot x_j$, x_i , $x_j \in J(x)$, $x_i \neq 1$, $x_j \neq 1$, $x_i \cdot x_j \leq \prod_{i=1}^{4} p_i$ }. See table 1.6.3.

4) According to $S(\prod_{i=1}^{5} p_i)=(\complement_{J(x)} f(x)) \cup \{ p_1, p_2, \ldots, p_5\}$, write the prime numbers(or prime number table) within the range of $\prod_{i=1}^{5} p_i$.

Table 1.6.1: $\prod_{i=1}^{5} p_i$ range (Ⅶ) symmetric solutions

a_i	**1**	−1	**11**	−11	**13**	−13	**17**	−17	**19**	−19	**23**	−23
k+t	k+0	k+0	k+10	k+10	k+1	k+1	k+5	k+5	k+7	k+7	k+0	k+0
k	k =0	k =0	k=1	k=1	k=10	k=0	k=6	k=6	k=4	k=4	k=0	k =0
0	1	2309	11	2299	13	2297	17	2293	19	2291	23	2287
1	211	2099	221	2089	223	2087	227	2083	229	2081	233	2077
2	421	1889	431	1879	433	1877	437	1873	439	1871	443	1867
3	631	1679	641	1669	643	1667	647	1663	649	1661	653	1657

ISSN 2347-1921

4	841	1469	851	1459	853	1457	857	1453	859	1451	863	1447
5	1051	1259	1061	1249	1063	1247	1067	1243	1069	1241	1073	1237
6	1261	1049	1271	1039	1273	1037	1277	1033	1279	1031	1283	1027
7	1471	839	1481	829	1483	827	1487	823	1489	821	1493	817
8	1681	629	1691	619	1693	617	1697	613	1699	611	1703	607
9	1891	419	1901	409	1903	407	1907	403	1909	401	1913	397
10	2101	209	2111	199	2113	197	2117	193	2119	191	2123	187

a_i	**29**	−29	**31**	−31	**37**	−37	**41**	−41	**43**	−43	**47**	−47
k+t	k+6	k+6	k+8	k+8	k+3	k+3	k+7	k+7	k+9	k+9	k+2	k+2
k	k=5	k=5	k=3	k=3	k=8	k=8	k=4	k=4	k=2	k=2	k=9	k=9
0	29	2281	31	2279	37	2273	41	2269	43	2267	47	2263
1	239	2071	241	2069	247	2063	251	2059	253	2057	257	2053
2	449	1861	451	1859	457	1853	461	1849	463	1847	467	1843
3	659	1651	661	1649	667	1643	671	1639	673	1637	677	1633
4	869	1441	871	1439	877	1433	881	1429	883	1427	887	1423
5	1079	1231	1081	1229	1087	1223	1091	1219	1093	1217	1097	1213
6	1289	1021	1291	1019	1297	1013	1301	1009	1303	1007	1307	1003
7	1499	811	1501	809	1507	803	1511	799	1513	797	1517	793
8	1709	601	1711	599	1717	593	1721	589	1723	587	1727	583
9	1919	391	1921	389	1927	383	1931	379	1933	377	1937	373
10	2129	181	2131	179	2137	173	2141	169	2143	167	2147	163

a_i	**53**	−53	**59**	−59	**61**	−61	**67**	−67	**71**	−71	**73**	−73
k+t	k+8	k+8	k+3	k+3	k+5	k+5	k+0	k+0	k+4	k+4	k+6	k+6
k	k =3	k =3	k =8	k =8	k=6	k=6	k=0	k =0	k=7	k=7	k=5	k=5
0	53	2257	59	2251	61	2249	67	2243	71	2239	73	2237
1	263	2047	269	2041	271	2039	277	2033	281	2029	283	2027
2	473	1837	479	1831	481	1829	487	1823	491	1819	493	1817
3	683	1627	689	1621	691	1619	697	1613	701	1609	703	1607
4	893	1417	899	1411	901	140	907	140	911	1399	913	1397

ISSN 2347-1921

						9		3				
5	1103	1207	1109	1201	1111	1199	1117	1193	1121	1189	1123	1187
6	1313	997	1319	991	1321	989	1327	983	1331	979	1333	977
7	1523	787	1529	781	1531	779	1537	773	1541	769	1543	767
8	1733	577	1739	571	1741	569	1747	563	1751	559	1753	557
9	1943	367	1949	361	1951	359	1957	353	1961	349	1963	347
10	2153	157	2159	151	2161	149	2167	143	2171	139	2173	137

a_i	**79**	−79	**83**	−83	**89**	−89	**97**	−97	**101**	−101	**103**	−103
k+t	k+1	k+1	k+5	k+5	k+0	k+0	k+8	k+8	k+1	k+1	k+3	k+3
k	k=10	k=10	k=6	k=6	k=0	k =0	k=3	k=3	k=10	k=10	k =8	k =8
0	79	2231	83	2227	89	2221	97	2213	101	2209	103	2207
1	289	2021	293	2017	299	2011	307	2003	311	1999	313	1997
2	499	1811	503	1807	509	1801	517	1793	521	1789	523	1787
3	709	1601	713	1597	719	1591	727	1583	731	1579	733	1577
4	919	1391	923	1387	929	1381	937	1373	941	1369	943	1367
5	1129	1181	1133	1177	1139	1171	1147	1163	1151	1159	1153	1157
6	1339	971	1343	967	1349	961	1357	953	1361	949	1363	947
7	1549	761	1553	757	1559	751	1567	743	1571	739	1573	737
8	1759	551	1763	547	1769	541	1777	533	1781	529	1783	527
9	1969	341	1973	337	1979	331	1987	323	1991	319	1993	317
10	2179	131	2183	127	2189	121	2197	113	2201	109	2203	107

Note:

(1) The small print is the multiple of 11, rather than the solution of (Ⅶ).

(2) $-a_i = -a_i + \prod_{i=1}^{r-1} p_i$, if a_i corresponds the solution x, the $-a_i$ corresponds the solution $-x+\prod_{i=1}^{r-1} p_i$.

Table 1.6.2: Reduced residue system $J(\prod_{i=1}^{5} p_i)$ of Module $\prod_{i=1}^{5} p_i$

13	151	293	439	589	731	877	1019	1159	1303	1451	1597	1739	1879	2029	2173
17	157	299	443	593	733	881	1021	1163	1307	1453	1601	1741	1889	2033	2179
19	163	307	449	599	739	883	1027	1171	1313	1457	1607	1747	1891	2039	2183
23	167	311	457	601	743	887	1031	1181	1319	1459	1609	1751	1901	2041	2197
29	169	313	461	607	751	893	1033	1187	1321	1469	1613	1753	1907	2047	2201
31	173	317	463	611	757	899	1037	1189	1327	1471	1619	1759	1909	2053	2203
37	179	323	467	613	761	901	1039	1193	1333	1481	1621	1763	1913	2059	2207
41	181	331	479	617	767	907	1049	1201	1339	1483	1627	1769	1919	2063	2209
43	191	337	481	619	769	911	1051	1207	1343	1487	1633	1777	1921	2069	2213
47	193	347	487	629	773	919	1061	1213	1349	1489	1637	1781	1927	2071	2221

ISSN 2347-1921

53	197	349	491	631	779	923	1063	1217	1357	1493	1643	1783	1931	2077	2227
59	199	353	493	641	787	929	1069	1219	1361	1499	1649	1787	1933	2081	2231
61	211	359	499	643	793	937	1073	1223	1363	1501	1651	1789	1937	2083	2237
67	221	361	503	647	797	941	1079	1229	1367	1511	1657	1801	1943	2087	2239
71	223	367	509	653	799	943	1081	1231	1369	1513	1663	1807	1949	2089	2243
73	227	373	521	659	809	947	1087	1237	1373	1517	1667	1811	1951	2099	2249
79	229	377	523	661	811	949	1091	1241	1381	1523	1669	1817	1957	2111	2251
83	233	379	527	667	817	953	1093	1247	1387	1531	1679	1819	1961	2113	2257
89	239	383	529	673	821	961	1097	1249	1391	1537	1681	1823	1963	2117	2263
97	241	389	533	677	823	967	1103	1259	1399	1541	1691	1829	1973	2119	2267
101	247	391	541	683	827	971	1109	1261	1403	1543	1693	1831	1979	2129	2269
103	251	397	547	689	829	977	1117	1271	1409	1549	1697	1843	1987	2131	2273
107	257	401	551	691	839	983	1121	1273	1411	1553	1699	1847	1993	2137	2279
109	263	403	557	697	841	989	1123	1277	1417	1559	1703	1849	1997	2141	2281
113	269	409	559	701	851	991	1129	1279	1423	1567	1709	1853	1999	2143	2287
127	271	419	563	703	853	997	1139	1283	1427	1571	1711	1861	2003	2147	2291
131	277	421	569	709	857	1003	1147	1289	1429	1577	1717	1867	2011	2153	2293
137	281	431	571	713	859	1007	1151	1291	1433	1579	1721	1871	2017	2159	2297
139	283	433	577	719	863	1009	1153	1297	1439	1583	1723	1873	2021	2161	2309
149	289	437	587	727	871	1013	1157	1301	1447	1591	1733	1877	2027	2171	1

Note: The trumpet figures not a prime number.

Table 1.6.3: f (x) the composite numbers within the range between 169 and 2310

169	403	589	767	899	1027	1159	1313	1391	1537	1681	1781	1909	2021	2147	2249
221	437	611	779	901	1037	1189	1333	1403	1541	1691	1807	1919	2033	2159	2257
247	481	629	793	923	1073	1207	1339	1411	1577	1703	1817	1921	2041	2171	2263
289	493	667	799	943	1079	1219	1343	1417	1591	1711	1819	1927	2047	2173	2279
299	527	689	817	949	1081	1241	1349	1457	1633	1717	1829	1937	2059	2183	2291
323	529	697	841	961	1121	1247	1357	1469	1643	1739	1843	1943	2071	2201	
361	533	703	851	989	1139	1261	1363	1501	1649	1751	1849	1957	2077	2209	
377	551	713	871	1003	1147	1271	1369	1513	1651	1763	1853	1961	2117	2227	
391	559	731	893	1007	1157	1273	1387	1517	1679	1769	1891	1963	2119	2231	

Table1.6. 4: The prime number table within the range of $\prod_{i=1}^{5} p_i$

2	83	197	331	461	607	751	907	1051	1217	1381	1543	1697	1879	2039	2213
3	89	199	337	463	613	757	911	1061	1223	1399	1549	1699	1889	2053	2221
5	97	211	347	467	617	761	919	1063	1229	1409	1553	1709	1783	2063	2237
7	101	223	349	479	619	769	929	1069	1231	1423	1559	1721	1867	2069	2239
11	103	227	353	487	631	773	937	1087	1237	1427	1567	1723	1901	2081	2243

13	107	229	359	491	641	787	941	1091	1249	1429	1571	1733	1907	2083	2251
17	109	233	367	499	643	797	947	1093	1259	1433	1579	1741	1913	2087	2267
19	113	239	373	503	647	809	953	1097	1277	1439	1583	1747	1931	2089	2269
23	127	241	379	509	653	811	967	1103	1279	1447	1597	1753	1933	2099	2273
29	131	251	383	521	659	821	971	1109	1283	1451	1601	1759	1949	2111	2281
31	137	257	389	523	661	823	977	1117	1289	1453	1607	1777	1951	2113	2287
37	139	263	397	541	673	827	983	1123	1291	1459	1609	1787	1973	2129	2293
41	149	269	401	547	677	829	991	1129	1297	1471	1613	1789	1979	2131	2297
43	151	271	409	557	683	839	997	1151	1301	1481	1619	1801	1987	2137	2309
47	157	277	419	563	691	853	1009	1153	1303	1483	1621	1811	1993	2141	
53	163	281	421	569	701	857	1013	1163	1307	1487	1627	1823	1997	2143	
59	167	283	431	571	709	859	1019	1171	1319	1489	1637	1831	1999	2153	
61	173	293	433	577	719	863	1021	1181	1321	1493	1657	1847	2003	2161	
67	179	307	439	587	727	877	1031	1187	1327	1499	1663	1861	2011	2179	
71	181	311	443	593	733	881	1033	1193	1361	1511	1667	1871	2017	2197	
73	191	313	449	599	739	883	1039	1201	1367	1523	1669	1873	2027	2203	
79	193	317	457	601	743	887	1049	1213	1373	1531	1693	1877	2029	2207	

2. Related Distribution of Prime Numbers[2]

2.1. Introduction

Several problems are posed as people study nature numbers and prime numbers: Is there any finite number of prime numbers with certain properties? Can prime numbers be expressed in the form of the polynomial? Can the prime-ness of a large number be determined? Can a composite number be divided into the products of several factor determinants? Such problems as these can be found in number theory, some of which have been solved with great efforts; but some are still to be resolved. That's why number theory invites the most endeavors. Below are discussions about the prime numbers.

2.2. Residual Model

In the expression of the prime numbers,

Theorem 1.4.4 If $S(\prod_{i=1}^{r} p_i)$ represents the prime number within the range of $\prod_{i=1}^{r} p_i$, then

$$S(\prod_{i=1}^{r} p_i)=(\complement_{J(x)} f(x))\cup\{ p_1, p_2, \ldots, p_r \}.$$

Here, $J(x)=\{x \mid x\equiv a_i \pmod{p_i}, i=1, 2, \ldots, n, x\in(1, \prod_{i=1}^{r} p_i)\}$,

$$f(x)=\{x \mid x= x_i \cdot x_j,\ x_i, x_j\in J(x),\ x_i \neq 1, x_j \neq 1, x_i \cdot x_j \leq \prod_{i=1}^{n} p_i \}.$$

$$\complement_{J(x)} f(x) =\{ x \mid x\in J(x), \text{且 } x\notin f(x) \}.$$

$$card(J(x))=card(J(\prod_{i=1}^{n} p_i))=\prod_{i=1}^{n}(p_i-1).$$

Theorem 2.2.1 If $\pi(\prod_{i=1}^{n} p_i)$ represents the prime number in the range of $\prod_{i=1}^{n} p_i$, then

$$\pi(\prod_{i=1}^{n} p_i)= card(S(\prod_{i=1}^{n} p_i)=card((\complement_{J(x)} f(x))\cup\{ p_1, p_2, \ldots, p_r\})=\prod_{i=1}^{r}(p_i-1)-card(f(x))+(n-1).$$

ISSN 2347-1921

Here, $J(x)=\{x \mid x\equiv a_i \pmod{p_i}, i=1, 2, \ldots, n, x\in(1, \prod_{i=1}^{n} p_i)\}$,

$f(x)=\{x \mid x= x_i \cdot x_j, x_i, x_j\in J(x), x_i \neq 1, x_j \neq 1, x_i \cdot x_j \leq \prod_{i=1}^{r} p_i\}$.

For example, r=4, $\prod_{i=1}^{4} p_i =210$, $\prod_{i=1}^{4}(p_i-1)=48$, $f(\prod_{i=1}^{4} p_i)=\{11*11,11*13,11*17,11*19,13*13\}$, $card(f(\prod_{i=1}^{4} p_i)=5$,

So, $\pi(\prod_{i=1}^{4} p_i)=48+3-5=46$. Namely, there are 46 prime numbers in the range of 210.

Similarly, r=5, $\prod_{i=1}^{5} p_i =2310$, $\prod_{i=1}^{5}(p_i-1)=480$, $f(\prod_{i=1}^{5} p_i)=\{13*13,13*17, \ldots 29*79\}$, $card(f(\prod_{i=1}^{5} p_i)=140$,

So, $\pi(\prod_{i=1}^{5} p_i)=480+4-140=344$.

In the range of p_{n+1}^2, $card(f(x))=0$.

Theorem 2.2.2 If $\pi(p_{n+1}^2)$ represents the prime number in the range of p_{n+1}^2, then

$$\pi(p_{n+1}^2)= [p_{n+1}^2 \cdot \frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n} p_i}]+(n-1).$$

Definition 2.2.1 In the range of p_{n+1}^2, $\frac{\prod_{i=1}^{n}(p_i-k)}{\prod_{i=1}^{n} p_i}$ ($k\in Z_+$) is called **the residual model** of related distribution of prime numbers.

The residual model of distribution of prime numbers is $\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n} p_i}$.

For example, in the range of p_{n+1}^2, the compare table the calculated and the actual number.

In the range of p_{n+1}^2, The Compare Table The Calculated and The actual number.

n	1	2	3	4	5	6	7	8	9	10
p_{n+1}^2	3^2	5^2	7^2	11^2	13^2	17^2	19^2	23^2	29^2	31^2
$\pi(p_{n+1}^2)$	4	9	15	30	39	60	71	97	145	160
$\pi'(p_{n+1}^2)$	4	9	15	30	39	61	72	98	146	162

n	11	12	13	14	15	16	17	18	19	20
p_{n+1}^2	37^2	41^2	43^2	47^2	53^2	59^2	61^2	67^2	71^2	73^2
$\pi(p_{n+1}^2)$	219	261	280	326	403	488	513	607	671	700

ISSN 2347-1921

$\pi'(p_{n+1}^2)$	219	263	283	329	409	495	519	609	675	705

n	21	22	23	24	25	26	27	28	29	30
p_{n+1}^2	79^2	83^2	89^2	97^2	101^2	103^2	107^2	109^2	113^2	127^2
$\pi(p_{n+1}^2)$	806	878	995	1166	1251	1288	11382	1415	1506	1880
$\pi'(p_{n+1}^2)$	811	886	1000	1163	1252	1294	1381	1423	1523	1877

n	31	32	33	34	35	36	37	38	39	40
p_n	131^2	137^2	139^2	149^2	151^2	157^2	163^2	167^2	173^2	179^2
$\pi(p_{n+1}^2)$	1984	2151	2199	2505	2556	2743	2936	3063	3269	3475
$\pi'(p_{n+1}^2)$	1976	2141	2190	2489	2547	2729	2915	3043	3241	3436

Note: $\pi'(p_{n+1}^2)$ is the actual number.

2.3. Related Distribution of Prime Numbers

2.3.1. Distribution of Prime Numbers

According to theorem 2.2.2,

$$\pi(p_{n+1}^2)=[p_{n+1}^2\cdot\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n}p_i}]+(n-1)=\frac{p_{n+1}^2}{p_n\cdot p_{n-1}}\cdot\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n-2}p_i}+(n-1).$$

$$\frac{p_{n+1}^2}{p_n\cdot p_{n-1}}>1,\quad \frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n-2}p_i}>1.$$

$$\lim_{n\to\infty}(\pi(p_{n+1}^2))=\infty.$$

Within the range of N, the prime numbers are infinite.

2.3.2. Distribution of Prime numbers in Arithmetic Series

$S_{(a,r)}$ represents the number of prime numbers which are in the form an+ r((a, r)=1), then

$$S_{(a,r)}=\frac{\pi(p_{n+1}^2)}{\varphi(a)},\ \varphi(a) \text{ is the Euler function of a.}$$

a is a constant and φ(a) is a constant.

$$\lim_{n\to\infty}S_{(a,r)}=\infty.$$

There are infinite prime numbers in the form of an+ r ((a, r)=1).

2.3.3. Distribution of Prime Numbers Between n^2 and $(n+1)^2$

Let $n^2=p_n^2$, $(n+1)^2=(p_n+1)^2$.

ISSN 2347-1921

$$\pi(n^2)=\pi(p_n^2)=[p_n^2\cdot\frac{\prod_{i=1}^{n-1}(p_i-1)}{\prod_{i=1}^{n-1}p_i}]+(n-2),$$

$$\pi((n+1)^2)=\pi((p_n+1)^2)=[(p_n+1)^2\cdot\frac{\prod_{i=1}^{n-1}(p_i-1)}{\prod_{i=1}^{n-1}p_i}]+(n-1).$$

$$\pi((n+1)^2)-\pi(n^2)=\pi((p_n+1)^2)-\pi(p_n^2)$$

$$=[(p_n+1)^2\cdot\frac{\prod_{i=1}^{n-1}(p_i-1)}{\prod_{i=1}^{n-1}p_i}]-[p_n^2\cdot\frac{\prod_{i=1}^{n-1}(p_i-1)}{\prod_{i=1}^{n-1}p_i}]=((p_n+1)^2-p_n^2)\frac{\prod_{i=1}^{n-1}(p_i-1)}{\prod_{i=1}^{n-1}p_i}=(2p_n+1)\frac{\prod_{i=1}^{n-1}(p_i-1)}{\prod_{i=1}^{n-1}p_i}.$$

$$\frac{2p_n+1}{p_{n-1}}>1,\ \frac{\prod_{i=1}^{n-1}(p_i-1)}{\prod_{i=1}^{n-2}p_i}>1.$$

$$\lim_{n\to\infty}\pi((n+1)^2)-\pi(n^2)=\infty.$$

The number of prime numbers between n^2 and $(n+1)^2$ increases along with the increasing of n.

In a small range, there is at least a prime number between n^2 and $(n+1)^2$. Therefore, there is at least a prime number between n^2 and $(n+1)^2$. And the larger the prime number is, the more the prime numbers there are between n^2 and $(n+1)^2$.

2.3.4. The Interval between Prime numbers p_{i-1} and p_i

In the distribution of prime numbers,

$$\pi(p_{n+1}^2)=[p_{n+1}^2\cdot\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n}p_i}]+(n-1)$$

Let $\overline{p_{i+1}-p_i}$ be the average interval between the two prime numbers p_{i+1} and p_i, then in the range of p_{n+1}^2,

$$\overline{p_{i+1}-p_i}=\frac{p_{n+1}^2}{\pi(p_{n+1}^2)}.$$

$$\frac{\pi(p_{n+1}^2)}{p_{n+1}^2}=\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n}p_i}+\frac{n-1}{p_{n+1}^2}.$$

$$\lim_{n\to\infty}\frac{\pi(p_{n+1}^2)}{p_{n+1}^2}=0.\ \lim_{n\to\infty}\overline{p_{i+1}-p_i}=\infty.$$

There is no maximum value of the average interval between primes p_{i+1} and p_i. Therefore, the maximum value of the average interval between primes p_{i+1} and p_i is infinite.

2.3.5. Distribution of Twins of Prime Numbers

Exclude the multiples of 2, 3 and 5 in natural numbers, the rest numbers can be categorized as eight numeric axes: A_1, B_1, A_3, B_3, A_7, B_7, A_9, B_9 (Axis A: 3n+2, axis B: 3n + 1).

The twins of prime numbers only appear on the axis pairs A_1-B_3 (or A_7-B_9 or A_9-B_1).

ISSN 2347-1921

According to theorem 2.2.2 and Definition 2.2.1, the corresponding model of twins of prime numbers is:

$$\frac{1*2*4}{2*3*5}\cdot\frac{5}{7}\cdot\frac{3}{8}\cdot\frac{\prod_{i=1}^{n}(p_i-2)}{\prod_{i=1}^{n}p_i}=\frac{1}{14}\cdot\frac{\prod_{i=1}^{n}(p_i-2)}{\prod_{i=1}^{n}p_i}.$$

L(p_{n+1}^2) represents the distribution of twins of prime numbers in the range of p_{n+1}^2 (p_{n+1}≥11), so

$$L(p_{n+1}^2)=\frac{p_{n+1}^2}{14}\cdot\frac{\prod_{i=1}^{n}(p_i-2)}{\prod_{i=1}^{n}p_i}+L(p_{n+1}).$$

For example, in the range of p_{n+1}^2, the compare table the calculated and the actual number.

In the range of p_{n+1}^2, The Compare Table The Calculated and The actual number.

n	1	2	3	4	5	6	7	8	9	10
p_n	11^2	13^2	17^2	19^2	23^2	29^2	31^2	37^2	41^2	43^2
L(p_{n+1}^2)	8	10	15	17	22	31	34	45	52	55
L '(p_{n+1}^2)	10	12	19	21	25	33	35	46	53	56

n	11	12	13	14	15	16	17	18	19	20
p_n	47^2	53^2	59^2	61^2	67^2	71^2	73^2	79^2	83^2	89^2
L(p_{n+1}^2)	62	75	89	93	107	117	121	137	147	164
L '(p_{n+1}^2)	67	80	93	98	117	128	131	146	160	174

n	21	22	23	24	25	26	27	28	29	30
p_n	97^2	101^2	103^2	107^2	109^2	113^2	127^2	131^2	137^2	139^2
L(p_{n+1}^2)	189	201	206	217	222	234	288	302	324	330
L '(p_{n+1}^2)	195	207	214	223	229	240	282	294	321	327

n	31	32	33	34	35	36	37	38	39	40
p_n	149^2	151^2	157^2	163^2	167^2	173^2	179^2	181^2	191^2	193^2
L(p_{n+1}^2)	372	378	403	427	442	468	495	501	551	558
L '(p_{n+1}^2)	376	386	406	423	444	467	492	505	554	561

Note: L '(p_{n+1}^2) is the actual number.

ISSN 2347-1921

Because $\frac{p_{n+1}^2}{p_n p_{n-1}} > 1,\ \frac{\prod_{i=1}^{n}(p_i-2)}{\prod_{i=1}^{n-2} p_i} > 1.$

$$\lim_{n\to\infty} L(p_{n+1}^2) = \infty .$$

There are infinite pairs of twins of prime numbers in natural numbers.

2.3.6. Distribution of Twins of Prime Numbers Within Ten

Definition 2.3.6.1 There are two pairs of twins of prime numbers within ten, **these two pairs of twins of prime numbers are called the twins of prime numbers within ten**.

For example, 11, 13, 17, 19 are twins of prime numbers within ten.

On number axis A_1-B_3-A_7-B_9, according to theorem 2.2.2 and definition 2.2.1, corresponding model of twins of prime numbers within ten is:

$$\frac{1*2*4}{2*3*5}\cdot\frac{3}{7}\cdot\frac{1}{8}\cdot\frac{\prod_{i=1}^{n}(p_i-4)}{\prod_{i=1}^{n} p_i} = \frac{1}{70}\cdot\frac{\prod_{i=1}^{n}(p_i-4)}{\prod_{i=1}^{n} p_i}.$$

$T(p_{n+1}^2)$ represents the distribution of twins of prime numbers within ten in the range of p_{n+1}^2 ($p_{n+1} \geq 11$),so

$$T(p_{n+1}^2) = \frac{p_{n+1}^2}{70}\cdot\frac{\prod_{i=1}^{n}(p_i-4)}{\prod_{i=1}^{n} p_i} + T(p_{n+1}).$$

For example, in the range of p_{n+1}^2, the compare table the calculated and the actual number.

In the range of p_{n+1}^2， The Compare Table The Calculated and The actual number.

n	1	2	3	4	5	6	7	8	9	10
p_n	11^2	13^2	17^2	19^2	23^2	29^2	31^2	37^2	41^2	43^2
$T(p_{n+1}^2)$	1	1	1	2	3	3	3	4	4	4
$T'(p_{n+1}^2)$	2	2	3	3	3	4	4	4	5	5

n	11	12	13	14	15	16	17	18	19	20
p_n	47^2	53^2	59^2	61^2	67^2	71^2	73^2	79^2	83^2	89^2
$T(p_{n+1}^2)$	4	5	6	6	6	7	7	7	7	8
$T'(p_{n+1}^2)$	7	7	9	9	9	9	9	10	10	10

n	21	22	23	24	25	26	27	28	29	30
p_n	97^2	101^2	103^2	107^2	109^2	113^2	127^2	131^2	137^2	139^2
$T(p_{n+1}^2)$	9	9	9	10	11	11	13	14	14	14
$T'(p_{n+1}^2)$	10	11	11	11	11	11	15	15	16	17

ISSN 2347-1921

n	31	32	33	34	35	36	37	38	39	40
p_n	149^2	151^2	157^2	163^2	167^2	173^2	179^2	181^2	191^2	193^2
T(p_{n+1}^2)	16	16	17	17	17	18	19	19	21	21
T '(p_{n+1}^2)	19	20	20	20	21	21	22	22	23	23

n	41	42	43	44	45	46	47	48	49	50
p_n	197^2	199^2	211^2	223^2	227^2	229^2	233^2	239^2	241^2	251^2
T(p_{n+1}^2)	22	22	24	26	27	27	27	28	28	30
T '(p_{n+1}^2)	23	23	24	24	25	25	25	26	26	27

n	51	52	53	54	55	56	57	58	59	60
p_n	257^2	263^2	269^2	271^2	277^2	281^2	293^2	307^2	311^2	317^2
T(p_{n+1}^2)	30	31	32	32	33	33	36	38	39	39
T '(p_{n+1}^2)	27	28	30	30	30	31	34	35	35	37

Note: T '(p_{n+1}^2) is the actual number.

Because $\frac{p_{n+1}^2}{p_n p_{n-1}} > 1$, $\frac{\prod_{i=1}^{n}(p_i - 4)}{\prod_{i=1}^{n-2} p_i} > 1.$

$$\lim_{n\to\infty} T(p_{n+1}^2) = \infty .$$

There are infinite twins of prime numbers within ten (For example, there are 37 pairs in the range of 10^5).

2.3.7. Distribution of n^2+1 Prime Numbers

Theorem 2.3.7.1 $4(mp+10x)^2+1 \equiv 4(mp-10x)^2+1 \pmod p$, and p is an odd prime number.

Proof $4(mp+10x)^2+1-4(mp-10x)^2-1=16\,mxp$. □□□

Theorem 2.3.7.2 If $x \pm y \not\equiv 0 \pmod p$, then $4(mp+10x)^2+1 \not\equiv (mp+10y)^2+1 \pmod p$.

Proof $4(mp+10x)^2+1-4(mp+10y)^2-1=80\,mp(x-y)+400(x+y)(x-y)$.

Because 400 and $x \pm y$ are not of congruence to the module p, this Lemma is true. □

n^2+1 is a composite number when n is an odd number; let n = 2t when n is an even number, and g is the unit digit of t. n^2+1 is the multiple of 5, when $n^2+1=4t^2+1$ and g=1,4,6,9. And g = 2,3, 5, 7, 8, 0 when $4t^2+1$ is a prime number.

$(4n^2+1, 4n+3)=1$ and we express the prime numbers in the form 4n + 1 as q_i.

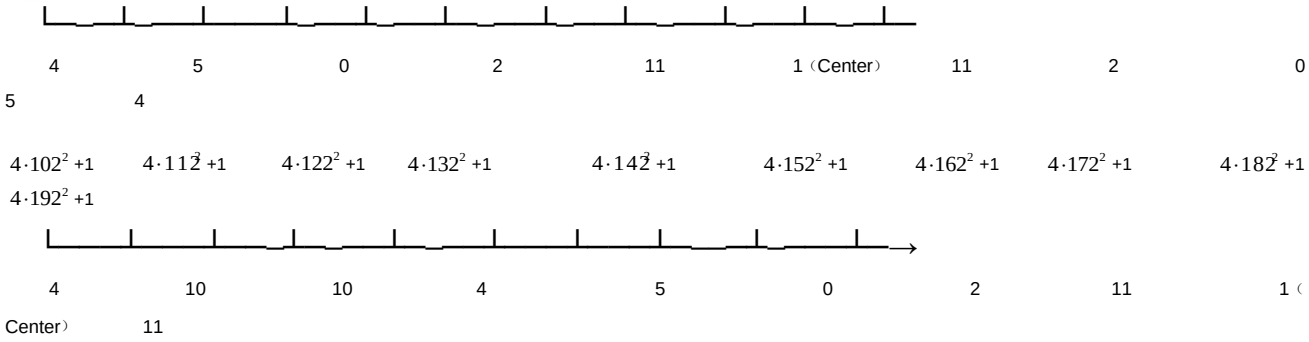
Theorem 2.3.7.3 On the number axis of $4t^2+1$, there are two multiples of q_i at every distance of q_i.

Proof By Theorem 2.3.7.1 and Theorem 2.3.7.2, on the number axis of $4t^2+1$, multiples of q_i, are center symmetric with $4(mq_i)^2+1$. □

For example, there are two multiples of 13 at every distance of 13 numbers on the number axis of $4(10k+2)^2+1$. (see Figure 2.3.7.1.)

$4\cdot 2^2+1$ $4\cdot 12^2+1$ $4\cdot 22^2+1$ $4\cdot 32^2+1$ $4\cdot 42^2+1$ $4\cdot 52^2+1$ $4\cdot 62^2+1$ $4\cdot 72^2+1$ $4\cdot 82^2+1$ $4\cdot 92^2+1$ $4\cdot 102^2+1$

ISSN 2347-1921



(Figure 2.3.7.1)

Note: Numbers, like 4,5,0, …below are the remainders of $4(10k+2)^2+1$ being divided by 13.

Therefore, the surplus model of distribution of n^2+1 prime numbers on number axis of $4(10k+2)^2+1$ is similar with that of distribution of twins of prime numbers on the number axis of A_1-B_3, and the trend is similar too. As a result, there is no maximum value of twins of prime numbers in natural numbers, and there are infinite prime numbers in the form of n^2+1.

2.3.8. Distribution of Triplet of Prime Numbers

If p_i, p_i+2, p_i+6 are all prime numbers, then the group of the three numbers is called the **triplet of prime numbers**.

On the number axes group A_1-B_3-A_7 (or A_7-B_9-A_3), according to theorem 2.2.2 and definition 2.2.1, the corresponding model of triplet of prime numbers is:

$$\frac{1*2*4}{2*3*5}\cdot\frac{4}{7}\cdot\frac{2}{8}\cdot\frac{\prod_{i=1}^{n}(p_i-3)}{\prod_{i=1}^{n}p_i}=\frac{4}{105}\cdot\frac{\prod_{i=1}^{n}(p_i-3)}{\prod_{i=1}^{n}p_i}.$$

$E(p_{n+1}^2)$ represents the distribution of the triplet of prime numbers in the range of p_{n+1}^2 ($p_{n+1}\geq 11$), so

$$E(p_{n+1}^2)=\frac{4p_{n+1}^2}{105}\cdot\frac{\prod_{i=1}^{n}(p_i-3)}{\prod_{i=1}^{n}p_i}+E(p_{n+1}).$$

Because $\frac{p_{n+1}^2}{p_n p_{n-1}}>1$, $\frac{\prod_{i=1}^{n}(p_i-3)}{\prod_{i=1}^{n}p_i}>1.$

$$\lim_{n\to\infty} E(p_{n+1}^2)=\infty.$$

There are infinite triplets of prime numbers in natural numbers.

2.3.9. Distribution of n^2-n+p_i Prime Number

Theorem 2.3.9.1 n^2-n only has $\frac{p+1}{2}$ different residual classes on the odd prime number p.

Proof n=1，(p±1)(p±0)≡0 (mod p)；n=2，(p±2)(p±1)≡2×1 (mod p)；

n=3，(p±3)(p±2)≡3×2 (mod p)；…；

$n=\frac{p-1}{2}$，$(p\pm\frac{p-1}{2})(p\pm\frac{p-3}{2})\equiv\frac{p-1}{2}\times\frac{p-3}{2}$ (mod p)；

ISSN 2347-1921

$n=\frac{p+1}{2}$, $(p\pm\frac{p+1}{2})(p\pm\frac{p-1}{2})\equiv\frac{p+1}{2}\times\frac{p-1}{2}$ (mod p);

$n=\frac{p+3}{2}$, $(p\pm\frac{p+3}{2})(p\pm\frac{p+1}{2})\equiv\frac{p+3}{2}\times\frac{p+1}{2}\equiv\frac{p-1+4}{2}\times\frac{p-3+4}{2}$

$\equiv\frac{p-1}{2}\times\frac{p-3}{2}+2p\equiv\frac{p-1}{2}\times\frac{p-3}{2}$ (mod p).

Namely, $f(\frac{p+3}{2})\equiv f(\frac{p-1}{2})$ (mod p).

Let f(n)=(p± n)(p±(n−1)) ≡n(n−1) (mod p).

$$\frac{p+1+2t}{2}\times\frac{p+1+2(t-1)}{2}=\frac{p+1-2t+4t}{2}\times\frac{p+1-2(t+1)+4t}{2}$$

$$=\frac{p+1-2t}{2}\times\frac{p+1-2(t+1)}{2}+2tp\equiv\frac{p+1-2t}{2}\times\frac{p+1-2(t+1)}{2}\ (\text{mod p}).$$

Namely, $f(\frac{p+1+2t}{2})\equiv f(\frac{p+1-2t}{2})$ (mod p).

Therefore, n^2-n has only $\frac{p+1}{2}$ different residual classes, 1*0，2*1，…， $\frac{p+1}{2}\cdot\frac{p-1}{2}$, on the prime number p. □

0≤n≤N, n^2-n+p_i are all prime numbers, and the first three numbers must be the triplet of prime numbers, and p_i must be on the A_1 (or A_7) number axis.

Theorem 2.3.9.2 Let $n^2-n\equiv r_2$ (mod p_i), $\frac{p_i+1}{2}$ residue classes on the A_1 number axes don't make the proposition true any more.

Proof Let $a\in A_1$, $a\equiv r_1$ (mod p_i)，r_1 =0,1, …, p_i-1.

$n^2-n\equiv r_2$ (mod p_i)，then according to theorem 2.3.9.1, r_2.=0,2,6, …, $\frac{p_i+1}{2}$.

If $r_1+r_2\equiv 0$ (mod p_i), $a+r_2\equiv 0$ (mod p_i), so $a+r_2$ is a composite number.

If any number in r_2 satisfies $r_1+r_2\equiv 0$ (mod p_i), then $a+r_2$ is a composite number. □

According to theorem 2.2.2, theorem 2.3.9.2and definition 2.2.1, the residue model of the distribution of n^2-n+p_i prime number is:

$$\frac{1*2*4}{2*3*5}\cdot\frac{6}{2*7}\cdot\frac{2}{8}\cdot\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n}(2p_i)}=\frac{1}{35}\cdot\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n}(2p_i)}.$$

$Q(p_{n+1}^2)$ represents the distribution of n^2-n+p_i prime number in the range of p_{n+1}^2 ($p_{n+1}\geq 11$), so

$$Q(p_{n+1}^2)=\frac{p_{n+1}^2}{35}\cdot\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n}(2p_i)}+E(p_{n+1})=\frac{p_{n+1}^2}{35\cdot 2^n}\cdot\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n}p_i}+E(p_{n+1}).$$

According to assumption of Bertrand, there is at least a prime number between n and 2n and there is at least a prime number between 2^{n-2} and 2^n. When n≥12 (p_{12}=53).

$$\frac{p_i^2}{2^i}<1,\ (i\geq 12),\quad \frac{p_i-1}{p_i}<1,\ (i=1,2,\ldots,n).$$

ISSN 2347-1921

Hence, $\lim_{n\to\infty} Q_n = 0$.

There are infinite prime numbers p_i , when N = 2, 3; n^2-n+p_i are all prime numbers when $0\le n\le N$;

There are only some special natural numbers N, when $N = p_i-1$; all n^2-n+p_i are all prime numbers when $0\le n\le N$. The greater N is, the less the proposition could be true.

Therefore, there are only 6 prime numbers (p_i = 2; 3; 5; 11; 17; 41) which make the proposition true.

Note: Some textbooks (or science books) say: "Recently some people concluded that when $0\le n\le 11000$, values of $n^2-n+72491$ are all prime numbers. This is the this type formula indicated one of the at most".

However, 72491=1021*71. Namely, when n = 0,1, the proposition is not true. So, the discourse complete odds with reality.

3. The Goldbach conjecture[3]

3.1. Introduction

Goldbach conjecture (prime pair of even numbers) states: every even number, not less than six, can be considered the sum of two odd prime numbers. This conjecture has been drawing great attention from mathematicians and math lovers since it was posed, and it fails all solutions from different possible attempts, even if it is tried with the individual even numbers from thousands of millions.

3.2. Axis Correspondence Form of Even Numbers

As shown in 3.2.1, in nature numbers except those with exact division by 2,3,5, the even number M corresponds to the sum of two residue numbers.

Table 3.2.1. Axis Correspondence Form of Even Numbers $C_M = \frac{175}{192M}[\pi(M_{\triangle})]^2$

E_1	E_2				E_3	E_4			E_5
	1	2	3	4		1	2	3	
O_2	A_1+B_1	A_3+B_9	A_9+B_3			$5+B_7$			$6\,C_M$
B_2	A_3+A_9				A_1+A_1	$3+B_9$	$5+A_7$		$3\,C_M$
A_2	B_3+B_9				B_1+B_1	$3+A_9$			$3\,C_M$
B_4	A_1+A_3				A_7+A_7	$2+2$	$3+B_1$	$5+A_9$	$3\,C_M$
A_4	B_1+B_3				B_7+B_7	$3+A_1$			$3\,C_M$
O_4	A_1+B_3	A_3+B_1	A_7+B_7			$5+B_9$			$6\,C_M$
O_6	A_9+B_7	A_7+B_9	A_3+B_3			$3+3$	$5+B_1$		$6\,C_M$
B_6	A_9+A_7				A_3+A_3	$3+B_3$	$5+A_1$		$3\,C_M$
A_6	B_9+B_7				B_3+B_3	$3+A_3$			$3\,C_M$
A_8	B_1+B_7				B_9+B_9	$3+5$			$3\,C_M$
O_8	A_1+B_7	A_7+B_1	A_9+B_9			$5+B_3$			$6\,C_M$
B_8	A_1+A_7				A_9+A_9	$5+A_3$			$3\,C_M$
B_0	A_1+A_9	A_3+A_7				$5+5$	$3+B_7$		$4\,C_M$
A_0	B_1+B_9	B_3+B_7				$3+A_7$			$4\,C_M$
O_0	A_1+B_9	A_9+B_1	A_3+B_7	A_7+B_3					$8\,C_M$

Note: "O_i", "B_i", "A_i"are numbers divided by 3 with remainders 0，1，2 (i is the number of unit).

ISSN 2347-1921

E_1: Category; E_2: Biaxial correspondence; E_3: Uniaxial correspondence; E_4 A single correspondence (3 or 5 plus another number indicates correspondence to the even number); E_5: the quantity of Prime pairs.

3.3. Correspondence Model

3.3.1. Correspondence Model Ⅰ:

Figure 1 shows the inverted sequence correspondence of B_1axis. If two numbers above and below the axis correspond to each other, then the correspondence means only a even number.

e.g.992=31+961=61+931=91+901= …=961+31.

Figure 6.3.1 A B_1Shaft in Reverse Order Correspondence.

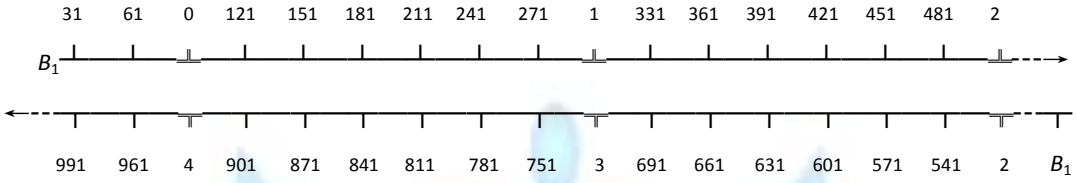


Figure 6.3.1

Note: in the figure, 7 numbers form a section, and the number at "⊥"is the multiple of 7.

3.3.2.Correspondence Model Ⅱ:

Section 1 corresponds to section n, section 2 corresponds to section n－1, …, this correspondence(two numbers together),they only correspond to Even numbers 11 of the same range. Before and after the corresponding to combined with, you can only corresponding to the seven even number.

e.g. section 1 corresponds to section 4; section 2 corresponds to section 3; the result is 872, 902, 932, 962, 992, 1022, 1052,1082,11121142,1172;

Section 1 corresponds to section 3; section 2 corresponds to section 3; the result is 62,692,722,752, 782,812,842,872,902,932,962;

Section 1 corresponds to section 5; section 2 corresponds to section 4; the result is 1082,1112,1142,1172,1202, 1232,1262,1292,1322,1352,1382.

If section 1 corresponds to section 4, the result is 872,902,932,962,992,1022,

1052, then the correspondence of 1082,1112,1142,1172 can be done with 872,902,

932,962 (the correspondence of section 1 to section 3) ;

If section 1 corresponds to section 4, the result is 992,1022,1052,1082,1112, 1142,1172, then the correspondence of 872,902,932,962 can be done with 1082,1112,1142,1172 (the correspondence of section 1 to section 5).

3.3.3. Correspondence Model Ⅲ:

u_i indicates the number of prime numbers on the i section. From Correspondence (II), the number of prime pair $\frac{1}{2}\sum_{i=1}^{n} u_i u_{n-i+1}$ from the correspondence of u_i to u_{n-i+1} is only the correspondence of 7 even numbers.

$M_{(r)} \equiv r \pmod 7$, C_M indicates the number of prime pair of even number M,

$$C_M=C_{M(0)} + C_{M(1)} + C_{M(2)} + C_{M(3)} + C_{M(4)} + C_{M(5)} + C_{M(6)} = \frac{1}{2}\sum_{i=1}^{n} u_i u_{n-i+1}.$$

If the position i in the section is marked with $p_{(i)}$,i=1,2,3,4,5,6.

$p_{(i)}$ corresponding to a total of 36 kinds of forms, wherein

$C_{M(0)}$ =card{($p_{(1)}$, $p_{(6)}$), ($p_{(2)}$, $p_{(5)}$), ($p_{(3)}$, $p_{(4)}$)}, $C_{M(0)}$ there are six kinds of corresponding form;

$C_{M(1)}$ =card{($p_{(1)}$, $p_{(3)}$), ($p_{(2)}$, $p_{(2)}$), ($p_{(5)}$, $p_{(6)}$)}, $C_{M(1)}$ there are five kinds of corresponding form;

$C_{M(2)}$ =card{($p_{(2)}$, $p_{(6)}$), ($p_{(3)}$, $p_{(5)}$), ($p_{(4)}$, $p_{(4)}$)}, $C_{M(2)}$ there are five kinds of corresponding form;

$C_{M(3)}$ =card{($p_{(1)}$, $p_{(4)}$), ($p_{(2)}$, $p_{(3)}$), ($p_{(6)}$, $p_{(6)}$)}, $C_{M(3)}$ there are five kinds of corresponding form;

$C_{M(4)}$ =card{($p_{(1)}$, $p_{(1)}$), ($p_{(3)}$, $p_{(6)}$), ($p_{(4)}$, $p_{(5)}$)}, $C_{M(4)}$ there are five kinds of corresponding form;

$C_{M(5)}$ =card{($p_{(1)}$, $p_{(5)}$), ($p_{(2)}$, $p_{(4)}$), ($p_{(3)}$, $p_{(3)}$)}, $C_{M(5)}$ there are five kinds of corresponding form;

$C_{M(6)}$ =card{($p_{(1)}$, $p_{(2)}$), ($p_{(4)}$, $p_{(6)}$), ($p_{(5)}$, $p_{(5)}$)}, $C_{M(6)}$ there are five kinds of corresponding form.

The probability is the same between prime numbers in n subsections 1 ~ 6. In the uniaxial correspondence,

$$C_{M(0)} = [\frac{6}{36}\cdot\frac{1}{2}\sum_{i=1}^{n}u_i u_{n-i+1}=\frac{1}{12}\sum_{i=1}^{n}u_i u_{n-i+1}]\ ;$$

$$C_{M(1)} = C_{M(2)} = C_{M(3)} = C_{M(4)} = C_{M(5)} = C_{M(6)} = [\frac{5}{36}\cdot\frac{1}{2}\sum_{i=1}^{n}u_i u_{n-i+1}=\frac{5}{72}\sum_{i=1}^{n}u_i u_{n-i+1}]\ .$$

([x] is the largest integer not more than x)

e.g. The B_1 axis, six small section,

u_1=5，u_2=2，u_3=6，u_4=2，u_5=3，u_6=5.

$C_{1292(4)}$= card{(241$_{(5)}$, 1051$_{(4)}$), (271$_{(6)}$, 1021$_{(3)}$), (541$_{(1)}$, 751$_{(1)}$), (601$_{(3)}$, 691$_{(6)}$), (631$_{(4)}$, 661$_{(5)}$)}=5;

$C_{1322(6)}$= card{(151$_{(2)}$, 1171$_{(1)}$), (271$_{(6)}$, 1051$_{(4)}$), (331$_{(1)}$, 991$_{(2)}$), (571$_{(2)}$, 751$_{(1)}$), (631$_{(4)}$, 691$_{(6)}$), (661$_{(5)}$, 661$_{(5)}$)}=6;

$C_{1352(1)}$= card{(151$_{(2)}$, 1201$_{(2)}$), (181$_{(3)}$, 1171$_{(1)}$), (331$_{(1)}$, 1021$_{(3)}$), (541$_{(1)}$, 811$_{(3)}$), (601$_{(3)}$, 751$_{(1)}$), (661$_{(5)}$, 691$_{(6)}$)}=6;

$C_{1382(3)}$= card{(151$_{(2)}$, 1231$_{(3)}$), (181$_{(3)}$, 1201$_{(2)}$), (211$_{(4)}$, 1171$_{(1)}$), (331$_{(1)}$, 1051$_{(4)}$), (571$_{(2)}$, 811$_{(3)}$), (631$_{(4)}$, 751$_{(1)}$), (691$_{(6)}$, 691$_{(6)}$)}=7;

$C_{1412(5)}$= card{(181$_{(3)}$, 1231$_{(3)}$), (211$_{(4)}$, 1201$_{(2)}$), (241$_{(5)}$, 1171$_{(1)}$), (421$_{(4)}$, 991$_{(2)}$), (601$_{(3)}$, 811$_{(3)}$), (661$_{(5)}$, 751$_{(1)}$)}=6;

$C_{1442(0)}$= card{(151$_{(2)}$, 1291$_{(5)}$), (211$_{(4)}$, 1231$_{(3)}$), (241$_{(5)}$, 1201$_{(2)}$), (271$_{(6)}$, 1171$_{(1)}$), (421$_{(4)}$, 1021$_{(3)}$), (631$_{(4)}$, 811$_{(3)}$), (691$_{(6)}$, 751$_{(1)}$)}=7;

$C_{1472(2)}$= card{(151$_{(2)}$, 1321$_{(6)}$), (181$_{(3)}$, 1291$_{(5)}$), (241$_{(5)}$, 1231$_{(3)}$), (271$_{(6)}$, 1201$_{(2)}$), (421$_{(4)}$, 1051$_{(4)}$), (661$_{(5)}$, 881$_{(3)}$)}=6.

Or

$C_{1412(5)}$= card{(181$_{(3)}$, 1231$_{(3)}$), (211$_{(4)}$, 1201$_{(2)}$), (241$_{(5)}$, 1171$_{(1)}$), (421$_{(4)}$, 991$_{(2)}$), (601$_{(3)}$, 811$_{(3)}$), (661$_{(5)}$, 751$_{(1)}$)}=6;

$C_{1442(0)}$= card{(151$_{(2)}$, 1291$_{(5)}$), (211$_{(4)}$, 1231$_{(3)}$), (241$_{(5)}$, 1201$_{(2)}$), (271$_{(6)}$, 1171$_{(1)}$), (421$_{(4)}$, 1021$_{(3)}$), (631$_{(4)}$, 811$_{(3)}$), (691$_{(6)}$, 751$_{(1)}$)}=7;

$C_{1472(2)}$= card{(151$_{(2)}$, 1321$_{(6)}$), (181$_{(3)}$, 1291$_{(5)}$), (241$_{(5)}$, 1231$_{(3)}$), (271$_{(6)}$, 1201$_{(2)}$), (421$_{(4)}$, 1051$_{(4)}$), (661$_{(5)}$, 881$_{(3)}$)}=6;

$C_{1502(4)}$= card{(181$_{(3)}$, 1321$_{(6)}$), (211$_{(4)}$, 1291$_{(5)}$), (271$_{(6)}$, 1231$_{(3)}$), (331$_{(1)}$,1171$_{(1)}$), (691$_{(6)}$,811$_{(3)}$), (751$_{(1)}$,751$_{(1)}$)}=6;

$C_{1532(6)}$= card{(151$_{(2)}$, 1381$_{(1)}$), (211$_{(4)}$, 1321$_{(6)}$), (241$_{(5)}$, 1291$_{(5)}$),(331$_{(1)}$, 1201$_{(2)}$), (541$_{(1)}$, 991$_{(2)}$)}=5;

$C_{1562(1)}$= card{(181$_{(3)}$, 1381$_{(1)}$), (241$_{(5)}$, 1321$_{(6)}$), (271$_{(6)}$, 1291$_{(5)}$), (331$_{(1)}$, 1231$_{(3)}$), (541$_{(1)}$, 1021$_{(3)}$), (571$_{(2)}$, 991$_{(2)}$) , (751$_{(1)}$, 811$_{(3)}$)}=7;

$C_{1592(3)}$= card{(211$_{(4)}$, 1381$_{(1)}$), (271$_{(6)}$, 1321$_{(6)}$), (421$_{(4)}$, 1171$_{(1)}$), (541$_{(1)}$, 1051$_{(4)}$), (571$_{(2)}$, 1201$_{(3)}$), (601$_{(3)}$, 991$_{(2)}$)}=6.

$C_M = \sum_{i=1}^{6}u_i u_{n-i+1}$ = (5×5+2×3+6×2+2×6+3×2+5×5)=86. So

$$C_{M(1)} = C_{M(2)} = C_{M(3)} = C_{M(4)} = C_{M(5)} = C_{M(6)} = [\frac{5}{72}\sum_{i=1}^{n}u_i u_{n-i+1}]=5;$$

ISSN 2347-1921

$C_{M(0)} = [\frac{1}{12}\sum_{i=1}^{n} u_i u_{n-i+1}] = 7$;

The section-to-section correspondence (the sum of two numbers) to indicate prime pair of even numbers is called **the correspondence model of even numbers**.

3.4. Prime Pairs of Even Numbers

3.4.1. Prime Pairs of Even Numbers

According to the **axis correspondence form of even numbers**, the prime pair of one even number from single correspondence is no more than 1, so no need to discuss it; From the correspondence model, Uniaxial correspondence $C_M = [\frac{5}{72}\sum_{i=1}^{n} u_i u_{n-i+1}]$; biaxial correspondence $C_M = [\frac{5}{36}\sum_{i=1}^{n} u_i u_{n-i+1}]$. Prime pair numbers of "B_i" and "A_i" are less than those of "O_i", so the calculation formula of prime pairs of even numbers is:

$$C_M = [\frac{5}{72}\sum_{i=1}^{n} u_i u_{n-i+1}] + [\frac{5}{36}\sum_{i=1}^{n} u_i u_{n-i+1}] = [\frac{5}{24}\sum_{i=1}^{n} u_i u_{n-i+1}].$$

Generally, u_1, u_2, …, $u_{n/2}$ are not less than $u_{n/2+1}$, $u_{n/2+2}$, …, u_n, $n = \frac{M}{210}$.

$$C_M = [\frac{5}{24}\sum_{i=1}^{n} u_i u_{n-i+1}] \geq [\frac{5}{12}\sum_{i=n/2+1}^{n} u_i^2] \geq [\frac{5}{6n}(\sum_{i=n/2+1}^{n} u_i)^2] = \frac{175}{M}(\frac{1}{8}\sum_{i=n/2+1}^{n} u_i)^2 = \frac{175}{64M}(\sum_{i=n/2+1}^{n} u_i)^2$$

$$= \frac{175}{64M}[\pi(M) - \pi(\frac{1}{2}M)]^2 = \frac{175}{64M}[\pi(M_{\triangle})]^2.$$

Table 3.4.1. Calculate the number C_M of and the actual number C'_M of Comparison Table

M	5×10^3	5.5×10^3	6×10^3	7×10^3	8×10^3	9×10^3	1×10^4	2×10^4
π(M△)	299	321	350	411	458	507	561	1035
C_M	65	68	148	105	95	208	114	195
C'_M	71	94	173	112	102	236	125	225

M	3×10^4	4×10^4	5×10^4	6×10^4	7×10^4	8×10^4	9×10^4	1×10^5
π(M△)	1496	1938	2371	2807	3203	3634	4038	4479
C_M	543	342	409	957	641	601	1321	731
C'_M	590	379	440	1074	706	643	1454	800

Note: $C_M = \frac{175\pi^2(M_{\triangle})}{48M}$,(3∤M); $C_M = \frac{175\pi^2(M_{\triangle})}{24M}$, (3|M); $C_M = \frac{35\pi^2(M_{\triangle})}{8M}$, (7|M); C'_M is the actual number.

3.4.2. The truth of Goldbach conjecture

Because $\frac{2\pi(M)}{3} - \pi(\frac{1}{2}M) = \frac{2M}{\ln M} - \frac{\frac{1}{2}M}{\ln\frac{1}{2}M} = \frac{M(2\ln\frac{1}{2}M - \ln M)}{2\ln M \cdot \ln\frac{1}{2}M} = \frac{M(\ln M - 2\ln 2)}{2\ln M(\ln M - \ln 2)} > 0.$

So $\pi(M) - \pi(\frac{1}{2}M) > \frac{\pi(M)}{3}$.

$$C_M = \frac{175}{64M}[\pi(M_{\triangle})]^2 = \frac{175}{64M}[\pi(M) - \pi(\frac{1}{2}M)]^2 \geq \frac{175}{64M}[\frac{\pi(M)}{3}]^2 = \frac{175\pi^2(M)}{576M}.$$

Lemma 3.4.2.1 If $\pi(p_{n+1}^2)$ represents the prime number in the range of p_{n+1}^2, then

$$\pi(p_{n+1}^2) = [p_{n+1}^2 \cdot \frac{\prod_{i=1}^{n}(p_i - 1)}{\prod_{i=1}^{n} p_i}] + (n-1).$$

By Lemma 3.4.2.1,

$$C_{p_{n+1}^2} = \frac{175\pi^2(M)}{576M} = \frac{175}{576M}[p_{n+1}^2 \cdot \frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n} p_i} + (n-1)]^2 > \frac{175}{576 p_{n+1}^2} \cdot [p_{n+1}^2 \cdot \frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n} p_i}]^2 = \frac{175}{576} \cdot [\frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n-1} p_i}]^2 .$$

Because $\frac{p_i - 1}{p_{i-1}} > 1$, so $\lim_{n\to\infty} C_{p_{n+1}^2} = \infty$.

For even numbers more than 2, all even numbers have prime number pairs in a smaller range. In a broader range, generally, the greater the even number is, the more prime numbers pairs it has. So every even integer greater than 2 can be expressed as the sum of two primes. This proves that **Goldbach conjecture** is true.

References

[1] Song, K; WANG, X. THE EXPRESSION ON PRIMES NUMBER VOLUME 5, ISSUE 1, FEBRUARY 2015, PAGES 1-22 ISSN 0976-8475 http://www.mililink.com/journals_eb.php?id=62

[2]. Song, K. Related Distribution of Prime Numbers ISSN 1925-251X [Print], ISSN 1925-2528 [Online].

Journal number: Vol. 5, No. 2, 2013, pp. [11-14] Web site: http://cscanada.net/index.php/pam/issue/current

[3]. Song, K . Prime Pairs of Even Numbers ISSN 1925-251X [Print], ISSN 1925-2528 [Online].

Issue number: Vol. 5, No. 2, 2013, pp. [11-14] Web site: http://cscanada.net/index.php/pam/issue/current

[4] . Song, K . Related Distribution of Prime Numbers. ISSN 1923-8444 [Print], ISSN 1923-8452 [Online].

Journal number: Vol. 6, No. 2, 2013, pp. [96-103] Web site:http://cscanada.net/index.php/sms/article/view/j.sms.1923845220130602.478

[5]. Xiong, Q. (1982). Elementary number theory (In Chinese). Wuhan: Hubei Education Press.

[6]. Song, K. (2007). Elementary number theory (In Chinese). Beijing: China Drama Press.

Author' biography with Photo

Kaifu Song, 1954-12-14; Undergraduate; Senior secondary school teachers(Associate professor level). Engaged in education for 40 years.

Has long been engaged in "Elementary Number Theory" research. 2007 published monograph Elementary number theory, The writings to trunk the contents elementary number theory , "Congruences" 、"One yuan congruences equation" 、"Quadratic congruence equation","Primitive root"、" Indeterminate equation"have improvement in or enrich，"Even number primes ","distribution of prime numbers"also discussed. Writings of hubei Province teaching and research won the 2007 outstanding achievement award.