

## Related Distribution of Prime Numbers

Kaifu SONG<sup>[a],\*</sup>

<sup>[a]</sup> East Lake High School, Yichang, Hubei, China.

\* Corresponding author.

Address: East Lake High School, Yichang 443100, Hubei, China; E-Mail: skf08@sina.com

Received: March 6, 2013/ Accepted: May 10, 2013/ Published: May 31, 2013

---

**Abstract:** The surplus model is established, and the distribution of prime numbers are solved by using the surplus model.

**Key words:** Surplus model; Distribution of prime numbers

---

Song, K. (2013). Related Distribution of Prime Numbers. *Studies in Mathematical Sciences*, 6(2), 96–103. Available from <http://www.cscanada.net/index.php/sms/article/view/j.sms.1923845220130602.478> DOI: 10.3968/j.sms.1923845220130602.478

---

### 1. SURPLUS MODEL

In the range of  $1 \sim N$ ,  $r_1$  represents the quantity of numbers which do not contain a factor 2,  $r_1 = [N \cdot \frac{1}{2}]$  ( $[x]$  is the largest integer not greater than  $x$ );  $r_2$  represents the quantity of numbers which do not contain factor 3,  $r_2 = [r_1 \cdot \frac{2}{3}]$ ;  $r_3$  represents the quantity of numbers do not contain factor 5,  $r_3 = [r_2 \cdot \frac{4}{5}]$ ; ...

In the range of  $1 \sim N$ ,  $r_i$  represents the quantity of numbers which do not contain factor  $p_i$ , the method of the surplus numbers  $r_{i-1}$  to  $r_i$  is called *the residual model of related distribution of prime numbers*.

In the range of  $1 \sim N$ , excluding all multiples of prime numbers which are not greater than  $\sqrt{M}$  ( $M \leq N$ ), then  $r$  is the surplus number. For the factor that  $[\frac{rM}{N}] \leq r$ , so there are at least  $[\frac{rM}{N}]$  related primes in the range of  $M$ .

## 2. RELATED DISTRIBUTION OF PRIME NUMBERS

### 2.1. Distribution of Prime Numbers

Exclusion the multiples of 2, 3, 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  $B$ :  $3n + 1$ ).

On number axis ( $A$ -axis or  $B$ -axis),  $r_0$  represents the quantity of numbers which do not contain factors 2, 3, 5, 7,  $r_0 = \lfloor \frac{8}{35} \cdot N \rfloor$ ;  $r_1$  represents the quantity of numbers which do not contain prime factor  $P_1$  ( $P_1 > 7$ ),  $r_1 = \lfloor r_0 \cdot \frac{p_1 - 1}{p_1} \rfloor$ ;  $r_2$  represents the quantity of numbers which do not contain prime factor  $P_2$ ,  $r_2 = \lfloor r_1 \cdot \frac{p_2 - 1}{p_2} \rfloor$ ; ...  
 $r_i = \lfloor r_{i-1} \cdot \frac{p_i - 1}{p_i} \rfloor$ .

The method of the surplus numbers  $r_{i-1}$  to  $r_i$  is called *the surplus model of distribution of prime numbers*.

$S_n$  is the quantity of prime numbers in the range of  $N$ , make  $M = p_n^2$ , by

$$S_n = \lfloor r_{n-1} \cdot \frac{p_n - 1}{p_n} \cdot \frac{M}{N} \rfloor = \lfloor r_{n-1} \cdot \frac{p_n - 1}{p_n} \cdot \frac{p_n^2}{N} \rfloor. \tag{1}$$

$$S_{n-1} = \lfloor \lfloor r_{n-2} \cdot \frac{p_{n-1} - 1}{p_{n-1}} \rfloor \frac{p_{n-1}^2}{N} \rfloor. \tag{2}$$

We can obtain

$$S_n = \lfloor \frac{(p_n - 1)p_n}{p_{n-1}^2} \cdot S_{n-1} \rfloor,$$

where  $S_1 = \lfloor \frac{8 \times 10 \times 11}{35} \rfloor = 25$ . ( $r_{n-1} = \lfloor \dots \lfloor \frac{8}{35} \cdot N \rfloor \frac{p_1 - 1}{p_1} \dots \rfloor \frac{p_{n-1} - 1}{p_{n-1}}$ ).

For the fact that  $\frac{(p_i - 1)p_i}{p_{i-1}^2} > 1$ , so  $\{ \lfloor \frac{(p_i - 1)p_i}{p_{i-1}^2} \cdot S_{i-1} \rfloor \}$  ( $i = 1, 2, \dots, n$ ) are ascending series in which all numbers are not less than 25. Therefore,  $\lim_{n \rightarrow \infty} S_n = \infty$ , there are infinite prime numbers in natural numbers.

### 2.2. Distribution of Primes in Arithmetic Series

$S_{(a,r)}$  is the quantity of prime numbers which have the form  $an + r$  ( $(a, r) = 1$ ), then

$$S_{(a,r)} = \frac{S_n}{\varphi(a)} = \lfloor \frac{p_n(p_n - 1)}{\varphi(a)p_{n-1}^2} \cdot S_{n-1} \rfloor,$$

where  $S_1 = 25$ . ( $\varphi(a)$ ) is Euler function of  $a$ .)

$a$  is a constant,  $\varphi(a)$  is a constant. There are infinite prime numbers which have the form  $an + r$  ( $(a, r) = 1$ ).

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

Make  $n^2 = p_n^2$ ,  $(n + 1)^2 = (p_n + 1)^2$ , then  $S'_n$  is the quantity of prime numbers in the range of  $(p_n + 1)^2$ ,

$$S'_n = \left[ \frac{(p_n + 1)(p_n + 1 - 1)}{p_n^2} \cdot S_n \right].$$

Let  $f(n) = S'_n - S_n = \left[ \frac{(p_n + 1)(p_n + 1 - 1)}{p_n^2} \cdot S_n \right] - [S_n] = \left[ \frac{[S_n]}{p_n} \right]$ , where  $S_1 = 25$ .

For  $f(n) = \left[ \frac{(p_n - 1)}{p_{n-1}} \left[ \frac{(p_{n-1} - 1)}{p_{n-2}} \left[ \frac{(p_{n-2} - 1)}{p_{n-3}} \left[ \dots \left[ \frac{(p_2 - 1)}{p_1^2} \cdot S_1 \dots \right] \right] \right] \right] \right]$ , and  $\frac{p_i - 1}{p_{i-1}} > 1$ . Then  $\lim_{n \rightarrow \infty} f(n) = \infty$ .

The quantity of prime numbers between  $n^2$  and  $(n + 1)^2$  are increasing along with the increasing of  $n$ . In a small range, there is at least one prime number between  $n^2$  and  $(n + 1)^2$ . Therefore, there is at least one prime number between  $n^2$  and  $(n + 1)^2$ ; and the quantity of the prime number are increasing along with the increasing of  $n$ .

### 2.4. The Interval Between Primes $p_{i-1}$ and $p_i$

During the distribution of prime numbers,

$$S_n = \left[ \frac{p_n}{p_{n-1}} \left[ \frac{(p_n - 1)}{p_{n-2}} \left[ \frac{(p_{n-1} - 1)}{p_{n-3}} \left[ \dots \left[ \frac{p_3 - 1}{p_1} \left[ \frac{p_2 - 1}{p_1} \cdot S_1 \right] \dots \right] \right] \right] \right] \right].$$

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

$$\overline{p_i - p_{i-1}} = \frac{p_n^2}{S_n} = \left[ \frac{p_n}{p_{n-1}} \left[ \frac{p_{n-1}}{p_{n-1} - 1} \left[ \dots \left[ \frac{p_2}{p_2 - 1} \left[ \frac{p_1^2}{S_1} \right] \dots \right] \right] \right] \right], \quad \frac{p_i}{p_{i-1}} > 1.$$

and  $\lim_{n \rightarrow \infty} \overline{p_i - p_{i-1}} = \infty$ .

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  $p_i$  tends to infinity.

### 2.5. Distribution of Twin Primes

On number axis pair  $(A_1 - B_3$  or  $A_7 - B_9$  or  $A_9 - B_1)$ ,  $r_0$  represents the quantity of numbers which do not contain factors 2, 3, 5, 7,  $r_0 = \left[ \frac{1}{14} \cdot N \right]$ ;  $r_1$  represents the quantity of numbers which do not contain factor  $p_1$ ,  $r_1 = \left[ r_0 \cdot \frac{p_1 - 2}{p_1} \right]$ ;  $r_2$  represents the quantity of numbers which do not contain factor  $p_2$ ,  $r_2 = \left[ r_1 \cdot \frac{p_2 - 2}{p_2} \right]$ ; ...  $r_i = \left[ r_{i-1} \cdot \frac{p_i - 2}{p_i} \right]$ .

The method of the surplus numbers  $r_{i-1}$  to  $r_i$  is called *the surplus model of distribution of twin primes*.

$L_n$  is the quantity of twin primes in the range of  $N$ , let  $M = p_n^2$ , by

$$L_n = [r_{n-1} \cdot \frac{p_n - 2}{p_n} \cdot \frac{M}{N}] = [r_{n-1} \cdot \frac{p_n - 2}{p_n} \cdot \frac{p_n^2}{N}] \tag{3}$$

$$L_{n-1} = [[r_{n-2} \cdot \frac{p_{n-1} - 2}{p_{n-1}}] \frac{p_{n-1}^2}{N}]. \tag{4}$$

We can obtain that

$$L_n = [\frac{(p_n - 2)p_n}{p_{n-1}^2} \cdot L_{n-1}],$$

where  $L_1 = [\frac{11 \times 9}{14}] = 7$ . ( $r_{n-1} = [\dots[\frac{1}{14}N] \frac{p_1 - 2}{p_1}] \dots] \frac{p_{n-1} - 2}{p_{n-1}}$ ).

For the fact that  $\frac{(p_i - 2)p_i}{p_{i-1}^2} > 1$ , so  $\{[\frac{(p_i - 2)p_i}{p_{i-1}^2} \cdot L_{i-1}]\}$  ( $i = 1, 2, \dots, n$ ) are ascending series in which all numbers are not less than 7. Therefore,  $\lim_{n \rightarrow \infty} L_n = \infty$ , there are infinite twin primes in natural numbers.

### 2.6. Distribution of Twin Prime Numbers Within Ten

There are two pairs of twin prime numbers within 10, these two pairs of twin prime numbers are called *twin prime numbers within ten*. For example, 11, 13, 17, 19 are twin prime numbers within ten.

On number axis pair  $(A_1 - B_3 - A_7 - B_9)$ ,  $r_0$  represents the quantity of numbers which do not contain factors 2, 3, 5, 7,  $r_0 = \frac{1}{70} \cdot N$ ;  $r_1$  represents the quantity of numbers which do not contain factor  $p_1$ ,  $r_1 = r_0 \cdot \frac{p_1 - 4}{p_1}$ ;  $r_2$  represents the quantity of numbers which do not contain factor  $p_2$ ,  $r_2 = r_1 \cdot \frac{p_2 - 4}{p_2}$ ;...  $r_i = r_{i-1} \cdot \frac{p_i - 4}{p_i}$ .

The method of the surplus numbers  $r_{i-1}$  to  $r_i$  is called *the surplus model of distribution of twin prime numbers within 10*.

$T_n$  indicates the quantity of twin prime numbers within 10, let  $M = p_n^2$ , by

$$T_n = r_{n-1} \cdot \frac{p_n - 4}{p_n} \cdot \frac{M}{N} = r_{n-1} \cdot \frac{p_n - 4}{p_n} \cdot \frac{p_n^2}{N}. \tag{5}$$

$$T_{n-1} = r_{n-2} \cdot \frac{p_{n-1} - 4}{p_{n-1}} \cdot \frac{p_{n-1}^2}{N}. \tag{6}$$

We can obtain that

$$T_n = \frac{(p_n - 4)p_n}{p_{n-1}^2} \cdot T_{n-1},$$

where  $T_1 = \frac{11 \times 7}{70} \cong 1.10$ . ( $r_{n-1} = \frac{1}{70} \cdot N \cdot \frac{p_1 - 4}{p_1} \cdot \dots \cdot \frac{p_{n-1} - 4}{p_{n-1}}$ ). By

$$\begin{aligned} T_n &= \frac{p_n(p_n - 4)}{p_{n-1}^2} \cdot \frac{p_{n-1}(p_{n-1} - 4)}{p_{n-2}^2} \cdot \frac{p_{n-2}(p_{n-2} - 4)}{p_{n-3}^2} \cdot \dots \cdot \frac{p_2(p_2 - 4)}{p_1^2} \cdot T_1 \\ &= \frac{p_n}{p_{n-1}} \cdot \frac{(p_n - 4)}{p_{n-2}} \cdot \frac{(p_{n-1} - 4)}{p_{n-3}} \cdot \dots \cdot \frac{p_3 - 4}{p_1} \cdot \frac{p_2 - 4}{p_1} \cdot T_1 \end{aligned}$$

For the fact that  $\frac{p_3 - 4}{p_1} \cdot \frac{p_2 - 4}{p_1} \cdot T_1 > 1$ ,  $\frac{p_i - 4}{p_{i-2}} > 1$  ( $i = 4, \dots, n$ ), so  $\lim_{n \rightarrow \infty} T_n = \infty$ , there are infinite twin prime numbers within 10 (For example, 36 pairs in the range of  $10^5$ ).

### 2.7. Distribution of $n^2 + 1$ Prime Numbers

**Lemma 7.1**  $4(mp + 10x)^2 + 1 \equiv 4(mp - 10x)^2 + 1 \pmod{p}$ , where  $p$  is an odd prime.

*Proof.*

$$4(mp + 10x)^2 + 1 - 4(mp - 10x)^2 - 1 = 16m xp.$$

□

**Lemma 7.2** If  $x \pm y \not\equiv 0 \pmod{p}$ , then  $4(mp + 10x)^2 + 1 \not\equiv 4(mp + 10y)^2 + 1 \pmod{p}$ .

*Proof.*

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

Because 400 and  $x \pm y \pmod{p}$  are not of congruence, then this Lemma is proved. □

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

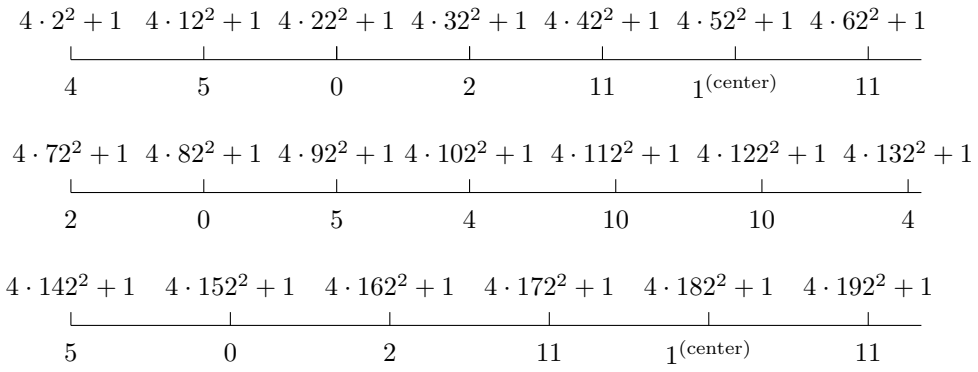
$(4n^2 + 1, 4n + 3) = 1$ , denote the prime numbers with the form  $4n + 1$  by  $q_i$ .

**Theorem 7.1** On the number axis  $4t^2 + 1$ , there are two multiples of  $q_i$  at every  $q_i$  distance.

*Proof.* By Lemma 7.1, Lemma 7.2 know,  $4t^2 + 1$  number axis appear multiples of the  $q_i$ , distributed  $4(mq_i)^2 + 1$  into a center of symmetry.

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

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



**Figure 1**

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

### 2.8. Distribution of Prime Triplet

If  $p_i, p_i + 2, p_i + 6$  are all prime numbers, then these three-digits group is called a *prime triplet*.

On number axes group ( $A_1 - B_3 - A_7$  or  $A_7 - B_9 - A_3$ ), similarly,  $r_0 = [\frac{4}{105} \cdot N]$ ;  
 $r_1 = [r_0 \cdot \frac{p_1 - 3}{p_1}]$ ;  $r_2 = [r_1 \cdot \frac{p_2 - 3}{p_2}]$ ; ...  $r_i = [r_{i-1} \cdot \frac{p_i - 3}{p_i}]$ .

The method of the surplus numbers  $r_{i-1}$  to  $r_i$  is called *the residual model of distribution of prime triplet*.

$E_n$  is a prime triplet in the range of  $N$ , let  $M = p_n^2$ , by

$$E_n = [r_{n-1} \cdot \frac{p_n - 3}{p_n} \cdot \frac{M}{N}] = [r_{n-1} \cdot \frac{p_n - 3}{p_n} \cdot \frac{p_n^2}{N}]. \tag{7}$$

$$E_{n-1} = [[r_{n-2} \cdot \frac{p_{n-1} - 3}{p_{n-1}}] \frac{p_{n-1}^2}{N}]. \tag{8}$$

We can obtain that

$$E_n = [\frac{(p_n - 3)p_n}{p_{n-1}^2} \cdot E_{n-1}],$$

where  $E_1 = [\frac{4 \times 11 \times 8}{105}] = 3$ . ( $r_{n-1} = [\dots [\frac{4}{105} \cdot N] \frac{p_1 - 3}{p_1}] \dots [\frac{p_{n-1} - 3}{p_{n-1}}]$ ).

For the fact that  $\frac{(p_i - 3)p_i}{p_{i-1}^2} > 1$ , so  $\{[\frac{(p_i - 3)p_i}{p_{i-1}^2} \cdot S_{i-1}]\}$  ( $i = 1, 2, \dots, n$ ) are ascending series in which all numbers are not less than 3. Therefore,  $\lim_{n \rightarrow \infty} E_n = \infty$ , there are infinite prime triplets in natural numbers.

### 2.9. Primes Distribution of $n^2 - n + p_i$ Primes

**Lemma 9.1** There are only  $\frac{p+1}{2}$  residual classes in  $n^2 - n$  for odd prime  $p$ .

*Proof.*  $n = 1, (p \pm 1)(p \pm 0) \equiv 0 \pmod{p}$ ;

$n = 2, (p \pm 2)(p \pm 1) \equiv 2 \times 1 \pmod{p}$ ;

$n = 3, (p \pm 3)(p \pm 2) \equiv 3 \times 2 \pmod{p}$ ;

...

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

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

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

That is  $f(\frac{p+3}{2}) \equiv f(\frac{p-1}{2}) \pmod{p}$ . Let  $f(n) = (p \pm n)(p \pm (n-1)) \equiv n(n-1) \pmod{p}$ ;

$$\begin{aligned} & \frac{p+1+2t}{2} \times \frac{p+1+2(t-1)}{2} = \frac{p+1-2t+4t}{2} \times \frac{p+1-2(t+1)+4t}{2} \\ & = \frac{p+1-2t}{2} \times \frac{p+1-2(t+1)}{2} + 2tp \equiv \frac{p+1-2t}{2} \times \frac{p+1-2(t+1)}{2} \pmod{p}. \end{aligned}$$

That is  $f(\frac{p+1+2t}{2}) \equiv f(\frac{p+1-2t}{2}) \pmod{p}$ .

Therefore, there are only  $1 \times 0, 2 \times 1, \dots, \frac{p+1}{2} \cdot \frac{p-1}{2}$  different residual classes in  $n^2 - n$  for prime  $p$ . □

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

**Lemma 9.2** Let  $n^2 - n \equiv r_2 \pmod{p_i}$ ,  $A_1$  number axes  $\frac{p_i+1}{2}$  residue class are no longer make proposition holds.

*Proof.* Let  $a \in A_1, a \equiv r_1 \pmod{p_i}, r_1 = 0, 1, \dots, p_i-1$ .

$$n^2 - n \equiv r_2 \pmod{p_i}, \text{ then by Lemma 9.1, } r_2 = 0, 2, 6, \dots, \frac{p_i+1}{2}.$$

If  $r_1 + r_2 \equiv 0 \pmod{p_i}$ , then  $a + r_2 \equiv 0 \pmod{p_i}$ ,  $a + r_2$  is a composite number.

Any number in  $r_2$  can make  $r_1 + r_2 \equiv 0 \pmod{p_i}$  established, then  $a + r_2$  is a composite number. □

Similarly,  $r_0 = [\frac{1}{35} \cdot N]$ ; surplus numbers (with the quantity of  $r_0$ ) divided by  $p_1$  respectively residual  $0, 1, 2, \dots, p_1-1$ .  $n^2 - n$  divided by  $p_1$  have different residue class,

by Lemma 9.2,  $p_1$  exclude  $[r_0 \cdot \frac{p_1+1}{2p_1}]$  numbers,  $r_1 = r_0 - [r_0 \frac{p_1+1}{2p_1}] = [r_0 \frac{p_1-1}{2p_1}]$ ;

$r_2$  represents the numbers which do not contain factor  $p_2, r_2 = [r_1 \cdot \frac{p_2-1}{2p_2}]$ ; ...

$$r_i = [r_{i-1} \cdot \frac{p_i-1}{2p_i}].$$

The method of the surplus numbers  $r_{i-1}$  to  $r_i$  is called *the residual model of distribution of  $n^2 - n + p_i$  prime numbers*.

$Q_n$  is a proposition holds the number of the  $N$ -range, let  $M = p_n^2$ , by

$$Q_n = [r_{n-1} \cdot \frac{p_n - 1}{2p_n} \cdot \frac{M}{N}] = [r_{n-1} \cdot \frac{p_n - 1}{2p_n} \cdot \frac{p_n^2}{N}]. \quad (9)$$

$$Q_{n-1} = [[r_{n-2} \cdot \frac{p_{n-1} - 1}{2p_{n-1}}] \frac{p_{n-1}^2}{N}]. \quad (10)$$

We can get:

$$Q_n = [\frac{(p_n - 1)p_n}{2p_{n-1}^2} \cdot Q_{n-1}],$$

where  $Q_1 = [\frac{11}{7}] = 1$ . ( $r_{n-1} = [\dots[\frac{1}{35} \cdot N] \frac{p_1 - 1}{2p_1} \dots] \frac{p_{n-1} - 1}{2p_{n-1}}$ ). and then

$$Q_n = [\frac{(p_n - 1)p_n}{2p_{n-1}^2} \cdot Q_{n-1}] \leq \frac{p_n^2}{35 \cdot 2^n} \prod_{i=1}^n \frac{p_i - 1}{p_i}.$$

Based of Bertrand assumption, there is at least one prime between  $n$  and  $2n$  and at least one prime between  $2^{n-1}$  and  $2^n$ . When  $n \geq 12$  ( $p_{12} = 53$ ),

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

Thereby,  $\lim_{n \rightarrow \infty} Q_n = 0$ .

There are infinitely primes  $p_i$  when  $N = 2, 3$ ; all  $n^2 - n + p_i$  are primes when  $0 \leq n \leq N$ ; only some special natural numbers  $N$  when  $N = p_i - 1$ ; all  $n^2 - n + p_i$  are primes when  $0 \leq n \leq N$ . The greater  $N$  is, the smaller possibility the proposition holds. Therefore, there are only 6 primes ( $p_i = 2, 3, 5, 11, 17, 41$ ) that make the proposition hold.

## REFERENCES

- [1] Hua, Loo-Keng. (1979). *An introduction to number theory* (In Chinese). Beijing: Science Press.
- [2] Song, K. (2007). *Elementary number theory* (In Chinese). Beijing: China Drama Press.