A Study of Ralationship of RSA with Goldbach's Conjecture and It's Properties

Chenglian Liu[1⋆] and Jian Ye[2]

School of Mathematics and Computer Science, Longyan University, Longyan 364012, China.
[1]chenglian.liu@gmail.com;[2]yoyoo20082005@sina.com

Abstract. The Goldbach's conjecture has plagued mathematicians for over two hundred and seventy years. Whether a professional or an amateur enthusiast, all have been fascinated by this question. Why do mathematicians have no way to solve this problem? Up until now, Chen has been recognized for the most concise proof his "$1 + 2$" theorem in 1973. In this article, the author will use elementary concepts to describe and indirectly prove the Goldbach conjecture.

Keywords: Symmetrical primes; Number axis; AKS algorithm;

1 Introduction

Until now, the best proof of the theorem is by Chen [3] in 1973 that states every large even integer can be written as the sum of a prime and the product of at most two primes. Recently, Bournas [2] proposed his contribution that proves the conjecture is true for all even integers greater than 362. Silva et al. [5] describes how the even Goldbach conjecture was confirmed to be true for all even numbers not larger than $4 \cdot 10^{18}$ and the odd Goldbach conjecture is true up to $8.37 \cdot 10^{26}$. Lu [14] proves an even integer x at most $\mathcal{O}(x^{0.879})$ can not be written as a sum of two primes. On the other hand, Zhang [23] proves that there are infinitely many pairs of primes that differ by less than $7 \cdot 10^7$. Zhang's result is huge step forward in the direction of the twin prime conjecture. Some people in related research also gave good contributions [7–11, 16, 20, 22]. In this paper, the author will introduce the fundamental concepts rather than the entire proof in its complexity.

⋆ Corresponding author: Chenglian Liu.

2 Review of Goldbach conjecture issue

The (strong) Goldbach conjecture states that every even integer N greater than six can be written as the sum of two primes such as

$$\begin{aligned} 138 &= 131 + 7 \\ &= 127 + 11 \\ &= 109 + 29 \\ &= 107 + 31 \\ &= 101 + 37 \\ &= \ 97 + 41 \\ &= \ 79 + 59 \\ &= \ 71 + 67. \end{aligned}$$

The expression of a given even number as a sum of two primes is called a 'Goldbach partition' of that number. For example: The integer 138 can be expressed in 8 ways. We say the GC number can be described in the form as

$$GC = P_i + P_j \longmapsto (P_i - 2n) + (P_j + 2n), \tag{1}$$

where the P_i and P_j are both primes. Let $R(n)$ be the number of representations of the Goldbach partition where $\prod_2$ is the twin prime constant [12], say $R(n) \sim 2\prod_2 \left(\prod_{P_k|n,k=2}\right) \frac{P_k-1}{P_k-2} \int_2^n \frac{dx}{(\ln x)^2}$. Ye and Liu [21] also gave the estimation formula $G(x) = 2C \prod_{p\geq 3} \frac{(p-1)}{(p-2)} \cdot \frac{(Li(x))^2}{x} + \mathcal{O}(x \cdot e^{-c\sqrt{\ln x}})$.

2.1 The RSA Cryptosystem

The signer prepares the prerequisite of an RSA signature: Two distinct large primes p and q, $n = pq$, Let e be a public key so that $\gcd(e, \phi(n)) = 1$, where $\phi(n) = (p-1)(q-1)$, then calculate the private key d such that $ed \equiv 1 \pmod{\phi(n)}$. The signer publishes (e, n) and keeps (p, q, d) secret. The notation in the same as in [19].

RSA Encryption and Decryption:

In RSA public-key encryption, Alice encrypts a plaintext M for Bob using Bob's public key (n, e) by computing the ciphertext

$$\begin{aligned} C &\equiv M^e \pmod{n} \\ M &\equiv C^d \pmod{n} \end{aligned} \tag{2}$$

where n, the modulus, is the product of two or more large primes, and e, the public exponent, is an (odd) integer $e \geq 3$ that is relatively prime to $\phi(n)$, the order of the multiplicative group $\mathbb{Z}_n^*$. The signer uses private key d to decrypt message M from the ciphertext C.

RSA Digital Signature:

$$s \equiv M^d \pmod{n} \tag{3}$$

where (n, d) is the signer's RSA private key. The signature is verified by recovering the message M with the signer's RSA public key (n, e):

$$M \equiv s^e \pmod{n} \tag{4}$$

2.2 The relationship of the Goldbach's conjecture and the RSA Cryptosystem

Constant [4] proposed the algebra factoring of the cryptography modulus and proof of Goldbach's conjecture. He connected each relationsip. His methodology is described as follows:

Step 1. We know the modulus $n = p \cdot q$, we assume

$$s = p + q. \tag{5}$$

Step 2. Compute

$$p^2 - sp + n = 0. \tag{6}$$

Step 3. Compute

$$p, q = \frac{1}{2}(s \pm c) \tag{7}$$

since

$$c = \sqrt{s^2 - 4n}. \tag{8}$$

Step 4. Compute $s^2 - c^2 + 4n$, or we can reexpress as

$$c^2 = s^2 - 4n. \tag{9}$$

Example 1:
We assume $n = 5353$, then $4n = 4 \cdot 5353 = 21412$. We also compute $\sqrt{4n} \approx 146.3283978$ since $s^2 > 4n$, we therefore start the integer s by 148. From Equation (7)

Table 1. Example 1 of $n = 5353$.

times	s	s^2	$4n$	c^2	c
1	148	21904	21412	$\sqrt{492}$	22.18
2	150	22500	21412	$\sqrt{1088}$	32.98
3	152	23104	21412	$\sqrt{1692}$	41.13
4	154	23716	21412	$\sqrt{2304}$	48
5	156	24336	21412	$\sqrt{2924}$	54.074

and Equation (8), we have $s = 154$, and $c = 48$, to calculate

$$p = \frac{154 + 48}{2} = \frac{202}{2} = 101, q = \frac{154 - 48}{2} = \frac{106}{2} = 53.$$

We obtained $p = 53$, and $q = 101$. The result shown in Table 1.
Example 2:

We assume $n = 15481$ where $s^2 > 4n$, namely $4n = 4 \cdot 15481 = 61924$. Since $\sqrt{61924} \approx 248.8$, we therefore start the integer s by 250. From above it is stated, the c must be an integer. Hence, we assume $s = 250$ and set $c = 24$. From Equation (7) and Equation (8), we have

$$p = \frac{250 + 24}{2} = \frac{274}{2} = 137, q = \frac{250 - 24}{2} = \frac{226}{2} = 113.$$

We obtained $p = 137$, and $q = 113$. The result shown in Table 2. When the modulus n goes up to 1024-bits or greater than 2048-bits length, is this methodology still efficient? This is an interesting question.

Table 2. Example 2 of $n = 15481$.

times	s	s^2	$4n$	c^2	c
1	250	62500	61924	576	24

3 Our Analysis

In this section, we introduce another methodology that analyzes the Goldbach's conjecture properties and the relationship with twin prime.

3.1 The Goldbach's conjecture properties

In this subsection, the authors describe the Goldbach's conjecture properties. Notations are described in the following.

Notation:

P_n: the nth prime number.
g_p: smallest prime factor of number m.
$P[m]$: largest prime factor of m.
$P_0[m]$: smallest prime factor of $m > 1$.
d_k: $= P_j - P_i$, gap or distance between two primes, it should be an even integer.
$\pi(x)$: the number of primes p, $p \leq x$.
$G(x)$: expresses the number of Goldbach partition.
GC: expresses an even number for the Goldbach Conjecture (GC) number.
PG: expresses an integer for the prime gaps (PG) number.
M: denotes $M = \frac{GC}{2}$.
$\overline{P_iM}$: expresses a distance value from point P_i to point M, this value difference with d_k if M is not a prime.
$\overline{MP_j}$: expresses a distance value from point M to point P_j, this value difference with d_k if M is not a prime.
SPN: the M is the center of symmetry in the two numbers where those are nearest primes at X axis line.
$2n|\overline{P_iM}$: the $2n$ divide the $\overline{P_iM}$.
Some basic properties are shown as follows:

Property 1. odd + even = odd.
Property 2. even + even = even.
Property 3. odd + odd = even.
Property 4. even − even = even.
Property 5. odd − odd = even.
Property 6. even − odd = odd.
Property 7. even · even = even.
Property 8. odd · even = even.
Property 9. odd · odd = odd.

The relationship diagram is shown in Figure 1. In this article, we classify the Gold-

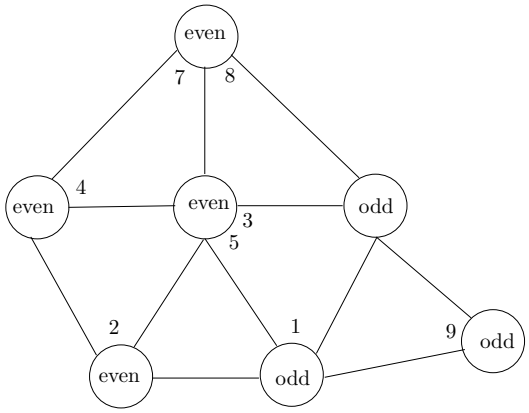

Fig. 1. The odd and even numbers relationship of properties in arithmetic.

bach Conjecture (GC) into three categories. The fundamental concepts in detail are shown in Figure 2. For convenience, we used the notation case 1, case 2 and case 3 to describe the following scenarios. We suppose an integer GC where $GC \geq 6$ and it is an even positive number, there also exists an integer M where $M = \frac{GC}{2}$. We use an X-axis line to express distance, see Figure 3.

Case 1: If M is a prime, there then exists a prime number, say P_i where $P_i = P_j$ and located on M point at X axis. (See Figure 4)
Case 2: If M is not a prime, and is an odd number, there exists at least one pair of symmetrical primes. Say P_i and P_j where the distance is $\overline{P_iM} = \overline{MP_j}$, and $2n|\overline{P_iM}$, $2n|\overline{MP_j}$. (See Figure 5)
Case 3: If M is not a prime, and is an even number, there exists at least one pair of symmetrical primes. Say P_i and P_j where the distance is $\overline{P_iM} = \overline{MP_j}$, and $2n+1|\overline{P_iM}$, $2n+1|\overline{MP_j}$. (See Figure 6)

Theorem 1 (Bertrand-Chebyshev Theorem). *For any one real number n where $n \geq 1$, there always exists at least a prime between n and $2n$ interval.*

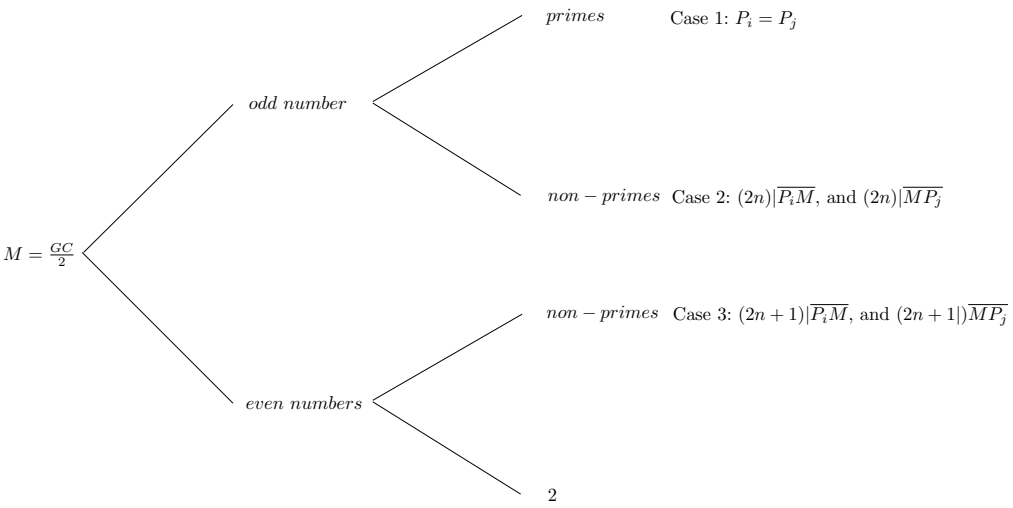

Fig. 2. The Goldbach conjecture's situation case.

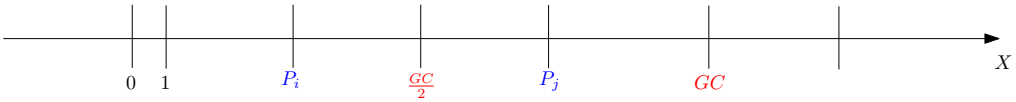

Fig. 3. The X-axis of number line.

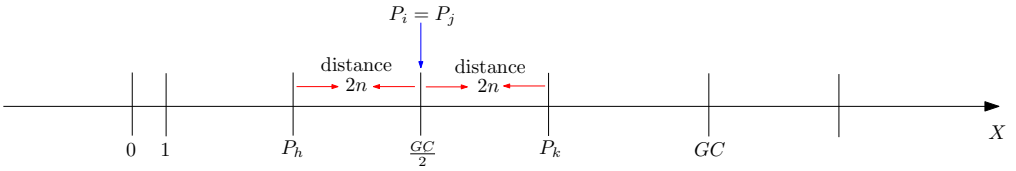

Fig. 4. The Case 1 situation.

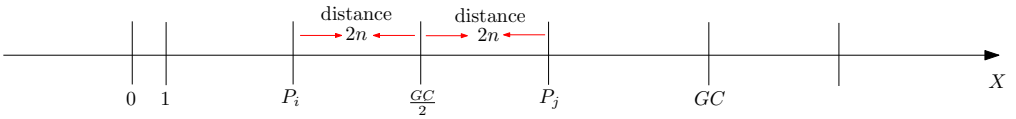

Fig. 5. The Case 2 situation.

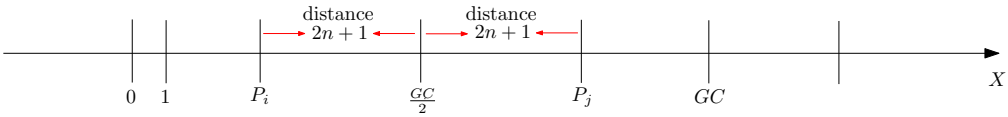

Fig. 6. The Case 3 situation.

Proof. We suppose that

$$\begin{aligned}\binom{2n}{n} &\leq \prod_{p\leq\sqrt{2n}} P^r \prod_{\sqrt{2n}<p\leq\frac{3}{2}n} P \prod_{m<p\leq 2n} P \\ &\leq \prod_{p\leq\sqrt{n}} (2n) \prod_{\sqrt{2n}<p\leq m} P \prod_{m<p<2m} P. \end{aligned} \tag{10}$$

For each n where $1 \leq n < 4010$, such as
$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, \ldots, 3967, 3989, 4001, 4003, 4007$.
We chose a small prime p, and another greater than n say p'. The relationship is as follows:

$$p \leq n \leq p' \leq 2p \leq 2n. \tag{11}$$

Thus, this finishes the proof.

Proposition 1. *If $M = \frac{GC}{2}$, where M is a prime, say $M = P_i = P_j$, and P_i located on M point at X axis. There exists at least one pair of symmetrical primes P_h and P_k where the distance value $\overline{P_hM} = \overline{MP_k}$.*

Proof. We assume M is prime, then $M - P_h = \overline{P_hM}$ is also an even integer, according to Property 5. The odd integers are subtracted to give an even integer. There are two symmetrical prime numbers, say P_h and P_k located on the two sides of M at the center point position. The distance $\overline{P_hM}$ is equal to distance $\overline{MP_k}$, divided by $2n$. If $\frac{P_h+P_k}{2} = M$ while $P_h \neq P_i \neq P_k$, it also matches $P_h + P_k = GC$. Thus, we have obtained the first solution $M = P_i = P_j$ if and only if M is prime. The second solution is $P_h + P_k = GC$ if and only if P_h, P_k are both primes.

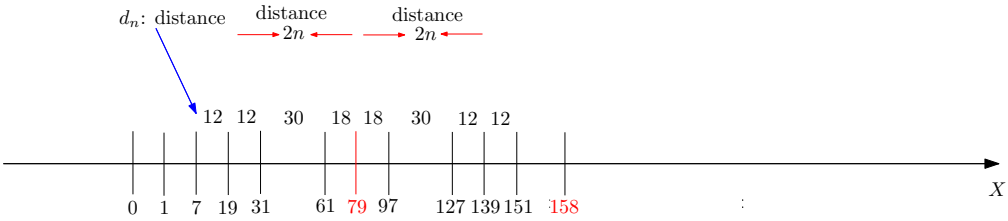

Fig. 7. An example of Case 1 situation.

Suppose $GC = 158$, and $\frac{GC}{2} = 79$.

$$\begin{aligned} 158 = & \ 7 + 151 \\ = & \ 19 + 139 \\ = & \ 31 + 127 \\ = & \ 61 + 97 \\ = & \ 79 + 79 \end{aligned}$$

Proposition 2. *If M is not a prime, but is an odd number, there exists at least two prime numbers, say P_h and P_k that are located on either side of the center point M. The distance from P_i to M equivalent M to P_j.*

Proof. We assume M is an odd number, then $M - P_i = P_j - M$. As stated previously $P_i + P_j = 2M = GC$, but $P_i \neq P_j$. From Property 5, the odd integers are subtracted to give an even integer. Thus, we understood the value $\overline{P_iM}$ of distance from P_i to M must be an even integer, and is divided $2n$. On the other hand, there is a similar situation from M to P_j since $2n|\overline{P_iM}, 2n|\overline{MP_j}$ while $P_i \neq P_j$. We have $P_i + P_j = 2M = GC$, because $P_i \neq P_j$ and $P_i < M < P_j$. This is one solution of symmetrical primes. The case 1 is a special situation of case 2.

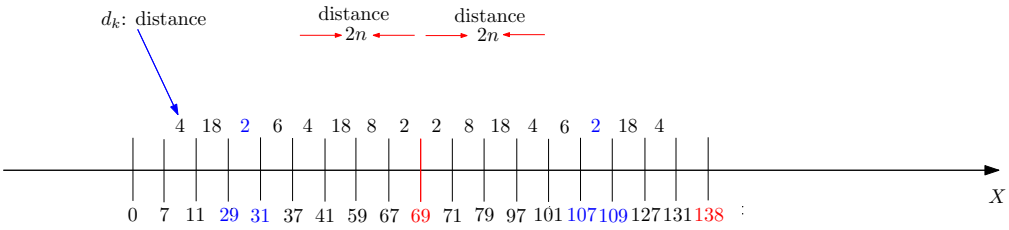

Fig. 8. An example of Case 2 situation.

Suppose $GC = 138$, and $\frac{GC}{2} = 69$.

$$\begin{aligned} 138 = & \ 131 + 7 \\ = & \ 127 + 11 \\ = & \ 109 + 29 \\ = & \ 107 + 31 \\ = & \ 101 + 37 \\ = & \ 97 + 41 \\ = & \ 79 + 59 \\ = & \ 71 + 67. \end{aligned}$$

Proposition 3. *If $M = \frac{GC}{2}$, is not a prime, but is an even number, there exists at least two primes, say P_i and P_j located on either side of M centerpoint position, where the distance $\overline{P_iM}$ equal $\overline{MP_j}$, $2n+1|\overline{P_iM}$, $2n+1|\overline{MP_j}$.*

Proof. We assume M is not a prime and is an even number. According to Property 6, the even number is subtracted from the odd number and the result is an odd number. We, therefore, know this distance value must be an odd integer while $P_j \neq P_j$. Hence, the relationship as $P_i < M < P_j$. Since $\overline{P_iM} = \overline{MP_j}$. We have $P_i + P_j = 2M = GC$, however $P_i \neq P_j$. Thus, we obtained one solution where two primes are symmetrical about the point of M on the X axis line. If and only if $n = 0$, where $M - P_i$ equal $P_j - M$, it has $P_j - P_i = 2$ since $P_i + P_j = 2M = GC$, say $(P_i,\ P_j)$ are twin primes. The twin prime is also a special situation of case 3.

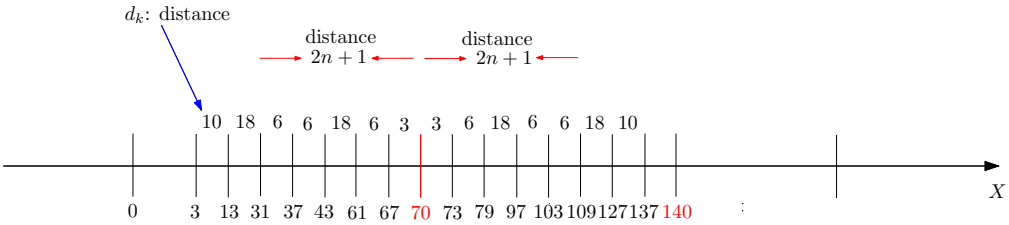

Fig. 9. An example of Case 3 situation.

Suppose $GC = 140$, and $\frac{GC}{2} = 70$.

$$\begin{aligned} 140 &= 3 + 137 \\ &= 13 + 127 \\ &= 31 + 109 \\ &= 37 + 103 \\ &= 43 + 97 \\ &= 61 + 79 \\ &= 67 + 73 \end{aligned}$$

Suppose $GC = 120$, and $\frac{GC}{2} = 60$.

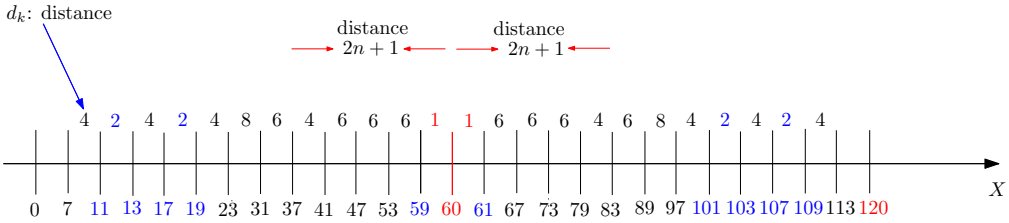

Fig. 10. An example of twin prime situation.

$$\begin{aligned}
120 = & \ 7 + 113 \\
= & \ 11 + 109 \\
= & \ 13 + 107 \\
= & \ 17 + 103 \\
= & \ 19 + 101 \\
= & \ 23 + 97 \\
= & \ 31 + 89 \\
= & \ 37 + 83 \\
= & \ 41 + 79 \\
= & \ 47 + 73 \\
= & \ 53 + 67 \\
= & \ 59 + 61
\end{aligned}$$

Theorem 2. *For all prime numbers that are greater than* 3*, the prime gap (PG, or distance) is an even integer.*

Proof. For any prime numbers that are greater than 3, the PG should be an odd number. From Property 5, the answer is an even number when two odd numbers are subtracted from each other. The prime gap is an even number if the prime is greater than 3.
Suppose two odd numbers p and q where $p < q$, and $p \neq q$. Since

$$\begin{aligned}
p &\equiv 1 \pmod 2 \\
q &\equiv 1 \pmod 2
\end{aligned}$$

We obtained $|p - q| \equiv 0 \pmod 2$.

Lemma 1. *We suppose the prime gap PG is a positive integer. From Theorem 2, the $\frac{PG}{2}$ has two results, it may have an even number, or may have an odd number. We rewrite the expression as*

$$\frac{PG}{2} \begin{cases} \equiv 0 \pmod 2, \textit{ this is an even number.} \\ \equiv 1 \pmod 2, \textit{ this is an odd number.} \end{cases}$$

When $\frac{PG}{2} \equiv 0 \pmod 2$, is an even integer; and $\frac{PG}{2} \equiv 1 \pmod 2$ is an odd integer.
Let $d = \frac{PG}{2}$, it then

$$q - d = \begin{cases} \textit{even number.} \\ \textit{odd number.} \end{cases}$$

We assume $d = \frac{PG}{2}$, and $q - d = s$.

1. *If d is an odd integer. From Property 5, the s should be an even integer.*
2. *If d is an even integer. From Property 6, the s should be an odd integer.*

Theorem 3 (Symmetric Prime Number Theorem). *For any two prime numbers* $p,\ q, p < q$ *that are greater than* 3*, with the X axis as the line of symmetry, the two prime numbers should be located on both sides of an integer* m*, the distance from* p *to* m *and* m *to* q *are proportionally equal.*

Proof. As known,

$$(q - m) = (m - p), \tag{12}$$

since

$$(q + p) = 2m. \tag{13}$$

From Theorem 1, there exists at least a prime between m and $2m$. In other words, there also exists at least a prime between $\frac{m}{2}$ and m. Hence, there are two prime numbers

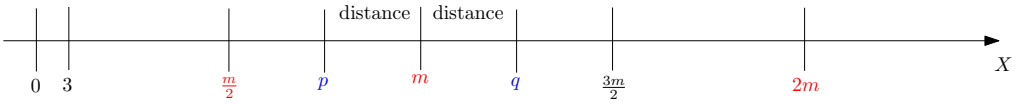

Fig. 11. The symmetric primes in X axis situation.

located on the X axis line between $\frac{m}{2}$ and $2m$. It can be seen, the prime p and q are symmetrical to m. If not, the $(q - p) = (m - p)$ is a contradiction.

There is some related literature about prime symmetric problems in [6, 15, 17, 18], but slightly different then what is discussed in this article.

3.2 The Goldbach's Conjecture and the Twin Prime relationship

In this subsection, the authors describe a relationship of Goldbach's conjecture and twin prime. Previously, we listed an example of a special situation in case 3, and drew a diagram in Figure 10. Here, we discuss in depth this issue. We describe the conception of prime combinations in Goldbach's conjecture. From equation (1), rewrite as the

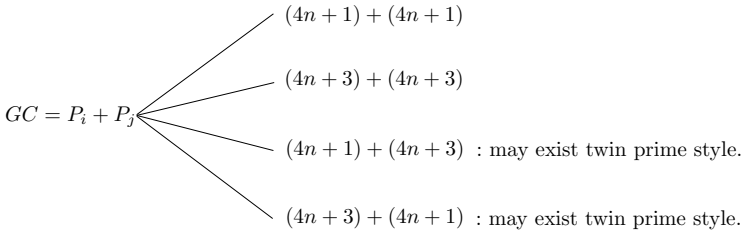

Fig. 12. The symmetric primes in X axis situation.

following:

$$P_i + P_j = \begin{cases} (4n+1)+(4n+1), \text{ those are both '}+1\text{' form.} \\ (4n+3)+(4n+3), \text{ those are both '}+3\text{' form.} \\ (4n+1)+(4n+3), \text{ those are mixed '}+1\text{' and '}+3\text{' form.} \end{cases}$$

Theorem 4. *For each twin prime pair (P_i, P_j) where the integers are greater than or equal to $(5,7)$, say $(P_i, P_j) \geq (5,7)$. There must belong this type of '$(4n+1)+(4n+3)$' or '$(4n+3)+(4n+1)$' forms.*

Proof. For each twin prime pair (P_i, P_j) where the values are greater than or equal to $(5,7)$. We assume an integer n where $n \geq 1$, namely

$$(4n+1) - (4n+1) = 0 \pmod 4, \tag{14}$$

and

$$(4n+3) - (4n+3) = 0 \pmod 4. \tag{15}$$

On the other hand,

$$(4n+3) - (4n+1) = 2 \pmod 4, \tag{16}$$

or

$$(4n+1) - (4n+3) = |-2| \equiv 2 \pmod 4. \tag{17}$$

This is to say, the twin prime pair (P_i, P_j) must be expressed '$(4n+1)+(4n+3)$' or '$(4n+3)+(4n+1)$' forms. Otherwise, it is a contradiction.

The relationship of twin prime pair (P_i, P_j), as shown in Figure 13 and Figure 14.

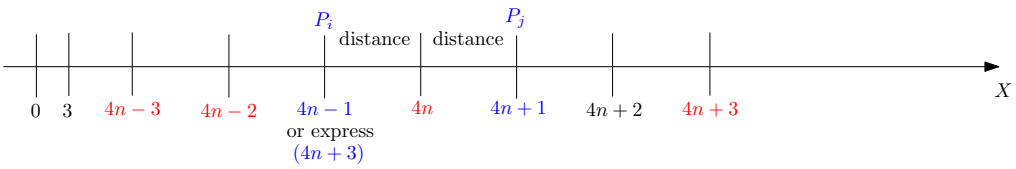

Fig. 13. An relationship of twin prime situation.

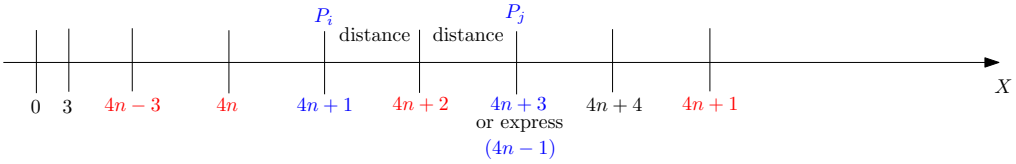

Fig. 14. An relationship of twin prime situation.

Proposition 4. *If* $P_i + P_j \equiv 0 \pmod 4 \equiv 0 \pmod 6 \equiv 4 \pmod 8$, *and* $\frac{P_i+P_j}{2} \equiv 2 \pmod 4 \equiv 0 \pmod 6 \equiv 2 \pmod 8$ *or* $\frac{P_i+P_j}{2} \equiv 2 \pmod 4 \equiv 0 \pmod 6 \equiv 6 \pmod 8$, *there may exist a twin prime where the* $(\frac{P_i+P_j}{2} - 1, \frac{P_i+P_j}{2} + 1)$ *is* $(4n+1)+(4n+3)$ *form.*

Proof. As known from Proposition 3, $\frac{P_i+P_j}{2}$ is an even number. Otherwise, it is a contradiction. According to property 6:

$$\begin{cases} \frac{P_i+P_j}{2} - 1 \text{ is an odd number.} \\ \frac{P_i+P_j}{2} + 1 \text{ is an odd number too.} \end{cases}$$

Note that $\frac{P_i+P_j}{2} \equiv 2 \pmod 4 \equiv 0 \pmod 6 \equiv 6 \pmod 8$, we see the $\frac{P_i+P_j}{2}$ is $4n+2$ form. Therefore, the $\frac{P_i+P_j}{2} - 1$ is $4n+1$ form, and $\frac{P_i+P_j}{2} + 1$ is $4n+3$ form.
Since $\frac{P_i+P_j}{2} \equiv 2 \pmod 4 \equiv 0 \pmod 6 \equiv 2 \pmod 8$.
By Theorem 4, we know $(\frac{P_i+P_j}{2} - 1, \frac{P_i+P_j}{2} + 1)$ is $(4n+1)+(4n+3)$ form.

Proposition 5. *If* $P_i + P_j \equiv 0 \pmod 4 \equiv 0 \pmod 6 \equiv 0 \pmod 8$, *and* $\frac{P_i+P_j}{2} \equiv 0 \pmod 4 \equiv 0 \pmod 6 \equiv 0 \pmod 8$ *or* $\frac{P_i+P_j}{2} \equiv 0 \pmod 4 \equiv 0 \pmod 6 \equiv 4 \pmod 8$, *there may exist a twin prime where the* $(\frac{P_i+P_j}{2} - 1, \frac{P_i+P_j}{2} + 1)$ *is* $(4n+3)+(4n+1)$ *form.*

Proof. As known, the $\frac{P_i+P_j}{2}$ is an even number.
Since $\frac{P_i+P_j}{2} \equiv 0 \pmod 4 \equiv 0 \pmod 6 \equiv 0 \pmod 8$. We see the $\frac{P_i+P_j}{2}$ is $4n$ form.
Hence $\frac{P_i+P_j}{2} - 1$ is $4n+3$ form.
Therefore $\frac{P_i+P_j}{2} + 1$ is $4n+1$ form.
Now, as $\frac{P_i+P_j}{2} \equiv 0 \pmod 4 \equiv 0 \pmod 6 \equiv 0 \pmod 8$, the $\frac{P_i+P_j}{2}$ is $4n$ form too.
Thus, the $\frac{P_i+P_j}{2}+1$ is $4n+1$ form. This inference is consistent with the above statement.

Proposition 6. *If* $\frac{P_i+P_j}{2}$ *is prime, the* $P_i + P_j$ *can not be combined with* $(4n+1)+(4n+3)$ *or* $(4n+3)+(4n+1)$ *forms. It can be represented as* $(4n+1)+(4n+1)$ *or* $(4n+3)+(4n+3)$ *forms. It is impossible to have* $(4n+3)+(4n+1)$ *or* $(4n+1)+(4n+3)$ *forms.*

Proof. We suppose P_i, P_h and P_j are three primes where $P_h = \frac{P_i+P_j}{2}$.
By Lemma 1, there exists an integer s where $s = P_h - P_i$. Note that Theorem 3 $P_j = P_h + s$. Since $2P_h = P_i + P_j$. If P_h is $4n+1$ form, then this is $(4n+1)+(4n+1)$ form, say P_h+P_j. From Proposition 1, if and only if P_h is $4n+1$ form, then $P_h - s = P_i$ where s is an even number. We rewrite as follows:
$(4n+1) - 2n = P_i$ is $4n+1$ form (while $n = 0$).
Alternatively, $(4n+1) + 2n = P_j$ is $4n+1$ form (while $n = 1$).
If and only if P_h is $4n+3$ form.
Then $P_h + s = P_j$. We rewrite the expression below: $(4n+3) + 2n = P_j$ is $4n+3$ form (while $n = 0$).
On other side, $(4n+3) + 2n = P_j$ is $4n+3$ form (while $n = 0$).

In summary,
Goldbach's conjecture $\supseteq (4n+1)+(4n+3) \subset$ twin prime.

3.3 The relationship between $G(x)$ and $\pi(x)$ in Goldbach's conjecture

In Table 3, the $G(x)$ is the number of prime pairs. For example, the positive integer $25,300$ has 314 prime pairs matched with the Goldbach's rule. And the integer $253,000$ has 2011 prime pairs matches. When the integer is approaching infinity, the $G(x)$ is also increases. However, item 5, 9, 11 and 14 are exceptions. Note that a pattern begins to surface beginning with the 4th item. The $G(x)$ term value is between 5 and 6 for every two rows following. When the positive integer is approaching infinity, then the number of prime numbers $\pi(x)$ also increasing; it shows a very steady positive growth. However the $G(x)$ does not follow this rule. Different even numbers GC for different swayed Goldbach partitions. There is no any strong relevance between each number GC_i to the other number GC_j. Hence, there are no rules to predict this status. The experimental results are shown in Table 3 and Figure 15.

Table 3. The relationship of Goldbach partition $G(x)$ with $\pi(x)$

item	Positive Integer	$G(x)$	$\pi(x)$	$\frac{\pi(x)}{G(x)}$
1	12650	186	1510	8.11
2	25300	314	2787	8.87
3	50600	553	5190	9.38
4	75900	1478	7473	5.05
5	101200	918	9691	10.55
6	126500	1140	11864	10.40
7	151800	2635	14007	5.31
8	177100	1802	16091	9.92
9	202400	1669	18178	10.89
10	227700	3688	20243	5.48
11	253000	2011	22280	11.07
12	278300	2130	24301	11.40
13	303600	4676	26289	5.62
14	318950	2059	27520	13.36
15	331600	2160	28533	13.20
16	344250	4652	29521	6.34
17	356900	2356	30512	12.95
18	369500	2321	31488	13.56
19	382200	6325	32460	5.13
20	394850	⋮	⋮	⋮
21	407500	⋮	⋮	⋮
22	420150	5264	35398	6.72

Note: this table does not include the prime number 2.

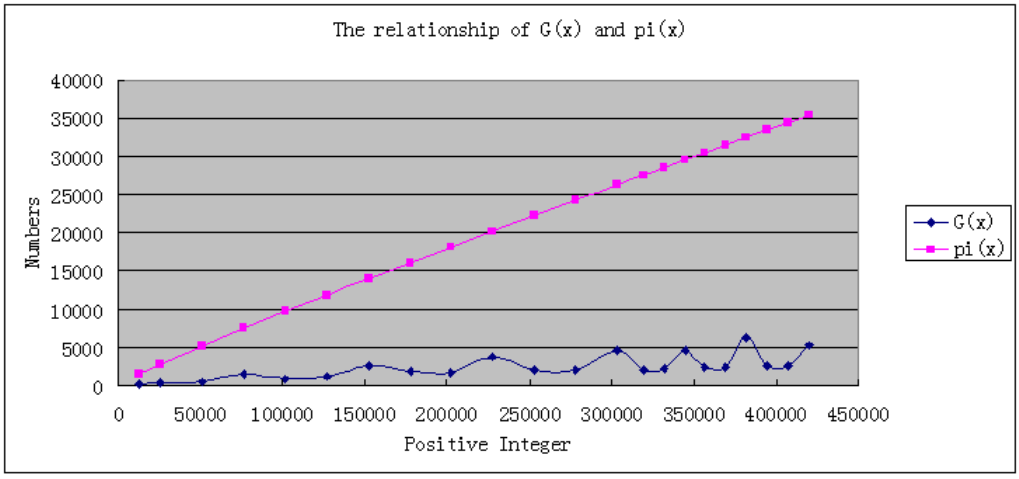

Fig. 15. A relationship of $G(x)$ with $\pi(x)$ in positive integers.

Open problems:

1). How did we know the $\frac{GC}{2}$ is a prime number? The AKS algorithm [1] determines whether a number is prime or composite within polynomial time, it may be a discrepancy in the method. Lenstra and Pomerance [13] primality testing is other solution.
2). If the twin prime problem is solved, could it also solve the Goldbach's conjecture? The author doubts this is the case. The twin prime situation is just a special case in Goldbach's conjecture.
3). If the puzzle of prime numbers is solved, will it may also solve the number of Goldbach partition?

4 Conclusion

We clearly described serval examples in this paper. For the prime number gaps problem, Zhang has a very good result. However, it is far from a way to solve the Goldbach conjecture. The authors pointed out the prime symmetrical situation, may be useful to assist in understanding about the Goldbach conjecture, even though they did not offer a general formula on the Goldbach partition. The prime symmetrical property may also solve the puzzle of prime numbers.

Acknowledgement

The authors would like to thank the reviewers for their comments that help improve the manuscript. This work is partially supported by the National Natural Science Foundation of China under the grant number 61103247, and also partially supported by the

project from department of education of Fujian province under the number JA12351, JA12353, JA12354 and JK2013062.

References

1. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in P. *Annals of Mathematics*, 160:781–793, 2004.
2. Redha M. Bournas. The Strong Goldbach Conjecture: Proof for All Even Integers Greater than 362. `http://arxiv.org/vc/arxiv/papers/1303/1303.4649v1.pdf`, September 2013.
3. Jing Run Chen. On the representation of a larger even integer as the sum of a prime and the product of at more two primes. *Sci. Sinica*, 16:157–176, 1973.
4. James Constant. Algebraic factoring of the cryptography modulus and proof of Goldbach's conjecture. `http://www.coolissues.com/mathematics/Goldbach/goldbach.htm`, July 2014.
5. Tomás Oliveira e Silva, Siegfried Herzog, and Silvio Pardi. Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \cdot 10^{18}$. *Mathematics of Computation*, November 18 2013. Accepted to appear.
6. Peter Fletcher, William Lindgren, and Carl Pomerance. Symmetric and asymmetric primes. *journal of number theory*, 58:89–99, 1996.
7. Jamel Ghanouchi. A proof of Goldbach and de Polignac conjectures. `http://unsolvedproblems.org/S20.pdf`.
8. Daniel A. Goldston, Janos Pintz, and Cem Y. Yildirim. Primes in tuples I. *Annals of Mathematics*, 170(2):819–862, September 2009.
9. Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167:481–547, 2008.
10. Benjamin Green and Terence Tao. Linear equations in primes. *Annals of Mathematics*, 171(3):1753–1850, May 2010.
11. Gilbert Ikorong. A reformulation of the goldbach conjecture. *Journal of Discrete Mathematical Sciences and Cryptography*, 11(4):465–469, 2008.
12. Wolfram Research Inc. Goldbach Conjecture. `http://mathworld.wolfram.com/GoldbachConjecture.html`.
13. H. W. Lenstra jr. and Carl Pomerance. Primality testing with gaussian periods. In Manindra Agrawal and Anil Seth, editors, *FST TCS 2002: Foundations of Software Technology and Theoretical Computer Science*, volume 2556. 2002. (version 20110412).
14. Wen Chao Lu. Exceptional set of Goldbach number. *Journal of Number Theory*, 130(10):2359–2392, October 2010.
15. Imre Mikoss. The prime numbers hidden symmetric structure and its relation to the twin prime infinitude and an improved prime number theorem. `http://www.ma.utexas.edu/mp_arc/c/06/06-314.pdf`.
16. Ikorong Anouk Gilbert Nemron. An original abstract over the twin primes, the goldbach conjecture, the friendly numbers, the perfect numbers, the mersenne composite numbers, and the sophie germain primes. *Journal of Discrete Mathematical Sciences and Cryptography*, 11(6):715–726, 2008.
17. Prime Number Patterns. Prime number symmetry. `http://primepatterns.wordpress.com/`, 2010.
18. Zhengdang Qin. *A Proof of the Goldbach's conjecture*. The Economic Daily Press, China, October 1995.

19. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communincation of ACM*, 21, February 1978.
20. Kent Slinker. A proof of Goldbach's conjecture that all even numbers greater than four are the sum of two primes. `http://arxiv.org/vc/arxiv/papers/0712/0712.2381v10.pdf`, January 2008.
21. Jian Ye and Chenglian Liu. A study of Goldbach's conjecture and Polignac's conjecture equivalence issues. Cryptology ePrint Archive, Report 2013/843, 2013. `http://eprint.iacr.org/2013/843.pdf`.
22. Shaohua Zhang. Goldbach conjecture and the least prime number in an arithmetic progression. *Comptes Rendus-Mathematique*, 348(5-6):241–242, March 2010.
23. Yitang Zhang. Bounded gaps between primes. *Annals of Mathematics*, 2013. Accepted to appear.