A Study of Relationship between RSA Public Key Cryptosystem and Goldbach's Conjecture Properties

Chenglian Liu[1]*, Chin-Chen Chang[2,3], Zhi-Pan Wu[1], Shi-Lin Ye[1]

(Corresponding author: C. C. Chang)

Department of Computer Science, Huizhou University[1]

Huizhou 516007, China.

Department of Information Engineering and Computer Science, Feng Chia University[2]

Taichung 40724, Taiwan.

The Department Computer Science and Information Engineering, Asia University[3]

Taichung 41354, Taiwan.

(Email: alan3c@gmail.com)

(Received Dec. 25, 2014; revised and accepted Mar. 4 & Apr. 21, 2015)

Abstract

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

Keywords: AKS algorithm, number axis, symmetrical primes

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. [6] 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 [16] showed 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 [26] proved that there are infinitely many pairs of primes that differ by less than $7 \cdot 10^7$. Zhang's result is a huge step forward in the direction of the twin prime conjecture. Some people in related research also gave good contributions [8–11, 13, 18, 22, 25].

In this paper, the authors will introduce the fundamental concepts rather than the entire proof in its complexity.

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 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 [14], say $R(n) \sim$

*Part of this work was carried out while the first author was at Longyang University supported by the information security team project. Email:chenglian.liu@gmail.com

$2\prod_2 \left(\prod_{P_k|n,k=2}\right) \frac{P_k-1}{P_k-2} \int_2^n \frac{dx}{(\ln x)^2}$. Ye and Liu [24] 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 RSA algorithm [21] is well known public key cryptosystem. It is widely used many application such as traitor tracing scheme [23], multi-secrect sharing scheme [5], and anonymous multi-receive encryption scheme [12] so on. We briefly introduce the principle of RSA in this subsection. 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 notations are the same as in [21].

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

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

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:

$$s \equiv M^d \pmod{n},$$

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):

$$M \equiv s^e \pmod{n}.$$

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 relationship. His methodology is described as follows:
Since we know the modulus $n = p \cdot q$, we assume

$$s = p + q.$$

Step 1. Compute

$$p^2 - sp + n = 0.$$

Step 2. Compute

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

since

$$c = \sqrt{s^2 - 4n}. \tag{3}$$

Step 3. Compute $s^2 = c^2 + 4n$, or we can reexpress as

$$c^2 = s^2 - 4n.$$

Example 1:
We assume $n = 721801$, then $4n = 4 \cdot 721801 = 2887204$. We also compute $\sqrt{4n} \approx 1699.177$ since $s^2 > 4n$, we therefore start the integer s by 1700. From Equation (2) and

Table 1: $n = 721801$

Times	s	s^2	$4n$	c^2	c
1	1700	2890000	2887204	$\sqrt{2796}$	52.87
2	1702	2896804	2887204	$\sqrt{9600}$	97.97
3	1704	2903616	2887204	$\sqrt{16412}$	128.10
4	1706	2910436	2887204	$\sqrt{23232}$	152.42
5	1708	2917264	2887204	$\sqrt{300600}$	173.37
6	1710	2924100	2887204	$\sqrt{36896}$	192.08
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
51	1800	3240000	2887204	$\sqrt{352796}$	593.96
52	1802	3247204	2887204	$\sqrt{360000}$	600

Equation (3), we have $s = 1802$, and $c = 600$, to calculate the following table.

$$\begin{aligned} p &= \frac{1802 + 600}{2} = 1201, \\ q &= \frac{1802 - 600}{2} = 601. \end{aligned}$$

We obtain $p = 1201$, and $q = 601$. The result is as shown in Table 1.

Example 2:
We assume $n = 321907$ where $s^2 > 4n$, namely $4n = 4 \cdot 321907 = 1287628$. Since $\sqrt{1287628} \approx 1134.73$, we therefore start the integer s by 1136. From above it is stated, c must be an integer. Hence, we assume $s = 1148$ and set $c = 174$. From Equation (2) and Equation (3), we have

$$\begin{aligned} p &= \frac{1148 + 174}{2} = 661, \\ q &= \frac{1148 - 174}{2} = 487. \end{aligned}$$

We obtain $p = 661$, and $q = 487$. The result is as 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: $n = 321907$

Times	s	s^2	$4n$	c^2	c
1	1136	1290496	1287628	$\sqrt{2868}$	53.55
2	1138	1295044	1287628	$\sqrt{7416}$	86.11
3	1140	1299600	1287628	$\sqrt{11972}$	109.41
4	1142	1304164	1287628	$\sqrt{16563}$	128.59
5	1144	1308736	1287628	$\sqrt{21108}$	145.28
6	1146	1313316	1287628	$\sqrt{25688}$	160.27
7	1148	1317904	1287628	$\sqrt{30276}$	174

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.

Notations:

- 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, $p \leq x$.
- $G(x)$: The number of Goldbach partition.
- GC: An even number for the Goldbach Conjecture (GC) number.
- PG: An integer for the prime gaps (PG) number.
- M: Denotes $M = \frac{GC}{2}$.
- $\overline{P_iM}$: A distance value from point P_i to point M, this value differs from d_k if M is not a prime.
- $\overline{MP_j}$: A distance value from point M to point P_j, this value differs from d_k if M is not a prime.
- SPN: Assume P_i and P_h are prime number pairs. M is the midpoint between P_i and P_h, where M, P_i, P_h lie on the X axis; say P_i and P_h are symmetric prime numbers to integer M on the X axis.
- $2n|\overline{P_iM}$: 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.

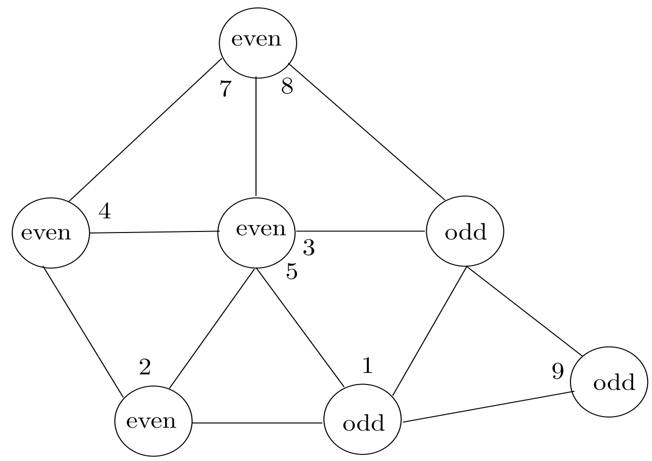

Figure 1: The odd and even numbers relationship of properties in arithmetic

In this article, we classify the Goldbach Conjecture (GC) into three categories. The fundamental concepts in detail are shown in Figure 2. For convenience, we used

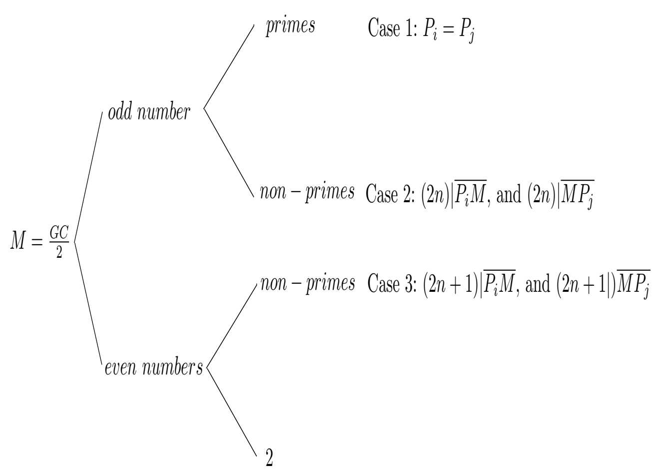

Figure 2: The Goldbach conjecture's situation case

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, then there exists a prime number, say P_i where $P_i = P_j$ and located on M point at X axis (See Figure 4).

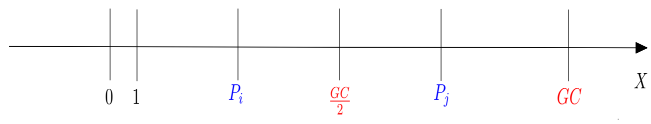

Figure 3: The X-axis of number line

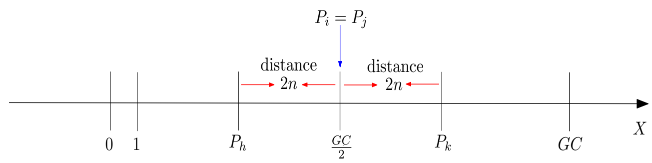

Figure 4: Case 1 situation

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).

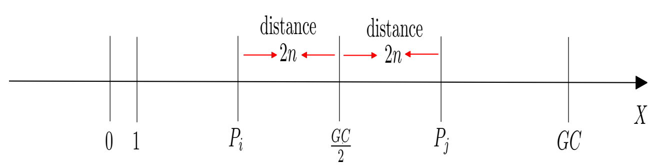

Figure 5: Case 2 situation

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).

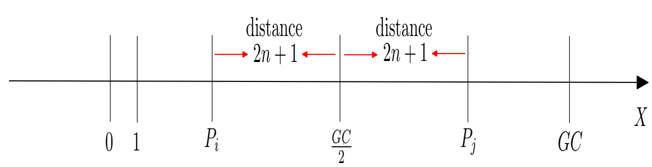

Figure 6: Case 3 situation

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

Proof. We suppose that

$$\begin{aligned} \binom{2n}{n} &\leq \prod_{p\leq\sqrt{2n}} P^r \prod_{\sqrt{2n}<p\leq\frac{3}{2}n} P \prod_{m<p\leq 2n} P \\ &\leq \prod_{p\leq\sqrt{n}} (2n) \prod_{\sqrt{2n}<p\leq m} P \prod_{m<p<2m} P. \end{aligned} \quad (4)$$

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

$$p \leq n \leq p' \leq 2p \leq 2n. \quad (5)$$

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 a prime. The second solution is $P_h + P_k = GC$ if and only if P_h and P_k are both primes. □

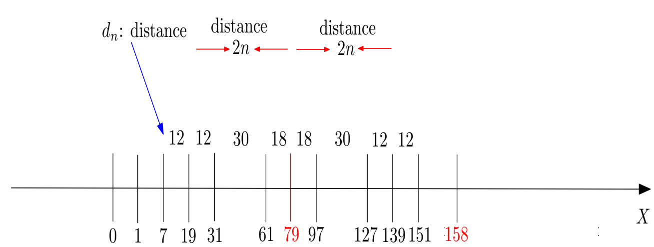

Figure 7: An example of Case 1 situation

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 is equivalent to that from 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 have 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. Case 1 is a special situation of Case 2. □

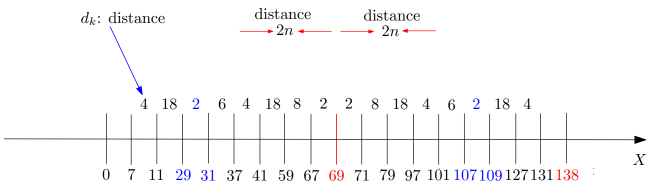

Figure 8: An example of Case 2 situation

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 $\overline{P_iM}$ equals $\overline{MP_j}$, $2n+1|\overline{P_iM}$, $2n+1|\overline{MP_j}$.*

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 $M - P_i$ equals $P_j - M$, 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. $\square$

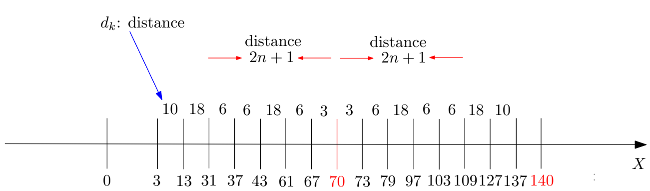

Figure 9: An example of Case 3 situation

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

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

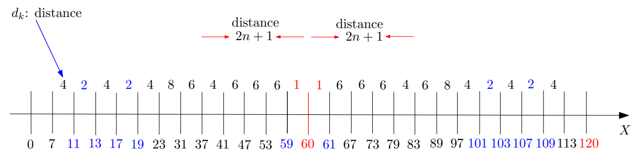

Figure 10: An example of twin prime situation

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

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

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

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

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

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 and 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,

$$(q - M) = (M - p),$$

since

$$(q + p) = 2M.$$

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

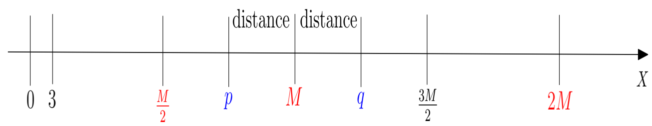

Figure 11: The symmetric primes on the X axis situation

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

There is some related literature about prime symmetric problems in [7,17,19,20], but slightly different than 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),

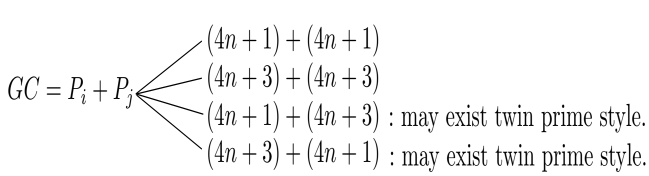

Figure 12: The twin prime of Goldbach's conjecture on the X axis situation

rewrite as the following:

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

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

$$(4n+1) - (4n+1) = 0 \pmod 4,$$

and

$$(4n+3) - (4n+3) = 0 \pmod 4.$$

On the other hand,

$$(4n+3) - (4n+1) = 2 \pmod 4,$$

or

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

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

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

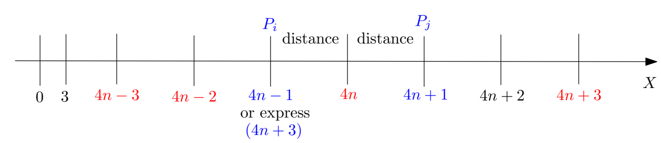

Figure 13: An relationship of twin prime situation I

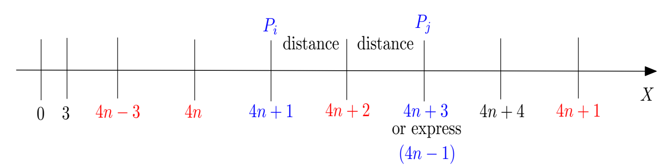

Figure 14: An relationship of twin prime situation II

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 $(\frac{P_i+P_j}{2}-1, \frac{P_i+P_j}{2}+1)$ 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 $s = P_h - P_i$. Since $P_j = P_h + s$ and $2P_h = P_i + P_j$, 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 it as follows:
$(4n+1) - 2n = P_i$ is $4n+1$ form (while $n=0$).
Alternatively, $(4n+1)+2n = P_j$ is $4n+3$ form (while $n=1$).
If and only if P_h is $4n+3$ form, then $P_h + s = P_j$. We rewrite the expression as below: $(4n+3)+2n = P_j$ is $4n+3$ form (while $n=0$).
On other side, $(4n+3)-2n = P_j$ is $4n+1$ form (while $n=1$). □

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 increased. However, Items 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

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 [15] primality testing is other solution.

2) If the twin prime problem is solved, could it also solve the Goldbach's conjecture? The authors 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 Conclusions

We clearly described two examples of relationship between RSA and Goldbach conjecture; this method suc-

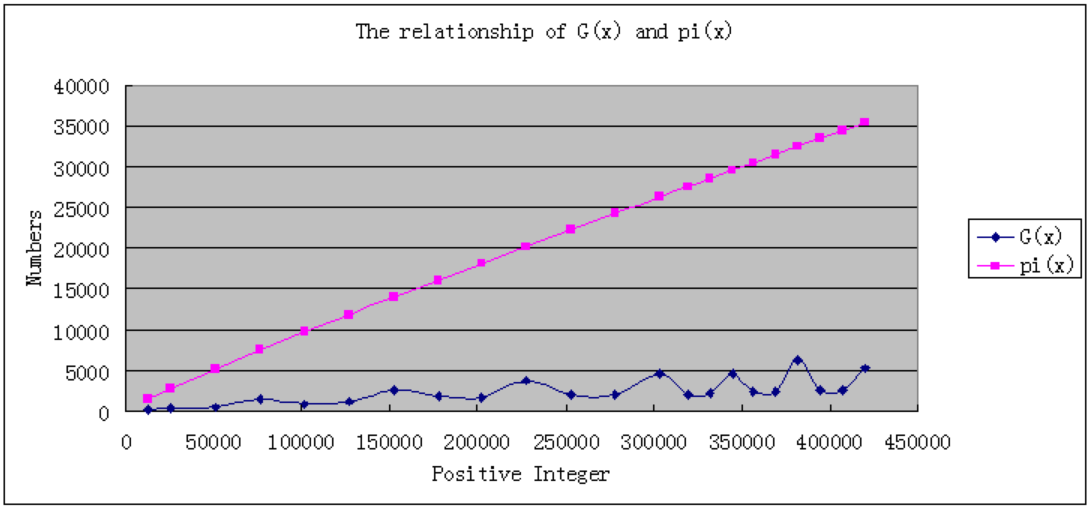

Figure 15: A relationship of $G(x)$ with $\pi(x)$ in positive integers

cessfully attack the RSA cryptosystem. Our contribution are useful to understand other algebra factoring methodology, when the modulus n goes up to over 1024 bits length, does it still efficiency to factor? It becomes to our future work. On the other hand, for the prime number gaps problem, Zhang has a very good result. However, it is still 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.

Acknowledgments

The authors would like to thank the reviewers for their comments that help improve the manuscript. The authors would like to thank the reviewers for their comments that help improve the manuscript. This work is partially supported by the project from department of education of Fujian province under the number JA12351 with JK2013062 and also partially supported from Guandong province special funds to foster the students' science and technology innovation under the number 139785 and 139802 (Climbing program funds).

References

[1] M. Agrawal, N. Kayal, and N. Saxena, "Primes is in P," *Annals of Mathematics*, vol. 160, pp. 781–793, 2004.

[2] R. M. Bournas, "The strong goldbach conjecture: Proof for all even integers greater than 362," Sep. 2013. (`http://arxiv.org/vc/arxiv/papers/1303/1303.4649v1.pdf`)

[3] J. R. Chen, "On the representation of a larger even integer as the sum of a prime and the product of at more two primes," *Sciencia Sinica*, vol. 16, pp. 157–176, 1973.

[4] J. Constant, "Algebraic factoring of the cryptography modulus and proof of Goldbach's conjecture," July 2014. (`http://www.coolissues.com/mathematics/Goldbach/goldbach.htm`)

[5] X. Dong, "A multi-secret sharing scheme based on the CRT and RSA," *International Journal of Network Security*, vol. 2, no. 2, pp. 69–72, 2015.

[6] T. O. e Silva, S. Herzog, and S. Pardi, "Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \cdot 10^{18}$," *Mathematics of Computation*, vol. 83, pp. 2033-2060, 2014.

[7] P. Fletcher, W. Lindgren, and C. Pomerance, "Symmetric and asymmetric primes," *Journal of Number Theory*, vol. 58, pp. 89–99, 1996.

[8] J. Ghanouchi, "A proof of Goldbach and de Polignac conjectures," 2015. (`http://unsolvedproblems.org/S20.pdf`)

[9] D. A. Goldston, J. Pintz, and C. Y. Yildirim, "Primes in tuples I," *Annals of Mathematics*, vol. 170, pp. 819–862, Sep. 2009.

[10] B. Green and T. Tao, "The primes contain arbitrarily long arithmetic progressions," *Annals of Mathematics*, vol. 167, pp. 481–547, 2008.

[11] B. Green and T. Tao, "Linear equations in primes," *Annals of Mathematics*, vol. 171, pp. 1753–1850, May 2010.

[12] L. Harn, C. C. Chang, and H. L. Wu, "An anonymous multi-receiver encryption based on RSA," *International Journal of Network Security*, vol. 15, no. 4, pp. 307–312, 2013.

[13] G. Ikorong, "A reformulation of the Goldbach conjecture," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 11, no. 4, pp. 465–469, 2008.

[14] Wolfram Research Inc, "Goldbach Conjecture," 2015. (`http://mathworld.wolfram.com/GoldbachConjecture.html`)

[15] H. W. Lenstra jr. and C. Pomerance, "Primality testing with Gaussian Periods," in *Proceedings of the 22nd Conference Kanpur on Foundations of Software Technology and Theoretical Computer Science (FST-TCS'02)*, vol. 2556, pp. 1, 2002.

[16] W. C. Lu, "Exceptional set of Goldbach number," *Journal of Number Theory*, vol. 130, pp. 2359–2392, Oct. 2010.

[17] I. Mikoss, "The prime numbers hidden symmetric structure and its relation to the twin prime infinitude and an improved prime number theorem," Technical Report MP-ARC-2006-314, 2006. (`http://www.ma.utexas.edu/mp_arc/c/06/06-314.pdf`)

[18] I. A. G. 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*, vol. 11, no. 6, pp. 715–726, 2008.

[19] Prime Number Patterns, "Prime number symmetry," 2010. (`http://primepatterns.wordpress.com/`)

[20] Z. Qin, *A Proof of the Goldbach's Conjecture*, The Economic Daily Press, China, Oct. 1995.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communincations of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[22] K. Slinker, "A proof of Goldbach's conjecture that all even numbers greater than four are the sum of two primes," Jan. 2008. (`http://arxiv.org/vc/arxiv/papers/0712/0712.2381v10.pdf`)

[23] Bo Yang, H. Ma, and S. Zhu, "A traitor tracing scheme based on the RSA system," *International Journal of Network Security*, vol. 5, no. 2, pp. 182–186, 2007.

[24] J. Ye and C. 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`)

[25] S. Zhang, "Goldbach conjecture and the least prime number in an arithmetic progression," *Comptes Rendus-Mathematique*, vol. 348, pp. 241–242, Mar. 2010.

[26] Y. Zhang, "Bounded gaps between primes," *Annals of Mathematics*, vol. 179, no. 3, pp. 1121-1174, 2014.

Chenglian Liu received his B.S degree in information management from National Union University (Taiwan) in 1992 and the MSc degree in national defense from National Defense University (Taiwan) in 2004. He studied his doctorate course at Royal Holloway, University of London from 2006 to 2009 under the supervised by Chris Mitchell. He is with a distinguished associate professor at Huizhou University since 2014. His research interests are in Key Agreement and Password Authentication, Number Theory and Cryptanalysis so on.

Chin-Chen Chang received his B.S. degree in applied mathematics in 1977 and the M.S. degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the college of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of the R.O.C. From 2002 to 2005, he was a Chair Professor of National Chung Cheng University. Since February 2005, he has been a Chair Professor of Feng Chia University. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures. He is a fellow of the IEEE.

Zhi-Pan Wu was born in 1975. He received his B.S degree in computer science at Xi-An University of Science and Technology in 1999, and received M.S. degree in software engineering at Central South University in 2006. He is with a senior lecturer at Huizhou University since 1999. His main research are image processing, computer vision and digital watermarking.

Shi-Lin Ye was born in 1992. He is an undergraduate of third grade student at Huizhou University currently. His main interests includes Network Security and Elementary Number Theory.