Mathematical Computation
December 2015, Volume 4, Issue 4, PP.71-76

Solve Goldbach Conjecture with Chandra Matrix Computation

Mi Zhou[1], Jun Steed Huang[23†], Qi Chen[2]

[1] Huaiyin Institute of Technology, Huaiyin, Jiangsu, 223003, China

[2] Dept. Telecommunications, Suqian College, Jiangsu University, Jiangsu, 223800, China

[3] Wireless Mobile Solution, San Diego, CA 92121, USA

[†]Email: junh@sqc.edu.cn

Abstract

This paper shows a fairly simple method of lifting Chandra matrices to explain Goldbach conjecture, by lifting we mean to add a nature number to every element of the matrix, in this way we constructed a set of Chandra matrices, which are equivalent to a modulo operations for a prime check. The advantage of this method is that it offers a quick computation of large prime partition for encryption key application. In this paper, it shows that all positive even integers $n \geq 40$ can be expressed as the sum of two primes, those $n < 40$ are trivial cases. We computed for n=40 to 400000 selectively with Matlab program. From which, we can verify that the conjecture is correct, and we can use it to construct the pseudo random key for encryption key exchanges.

Keywords: Chandra Matrix, Goldbach Partition, Key Exchange

1 INTRODUCTION

Goldbach's original conjecture was written in June 7, 1742 letter to Euler, stated "at least it seems that every number that is greater than 2 is the sum of three primes". Goldbach's conjecture is one of the oldest and best-known unsolved problems in number theory. Today it stands as: "Every even integer greater than 4 can be expressed as the sum of two primes" [1]. The conjecture has been shown to hold up through 4×10^18 [2] as of today, but remains unproven in a strictly mathematical sense, despite considerable effort from researchers all over the world.

For an engineer, any small number can be thought as a relatively large number; for mathematician, however, any large number is still a small number. Bearing this philosophy in mind, we made following matrix based derivations, inspired by Chandra matrix, hoping it will be beneficial to both engineers and scientists communities.

Note that here Goldbach considered the number 1 to be a prime, a convention that is no longer followed. As re-expressed by Euler, an equivalent form of this conjecture: Every even integer greater than 4 can be expressed as the sum of two primes. There are a number of ways to approach this conjecture, the most authentic way is to use the circle method [3], which is hard to understand; the next practical method is to use the Chen's Sieve [4], still not that easy to get it, another way is to use probabilistic analysis [5], preferred more by engineers; the modern one is using the matrix [6], which is very intuitive; anyway, what we are interested in here is some construction of relatively large numbers, that are used to manipulate the encryption key [7], as such we focus on the latest matrix method.

The increasing popularity of computer network technology is involved in all aspects of our life, including economy, military, commerce and others. However, information and network security is constantly challenged, which may affect the social stability. In response to the potential threat, we take encryption method to protect information and network security, such as symmetric encryption and asymmetric encryption (public key exchange). The key of symmetric encryption is based on the password. However, the password needs to be transferred through public key encryption that is asymmetric, including a different encryption key and decryption key, which guarantees the banking security.

The core of public key encryption algorithm is to find one-way hash function with irreversible function, used to

encrypt the message and ensure the privacy and security of communications network. For these reasons, based on the way we work with Goldbach's Conjecture, we designed an algorithm that can be used to implement the public-key encryption method mentioned in [8]. A number of Public key cryptography algorithms are based on the Goldbach Conjecture. Given a large even number consists of two prime factors. It is very difficult to know which two they are. With this feature, we can design a public key encryption algorithm as below.

The steps could be explained as shown here:

1. User A sends a request to Bank along with binary k as k+h(a), h is a hash function.

2. At the Bank, binary k is rendered using the secret key of user A called a

3. Bank generates binary sequence using Goldbach partition number or ellipse equation with k value.

4. n = a + b, where b is the key of user B, which user A doesn't know

5. m (even number) = n + random number (composite number from partition Case D).

6. One of the many pure prime (Case A) or half prime (Case B or Case C) partition pairs of m is selected say p and q.

7. Binary key is generated using the index p and q.

8. This binary key is sent to both user A and user B using their secret key a and b.

Cases A, B, C, D are the even number partition pattern defined in detail by next section, where Case A is the traditional Goldbach partition, and Case D is the similar but opposite partition, which is of interests to modern Quantum physics. Cases B and C are in between, and are of interests to both mathematics and physics.

2 MAIN DERIVATIONS

Let's look at a matrix: in 1934, one ground breaking mathematician from the Indian/ Bangladesh region Harish Chandra (1923–1983), in the field of number theory, had made a founding contribution of harmonic analysis on semisimple Lie groups. This subject is equally important for an engineer, as a synthesis of Fourier analysis, special functions and invariant theory etc., and it had also become a basic tool in analytic number theory, via the theory of automorphic forms, leading to modern Langlands program eventually. It became one of the major mathematical edifices of the second half of the twentieth century [9].

Chandra matrix is a square sieve, where the first row of the square sieve consists of the first element of 4, the difference between next every two adjacent numbers is 3, forms an arithmetic sequence: 4,7,10, ... The first column equals to the first row. The second row, third row, ... any subsequent rows are also arithme 垚 tic sequence, but the difference between two adjacent numbers gradually becomes larger, and they are 5,7,9,11,13, ... respectively, and they are all odd numbers, and the matrix is symmetrical, as shown below with modulo equivalent representation:

4	7	10	13	16	19	22	25	……	i.e. mod(n,3)=1
7	12	17	22	27	32	37	42	……	i.e. mod(n,5)=2
10	17	24	31	38	45	52	59	……	i.e. mod(n,7)=3
13	22	40	40	49	58	67	76	……	i.e. mod(n,9)=4
16	27	49	49	60	71	82	93	……	i.e. mod(n,11)=5
19	32	58	58	71	84	97	110	……	i.e. mod(n,13)=6

.....

The secret of this square sieve is: If a natural number N appears in the table, then 2N+1 certainly is not a prime number, because 2 times of remaining plus 1 is at least one of the divisors in the above modulo operations. If N does not appear in the table, then 2N+1 is definitely a prime number. Because 2 times of remaining plus 1 is not any of the divisors in the above modulo operation. Primes are left out. Almost all primes can be launched from this table, assume that the number of primes follow the prime number theorem: x/ln(x), in the arithmetical range of the numbers.

Based on above observations, we made a few similar matrices accordingly (lifting it by x):

4+x	7+x	10+x	13+x	……	i.e. mod(n,3)=1+ mod(x,3)
7+x	12+x	17+x	22+x	……	i.e. mod(n,5)=2+ mod(x,5)
10+x	17+x	24+x	31+x	……	i.e. mod(n,7)=3+ mod(x,7)
.....					

Lifting by any positive integer can be obtained if the natural number N in the matrix, 2*N-(2x-1) is certainly not a prime number, otherwise 2*N-(2x-1) must be a prime number. Notice that minuend 2N is an even number, and the subtrahend are all odd numbers, now let's only consider the lifted matrices that corresponding to the prime number 2x-1, skip all others, then 2N can be expressed as a sum of two prime numbers, in another word. There are four kinds of situations:

Case A: 2N-prime = prime number

Case B: 2N-prime = composite number

Case C: 2N-composite number = prime number

Case D: 2N-composite number = composite number

Case B and Case C can be transformed into each other, because a-b=c, then the a-c=b, the N in B is the numbers which appear in the matrix beginning of minus prime numbers, the N in C is the numbers not appear in the matrix beginning of minus composite numbers, the two N are of the same family, that is to say, all the numbers which appear in the matrix beginning of minus prime numbers are the same as the numbers not appear in the matrix beginning of minus composite numbers, then all the numbers which not appear in the matrix beginning of minus prime numbers is same as the numbers appear in the matrix beginning of minus composite number, so the N in A and D is of same family as well.

Based on Chen's theorem, the family of B & C goes all over the entire integer range until infinite, by using Goldbach partition pyramid as shown in Figure 1, it is not hard to prove that the family A & D sit right in between the family B & C, as such, both families should have the comparable size, moreover, the case A also sits in between case D, as such, 2N will cover all even numbers above 40, as shown below.

For example, all the even numbers not less than 40 can be expressed as an odd composite number plus an odd composite number, reason, due to the end of n must be 0,2,4,6,8, in another word:

$$\mathrm{mod}(n,10) = 2k \ (k=0,1,2,3,4)$$

can be rewritten as

$$\mathrm{mod}(p,5)+\mathrm{mod}(q,5) = 2k \ (k=0,1,2,3,4)$$

In summary, any even number not less than 40 can be expressed as an odd composite number plus an odd composite number. So the N in D include all even numbers bigger than 20, equivalently the N in A also contains all the numbers, A; 2N- prime number = prime number then 2N can be expressed as the sum of two prime numbers, so all the even numbers greater than 40 can be expressed as the sum of two prime numbers.

3 MATLAB COMPUTATIONS

There are a number of computation programs been developed [10], around the Goldbach conjecture. To verify our derrivations, we have coded four Matlab programs, each is dedicated to treat the case mentioned above. The flow diagram for Case A is the most complicated one, the rest Cases are similar, Case A pseudo code is shown below:

```
% Read
LargeNum ;
N = LargeNum/2;
Fv1 = ones(1,N);
```

```
Fv2 = zeros(1,N);
% Calculate
for i1=1:N  j=1:N
      m=2*j+1;
    if (i1>3*j)&(mod(i1,m)==j)
      Fv1(i1)=Fv1(i1)*0;
    Else     PrimeSeed(i1)=Fv1(i1)*i1;
    PrimeKeyOne=(2*PrimeSeed+1).*Fv1
    x=floor((PrimeKeyOne+1)/2);
    y=2*N-PrimeKeyOne;
for k=1:N  m=1:N
    if(y(k)==PrimeKeyOne(m))
      Fv2(k)=PrimeKeyOne(m);
   Else     PrimeKeyTwo(k)=Fv2(k);
  Mask=min(1,PrimeKeyTwo);
% Ouput
PrimeKeyOneSelected=(2*N-Fv2).*Mask
PrimeKeyTwoSelected=PrimeKeyTwo
ChandraLift=x.*Mask;
```

As the case A pseudo code shows, it includes read, calculate and output sections. The first step is to read data into LargeNum and to generate initial matrix Fv1 and Fv2. The second step is to calculate. According to the Chandra symmetrical matrix, taking advantage of cycle judgment, the prime will be obtained, which will be marked as primeKeyOne. Next, follow the formula: 2N-prime = prime number, using the similar way, we can get the other prime. The last step is to output the results.

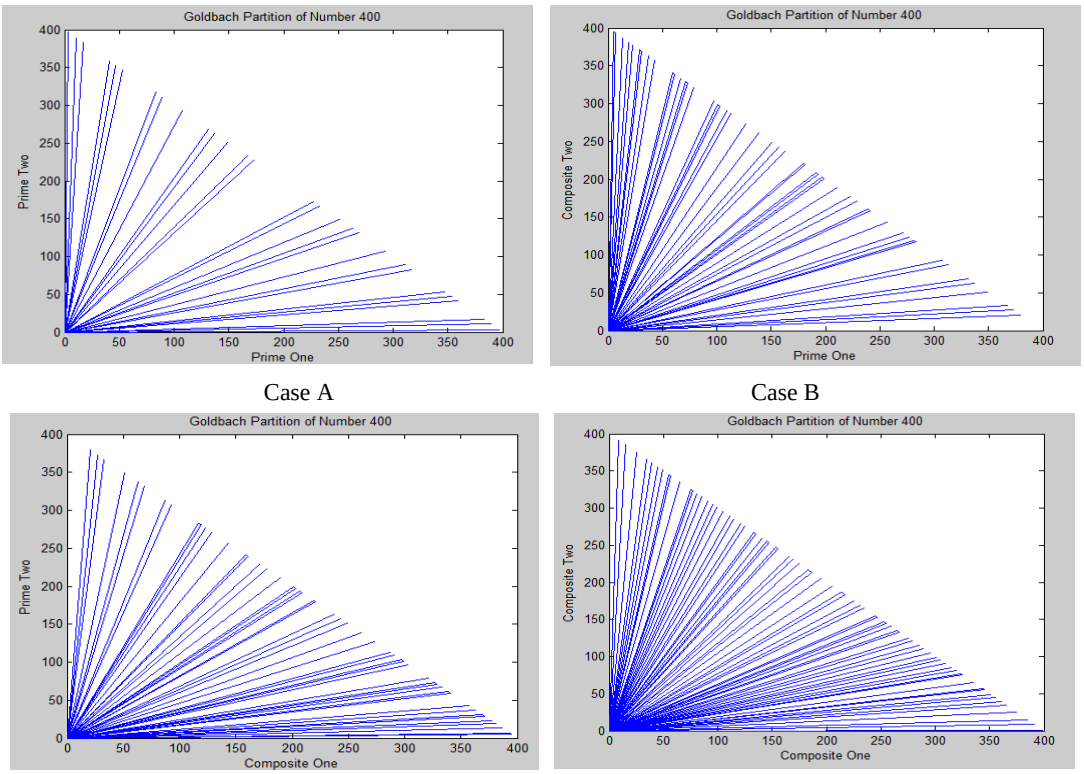
Here is the table 1 showing the combinations of A, B, C and D for selected different numbers 2N

TABLE 1 PARTITION COUNT FOR CASE A/ B/ C/ D

Even 2N	Case A	Case B	Case C	Case D
40	6	5	5	2
126	20	9	9	23
400	28	49	49	72
1264	52	152	152	274
4000	130	419	419	1030
12648	496	1014	1014	3799
40000	778	3424	3424	12372
126490	2574	9287	9287	42095
400000	4974	28885	28885	137254

The figure 1 show the results of 2N=400.

From which we can clearly see that Case A and Case D are strictly symmetrical by itself, rooted from the interleaved symmetrical Chandra matrix itself, Case B and Case C are symmetrical with respect to each other rooted from the row versus column lifting effect. From Case A, we can see that the prime is always mirrorly paired with some one else, or itself if it sits right on the mirror at 45 degree's position.



Case A Case B

Case C Case D

FIG. 1 SYMMETRICAL PATTERN OF PARTITION OF EVEN NUMBER

4 CONCLUSIONS

All the even numbers greater than 40 can be expressed as the sum of two prime numbers, finding these primes are hard by using hand calculation though, as such, we made a program in Matlab to compute that. This matrix based method is supported with the Matlab program available on Matlab server, showing that any even number can be split into two prime numbers. And we can use it to fulfil the tasks of the public or private key generation and distribution, with the variations of two prime partition algorithms.

5 AUTHOR CONTRIBUTIONS

Mr. Zhou conceived and derived the original work that led to this submission. Mr. Chen played an important role in completing the intensive Matlab computations. Prof. Huang contributed to polishing of the manuscript, besides providing the detail guidance.

REFERENCES

[1] Eric W. Weisstein, "Goldbach Number", MathWorld; http://mathworld.wolfram.com/GoldbachNumber.html

[2] Tomás Oliveira e Silva, "Goldbach conjecture verification", http://sweet.ua.pt/tos/goldbach.html

[3] Jeff Law, "The Circle Method on the Binary Goldbach Conjecture", 36 Pages Report, Mathematics Department, Princeton University, April 3, 2005

[4] Jingrun Chen, "On the representation of a large even integer as the sum of a prime and the product of at most two primes". Kexue Tongbao 11 (9): 385-386, 1966

[5] Henry F. Fliegel; Douglas S. Robertson, "Goldbach's Comet: the numbers related to Goldbach's Conjecture", Journal of Recreational Mathematics, v21(1) 1-7, 1989

[6] Roger Ellman, A PROOF OF "GOLDBACH'S CONJECTURE", May 10, 2000, Roger Ellman, 320 Gemma Circle, Santa Rosa, CA 95404, USA

[7] Subhash Kak, Goldbach Partitions and Sequences, Resonance, Volume 19, Issue 11, pp 1028-1037, November 2014

[8] S Kak, Encryption and error-correction coding using D sequences, IEEE Transactions on Computers, Vol.C-34, pp.803-809, 1985

[9] Roger Howe, “A Biographical Memoir for Harish Chandra”, National Academy of Sciences, 2011

[10] L E Dickson, Goldbach’s Empirical Theorem: Every Integer is a Sum of Two Primes. In History of the Theory of Numbers, Vol.1, Divisibility and Primality, New York: Dover, pp.421-424, 2005

AUTHORS

Mi Zhou was born in Suqian, China. He is student in Huaiyin Institute of Technology. He graduated from Suqian Economic and Trade Vocational College recently. His current research interest is number theory, Mathematical Olympiad mentoring.

Qi Chen was born in Suqian, China. He received B.E. degree in Department of Telecommunications Engineering form Jiangsu University this year. Now he is studying for master at Shanghai. His technical interest includes wireless sensor image processing and network programming.

Jun Steed Huang was born in Shanghai, China. He received his doctor's degree in 1992 from a Joint Ph.D program between Southeast University China and Concordia University Canada. He worked at Bell Canada, Lockheed Martin USA, Ottawa University. He is a Professor of Suqian College with Jiangsu University. He has been invited as board level advisor for a number of organizations from North American.