International Journal of Innovation in Science and Mathematics
Volume 4, Issue 2, ISSN (Online): 2347–9051

Infinite Cunningham Chains and Infinite Arithmetic Primes

Mi Zhou
Huaiyin Institute of Technology, Jiangsu 223003, China,
zhoumi19920626@163.com

Jun Steed Huang
Suqian College, Suqian, Jiangsu 223800,
Cooresponding author
steedhuang@ujs.edu.cn

Yiwen Xia,
Carleton University, Ottawa, Ontario K2P 2G6, Canada,
iwen@genieview.com

Abstract **– This paper shows a fairly simple method of using Chandra matrices to explain the property of Cunningham chains that are related to Green-Tao theorem, which states that the sequence of prime numbers contains arbitrarily long arithmetic progressions. In other words, for every natural number k, there exist arithmetic progressions of primes with k terms. The main reason we study this relationship is to find a systematic computation method for finding the large safe prime which is needed for construction of the Elgamal signature scheme for an agriculture application. In this paper, it shows that the density of safe primes are uniform in logarithm scale, we plot them with Matlab program. From which, we can see that the collection of the primes obtained from the Chandra matrices approach can be used for the set of signatures for the pesticide residue testing certificate, across a number of products demanding progressively different level of residual concentrations.**

Keywords **– Chandra matrix, Cunningham Chain, Arithmetic Primes, Flgamal Signature, Pesticide Residual.**

I. INTRODUCTION

In mathematics, a Cunningham chain is a certain sequence of prime numbers. It is named after mathematician A. J. C. Cunningham (Delhi 1842 – London 1928). They are also called chains of nearly doubled primes [1]. Cunningham chains are very useful in cryptographic systems since they provide suitable safe settings for the Elgamal crypto system [2]. The Elgamal encryption system is an asymmetric key encryption algorithm for the public-key cryptography which is based on the Diffie–Hellman key exchange [3]. It was described by Taher Elgamal in 1985[4]. Elgamal encryption is used in the free GNU privacy guard software [5]. The popular DSA (Digital Signature Algorithm) [6] is a variant of the Elgamal signature scheme. In this paper, we focused on the signature scheme, and we devised a set of signature algorithm that is good for pesticide residue testing certification process [7].

It follows from Dickson's conjecture, which is widely believed to be true, that for every k there are infinitely many Cunningham chains of length k. There are, however, no known direct methods of generating such chains, we can only search for it with computer programming, such as the one we proposed in this paper, by using Chandra matries. Dickson's conjecture [8] is the conjecture proposed by Dickson (1904) that for a finite set of linear forms $a_1 + b_1n$, $a_2 + b_2n$, ..., $a_k + b_kn$ with $b_i \geq 1$, there are infinitely many positive integers n for which they are all prime. Two other special cases are well known conjectures: there are infinitely many twin primes (n and 2 + n are primes) [9], and there are infinitely many Sophie Germain primes (n and 2n+1 are primes) [10].

On the other hand, Green–Tao theorem, proved by Ben Green and Terence Tao in 2004 [11] states that the sequence of prime numbers contains infinite long arithmetic progressions. That is for every natural number k, there exist arithmetic progressions of primes with k terms. Unfortunately, the proof is based on the ergodicity of the analytic number, it doesn't tell you how to find them at all. In this paper, we use the Chandra matrices to bridge the connection between the Green-Tao theorem with the property of the Cunningham chains, and use it to generate the primes for digital signatures of various strengths.

The increasing popularity of computer cloud technology is involved in all aspects of our life, including industry, agriculture, military, education and commerce. However, information and network security is constantly challenged, which may affect the global stability. In response to the potential fraud and threat, we take product specific signature method to protect information and network security for food industry, such as digitally signed green product specific certificate. A number of DSA algorithms are based on the safe primes. Given a large number if not infinite of Cunningham chains, it is very difficult to know which prime of which chain is actually used to code which product for what concentration of the pesticide residual. With this feature, we can design a pesticide residual testing certificate algorithm as below.

Let H be a hash function.

Let p be a large prime.

Let g<p be a randomly chosen generator.

The steps could be explained as shown here:

1. Choose a Cunningham chain with the length matches with the number of products. Number the product in a sequence according to the residue concentration. Set the prime number p =2n+1. Repeat above until the product number to be certified.

2. Randomly choose a secret key x with $1 < x < p - 1$. Compute y = g ^ x mod p. The public key is y. The secret key is x.

3. To sign a message m the signer performs the following steps. Choose a random k such that $1 < k < p - 1$ and gcd (k, p − 1) = 1. Compute r = g^k mod p. Compute s = (H(m)-xr)/k mod{p-1}. If s = 0 start over again. Then the pair (r,s) is the digital signature of m.

4. A signature (r,s) of a message m is verified as follows. 0<r<p and 0<s<p-1. g^{H(m)} = y^r r^s mod p. The verifier accepts a signature if all conditions are satisfied and rejects it otherwise.

5. If the specific verifier for the product is accepted, declared the product is genius, otherwise, the product certificate is said faked.

Where the first and the last step is product specific selection, step 2 is key selection, step 3 is sign process, and step 4 is verification process. All steps can be implemented in embedded system, PC or even APP on Smart Phone.

II. Main Derivations

Cunningham chain has a number of interesting properties "it is always a complete finite set", however the number of finite length Cunningham chains is infinite. We use two mathematical theoretical tools, i.e. Chandra matrix and a theorem from Terence Tao et al "existence of any length prime arithmetic sequence".

Let's look at a matrix: in 1934, one ground breaking mathematician from the Indian/ Bangladesh region Harish Chandra (1922-1983), in the field of number theory, has made a founding contributions of harmonic analysis on semi simple Lie groups. 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 arithmetic sequence, but the difference between two adjacent numbers gradually become larger, and they are 5,7,9,11,13, ... respectively, and they are all odd numbers, and the matrix is symmetrical, as shown below

4	7	10	13	16	19	22	25
7	12	17	22	27	32	37	42
10	17	24	31	38	45	52	59
13	22	31	40	49	68	67	76
16	27	38	49	60	71	82	93
19	32	45	58	71	84	97	110

…….

The subtle of this square sieve matrix is that a 2N+1 cannot be a prime if the natural number N exist in this matrix. On the contrary the 2N+1 will be a prime if the natural number N cannot be found in this matrix. The safe primes we are looking for are those prime (2N+1) infinite subsets with finite length, with which N is also a prime. In fact, if N=2mn+m+n, then 2N+1=2(2mn+m+n)+1=4mn+ 2m+2n+1=(2m+1)(2n+1), which means that 2N+1 cannot be a prime. Otherwise, if N is not exist in this matrix, which means 2N+1 is not a prime, than 2N+1 must be product of odd number, shown as 2N+1=(2m+1)(2n+1)= 4mn+2m+2n+1, and we get N=2mn+m+n, which will appear in this matrix. This violate the hypothesis, so the 2N+1 will be prime when the N is not in the matrix. 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 arithmetical range of the numbers.

Terence Tao proved the existence of any length arithmetic sequence of prime numbers, then it exists a prime number arithmetic sequence of infinite length, the number of each column can be expressed as the form 2n + 1, n does not appear in the above matrix.

Assume it has the existence of an infinite Cunningham chain length:

n, 2n+1, 4n+3, 8n+7, 16n+15, 32n+31…

This chain contains a difference steps: n+1, 2n+2, 4n+4, 8n+8, etc.

If we want to construct an arithmetic sequence of prime numbers from this chain, we need to progressively add more next primes, until infinite, which means there is no infinite length sequence. This contradicts with Green-Terence theorem. As such, we conclude that the Cunningham chain is of finite length.

However, as the Chandra matrix is infinite in size, there are infinite numbers of the sectioned Chains to be added with different steps, to map to the infinite length of arithmetic sequence that Tao predicted.

In summary, we can find enough Cunningham chains first, and then by adding some primes, we can construct a long enough arithmetic sequence, if we want.

III. Matlab Computation

There are a number of computation programs been developed [12], around the safe prime computations. To verify our derivations, we have coded a Matlab programs, dedicated to visualize the cases mentioned above. The 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);
   ElsePrimeKeyTwo(k)=Fv2(k)；
   Mask=min(1,PrimeKeyTwo);

% Ouput
   PrimeKeyOneSelected=(2*N-Fv2).*Mask
   PrimeKeyTwoSelected=PrimeKeyTwo
   ChandraLift=x.*Mask;

%Plot
length= size(Fv1');
bar(length,Fv1);
bar(length,log(Fv1));
```

As the 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 next prime. Where N itself is also prime. The last step is to output and print the results. Table 1 shows the results.

Table 1. List of Safe Prime Chains

5, 11, 17, 23, 29 is an arithmetic sequence
5, 11, 23, 47 is a Cunningham chain
41, 83, 167 is a Cunningham chain
89, 179, 269, 359, 449 is an arithmetic sequence
89, 179, 359, 719, 1439, 2879 is a Cunningham chain
2759832934171386593519， 2759832934171386593519*2+1， 2759832934171386593519*4+3 ditto

The Figure 1-4 are the results of systematic pattern of safe primes from the chains and unsafe primes of all.

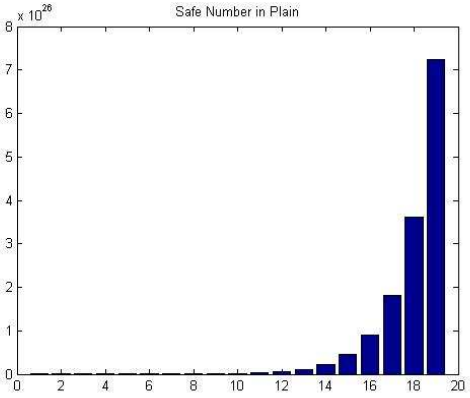

Fig. 1. Value of Prime from Chains

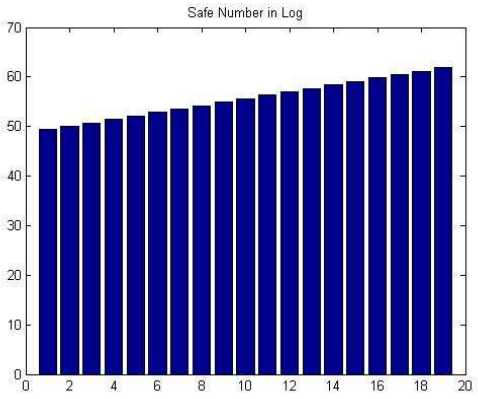

Fig. 2. Systematic Pattern of Prime from Chains

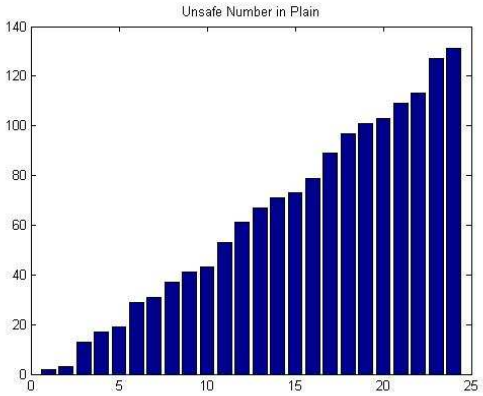

Fig. 3. Value of Unsafe Primes

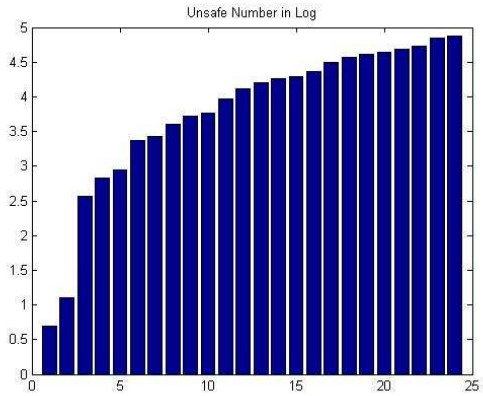

Fig. 4 Pattern of Unsafe Primes

From which we can clearly see that the safe and the unsafe primes are quite different, safe prime chain has geometric pattern and behavior strictly linear in logarithmic plot, while the unsafe primes has roughly linear looking in plain plot, while behavior nonlinear in logarithmic scale.

IV. CONCLUSION

By using Chandra matrix, we demonstrated that the Cunningham chains of type two exist infinite of which, we can concatenate a number of them to form an arithmetic prime sequence, by adding each chain with extra primes geometrically. Finding these primes are hard by using hand calculation though, 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 an arithmetic prime sequence can be associated with many geometrical prime chains, which can be used to sign a digital signature. The higher the chain's value, the harder to reverse engineering it. As such, we can use it to fulfill the tasks of the public or private authentication key generation and distribution, with the variations of Elgamal signature algorithms for the agricultural application.

V. AUTHOR CONTRIBUTIONS

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

REFERENCES

[1] Tony Forbes "Prime Clusters and Cunningham Chains" Mathematic of Computation, Volume 68, Number 228, pp.1739-1747, 1999.
[2] Patrick Horster, Markus Michels, Holger Petersen "Generalized ElGamal signatures for one message block" Technical Report TR-94-3, 1994.
[3] Simson L. Garfinkel "Public key cryptography" Computer, Volume 29, Issue 6, pp.101-104, 1996.
[4] Taher Elgamal "A subexponential-time algorithm for computing discrete logarithms over GF(p^2)" IEEE transactions on information theory, vol. IT-31, NO.4, 1985.
[5] Richard Stallman "The GNU Project" Open Sources, Available: org.noemalab.eu/sections/ideas/ideas_art icles/pdf/stallman_eng.pdf, 1998.
[6] Gunjan Jain "Digital Signature Algorithm" International Journal of Innovations in Computing, Vol.1, Issue 1, 2005.
[7] Karim L, Anpalagan A, Nasser N, et al. "Sensor-based M2M agriculture monitoring systems for developing countries: state and challenges" Network Protocols and Algorithms, pp.68-86, 2013.
[8] Zhang S. "Notes on Dickson's Conjecture" arXiv preprint arXiv:0906.3850, 2009.
[9] Zhang Y. "Bounded gaps between primes" Annals of Mathematics, 179(3), pp.1121-1174, 2014.
[10] Dubner H. "Large Sophie Germain primes" Mathematics of Computation of the American Mathematical Society, 65(213), pp.393-396, 1996.
[11] Green B, Tao T. "The primes contain arbitrarily long arithmetic progressions" Annals of Mathematics, pp.481-547, 2008.
[12] Wagstaff S. "The Cunningham Project" High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Institute Communications, pp.367-378, 2004.

AUTHOR'S PROFILE

Zhou Mi was born in Suqian, China. He is a 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.

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 advisor for a number of organizations from North American.

Yiwen Xia was born in Beijing, China. He graduated from Beijing University of Post and Telecommunication in 2014 major Electronic Information Engineering. Now he is studying for master at Carleton. His technical interest includes online stores and network programming.