On the Sophie Germain prime conjecture

FENGSUI LIU
Department of Mathematics
University of NanChang
NanChang
China
liufengs@tom.com

Abstract: - By extending the operations $+,\times$ on natural numbers to the operations on finite sets of natural numbers, we founded a new formal system of a second order arithmetic $\langle P(N), N, +, \times, 0, 1, \in\rangle$. We designed a recursive sieve method on residue classes and obtained recursive formulas of a set sequence and its subset sequence of Sophie Germain primes, both the set sequences converge to the set of all Sophie Germain primes. Considering the numbers of elements of this two set sequences, one is strictly monotonically increasing and the other is monotonically increasing, the order topological limits of two cardinal sequences exist and these two limits are equal, we concluded that the counting function of Sophie Germain primes approaches infinity. The cardinal function is sequentially continuous with respect to the order topology, we proved that the cardinality of the set of all Sophie Germain primes is $\aleph_0$ using modular arithmetical and analytic techniques on the set sequences. Further we extended this result to attack on Twin primes, Cunningham chains and so on.

Key − Words: Second order arithmetic, Recursive sieve method, Order topology, Limit of set sequences, Sophie Germain primes, Twin primes, Cunningham chain, Ross-Littwood paradox

1 Introduction

Primes are mysterious, in WSEAS there is a recent research also [7].

In number theory there are many hard conjectures about primes, the Sophie Germain prime conjecture is one from them.

If $a, 2a+1$ are simultaneously prime, we call this natural number a be a Sophie Germain prime and denote it with a predicate S(2, a).

The first few Sophie Germain primes are

3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131,…… .

Like the twin prime conjecture, it is a conjecture that there are infinitely many Sophie Germain primes. We may express this conjecture with a very simple formal sentence

$$\forall_b \exists_{a>b} S(2,a),$$

but it is very hard to prove this sentence rigorously.

Sophie Germain primes play an important role in number theory. Here are two examples.

These primes were named after her when French woman mathematician Sophie Germain (around 1825) proved that Fermat's Last Theorem holds true for such primes, this is the first general result toward a proof of Fermat's Last Theorem. This beautiful result was extended by Legendre, and also by Denes (1951), and more recently by Fee and Granville (1991) [4].

There is a theorem about Mersenne composites.

If $a \equiv 3 \bmod 4$, then a is a Sophie Germain prime if and only if

$$2a+1 | M_a.$$

Where M_a is a Mersenne number

$$M_a = 2^a - 1.$$

This theorem is stated by Euler in 1750 and proved by Lagrange in 1775.

Thus the proof of the Sophie Germain prime conjecture is a proof of another open problem, that there are infinitely many Mersenne composites.

On the basis of heuristic prime number theory and the prime theorem, Hardy and Littlewood formulated the Sophie Germain prime conjecture as follows.

The number $\pi(x, S)$ of Sophie Germain primes less than or equal to a given real number x is approximately [2]

$$\pi(x,S) \sim 2c_2 \int_2^x \frac{dt}{\log t \log 2t} \sim \frac{2c_2\, x}{\log^2 x}.$$

This formula gives accurate predications. It is extremely difficult to prove this formula rigorously in analytic number theory.

In 2006, Terence Tao expounded additive patterns in primes and said: "Prime numbers have some obvious structure. (They are mostly odd, coprime to 3, ect.) We don't know if they also have some additional exotic structure. Because of this, we have been unable to settle many questions about primes."[21].

In 2007, G.Harman described the rapid development in recent decades of sieve methods and analytic number theory, stressed again: "As is well known, the solution to these problems seems to be well beyond all our current method."[6]

Many remarkable results have been proved using modern sieve theory. Because the parity problem, a formidable obstacle, the traditional sieve theory is unable to settle those conjecture [9] [21]. One needs to recast the sieve method.

Based on the modern progress of model theory, set theory, general topology and recursion theory we try to tackle those problems with a new sieve method.

In an exotic realm of a second order arithmetic P(N), we introduce set sequences of natural numbers, and use the Chinese remainder theorem to recast or refine Eratosthene's sieve method, then we can capture some enough usable secret structures about prime sets and use limits of set sequences to directly determine the set of all Sophie Germain primes and its cardinality.

$$\{a: S(2,a)\} = \lim A_i' = \lim T_i',$$
$$|\{a: S(2,a)\}| = |\lim A_i'| = |\lim T_i'| = \lim |T_i'| = \aleph_0.$$

By this formulation, it is comparatively easy to prove the Sophie Germain prime conjecture, because this formula itself has discerned a logical structure of the set of all Sophie Germain primes. The parity problem in the traditional sieve theory would naturally be circumvented.

2 A formal system

First of all we define several operations on finite sets of natural numbers.

Let

$$A = \langle a_1, a_2, \dots, a_i, \dots, a_n \rangle,$$
$$B = \langle b_1, b_2, \dots, b_j, \dots, b_m \rangle$$

be arbitrary finite sets of natural numbers, we define

$$A + B = \langle a_1 + b_1, a_2 + b_1, \dots, a_i + b_j, \dots, a_{n-1} + b_m, a_n + b_m \rangle,$$
$$AB = \langle a_1 b_1, a_2 b_1, \dots, a_i b_j, \dots, a_{n-1} b_m, a_n b_m \rangle.$$

For the empty set $\emptyset$, let

$$\emptyset + A = \emptyset,$$
$$\emptyset A = \emptyset.$$

Let $A \backslash B$ be the set subtraction.

Define the solution of the system of congruences

$$X \equiv A = \langle a_1, a_2, \dots, a_i, \dots, a_m \rangle \bmod a,$$
$$X \equiv B = \langle b_1, b_2, \dots, b_j, \dots, b_m, \rangle \bmod b$$

to be

$$X \equiv D = \langle d_{11}, d_{21}, \dots, d_{i\,j}, \dots, d_{n-1\,m}, d_{n\,m} \rangle \bmod ab.$$

Where

$$x \equiv d_{i\,j} \bmod a\,b$$

is the solution of the system of congruences

$$x \equiv a_i \bmod a,$$
$$x \equiv b_j \bmod b.$$

If a, b are coprime gcd(a,b)=1, by the Chinese remainder theorem the solution is unique and computable.

Except extending +, × to finite sets of natural numbers, we continue the traditional interpretation of symbols $+, \times, \in$, then we founded a now model of the arithmetic of natural numbers by a two-sorted logic

$$\langle P(N),\ N,\ +,\ \times,\ 0, 1, \in \rangle.$$

Where N is the set of natural numbers and P(N) is the power set of N.

In contrast to the usual first order arithmetical model

$$\langle N, +, \times, 0, 1 \rangle,$$

we call this new model be a second order arithmetical model or algebraic structure and denote it with P(N).

Mathematicians assume that $\langle N, +, \times, 0, 1 \rangle$ is the standard model of Peano theory PA, similarly, we assume that $\langle P(N), N, +, \times, 0, 1, \in \rangle$ is the standard model of the theory of the second order arithmetic PA ∪ ZF, which is a joint theory of PA and ZF, in other words the P(N) not only is a model of Peano theory PA but also is a model of set theory ZF.

As a model of set theory ZF, the natural numbers are atoms or urelements, objects that have no element. We discuss the sets of natural numbers and sets of sets of natural numbers.

In the second order formal system P(N), we formalize natural numbers and sets thereof as individuals, terms or points. A determined set not only contains its all elements but also includes all information of the distribution of its elements, especially the number of elements in this set.

The second order language $\langle +, \times, 0, 1, \in \rangle$ has stronger expressive power. The second order model has richer mathematical structures. The second order theory is more powerful and flexible.

Except inheriting usual theorems of the first order arithmetic, in P(N) we may introduce a new sort of mathematical structures and to prove some hard conjectures about primes. The first order arithmetic N has no well formed formula to represent such new structures and to prove those conjectures about primes.

In particular we introduce a new sort of arithmetic functions

$$f:\ N \to P(N),$$

which is a set valued function defined on the set N, i.e., set sequences of natural numbers, to obtain a recursive sieve method on the residue classes.

We may use the recursive sieve method to look for a string of logical reasoning that demonstrates the truth of the Sophie Germain prime conjecture is built into the structures of prime sets in the framework of recursion theory and general topology, rather than to look for good approximations or non-trivial lower bounds of the counting function $\pi(x, S)$.

"A well chosen notation can contribute to making mathematical reasoning itself easier, or even purely mechanical."[11].

As a simple example of the recursive sieve method, deleting the congruence class $0 \bmod p_i$ from the set of all natural numbers successively, i.e., all numbers a such that the least prime factor of a is p_i, instead the multiples of p_i in a given range, leaving the reduced residue system$T_{i+1} \bmod m_{i+1}$, we obtain an exact formula producing all primes[16]:

$$T_1 = \langle 1 \rangle,$$
$$p_1 = 3,$$
$$T_{i+1} = (T_i + \langle m_i \rangle \langle 0,1,2,\ldots,p_i - 1 \rangle) \setminus D_i,$$
$$p_{i+1} = U(T_{i+1}). \qquad (1)$$

Where the $U(T_{i+1})$ is a projective function

$$U(\langle t_1, t_2, \ldots, t_n \rangle) = t_2,$$
$$p_0 = 2,$$
$$m_{i+1} = \prod_0^i p_j,$$

and

$$X \equiv D_i = \langle p_i \rangle T_i \bmod m_{i+1}$$

is the solution of the system of congruences

$$X \equiv \langle 0 \rangle \bmod p_i,$$
$$X \equiv T_i \bmod m_i.$$

The first few terms of this formula are:

$$T_1 = \langle 1 \rangle,$$
$$p_1 = 3,$$
$$T_2 = \langle 1,3,5 \rangle \setminus \langle 3 \rangle = \langle 1,5 \rangle,$$
$$p_2 = 5,$$
$$T_3 = \langle 1,5,7,11,13,17,19,23,25,29 \rangle \setminus \langle 5,25 \rangle$$
$$= \langle 1,7,11,13,17,19,23,29 \rangle$$
$$P_3 = 7$$
$$T_4 = \langle 1,7,11,13,17,\ldots,199,203,209 \rangle \setminus$$
$$\langle 7,49,77,91,119,133,161,203 \rangle$$
$$= \langle 1,11,13,17,\ldots,197,199,209 \rangle$$
$$p_4 = 11,$$

It is easy to prove this formula by means of mathematical induction: the least number except 1 in the reduced residue system T_{i+1} is the prime p_{i+1}.

One plugs i into this formula, this formula will produce the i-th prime. This primitive recursive formula actually exhibits infinitely many primes by $+, \times$, it provides a constructive proof of Euclid's theorem using the new sieve method[19].

It reveals a fundamental rule of the distribution of primes. Now the primes appear in a highly regular pattern.

Note, the traditional sieve theory itself is unable to prove Euclid's theorem [21].

We do not discuss further this formal system in view from logic [14].

3 A recursive formula and its simple consequences

An ancient Greek mathematician Eratosthenes created a sieve method for fining the primes in a given range.

Based on the inclusion-exclusion principle, Lagendre used the sieve method of Eratosthenes to estimate the size of sifted sets of integers in a given range. A main difficult is the accumulation of error terms

Taking a partial summation from the formula of the inclusion-exclusion principle, Brun estimated the size of sifted sets for almost primes, products of at most k primes.

According to carefully chosen weight functions, Selberg given a better estimate for the almost primes.

Some partial successes of the traditional sieve theory include: Brun's theorem the sum of the reciprocals of twin primes converges, Chen's theorem there are infinitely many primes *p* such that *p* + 2 is the product of at most two primes[3], and the fundamental lemma of sieve theory.

One of original purposes of the traditional sieve theory was to settle prime patterns of various forms, example the twin primes or the Sophie Germain primes.

It has proven that the traditional sieve theory is unable to provide non-trivial lower bounds on the size of prime patterns. Also, any upper bounds must be off from the truth by a factor of 2 or more. This is the parity problem[21].

It seems that one needs basically to recast the traditional sieve theory to get around the parity problem.

Now we recast the sieve method of Eratosthenes using the Chinese remainder theorem. We try to understand what is the sieve of Eratosthenes in view from modern mathematics and logic, and then to prove Sophie Germain prime conjecture.

Let p_i be the i-th prime, $p_0 = 2$.

For any prime $p_i > 2$, we consider the congruence classes

$$B_i = \{a : a \equiv 0 \bmod p_i \ \vee \ 2a + 1 \equiv 0 \bmod p_i\}$$
$$\equiv \langle 0, \tfrac{1}{2}(p_i - 1) \rangle \bmod p_i.$$

Let

$$m_{i+1} = \prod_0^i p_j.$$

From the set of all odd numbers

$$X \equiv \langle 1 \rangle \bmod 2$$

we successively delete the congruence classes

$$X \equiv B_i \bmod p_i,$$

i.e., all numbers a such that the least prime factor of a or 2a+1 is p_i, and obtain the congruence classes

$$X \equiv T_{i+1} \bmod m_{i+1}$$

such that if $a \in X$ then a and 2a+1 do not contain any prime $p_j \leq p_i$ as a factor.

So that a recursive formula of T_{i+1} which is the set of the least nonnegative representatives of the residue class mod m_{i+1} is as follows:

$$T_1 = \langle 1 \rangle,$$

$$T_{i+1} = (T_i + \langle m_i \rangle \langle 0,1,2,\dots,p_i - 1 \rangle) \backslash D_i. \quad (2)$$

Where

$$X \equiv D_i \bmod m_{i+1}$$

is the solution of the system of congruences

$$X \equiv T_i \bmod m_i$$
$$X \equiv B_i \bmod p_i.$$

The number of elements of the set T_{i+1} is

$$|T_{i+1}| = \prod_1^i (p_j - 2). \quad (3)$$

The first few terms of those sets T_i are

$$T_1 = \langle 1 \rangle,$$
$$T_2 = (\langle 1 \rangle + \langle 0,2,4 \rangle) \backslash \langle 1,3 \rangle = \langle 5 \rangle,$$
$$T_3 = (\langle 5 \rangle + \langle 0,6,12,18,24 \rangle) \backslash \langle 5,17 \rangle,$$
$$= \langle 11,23,39 \rangle,$$
$$T_4 = (\langle 11,23,29 \rangle + \langle 0,30,\dots,150,180 \rangle)$$
$$\backslash \langle 59,101,119,143,161,203 \rangle$$
$$= \langle 11,23,29,41,53,\dots,173,179,191,209 \rangle.$$

It is easy to prove the formulas (2), (3) by means of mathematical induction.

Like Eratosthene's sieve, the number 1 is hidden, which does not enter the filtration, all odd numbers a > 1 are filtrated.

We delete the numbers a in the congruence classes

$$X \equiv B_i \bmod p_i$$

under the divisible condition

$$\{a: (a \equiv 0 \bmod p_i \vee 2a + 1 \equiv 0 \bmod p_i) \wedge a \geq p_i\},$$

then except $a = p_i$ itself may be a Sophie Germain prime, other numbers a all are not Sophie Germain prime.

Now we list some simple consequences from the recursive formula T_i, their proof is easy.

1) Let min T_i is the least number in the set T_i, then a criterion of Sophie Germain prime is

$$S(2,a) \leftrightarrow a = \min T_i = p_i \geq 3. \quad (4)$$

This criterion recursively enumerates all Sophie Germain primes.

2) Using the recursive formula (2), we easily compute Sophie Germain primes, in fact, we had computed out the first few Sophie Germain primes 3,5,11,23,29,41,53,83,89,113,131,173,179 ,191,….

3) If $a \geq p_i$ is a Sophie Germain prime, then the natural number a belongs to the congruence class T_i

$$a \in T_i \bmod m_i.$$

As an algorithm for Sophie Germain primes, like the prime formula, one may further observe a fact that the least number in the set T_i min T_i is a Sophie Germain prime for all i

$$a = \min T_i \rightarrow S(2,a),$$

then intuitively our sieve method provides a conclusion that there are infinitely many Sophie Germain primes, but it is not easy to directly prove this fact. We do not discuss this problem in detail.

4 A Sophie Germain prime theorem

The sifting process on residue classes products a recursive set sequence T_i, we refine this recursive set sequence to determine the set of all Sophie Germain primes and its cardinality using analytic techniques.

Let B_i' denote the set of all non-Sophie Germain primes in the congruence classe B_i

$$B_i' = \{a: (a \equiv 0 \bmod p_i \vee 2a + 1 \equiv 0 \bmod p_i) \wedge a > p_i\}$$

We delete the set B_i' and save the natural number a as a survivor if a is a Sophie Germain prime.

Let A_i be the set of all Sophie Germain primes less than p_i

$$A_i = \{a: a < p_i \wedge S(2,a)\}.$$

We adjust the set T_i to be

$$T_i' = A_i \cup T_i \quad (5)$$

Except saving all Sophie Germain primes $a < p_i$ as survivors in the set T_i', two set sequences T_i' and T_i are same.

Let $|A_i|$ be the number of all Sophie Germain primes less than p_i, then the number of elements of the set T_i' is

$$|T_i'| = |A_i| + |T_i|. \quad (6)$$

Let A_i' be the Sophie Germain prime subset of the set T_i'

$$A_i' = \{a: a \in T_i' \wedge S(2,a)\} \quad (7)$$

4.1 An informal argument

Now we describe how the sifting process T_i', A_i' approaches the infinite set of all Sophie Germain primes in the framework of an order topology.

Obtained the set T_i' from the formula (5), let $a \in T_i'$, if

$$2a+1 < p_i^2,$$
then the number a is a Sophie Germain prime, which belongs to all T_r' for $r > i$ and will never be deleted.

Obtained the set T_i' from the formula (5), let $a \in T_i'$, if
$$2a+1 \geq p_i^2,$$
then a is a good candidate for the Sophie Germain prime, a and 2a+1 do not contain any one of the first i -1 primes as a factor. In this case, if a is a Sophie Germain prime, then a belongs to all T_r' for $r > i$, otherwise the a is an "error term", there is a prime p_k such that
$$p_k | a \vee p_k | 2a+1,$$
a does not belong to any T_r' for $r > k$.

Our sieve method itself will delete all error terms and needs not estimate the number of error terms.

Each non- Sophie Germain prime is deleted exactly once, our sieve method needs not the inclusion-exclusion principle. There is no accumulation of error terms.

As i goes to infinity we delete more and more non-Sophie Germain primes, exhibit more and more Sophie Germain primes or candidates of Sophie Germain primes in the set T_i', the set sequence T_i gets as close as we want to the infinite set of Sophie Germain primes, the set sequences T_i', A_i' get as close as we want to the infinite set {a:S(2,a)} of all Sophie Germain primes.

If i is extremely large, example
$$i=c=10^{10^{1000}},$$
theoretically we can construct a set by the formula (5), which has approximated to the set {a:S(2,a)}of all Sophie Germain primes.

By the prime theorem, the set T_c' has exactly exhibited all Sophie Germain primes

$$a < 1/2p_c^2 \sim 10^{1000} \times 10^{10^{1000}} \times 2.3 \times 10^{1000} \times 10^{10^{1000}}$$

The set T_c' has
$$|T_i'| > \prod_1^{10^{10^{1000}}} (p_j - 2)$$
elements a such that a and 2a+1 do not contain any one of the first $10^{10^{1000}}$-1 primes as a factor except itself, in other words, if a or 2a+1 has prime factors except itself, they are large than
$$2.3 \times 10^{1000} \times 10^{10^{1000}}.$$

In the approximate sense the set T_c' may be regarded as a set of Sophie Germain primes and the number of elements of this set may be regarded as an infinity. Against our daily standard the set T_c' is an infinite set of Sophie Germain primes.

Ultimately, as the limit of the set sequences T_i', A_i' we have deleted all non- Sophie Germain prime sets B_i' successively, philosophers of mathematics said that one performed a supertask [13], and have obtained infinitely many natural numbers a such that a and 2a+1 do not contain any prime as a factor except itself, these infinitely many natural numbers a exactly constitute the set of all Sophie Germain primes.

Our sieve method can exactly determine that the numbers of elements of the set sequence T_i' is strictly monotonically increasing, we need not estimate the lower bounds or upper bounds of the counting function $\pi(x, S)$ through the almost primes. We get around the parity problem.

Our proof needs not the Cramer random model or The Riemann Hypothesis.

This is an informal argument, which shows the Sophie Germain prime conjecture is true.

We give a formal proof in the sense of logic using analytic techniques in an order topological space.

4.2 A formal argument

Lemma 1 *The set sequences T_i', A_i' converge to the set of all Sophie Germain primes.*

Proof: First of all we quote a definition of the set theoretic limit of a set sequence from the textbook "Set Theory, with an introduction to descriptive set theory" by K.Kuratowski and A.Mostowski [15].

Let F_n denote a set sequence, we define
$$\limsup_{n=\infty} F_n = \cap_{n=0}^{\infty} \cup_{i=0}^{\infty} F_{n+i},$$
$$\liminf_{n=\infty} F_n = \cup_{n=0}^{\infty} \cap_{i=0}^{\infty} F_{n+i},$$
If
$$\limsup_{n=\infty} F_n = \liminf_{n=\infty} F_n,$$
we say that the set sequence F_n converges to the limit
$$\lim F_n = \limsup_{n=\infty} F_n = \liminf_{n=\infty} F_n.$$
Let
$$T_e = \{a: S(2, a)\}$$
be the set of all Sophie Germain primes, the sifted set, which is the end result by deleting all non-Sophie Germain primes from the set of all odd numbers.

Let X_i be the whole congruence class mod m_i with the representatives T_i,
$$X_i \equiv T_i \bmod m_i$$
Let
$$X_i' = A_i \cup X_i$$
Then
$$X_1' \supset X_2' \supset \ldots \supset X_i' \supset \ldots\ldots,$$
according to the definition of the set theoretic limit of a set sequence we have
$$\lim X_i' = \cap X_i' = T_e.$$

Obviously

$$A'_1 \subset A'_2 \subset \dots \subset A'_i \subset \dots \dots,$$

we have also

$$\lim A'_i = \cup A'_i = T_e.$$

Obviously,

$$A'_i \subset T'_i \subset X'_i$$

It is easy to prove

$$\limsup T'_i \subset \limsup X'_i = \lim X'_i,$$

$$\liminf T'_i \supset \liminf A'_i = \lim A'_i$$

$$\liminf T'_i \subset \limsup T'_i.$$

Thus

$$\lim T'_i = T_e.$$

In the sense of the set theoretic limit we have proved that both the set sequences T'_i, A'_i converge to their common limit point T_e

$$\lim T'_i = \lim A'_i = T_e. \quad (8)$$

We want to determine the cardinality of the set of all Sophie Germain primes by convergence and continuity of the cardinal function, where continuous function is a map preserving the topological structure between topological spaces. The set theoretic limit itself does not involve any topology, it is unable to determine the cardinality of the set of all Sophie Germain primes directly. We need to reveal an order topological structure of the equality (8).

Now we quote a definition of the order topology from the textbook "Topology" by J.R. Munkres [12].

The order topology is a topology on the non-empty linear order set, which contains more than one element, their open sets are the sets that are the unions of open intervals (c, d) and half-open intervals $[c_0, d)$, $(c, d_0]$, where c_0 is the smallest element and d_0 is the largest element of the linear order set. The empty and the sets with a single element have no linear order structure, they have no order topology.

According on the sifting procedure (5), the particular set theoretic limit above

$$\lim T'_i = \lim A'_i = T_e.$$

has equipped a natural order structure. In other words, both the set sequences T'_i,A'_i and their limit point T_e construct non-empty well ordered sets with the order type $\omega + 1$

$$X: \ T'_1, T'_2, \dots, T'_i, \dots \dots;\ T_e. \quad (9)$$

$$X: \ A'_1, A'_2, \dots, A'_i, \dots\dots;\ T_e. \quad (10)$$

We try to endow the well ordered sets (9), (10) with an order topology.

From the formula (7), A'_i is the Sophie Germain prime subset of T'_i

$$A'_i \subset T'_i,$$

hence when we endow the well ordered set (9) with an order topology, the well ordered set (10) will be automatically endowed an order topology.

We had computed out patterns of the first few Sophie Germain primes

a=3,5,11,23,29,41,53,83,89,113,131,173,179 ,191, hance the numbers of elements of both the well ordered sets (9),(10) are more than one. We can safely endow the well ordered set (9) with a naturally compatible order topology, such that the well ordered set (10) is automatically endowed an order topology.

Obviously, for every neighborhood $(c, T_e]$ of T_e there is a natural number i_0, for all $i > i_0$,

$$T'_i \in (c, T_e],$$

$$A'_i \in (c, T_e]$$

thus both the set sequences T'_i, A'_i converge to their common limit point T_e.

$$\lim T'_i = \lim A'_i = T_e. \quad (11)$$

In the sense of the order topological limit we have proved also that both the set sequences T'_i, A'_i converge to the identical limit point T_e.

□

If the sifted set T_e is empty $T_e = \emptyset$ under some sifting conditions, the sequence (10) contains only one element $\emptyset$, it has no linear order structure, we can not endow the sequence (10) with an order topology by the definition. Otherwise we will fall into a Ross-Littwood paradox. In the last of this section we will discuss this paradox in detail.

Lemma 2 *The cardinal sequences $|T'_i|$, $|A'_i|$ converge to the smallest infinite cardinality $\aleph_0$.*

Like Euler used the product formula for the Riemann zeta function

$$\sum \frac{1}{p^s} = \prod \left(1 - \frac{1}{p^s}\right)^{-1}$$

to reprove Euclid's theorem that there are infinitely many primes [5], we take the cardinality on two sides of the equality (11) and consider the limits of cardinal sequences $|T'_i|$, $|A'_i|$ as

$$T'_i, A'_i \to T_e$$

to determine the cardinality of the sifted set T_e.

About the limit of a function, in general topology it is easy to prove:

"If the space X satisfies the first axiom of countability at the point x_0 and the space Y is Hausdorff, then for the existence of the limit $\lim_{x \to x_0} f(x)$ of a mapping

$$f: E \to Y, E \subset X,$$

it is necessary and sufficient that for any sequence

$$x_n \in E, \ n=1,2,3,\dots\dots,$$

such that $\lim_{n\to\infty} x_n = x_0$, the limit $\lim_{n\to\infty} f(x_n)$ exists. If this condition holds, the limit

$$\lim_{n\to\infty} f(n)$$

does not depend on the choice of the sequence x_n, and the common value of these limits is the limit of f at x_0 ." [18].

In other words for every sequence satisfying this condition x_n, the limits of functions

$$\lim_{n\to\infty} f(n)$$

are equal.

Proof: From the formula (6) we have

$$|T_i'| \geq |T_i|.$$

From the formula (3) we obtain that the cardinal sequence $|T_i'|$ of the sets T_i', is strictly monotonically increasing

$$|T_i'| < |T_{i+1}'|.$$

Thus

$$\lim_{T_i' \to T_e} |T_i'| = \cup |T_i'| = \aleph_0.$$

The cardinal sequence $|T_i'|$ and its limit point $\aleph_0$ construct a non-empty well ordered set with the order type $\omega + 1$

$$Y: \quad |T_1'|, |T_2'|, \ldots, |T_i'|, \ldots\ldots; \ \aleph_0. \qquad (12)$$

Like the lemma 4.1, endowing this well ordered set with an order topology, in the sense of the order topological limit we obtain that the cardinal sequence $|T_i'|$ of the sets T_i' converges to the smallest infinite cardinality $\aleph_0$ as $T_i' \to T_e$

$$\lim_{T_i' \to T_e} |T_i'| = \cup |T_i'| = \aleph_0. \qquad (13)$$

Obviously the cardinal sequence $|A_i'|$ of the sets A_i' is monotonically increasing

$$|A_i'| \leq |A_{i+1}'|.$$

Thus

$$\lim_{A_i' \to T_e} |A_i'| = \cup |A_i'|.$$

The limit of the cardinal sequence $|A_i'|$ exists, although we do not know whether $\cup |A_i'|$ is infinite or not.

For the Sophie Germain primes we know

$$T_e \neq \emptyset,$$

the cardinal sequence $|A_i'|$ and its limit point $\cup |A_i'|$ construct a non-empty well ordered set

$$Y: \quad |A_i'|, |A_i'|, \ldots, |A_i'|, \ldots\ldots; \cup |A_i'|, \qquad (14)$$

may be endowed with an order topology and in the sense of the order topological limit we have

$$\lim_{A_i' \to T_e} |A_i'| = \cup |A_i'|. \qquad (15)$$

The order topological space is first countable and Hausdorff. Like the Euler product formula, the limits of the cardinal sequences of two sides of the equality (11) exist, two limits are equal

$$\lim |A_i'| = \lim |T_i'| = \aleph_0. \qquad (16)$$

In the traditional sieve theory or analytic number theory, one uses the counting function $\pi(x, S)$, which is a real function, to model the number of Sophie Germain primes and tries to prove the Sophie Germain prime conjecture by proving that $\lim \pi(x, S)$ is infinite. Unfortunately, one has never proved that $\lim \pi(x, S)$ is infinite or not by using all our current method.

We regard $|A_i'|$, $|T_i'|$ as the real functions.

Obviously

$$\lim \pi(x, S) = \lim \pi(m_i, S),$$

now we easily obtain

$$\lim \pi(x, S) = \lim \pi(m_i, S) = \lim |A_i'| = \lim |T_i'| = \infty. \qquad (17)$$

Then we directly prove that $\lim \pi(x, S)$ is infinite using the recursive sieve method. In the usual sense we have proved the Sophie Germain prime conjecture.

□

From topology we know that the value $|T_e|$ of counting functions at T_e is irrelevant to the definition of the limits of cardinal functions $\lim |T_i'|$, $\lim |A_i'|$, $\lim \pi(x, S)$. We need to prove the continuity of the cardinal function at the point T_e, then obtain

$$|T_e| = \aleph_0.$$

Theorem 1 *The set of all Sophie Germain primes is an infinite set.*

Proof: Let f: $X \to Y$ be the cardinal function from the order topological space X to the order topological space Y,

$$f(T) = |T|,$$

$$X: \quad T_1', \ T_2', \ldots, \ T_i', \ldots\ldots; \quad T_e,$$

$$Y: \quad |T_1'|, \ |T_2'|, \ldots, |T_i'|, \ldots\ldots; \ \aleph_0.$$

It is easy to cheek: for every open set $[|T_1'|, |d|), (|c|, |d|), (|c|, \aleph_0]$ in Y, their preimages $[T_1', d)$, (c, d), $(c, \aleph_0]$ are open sets also in X, thus the cardinal function f (T)= |T| is continuous with respect to the above order topology.

Both the order topological spaces are first countable, thus the cardinal function |T| is sequentially continuous. By the usual topological theorem, the cardinal function |T| preserves limit,

$$|\lim T_i'| = \lim |T_i'|$$

Order topological spaces are Hausdorff spaces, in Hausdorff spaces the limit points of the set sequence T_i' and the cardinal sequence $|T_i'|$ are unique provided that it exists.

The lemmas 1), lemmas 2) have proved that there exist the order topological limits $\lim T_i'$, $\lim |T_i'|$ and the condition for existence of both the limits is sufficient.

From the lemmas 2) we have

$$|\lim T_i'| = \lim|T_i'| = \aleph_0$$

From the lemmas 1) we obtain that the set of all Sophie Germain primes is an infinite set

$$|\{a:S(2,a\}| = |\lim A_i'| = |\lim T_i'| = \lim|T_i'| = \aleph_0. \quad (18)$$

In other words, we have rigorously proved the Sophie Germain prime theorem that there are infinitely many Sophie Germain primes.

Similarly, we can prove the continuity of the counting functions $|A_i'|$ or $\pi(x, S)$ at the point T_e.

□

We known, one hardly handles the counting functions $|A_i'|$, $\pi(x, S)$, and their limits $\lim|A_i'|$ $\lim \pi(x, S)$ directly, but easily handles the function $|T_i'|$, and its limit $\lim|T_i'|$. Taking the cardinality on two sides of the equality (11), we had assembled an order topological structure of the set of all Sophie Germain primes piecemeal by the sifting process T_i', A_i', the difficulty is reduced to a proof of the existence about the limit of the cardinal sequence $|A_i'|$. For Sophie Germain primes, $T_e \neq \emptyset$, the order topology (9) induces a natural order topology (10) on the set T_e, corresponding with this, (9) induces a natural order topology on the cardinal sequence (14), it is easy to prove the existence (15) of the limit $\lim|A_i'|$, then we discern the mystery about primes a little by the recursive sieve method.

4. 3 About the Ross-Littwood paradox

Like Euler product formula, using the order topological limits we need to be a little careful about whether two sides of a formula converge [5].

Only if there is not any survivor as a pattern under some sifting conditions, the set theoretical limit (8)

$$\lim T_i' = \lim A_i' = T_e = \emptyset.$$

Obviously $|T_e| = 0$. Nothing may be proved by the above order topological reasoning, because empty set sequence (10) has no any order topology, we can not endow the set sequence (9) with an order topology also, needless say continuous or not.

In the informal argument, like $\lim \pi(x, S)$, one extends the reasoning paradigm and regards $\lim|T_i'|$ as a cardinality of the empty, then falls into a Ross-Littwood paradox [10] [17] [20], today this paradox is an argumentative problem also.

1953. J.E. Littlewood described the following paradox about infinity.

Balls numbered

$$T_i = \langle i+1, i+2, \ldots, 10i\rangle$$

are put into a urn. How many balls are in the urn at the end as $i \to \infty$?

We ignore physically plausible space-time continuity conditions and consider what is the limit $\lim T_i$ of the set sequence T_i.

A similar example concerning the distribution of primes is the primes in the reducible polynomial

$$a^2 - 1,\ a > 2.$$

Under the sifting condition

$$B_i = \langle 1, -1\rangle \bmod p_i.$$

One seeks for the $\lim T_i$, where the number a = 2, a - 1 = 1 does not enter the filtration.

Their set theoretic limit is empty

$$\lim T_i = \emptyset.$$

Their cardinal limit itself is infinite

$$\lim|T_i| = \aleph_0$$

At first sight this is a contradiction.

Through thorough investigation, the condition for the existence of the cardinal limit $\lim|T_i|$ is not sufficient with respect to the order topology, because the cardinal sequence $A_i' = \emptyset$ has no order topological limit. There is no continuity, $|T_e|$ and $\lim|T_i|$ are irrelevant, there is no contradiction.

One can not regard $\lim T_i$ as a cardinality of the empty. In view from pour mathematics, the order topology distinguishes non-empty sifted sets from the empty sifted set and provides a formal solution of the Ross-Littwood paradox.

If we relax the restrictive condition and seek for a natural number a such that

$$a^2 - 1,\ a > 2,$$

is a product of at most two primes, an almost prime, or a product of exactly two primes, a semiprime, then such natural numbers a have patterns

a=4,6,12,18,30,42,60,72,102,108,138,150,…,

$a^2 - 1 = 3\times 5, 5\times 7, 11\times 13, 17\times 19, 29\times 31, \ldots$,

and the set $\lim T_i' = T_e$ of all such numbers a is infinite.

This result is similar to the famous results of J.R.Chen [3] or H.Iwaniec [8].

It is interesting that this is a proof of the twin prime conjecture via the polynomial $a^2 - 1$.

5 A Cunningham chain theorem

We may uniformly extend the above sieve method and reasoning to a wide variety of additive patterns in primes.

Let B_i be the solution of the congruence

$$cx + d \equiv o \bmod p_i,$$

we obtain a different proof of Dirichlet's theorem that there are infinitely many primes of the form

$$cx + d,\ \gcd(c, d) = 1.$$

Let B_i be the solution of the congruence

$$x^2 + 1 \equiv 0 \bmod p_i,$$

we prove that the number of primes of the form $x^2 + 1$ is infimite.

Let

$X \equiv B_i = \langle 1, -2 \rangle \bmod p_i$,

We prove the twin prime conjecture. Similarly we may prove the k-tuple prime conjecture.

Let

$X \equiv B_i = \langle 1, \frac{p_i - 1}{4} \rangle \bmod p_i$,

repeat the above reasoning, we prove that there exist infinitely many primes p such that 4p+1 is prime.

It is easy to prove that if there exist infinitely many primes p such that 4p+1 is prime, then 2 is a primitive root modulo q for infinitely many primes

$q = 4p + 1.$

Thus we prove that Artin's conjecture, an open problem, is true at 2.

One naturally extends Sophie Germain primes to Cunningham chains [1].

A Cunningham chain of length k is a finite set of primes

$a_1, a_2, \dots, a_k$,

Where

$a_{r+1} = 2a_r + 1,\ r = 1, 2, \dots, k - 1$,

each which is twice the proceeding one plus one.

For example:

2, 5, 11, 23, 47 ;

89, 179, 359, 719, 1439, 2879.

Like the k-tuple prime conjecture, it is conjectured that there are infinitely many Cunningham chains of length k.

Extending the above proof we obtain a theorem following.

Theorem 2 *The number of admissible Cunningham chains known of length k is infinite.*

Proof: For any Cunningham chain

$\langle a_1, a_2, \dots, a_k \rangle$,

let

$B_i = \langle b_1, b_2, \dots, b_r, \dots, b_k \rangle$,

where b_r is the solution of the congruence

$2^r x + 2^r - 1 \equiv 0 \bmod p_i$,

r = 1, 2, ..., k.

Let w_i be the number of congruence classes in $B_i \bmod p_i$,

If there is a prime p_i, the Cunningham chain covers all congruence classes mod p_i

$B_i \equiv \langle 0, 1, 2, \dots, k - 1 \rangle \bmod p_i$,

we say that this Cunningham chain is inadmissible.

For an inadmissible Cunningham chain, obviously, if n > i, then the set T_n is empty, the recursive sieve method itself proves that there is no any natural number $c > p_i$ such that

$\langle a_1 + c, a_2 + c, \dots, a_k + c \rangle$

are simultaneously prime.

Thus we only discuss the admissible Cunningham chains.

Like above proof, from the set of all odd numbers

$X \equiv \langle 1 \rangle \bmod 2$,

we delete the congruence classes

$X \equiv B_i = \langle b_1, b_2, \dots, b_r, \dots, b_k \rangle \bmod p_i$,

successively, and obtain the recursive formula T_i. The number of elements of the set T_i is

(19) $|T_i| = \prod_1^{i-1} (p_j - w_j)$

If $p_j >$ k+1, $w_j \leq k$, then the $|T_i|$ is strictly monotonically increasing for $i > j$.

We have known that there is a pattern a_1 of the Cunningham chain, thus the sifted set is not empty.

We refine this recursive set sequence T_i and obtain two set sequences T_i', A_i'.

Further we prove that both the set sequences T_i', A_i' converge to the sifted set T_e, the cardinal functions $|T_i'|$, $|A_i'|$ are continuous with respect to the order topology.

Thus we proved the Cunningham chain theorem.

$|\{a:S(k,a)\}| = |\lim A_i'| = |\lim T_i'| = \lim |T_i'| = \aleph_0.$ (20)

This completes the proof.. □

We do not know whether there exists a Cunningham chain of length k > 17, if we find a Cunningham chain of length k > 17 and it is admissible then its number is infinite.

According our sieve method, many additive patterns in primes have the same structure of set theory, structure of order topology and recursive structure, although they have different arithmetical structures. The methods proving infinity or not of various sifted sets T_e all are same. In this short paper we do not discuss those problems in detail.

Acknowledgements: I'd like to thank Professor Wang ShiQiang of Beijing Normal University, who gave me directions on model theory. My thanks also go to Professor Mo ShaoKui of NanJing University, with his guidance on recursion theory, Thanks Professor Fu WanTao and Lai YingHua for their excellent advice.

References:

[1] A. Cunnningham, On hyper-even numbers and on Fermat's numbers, *Proc. Lond. Math. Soc., series* 2, 5, 1907, pp237--274.

[2] Chris K. Caldwell, An amazing prime heuristic, 2000. http://www.utm.edu./caldweii//

[3] J. R. Chen, On the Representation of a Large Even Integer as the Sum of a prim and the

Product of at Most Two Primes, *Kexue Tongbao* Vol 17, 1966, pp385—386.
J. R Chen, On the Representation of a Large Even Integer as the Sum of a prime and the Product of at Most Two Primes, *I.Sci.Sinica* Vol 16, 1973, pp157—176.
J. R. Chen, On the Representation of a Large Even Interger as the Sum of a prime and the Product of at Most Two Primes, *II.Sci.Sinica* Vol 16, 1978, pp412—430.
[4] G. Fee and A. Granville, The prime factors of Wendt's binomial circulant determinant, *Math. Comp.*, Vol 57:196, 1991, pp 839—848.
[5] A. Granville, Analytic number theory, http://www.dms.umontreal.ca/%7Eandrew/PDF/PrinceComp.pdf
[6] G. Harman, *Prime-detecting sieve*, Princeton university press, 2007
[7] E. Hibbs, Applying the new primer on prime numbers, *WSEAS Transactions on mathematics*, Vol. 9, 2010, pp.234-243.
[8] H. Iwanies, Almost-primes represented by quadratic polynomials, *Ivent.Math*. Vol 47, 1978, pp171—188.
[9] J. Friedlander, H. Iwanies, What is the perity phenomenon?, http//www.ams.org/ notices/2009 07/ rtx090700817p.pdf
[10] Jon Byl, On Resolving the Littlewood-Ross Paradox, *Missouri Journal of Mathematical Sciences*, Vol.12, No. 1, Winter 2000, pp.42–47
[11] J Harrison, formal proof --- theory and practice, *Notices of AMS*, 2008, http://www.ams.org/notices /200811/tx081101395p.pdf
[12] J.R. Munkres, Topology, 2rd edition, *Prentice Hall, Upper Saddle River*, 2000.
[13] Jon Pérez Laraudogoitia, "Supertasks", *Stanford Encyclopedia of Philosophy*, 2004, http://plato.stanford.edu/entries/spacetime supertasks/
[14] Jouko vaananrn, Second-order logic and foundations of mathematics, *The bulletin of symbolic logic*, Vol 7, 2001, pp.504—520.
[15] K.Kuratowsky and A. Mostowsky, *Set theory, With an introduction to descriptive set theory*, North-Holland Publishingcom.1976, pp.118—120.
[16] Fengsui Liu, On the prime k-tuple conjecture I, *WSEAS Transactions on mathematics*, Vol. 3, 2004, pp.744--747.
[17] J. E. Littlewood, *Littlewood's Miscellany* (ed. Bela Bollobas) Cambridge University Press, Cambridge, 26, 1986
[18] Michiel Hazewinkel, Encyclopaedia of Mathematics,limit. http://eom.springer.de/l/l058820.htm
[19] P. Ribenboim, *The new book of prime number records*, 3rd edition, Springer-Verlag, New York, 1996.
[20] S.Ross, *A First Course in Probability*, third edition, New York and London, Macmillan, 1988.
[21] Terence Tao, *Open question: The parity problem in sieve theory*, http://terrytao.wordpress.com/2007/06/05/open-question-the-parity -problem-in-sieve-theory/
Terence Tao, Long arithmetic progressions in the primes, *Auatrarian mathematical sosiety meeting*, 2006.