Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 14, Number 1 (2018), pp. 161-180

http://www.ripublication.com/gjpam.htm

Which polynomials represent infinitely many primes?

Feng Sui Liu
Department of Mathematics,
NanChang University, NanChang, China.

Abstract

In this paper a new arithmetical model has been found by extending both basic operations $+$ and $\times$ into finite sets of natural numbers. In this model we invent a recursive algorithm on sets of natural numbers to reformulate Eratosthene's sieve. By this algorithm we obtain a recursive sequence of sets, which converges to the set of all natural numbers x such that $x^2 + 1$ is prime. The corresponding cardinal sequence is strictly increasing. Test that the cardinal function is continuous with respect to an order topology, we immediately prove that there are infinitely many natural numbers x such that $x^2 + 1$ is prime. Based on the reasoning paradigm above we further prove a general result: if an integer valued polynomial of degree k represents at least $k+1$ positive primes, then this polynomial represents infinitely many primes.

AMS subject classification: Primary 11N32; Secondary 11N35, 11U09,11Y16, 11B37.
Keywords: primes in polynomial, twin primes, arithmetical model, recursive sieve method, limit of sequence of sets, Ross-Littwood paradox, parity problem.

1. Introduction

Whether an integer valued polynomial represents infinitely many primes or not, this is an intriguing question.

Except some obvious exceptions one conjectured that the answer is yes.

Example 1.1. Bouniakowsky [2], Schinzel [35], Bateman and Horn [1].

In this paper a recursive algorithm or sieve method adds some exotic structures to the sets of natural numbers, which allow us to answer the question: which polynomials represent infinitely many primes?

In 1837, G.L. Dirichlet proved that if b and c are relatively prime positive integers, then the arithmetic progression $bx + c$ contains infinitely many primes [8]. This is the only non-trivial solution known.

The next natural step seems to determine that the simplest quadratic polynomial x^2+1 represents infinitely many primes. At the 1912 International Congress of Mathematicians in Cambridge, Edmund Landau listed four basic questions about primes, this is the first question, and said that they are "unattackable at the present state of science".

Adapted the normal sieve method and employed analytic techniques, some works on approximations to those questions has been done.

In 1973, J.R. Chen proved that for infinitely many primes p the number $p + 2$ is either a prime or a product of two primes [3].

In 1978, H. Iwaniec proved that there are infinitely many natural numbers x such that $x^2 + 1$ is a product of at most two primes [22].

In 1998, J. B. Friedlander and H. Iwaniec proved a celebrated result that there are infinitely many primes of the form $n^2 + m^4$ [9].

Similarly, in 2001, D.R. Heath-Brown proved that the binary cubic form $x^3 + 2y^3$ represents infinitely many primes [19].

In 2012, Robert J. Lemke Oliver extended Iwaniec's result to general quadratic polynomials, but very little is known about $x^2 + 1$ yet [33].

These results are far from solving questions. One guessed that the structure of prime sets is still not well understood [13]. Today those conjectures are still extremely difficult if not hopeless questions.

One needs new ideas, structures, notations, algorithms, or sieve theory without the parity obstruction to solve these questions.

Based on current advances in set theory, model theory, recursion theory and general topology, we try to tackle those questions.

In 2011, author used the recursive sieve method to prove the Sophie Germain prime conjecture: there are infinitely many primes p such that $2p + 1$ is also prime [29].

In this paper we introduce a new arithmetical model to reformulate Eratosthene's sieve method. We invent a recursive algorithm on sets of natural numbers and recursively define a sequence of sets (T_i'), formula (4.4), which converges to the set T_e of all natural numbers x such that x^2+1 is prime. The corresponding cardinal sequence $(|T_i'|)$ is strictly increasing and the cardinal function is continuous with respect to an order topology. Therefore we obtain some enough useable structures, the set T_e and its cardinality $|T_e|$ are exhaustively defined by their place in the exotic structures.

$$\lim T_i' = T_e,$$

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

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

Thus we easily prove a structural result that the cardinality of the set T_e is infinite

$$|\{x : x^2 + 1 \text{ is prime}\}| = \aleph_0.$$

In the other words, there are infinitely many primes of the form $x^2 + 1$.

In general we prove: if an integer valued polynomial $f(x)$ of degree k represents at least $k + 1$ positive primes, then the set of all primes of the form $f(x)$ is a infinite set.

We repeat some contents in [29] for self-contained.

2. A formal system

For reformulating Eratosthene's sieve method by well formed formulas, we extend both basic operations addition and multiplication $+$, $\times$ into finite sets of natural numbers.

We use small letters a, x, t to denote natural numbers and capital letters A, X, T to denote sets of natural numbers.

For arbitrary both finite sets of natural numbers A, B we write

$$A = \langle a_1, a_2, \dots, a_i, \dots, a_n \rangle,\ a_1 < a_2 < \dots < a_i < \dots < a_n,$$

$$B = \langle b_1, b_2, \dots, b_j, \dots,\ b_m \rangle,\ b_1 < b_2 < \dots < b_j < \dots < b_m.$$

We define

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

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

Example 2.1.

$$\langle 4, 6, 10 \rangle + \langle 0, 10, 20, \dots, 100, 110, 120 \rangle = \langle 4, 6, 10, \dots, 124, 126, 130 \rangle,$$

$$\langle 2 \rangle \langle 0, 1, 2, 3, 4 \rangle = \langle 0, 2, 4, 6, 8 \rangle.$$

This definition is similar to Minkowski sum and product

$$A + B = \{a + b : a \in A,\ b \in B\},\ AB = \{ab : a \in A,\ b \in B\}.$$

For the empty set $\emptyset$ we define $\emptyset + B = \emptyset$ and $\emptyset B = \emptyset$.

We write $A \setminus B$ for the set difference of A and B

Let

$$X \equiv A = \langle a_1, a_2, \dots, a_i, \dots, a_n \rangle \mod a$$

be several residue classes $\mod a$.

If $\gcd(a, b) = 1$, we define the solution of the system of congruences

$$X \equiv A = \langle a_1, a_2, \dots, a_i, \dots, a_n \rangle \mod a,$$

$$X \equiv B = \langle b_1, b_2, \dots, b_j, \dots, b_m \rangle \mod b$$

to be

$$X \equiv D = \langle d_{11}, d_{21}, \dots, d_{ij}, \dots, d_{n-1m}, d_{nm} \rangle \mod ab,$$

where $x \equiv d_{ij} \mod ab$ is the solution of the system of congruences

$$x \equiv a_i \mod a,$$

$$x \equiv b_j \mod b.$$

The solution $X \equiv D \mod ab$ is computable and unique by the Chinese remainder theorem.

For example, $X \equiv D = \langle 34, 44, 60, 70, 86, 96\rangle \mod 130$ is the solution of the system of congruences

$$X \equiv \langle 4, 6, 10\rangle \mod 10,$$

$$X \equiv \langle 5, 8\rangle \mod 13.$$

Except extending $+, \times$ into finite sets of natural numbers, we continue the traditional interpretation of the formal symbols $+, \times, \in, 0, 1$. The reader who is familiar with model theory may know that we have founded a new model or structure of second order arithmetic by a two-sorted logic

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

where N is the set of all natural numbers, and $P(N)$ is the power set of N.

We denote this model by $P(N)$.

Mathematicians assume that $\langle N, +, \times, 0, 1\rangle$ is the standard model of Peano theory PA,

$$N \models PA.$$

Similarly, we assume that $\langle P(N), N, +, \times, 0, 1, \in\rangle$ is the standard model of a new arithmetical theory $PA \bigcup ZF$,

$$P(N) \models PA \bigcup ZF.$$

This is a joint theory of PA and ZF, in other words $P(N)$ not only is a model of Peano theory PA but also is a model of set theory ZF.

As a model of Peano theory PA, the natural numbers in $P(N)$ and the natural numbers in N are the same.

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

The model $P(N)$ and the theory $PA + ZF$ construct a new formal system. In this formal system we may regard natural numbers and sets of natural numbers as individuals, terms or points.

We emphasize on the formalization, because we try to attack some very elusive conjectures, behind which hides a paradox.

The new formal language $\langle +, \times, \in, 0, 1\rangle$ has stronger expressive power. The new formal system has some additional exotic structures, which allow us to settle many questions about primes.

In the new formal system, we may introduce a recursive algorithm or sieve method and produce some recursive sequences of sets. A new notation, the sequence of sets, reveals some exotic structures of various prime sets. We may carefully construct a logical deduction, which is built into the structures of the natural numbers and their sets, to prove some old prime conjectures in pure mathematics.

"A well chosen notation can contribute to making mathematical reasoning itself easier, or even purely mechanical." [21]

We do not further discuss this formal system in view from logic and mathematical foundation [23].

3. A recursive sieve method

An ancient Greek mathematician Eratosthene created a sieve method to find and count primes up to any given limit x. This is a simple west ancient algorithm : listing $1, 2, 3, 4, \ldots, x$, we stroked out from this list all multiples of $2, 3, 5, \ldots, \sqrt{x}$, then the natural numbers remained are primes and 1.

Based on the inclusion-exclusion principle, Legendre formulated this algorithm just for counting the number of primes less than or equal to x,

$$\pi(x) = \sum_{d|P} \mu(d)[\frac{x}{d}] + \pi(\sqrt{x}) - 1.$$

Within the framework of real analysis, one gives up exactness, by carefully estimating the main terms and error terms, one developed modern sieve theory [18], [9]. This is a quantitative model of the sets of primes.

"The basic purpose for which the sieve was invented was the successful estimation of the number of primes in interesting integer sequences." said John B. Friedlander [9].

For primes in the polynomial with two variable $x^2 + y^4$ or some almost primes, this purpose had been achieved. For primes of the form $x^2 + 1$ or twin primes this purpose has never been achieved. There is a formidable obstacle in modern sieve theory, i.e., the parity problem.

Sieve theory is unable to provide non-trivial lower bounds on the size of the prime sets. Also any upper bounds must be off from the truth by a factor of 2 or more [36].

Primes have some obvious structures. We don't know if they also have some additional exotic structures. Because of this, we have been unable to settle many questions about primes [36].

Normal sieve method is not a perfect tool. It seems that we need to look for a different sieve or a new algorithm.

In contrast with normal sieve theory, within the framework of recursion theory we reformulate Eratosthene's sieve by successively deleting congruence classes, and invent a novel algorithm—recursive sieve method.

The basic purpose of recursive sieve theory is to capture enough useable exotic structures of various prime sets, which allow us to settle many questions about primes by exact formulas.

Like algebraic number theory, we do not use any estimation in recursive sieve theory, we do not give up exactness. We insist on the dichotomous viewpoint.

We consider the simplest quadratic polynomial $x^2 + 1$ as an example.

Instead of primes x^2+1 we look for the natural numbers x such that x^2+1 is prime, for example, $x = 2, 4, 6, 10, \ldots$. We call such a natural number x a survivor of the sifting progress or a pattern sometimes.

We shall determine the set T_e of all survivors of the sifting progress.

$$T_e = \{x : x^2 + 1\, is\ prime\}$$

as the limit of a sequence of sets. We call the set T_e the end-sifted set.

We shall prove that the cardinality of the end-sifted set is infinite

$$|T_e| = \aleph_0.$$

Then we obtain that there are infinitely natural numbers x such that $x^2 + 1$ is prime, in other words, the quadratic polynomial $x^2 + 1$ represents infinitely many primes.

For any prime $p_i > 2$, we consider the dividable relation $p_i \mid x^2 + 1$, namely the congruence

$$x^2 + 1 \equiv 0 \mod p_i.$$

This is a quadratic congruence. By Euler's criterion we know that -1 is a quadratic residue of the prime p_i if and only if $p_i \equiv 1 \mod 4$. If -1 is not a quadratic residue of the prime p_i, then the prime p_i does not divide $x^2 + 1$ for all x, and we overlook such a prime p_i.

Let $q_0 = 2$, we list the primes q_i of the form $4k + 1$

$$5, 13, 17, 29, 37 \ldots, q_i, \ldots\ldots .$$

This is an infinite sequence.

Let

$$X \equiv B_i \mod q_i,$$

be the solution of the congruence

$$x^2 + 1 \equiv 0 \mod q_i.$$

Example 3.1.

$$\begin{aligned}
B_0 &= \langle 1 \rangle \mod 2,\\
B_1 &= \langle 2, 3 \rangle \mod 5,\\
B_2 &= \langle 5, 8 \rangle \mod 13,\\
B_3 &= \langle 4, 13 \rangle \mod 17,\\
B_4 &= \langle 12, 15 \rangle \mod 29,\\
B_5 &= \langle 6, 31 \rangle \mod 37.
\end{aligned}$$

Let

$$m_{i+1} = \prod_{0}^{i} q_j.$$

From the set N of all natural numbers we successively delete the congruence classes $B_0 \mod q_0$, …, $B_i \mod q_i$ and leave the congruence class $T_{i+1} \mod m_{i+1}$. Then the left congruence class $T_{i+1} \mod m_{i+1}$ is the set of all numbers x such that $x^2 + 1$ does not contain any prime $q_j \leq q_i$ as a factor $(x^2 + 1, m_{i+1}) = 1$. This is the recursive sieve method.

Let $X \equiv D_i \mod m_{i+1}$ is the solution of the system of congruences

$$X \equiv T_i \mod m_i,$$

$$X \equiv B_i \mod q_i.$$

Let T_{i+1} be the set of the least positive representatives of the left congruence class $T_{i+1} \mod m_{i+1}$.

In the formal system $P(N)$ with the definitions in section 2, we may express the algorithm for the set T_{i+1} by a recursive formula.

$$\begin{aligned} T_1 &= \langle 2 \rangle, \\ T_{i+1} &= (T_i + \langle m_i \rangle \langle 0, 1, 2, \ldots, q_i - 1 \rangle) \setminus D_i. \end{aligned} \tag{3.1}$$

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

$$|T_{i+1}| = \prod_{1}^{i} (q_j - 2), \quad |T_1| = 1. \tag{3.2}$$

We exhibit the first few terms of formula (3.1) and briefly sketch that the algorithm is valid.

From $B_0 = \langle 1 \rangle \mod 2$, obviously we have

$$T_1 = \langle 2 \rangle.$$

The congruence class $T_1 \mod 2$ is the set of all numbers x such that $(x^2 + 1, 2) = 1$. Now $X \equiv \langle 2 \rangle \mod 2$ is equivalent to $X \equiv (\langle 2 \rangle + \langle 2 \rangle \langle 0, 1, 2, 3, 4 \rangle) \mod 10$, from them we delete the solution of the system of congruences $D_1 = \langle 2, 8 \rangle \mod 10$, and leave

$$T_2 = (\langle 2 \rangle + \langle 2 \rangle \langle 0, 1, 2, 3, 4 \rangle) \setminus \langle 2, 8 \rangle = \langle 4, 6, 10 \rangle.$$

The congruence class $T_2 \mod 10$ is the set of all numbers x such that $(x^2 + 1, 10) = 1$. Now $X \equiv \langle 4, 6, 10 \rangle \mod 10$ is equivalent to

$$X \equiv (\langle 4, 6, 10 \rangle + \langle 10 \rangle \langle 0, 1, 2, \ldots, 12 \rangle) \mod 130,$$

from them we delete the solution of the system of congruences

$$D_2 = \langle 34, 44, 60, 70, 86, 96\rangle \mod 130,$$

and leave

$$\begin{aligned} T_3 &= (\langle 4, 6, 10\rangle + \langle 10\rangle\langle 0, 1, 2, \ldots, 12\rangle) \setminus \langle 34, 44, 60, 70, 86, 96\rangle \\ &= \langle 4, 6, 10, 14, 16, 20, 24, 26, 30, 36, 40, 46, 50, 54, 56, 64, 66, 74, 76, 80, 84, 90, \\ &\quad 94, 100, 104, 106, 110, 114, 116, 120, 124, 126, 130\rangle. \end{aligned}$$

The congruence class $T_3 \mod 130$ is the set of all numbers x such that $(x^2+1, 130) = 1$. And so on.

Suppose that the congruence class $T_i \mod m_i$ is the set of all numbers x such that $(x^2 + 1, m_i) = 1$. We delete the congruence class $B_i \mod q_i$ from them, in other words, we delete the solution $X \equiv D_i \mod m_{i+1}$ of the system of congruences

$$X \equiv T_i \mod m_i,$$
$$X \equiv B_i \mod q_i.$$

Now the congruence class $T_i \mod m_i$ is equivalent to the congruence class $(T_i + \langle m_i\rangle\langle 0, 1, 2, \ldots, q_i - 1\rangle) \mod m_{i+1}$, this is the operation replacing $\mod m_i$ by $\mod m_{i+1}$, from them we delete the solution $D_i \mod m_{i+1}$, which is the set of all numbers x such that $x^2 + 1 \equiv 0 \mod q_i$, it follows that the left congruence class $T_{i+1} \mod m_{i+1}$ is the set of all numbers x such that $(x^2 + 1, m_{i+1}) = 1$. Our algorithm is valid. It is easy to compute $|T_{i+1}| = |T_i|(q_i - 2)$ by the above algorithm.

We may rigorously prove formulas (3.1), (3.2) by mathematical induction, the proof is left to the reader.

The number 1 is not prime, the number $x = 0$ such that $x^2 + 1 = 1$ does not enter the sifting process, thus we take the set of the least positive representatives $T_1 = \langle 2\rangle$.

Now we list a few elementary conclusions from the recursive formula T_i. We omit the proofs here since their proofs are easy.

1. Let $s_i = \min T_i$ be the smallest number of the set T_i. Then a criterion of the survivor x is
$$x = s_i \bigwedge s_i^2 + 1 = q_i.$$
Example $s_1 = 2,\ 2^2 + 1 = q_1 = 5,\ s_2 = s_3 = 4,\ 4^2 + 1 = q_3 = 17$. This criterion recursively enumerates all survivors x such that $x^2 + 1$ is prime.

2. Using the recursive algorithm T_i, we can easily and quickly compute the numbers x such that $x^2 + 1$ is prime, in fact we had computed out the first few numbers x,
$$\begin{aligned} x &= 2, 4, 6, 10, 14, 16, 20, 24, 26, 40, \\ x^2 + 1 &= 5, 17, 37, 101, 197, 257, 401, 577, 677, 1601. \end{aligned}$$

3. If a number $x^2 + 1$ greater than or equal to q_i is prime, then the corresponding natural number x belongs to the congruence classes $T_i \mod m_i$.

In the next section we shall refine formula (3.1), (3.2) and prove the main theorem: the quadratic polynomial $x^2 + 1$ represents infinitely many primes.

4. The main theorem

According to the recursive sieve method, formula (3.1), we successively delete all numbers x such that $x^2 + 1$ contains the least prime factor q_i. We delete all composites of the form $x^2 + 1$ or all composites together with a prime of the form $x^2 + 1$. The sifting condition or 'sieve' is

$$x^2 + 1 \equiv 0 \; mod \, q_i \bigwedge q_i \le x^2 + 1.$$

Now we modify the sifting condition to be

$$x^2 + 1 \equiv 0 \; mod \, q_i \bigwedge q_i < x^2 + 1. \tag{4.1}$$

According to this new sifting condition, we successively delete the set C_i of all numbers x such that $x^2 + 1$ is composite with the least prime factor q_i,

$$C_i = \{x : x \in X \equiv T_i \mod m_i \bigwedge x^2 + 1 \equiv 0 \mod q_i \bigwedge q_i < x^2 + 1\}.$$

Let C_0 be the set of all odd numbers. We delete all sets C_j with $j < i$ from the set N of all natural numbers and leave the set

$$L_i = N \setminus \bigcup_0^{i-1} C_j. \tag{4.2}$$

The end-sifted set is

$$T_e = N \setminus \bigcup_0^{\infty} C_i.$$

The recursive sieve (4.1) is a perfect tool, with this tool we delete all composites of the form x^2+1 and leave all primes of the form x^2+1. So that we only need to determine the number of all primes of the form $x^2 + 1$, the cardinality $|T_e|$ of the end sifted set. If we successfully do so, then the parity obstruction, a ghost in house of primes, has been automatically evaporated.

By the recursive sieve (4.1), each composite of the form $x^2 + 1$ is deleted exactly once, there is no need for the inclusion-exclusion principle or the estimation of error terms, which causes all the difficulty in normal sieve theory.

Let A_i be the set of all survivors x such that $x^2 + 1 < q_i$.

$$A_i = \{x : x^2 + 1 < q_i \bigwedge x^2 + 1 \, is \;\; prime\}.$$

Example 4.1.

$$A_1 = \emptyset, \; A_2 = A_3 = \langle 2 \rangle, \; A_4 = \langle 2, 4 \rangle, \ldots\ldots.$$

Then the left set L_i is the union of the set A_i of survivors and the congruence class $T_i \mod m_i$,

$$L_i = A_i \bigcup T_i \mod m_i. \tag{4.3}$$

Now we intercept the initial segment T_i' from the left set L_i, which is the union of the set A_i of survivors and the set T_i of least positive representatives. Then we obtain a new recursive formula

$$T_i' = A_i \bigcup T_i. \tag{4.4}$$

Example 4.2.

$$\begin{aligned}
T_1' &= \langle 2\rangle,\\
T_2' &= \langle 2, 4, 6, 10\rangle,\\
T_3' &= \langle 2, 4, 6, 10, 14, 16, 20, 24, 26, 30, 36, 40, 46, 50, 54, 56, 64, 66, 74, 76, 80,\\
&\quad 84, 90, 94, 100, 104, 106, 110, 114, 116, 120, 124, 126, 130\rangle.
\end{aligned}$$

Formula (4.4) expresses the recursively sifting process according to the sifting condition (4.1), and provides a recursive definition of the initial segment T_i'. We shall consider some properties of the initial segment T_i', and reveal some structures of the sequence of the initial segments (T_i') to determine the set of all survivors and its cardinality.

Let $|A_i|$ be the number of survivors x such that $x^2 + 1 < q_i$. Then the number of elements of the set T_i' is

$$|T_i'| = |A_i| + |T_i|. \tag{4.5}$$

From formula (3.2) we deduce that the cardinal sequence $(|T_i'|)$ is strictly increasing

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

Based on order topology obviously we have

$$\lim |T_i'| = \aleph_0. \tag{4.6}$$

Intuitively we see that the sequence of sets (T_i') approaches the end-sifted set T_e, and the corresponding cardinal sequence $(|T_i'|)$ approaches infinity, thus the end-sifted set is an infinite set.

4.1. An informal argument

In computability theory, the real number e is limit computable in the first order formal system R of real numbers

$$(1 + 1/i)^i \to e,\ i \to \infty.$$

Let $i = 1000$, we may take $(1 + 1/1000)^{1000}$ as a well approximate value of the real number e.

Similarly, the end-sifted set T_e is a limit computable set in the formal system $P(N)$, that is the end-sifted set T_e is the limit of the computable sequence of sets (T_i') or structured objects

$$T_i' \to T_e,\ |T_i'| \to \aleph_0,\ i \to \infty.$$

Theoretically we may take $i = c = 10^{10^{1000}}$, and consider what is an approximate set of the end-sifted set T_e.

The set T'_c has

$$|T'_c| > \prod_{1}^{10^{10^{1000}}-1} (q_i - 2)$$

elements x such that $x^2 + 1$ does not contain any one of the first $2 \times 10^{10^{1000}} - 2$ primes as a factor except itself. Namely, if $x^2 + 1$ has prime factors except itself, then by the prime theorem they are greater than

$$2.3 \times 10^{1000} \times 2 \times 10^{10^{1000}}.$$

In approximate sense, the set T'_c may be regarded as a set of numbers x such that $x^2 + 1$ is prime, and the number of elements of this set may be regarded as infinity.

Of course, we may take $i = c = 10^{10^{10000}}$, then obtain a more precise approximate set T'_c of the end-sifted set T_e.

Ultimately, as the limit of the infinite sequence of sets (T'_i), we have deleted all sets C_i of numbers x such that $x^2 + 1$ is composite. Philosophers of mathematics said that one had performed a super task [26]. We obtain infinitely many natural numbers x such that $x^2 + 1$ does not contain any prime as a factor except itself, these infinitely many natural numbers x exactly constitute the set of all numbers x such that $x^2 + 1$ is prime.

Intuitively, the recursive sifting process itself shows that there are infinitely many primes of the form $x^2 + 1$.

The informal argument is unable to treat a hidden paradox. We give a formal proof by some techniques from general topology.

4.2. A formal proof

Let A'_i be the subset of all numbers x such that $x^2 + 1$ is prime in the set T'_i,

$$A'_i = \{x \in T'_i : x^2 + 1 \, is \;\; prime\}. \tag{4.7}$$

Example 4.3.

$$\begin{aligned}
A'_1 &= \langle 2 \rangle, \\
A'_2 &= \langle 2, 4, 6, 10 \rangle, \\
A'_3 &= \langle 2, 4, 6, 10, 14, 16, 20, 24, 26, 40, 54, 56, 66, 74, 84, 90, 94, 110, \\
&\quad\; 116, 120, 124, 126, 130 \rangle.
\end{aligned}$$

We consider properties of the sequences of both sets (T'_i) and (A'_i) to prove that there are infinitely many primes of the form $x^2 + 1$.

Theorem 4.4. The sequence of sets (T'_i) and the sequence of its subsets (A'_i) both converge to the end-sifted set T_e.

First from set theory, next from order topology we prove this theorem.

Proof. For the convenience of the reader, we quote a definition of the set theoretic limit of a sequence of sets [27].

Let (F_n) be a sequence of sets, we define $\limsup_{n=\infty} F_n$ and $\liminf_{n=\infty} F_n$ as follows

$$\begin{aligned}\limsup_{n=\infty} F_n &= \bigcap_{n=0}^{\infty}\bigcup_{i=0}^{\infty} F_{n+i},\\ \liminf_{n=\infty} F_n &= \bigcup_{n=0}^{\infty}\bigcap_{i=0}^{\infty} F_{n+i}.\end{aligned}$$

It is easy to check that $\limsup_{n=\infty} F_n$ is the set of those elements x which belongs to F_n for infinitely many n. Analogously, x belongs to $\liminf_{n=\infty} F_n$ if and only if it belongs to F_n for almost all n, that is it belongs to all but a finite number of the F_n. If

$$\limsup_{n=\infty} F_n = \liminf_{n=\infty} F_n,$$

we say that the sequence of sets (F_n) converges to the limit

$$\lim F_n = \limsup_{n=\infty} F_n = \liminf_{n=\infty} F_n.$$

From formula (4.3) we know that the sequence of left sets (L_i) is descending

$$L_1 \supset L_2 \supset \cdots \supset L_i \supset \cdots\cdots .$$

According to the definition of the set theoretical limit of a sequence of sets, we obtain that the sequence of left sets (L_i) converges to the end-sifted set T_e,

$$\lim L_i = \bigcap L_i = T_e.$$

On the other hand, from

$$A_1' \subset A_2' \subset \cdots \subset A_i' \subset \cdots\cdots ,$$

we obtain that the sequence of sets (A_i') converges to the end-sifted set T_e,

$$\lim A_i' = \bigcup A_i' = T_e.$$

The set T_i' is located between two sets A_i' and L_i,

$$A_i' \subset T_i' \subset L_i.$$

It is easy to prove

$$\begin{aligned} \limsup T_i' &\subset \limsup L_i = \lim L_i, \\ \liminf T_i' &\supset \liminf A_i' = \lim A_i', \\ \liminf T_i' &\subset \limsup T_i'. \end{aligned}$$

Thus the sequence of sets (T_i') converges to the end-sifted set T_e,

$$\lim T_i' = T_e.$$

According to the set theoretical limit, we have proved that the sequence of sets (T_i') and the sequence of its subsets (A_i') both converge to the common limit point T_e,

$$\lim T_i' = \lim A_i' = T_e. \tag{4.8}$$

We need to reveal an order topological structure of equality (4.8) to determine the cardinality $|T_e|$ of the end-sifted set T_e.

We quote a definition of the order topology [25]. The order topology is a topology on the non-empty linear order sets, they contain 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 sets. On the empty set or sets with a single element there is no order topology.

The recursive sifting process formula (4.4) produces both sequences of sets together with their common set theoretical limit point T_e.

$$\begin{aligned} \mathbf{X_1}: &\quad T_1', T_2', \ldots, T_i', \ldots\ldots; T_e, \\ \mathbf{X_2}: &\quad A_1', A_2', \ldots, A_i', \ldots\ldots; T_e. \end{aligned}$$

We further consider the structures of this both sets $\mathbf{X_1}$ and $\mathbf{X_2}$ using recursive sifting process (4.4) as an order relation

$$i < j \to T_i' < T_j', \ \forall i (T_i' < T_e),$$

$$i < j \to A_i' < A_j', \ \forall i (A_i' < T_e).$$

The set $\mathbf{X_1}$ has no repeated term. It is a well ordered set with the order type $\omega + 1$ using recursive sifting process (4.4) as an order relation. It may be endowed an order topology.

In general, the set $\mathbf{X_2}$ may have no repeated term, or may have some repeated terms or may be a set with a single element $\mathbf{X_2} = \{\emptyset\}$.

When the end-sifted set T_e is non-empty $T_e \neq \emptyset$, the set $\mathbf{X_2}$ is a linear order set with more than one element, it may be endowed an order topology.

We had computed out some patterns of the first few numbers x such that $x^2 + 1$ is prime. The end-sifted set T_e is not empty, the set $\mathbf{X_2}$ contains more than one element, may be endowed an order topology using recursive sifting process (4.4) as an order relation.

Obviously, for every neighborhood $(c, T_e]$ of T_e there is a natural number i_0, for all $i > i_0$, we have $T_i' \in (c, T_e]$ and $A_i' \in (c, T_e]$, thus sequences of both sets (T_i') and (A_i') converge to the common limit point T_e using recursive sifting process (4.4) as an order relation.

$$\begin{aligned} \lim A_i' &= T_e, \\ \lim T_i' &= T_e. \end{aligned}$$

According to the order topological limit, we have again proved that sequences of both sets (T_i') and (A_i') converge to the identical limit point T_e,

$$\lim T_i' = \lim A_i'. \tag{4.9}$$

The formula T_i' is a recursive asymptotic formula of the end-sifted set T_e. ■

The set A_i' is a subset of T_i', hence when we endow the well ordered set $\mathbf{X_1}$ with an order topology using recursive sifting process (4.4) as an order relation, linear order set $\mathbf{X_2}$ will be automatically endowed an order topology.

Only if the end-sifted set T_e is empty $T_e = \emptyset$ under some sifting conditions, namely there is no survivor or pattern, then the set $\mathbf{X_2}$ contains only one repeated term $\emptyset$. We can not endow the set $\mathbf{X_2}$ with an order topology. We can not endow the set $\mathbf{X_1}$ with an order topology also. Otherwise we will fall into a Ross-Littwood paradox. At the end of this section we will discuss this paradox.

Theorem (4.1) reveals some structures of the set of all survivors built into the sequences of sets. Now we easily prove that the cardinality of the set of all numbers x such that $x^2 + 1$ is prime is infinite.

Theorem 4.5. The set of all natural numbers x such that $x^2 + 1$ is prime is infinite.

We give two proofs.

Proof. We consider the cardinalities $|T_i'|$ and $|A_i'|$ of sets on both sides of the equality (4.9) $\lim T_i' = \lim A_i'$ and the limits of the cardinal sequences $\lim |T_i'|$ and $\lim |A_i'|$, as T_i' and A_i' both tend to T_e, to determine the cardinality of the end-sifted set T_e.

From general topology we know:"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 $\lim\limits_{x \to x_0} f(x)$ of a mapping $f : E \to Y, E \subset X$, it is necessary and sufficient that for any sequence $x_n \in E, n = 1, 2, 3, \ldots\ldots$, such that $\lim\limits_{n\to\infty} x_n = x_0$, the limit $\lim\limits_{n\to\infty} f(x_n)$ exists. If this condition holds, the limit $\lim\limits_{n\to\infty} f(x_n)$ 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." [17]

It follows that if the both limits of cardinal sequences $(|T_i'|)$ and $(|A_i'|)$ on both sides of the equality $\lim T_i' = \lim A_i'$ exist, then both limits are equal.

We known that the set T_e is nonempty $T_e \neq \emptyset$, the formula (4.9) is valid, the order topological limits $\lim |A_i'|$ and $\lim |T_i'|$ on two sides of the equality (4.9) exist, thus both limits are equal

$$\lim |A_i'| = \lim |T_i'|. \tag{4.10}$$

In traditional sieve theory or analytic number theory, one uses the counting function $\pi(n, 2)$ to count the number of primes of the form $x^2 + 1$, and tries to prove the conjecture by proving that $\lim \pi(n, 2)$ is infinite. Unfortunately, one has never proved that $\lim \pi(n, 2)$ is infinite or not by using all our current methods.

By the recursive sieve method we have

$$\begin{aligned} \lim \pi(n, 2) &= \lim \pi(m_i, 2), \\ \lim \pi(m_i, 2) &= \lim |A_i'|. \end{aligned}$$

From formula (4.6) and (4.10) we obtain

$$\lim \pi(n, 2) = \aleph_0. \tag{4.11}$$

We have directly proved that $\lim \pi(n, 2)$ is infinite. In the usual sense we have proved the conjecture. ■

From general topology, we know that the value $|T_e|$ of the counting function $\pi(n, 2)$ at T_e is irrelevant to the definition of $\lim \pi(n, 2)$. We need to prove the continuity of the cardinal function at the point T_e, then precisely obtain $|T_e| = \aleph_0$.

Proof. Let $f : \mathbf{X} \to \mathbf{Y}$ be the cardinal function $f(T) = |T|$ from the order topological space $\mathbf{X}$ to the order topological space $\mathbf{Y}$

$$\begin{aligned} \mathbf{X} &: \quad T_1',\ T_2',\ \ldots,\ T_i', \ldots\ldots;\ T_e, \\ \mathbf{Y} &: \quad |T_1'|, |T_2'|, \ldots, |T_i'|, \ldots\ldots; \aleph_0. \end{aligned}$$

It is easy to check that for every open set $[|T_1'|, |d|)$, $(|c|, |d|)$, $(|c|, \aleph_0]$ in $\mathbf{Y}$ the preimage $[T_1', d)$, (c, d), $(c, T_e]$ is also an open set in $\mathbf{X}$. Thus the cardinal function $|T|$ is continuous at T_e with respect to the above order topology.

Both order topological spaces are first countable, so the cardinal function $|T|$ is sequentially continuous. By a usual topological theorem, the cardinal function $|T|$ preserves limits,

$$|\lim T_i'| = \lim |T_i'|. \tag{4.12}$$

Order topological spaces are Hausdorff spaces. In Hausdorff spaces the limit points of the sequence of sets (T_i') and cardinal sequence $(|T_i'|)$ are unique provided that both exist [17].

Theorem 4.1 and formula (4.6) have proved that both order topological limits $\lim T_i' = T_e$ and $\lim |T_i'| = \aleph_0$ exist, the condition for the existence of two limits is sufficient.

We have deduced that the set of all natural numbers x such that $x^2 + 1$ is prime is infinite.

$$|\{x : x^2 + 1 \ is \ \ prime\}| = \aleph_0. \tag{4.13}$$

Without using any estimation , without the Riemann hypothesis, we have rigorously proved that the prime conjecture about $x^2 + 1$ is true. ■

4.3. About the Ross-Littwood paradox

When we consider the cardinalities of the sets on both sides of the equality (4.9) $\lim T_i' = \lim A_i'$ and their limits, according to general topology we need to be a little careful about whether exist the limits on the both sides of equality (4.9). If there is no $\lim A_i'$, then the equality (4.9) is not valid and the condition for the existence of the limit $\lim T_i'$ is not sufficient.

According to the definition of order topology, only if there is no any survivor or pattern under some sifting conditions, then $T_i' = T_i$ for all i, the set theoretical limit is empty $\lim T_i' = \lim A_i' = T_e = \emptyset$, obviously $|T_e| = 0$. There is no order topological limit $\lim A_i'$ or $\lim |A_i'|$ and the condition for the existence of the limit $\lim T_i$ or $\lim |T_i|$ is not sufficient. Nothing may be proved by an order topological reasoning.

In some informal arguments, when $T_e = \emptyset$, one directly regards $\lim |T_i| = \lim |T_i'| = \aleph_0$, usually in a metric space, as the cardinality of the end-sifted set T_e, then falls into a Ross-Littwood paradox. This paradox is an still argumentative problem as of today [24] [31] [34] [38].

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

Balls numbered

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

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

We ignore the physical plausible, space-time continuity, and consider what is the limit of the sequence of sets (T_i).

The problem of primes in the reducible polynomial $x^2 - 1$ is a similar example. Under the sifting condition $B_i \equiv \langle 1, -1 \rangle \mod p_i$, one seeks for the limit of the sequence of sets (T_i). Where the number $x = 2$ making $x - 1 = 1$ does not enter the sifting process, it is not a survivor, although it makes $x^2 - 1$ prime. There is no prime pattern in this reducible polynomial.

In both examples above, we know that their cardinal limit itself is infinite $\lim |T_i| = \lim |T_i'| = \aleph_0$ and their end-sifted set T_e is empty. At first glance this is a contradiction that the empty has an infinite cardinality. But in the formal proof this contradiction is tractable, since there is no order topological limit, there is no contradiction. In analytical number theory we can not prove the continuity of the cardinal function, the empty and the infinite cardinality are irrelevant.

If we relax the restrictive condition and seek for a natural number x such that $x^2 - 1$ is a product of at most two primes, an almost prime, or a product of exactly two primes, a semiprime, rather than the primes of the form $x^2 - 1$, then such natural numbers x have patterns

$$x = 4, 6, 12, 18, 30, 42, 60, 72, 102, 108, 138, 150, \dots\dots,$$

$$x^2 - 1 = 3 \times 5, 5 \times 7, 11 \times 13, 17 \times 19, 29 \times 31, 41 \times 43 \dots\dots$$

and such an end sifted set $\lim T_i' = T_e$ is infinite by the recursive sieve method.

This result is similar to the famous results of H. Iwaniec: there are infinitely many natural numbers x such that $x^2 + 1$ is a product of at most two primes.

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

5. A general theorem

Applying the above reasoning paradigm, we check whether an integer valued polynomial represents infinitely many primes or not.

In the formal system $P(N)$ we only consider positive primes.

Let

$$f(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$$

be an integer valued polynomial of degree k, where $c_k > 0$ and $c_k, \ldots, c_0$ are integers.

Let

$$X \equiv B_i \bmod p_i$$

be the solution of the congruence

$$f(x) \equiv 0 \bmod p_i.$$

We substitute this solution for recursive formula (3.1) to decide whether an integer valued polynomial $f(x)$ represents infinitely many primes or not.

The number of solutions of the congruence $f(x) \equiv 0 \bmod p_i$ does not exceed the degree k of the polynomial $f(x)$ by Lagrange's theorem.

If there is a prime $p_i \leq k$ such that the solution B_i of the congruence includes all of the residue classes $\langle 0, 1, 2, \ldots, p_i - 1\rangle \bmod p_i$, we say that this prime p_i is an obstruction and the polynomial is inadmissible. For an inadmissible polynomial the recursive sieve method itself shows that T_j is empty for all $j > i$. There is no prime of the form $f(x)$ greater than p_i.

It is easy to prove that if $f(x)$ represents at least $k+1$ primes, then $f(x)$ is admissible. We only consider admissible polynomials.

Let w_i be the number of solutions $w_i = |B_i|$. Since $f(x)$ is admissible we have $w_i < p_i$ for all $p_i \leq k$, and for all $p_i > k$ the cardinal sequence $|T_i'|$ is strictly increasing $|T_i'| < |T_{i+1}'|$.

It remains to establish whether there is a survivor of the sifting process or a pattern.

For a reducible polynomial $f(x) = g(x)h(x)$, essentially we look for the survivors x, which makes $g(x)$ and $h(x)$ simultaneously prime, the conjecture of Schinzel and Sierpinski, like the twin prime conjecture $(x - 1), (x + 1)$. Using the recursive sieve method we may prove that if $a_1, a_2, \ldots, a_k$ is an admissible prime k-tuple (an admissible prime pattern, rather than an admissible set), then there are infinitely many integers n such that $n + a_1, n + a_2, \ldots, n + a_k$ are all prime. In this paper we do not discuss this problem.

For a reducible polynomial $f(x) = g(x)h(x)$, the sifting condition becomes

$$f(x) \equiv 0 \bmod p_i \bigwedge p_i \leq g(x) \bigwedge p_i \leq h(x).$$

A number x satisfying $g(x) = 1$ or $h(x) = 1$ do not enter the sifting process, such a number x is not a survivor of the sifting progress, although it may make $f(x)$ prime, it is not a pattern making $f(x)$ prime.

For $g(x) > 1$ and $h(x) > 1$, the polynomial $f(x) = g(x)h(x)$ does not represent any prime, it has no survivor or pattern, the set theoretical limit is empty $\lim T_i' = \lim A_i' = \emptyset$, there is no order topological limit by the recursive sieve method.

In 2002, Yong-Gao Chen, Gábor Kun, Gábor Pete, Imre Z. Ruzsa and Àdàm Timár showed that the number of positive prime values in the reducible polynomial of degree k is at most k [6]. It follows that if an integer valued polynomial $f(x)$ of degree k represents at least $k + 1$ positive primes, then this polynomial is irreducible and admissible, it has survivors or patterns $T_e \neq \emptyset$.

Under those conditions, the set of all numbers x such that $f(x)$ is prime and the set of all numbers x such that $x^2 + 1$ is prime have the same recursive structure, set theoretical structure and order topological structure. The recursive sifting process itself has mechanically yielded a proof that the prime set of the form $f(x)$ is infinite.

We obtain a general theorem about which polynomials represent infinitely many primes.

Theorem 5.1. If an integer valued polynomial of degree k represents at least $k + 1$ positive primes then the polynomial represents infinitely many primes.

References

[1] P. T. Bateman and R. A. Horn., A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, **16**(1952), 363–367.

[2] V. Bouniakowsky and A. Nouveaux, théorémes relatifs á la distinction des nombres premiers et á la décomposition des entiers en facteurs, *Sc. Math. Phys.*, **6** (1857), 305–329.

[3] Chen. J.R. On the Representetion of a Large Even Interger as the Sum of a prime and the Product of at Most Two Primes. *Kexue Tongbao*, **17**(1966), 385–386.

[4] Chen. J.R. On the Representetion of a Large Even Interger as the Sum of a prime and the Product of at Most Two Primes I. *Sci.Sinica*, **16**(1973), 157–176.

[5] Chen. J.R. On the Representetion of a Large Even Interger as the Sum of a prime and the Product of at Most Two Primes II. *Sci.Sinica*, **16**(1978), 412–430.

[6] Yong-Gao Chen and Imre Z. Ruzsa, Prime values of reducible polynomials, I, *Acta Arith.*. **XCV.2** (2000), 185–193.

[7] Yong-Gao Chen, Gabor Kun, Gabor Pete, Imre Z. Ruzsa, Adam Timar, Prime values of reducible polynomials, II, *Acta Arith.*, **104** (2002), 117–127.

[8] L.E.Dikson, A new extension of Dirichlet's theorem on prime numbers, *Massenger of Mathematics*, **l** 33 (1903–04), 155–161.

[9] J. Friedlander, Producing Prime Numbers via Sieve Methods, *Lecture Notes in Mathematics*. (2002)

[10] J. Friedlander and H. Iwaniec, The polynomial $x2 + y4$ captures its primes, *Ann. of Math.*, **2**, 148 (1998), 945–1040.

[11] J. Friedlanderand H. Iwaniec, Opera De Cribro, American Mathematical Soc., (2010).

[12] Green, Ben, Tao, Terence (2008), "The primes contain arbitrarily long arithmetic progressions", *Annals of Mathematics* 167 (2): 481–547, arXiv:math.NT/0404188, doi:10.4007/annals.2008.167.481 .

[13] A. Granville, Analytic number theory, [Online] Available: http://www.dms.umontreal.ca/7Eandrew/PDF/PrinceComp.pdf.

[14] A. Granville, Different Approaches to the Distribution of Primes, Milan j. math. 78 (2009), 1–25.

[15] A. Granville, International Team Shows that Primes Can Be Found in Surprising Places, [Online] Available: http://www.ias.ac.in/resonance/Mar1998/pdf/Mar1998ResearchNews.pdf

[16] A. Granville, Primes in intervals of bounded length. preprint.

[17] Hazewinkel, Michiel, ed. (2001) [1994], "Limit", Encyclopedia of Mathematics, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4

[18] Heine Halberstam, Hans Egon Richert. *Sieve Methods*, Dover Publications. (2011).

[19] D.R. Heath-Brown, Primes represented by $x3 + 2y3$; *Acta Mathematica*, 186 (2001), 1–84.

[20] G. Harman, *Prime-detecting sieve*, Princeton university press, (2007).

[21] J. Harrison, formal proof —- theory and practice, *Notices of AMS*, 2008, [Online] Available: http://www.ams.org/notices/200811/tx081101395p.pdf.

[22] H. Iwanies, Almost-primes representated by quadratic polynomials, *Ivent. Math.*, **47** (1978), 171–188.

[23] Jouko vaananrn, Second-order logic and foundations of mathematics, *The bulletin of symbolic logic*, **l** 7 (2001), 504–520.

[24] Jon Byl, On Resolving the Littlewood-Ross Paradox, *Missouri Journal of Mathematical Sciences*, **12** 1, Winter (2000), 42–47

[25] J.R. Munkres, *Topology*, (2rd ed.), Prentice Hall, Upper Saddle River, (2000).

[26] Jon P'rez Laraudogoitia, "Supertasks", Stanford Encyclopedia of Philosophy, [Online] Available: http://plato.stanford.edu/entries/spacetime-supertasks/,(2004).

[27] K. Kuratowsky and A. Mostowsky, *set theory, With an introduction to descriptive set theory*, North-Holland Publishingcom, (1976), 118–120.

[28] Michiel Hazewinkel, Encyclopaedia of Mathematics, limit, [Online] Available: http://eom.springer.de/l/l058820.htm.

[29] Fengsui Liu, On the prime k-tuple conjecture I, *WSEAS Transactions on mathematics*, **l** 3 (2004), 744–747.

[30] Fengsui Liu, On the Sophie Germain Prime Conjecture *WSEAS Transactions on mathematics*, **l0** 12 (2011), 421–430.

[31] J.E. Littlewood, [1953], *Littlewood's Miscellany*, (ed. Bela Bollobas), Cambridge University Press, Cambridge, (1986), p. 26.

[32] D.H.J. Polymath, The "bounded gaps between primes" Polymath project - a retrospective.
http://arxiv.org/pdf/1409.8361

[33] Robert J. Lemke Oliver, Almost-primes represented by quadratic polynomials, *Acta Arith.*, 151–3. (2012), 241–261.

[34] S. Ross, *A First Course in Probability* , (3rd ed.), New York and London, Macmillan, (1988).

[35] Schinzel, A., Sierpifiski, W., Sur certaines hypotheses concernant les hombres premiers. *Acta Arith.*, **4**(1958), 185–208.

[36] Terence Tao, Open question: The parity problem in sieve theory, [Online] Available: http://terrytao.wordpress.com/2007/06/05/open-question-the-parity
-problem-in-sieve-theory.

[37] Terence Tao, Long arithmetic progressions in the primes, Australian Mathematical Society Meeting 26 September 2006.
http://www.math.ucla.edu/ tao/preprints/Slides/austms.pdf

[38] J.P. Van Bendegem, 'Ross' paradox is an Impossible Super-Task, *British Journal for the Philosophy of Science*, **45** (1994), 743–748.