

A Proof of Goldbach Conjecture by Mirror Prime Decomposition

YINGXU WANG

Dept. of Electrical and Software Engineering
 Schulich School of Engineering and Hotchkiss Brain Institute, University of Calgary
 2500 University Drive NW, Calgary, Alberta, CANADA T2N 1N4

Abstract: This work presents a formal proof of Goldbach conjecture based on a novel theory of Mirror-Prime Decomposition (MPD) for arbitrary even integers. A new concept of mirror primes $\mathbb{P}_\mu \subset \mathbb{P} \times \mathbb{P}$ is introduced as a set of pairs of primes that are symmetrically adjacent to any pivotal even number $n_e \in \mathbb{N}_e \subset \mathbb{N}$ on both sides in finite distance k bounded by $1 \leq k \leq (n_e/2) - 2$. As a counterpart of the *Euclidean Fundamental Theorem of Arithmetic for natural number factorization*, the MPD theory enables arbitrary even number decomposition by mirror primes. MPD paves a way to prove the Goldbach conjecture, i.e., where denoted by the *big-R calculus* for representing recursive structures and manipulating recursive functions. An algorithm of Goldbach conjecture testing is designed for demonstrating the formal proof of the Goldbach theorem. i.e. $\forall 4 \leq \frac{n_e}{2} < \infty$,

$$n_e = f(p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) = \prod_{k=1}^{(n_e/2)-2} (p_{\mu^-}^{n_e/2} + p_{\mu^+}^{n_e/2}) \text{ where } (p_{\mu^-}^{n_e/2} = \frac{n_e}{2} - k, p_{\mu^+}^{n_e/2} = \frac{n_e}{2} + k) \in \mathbb{P}_\mu$$

denoted by the big-R *calculus* for representing recursive structures and manipulating recursive functions. An algorithm of Goldbach conjecture testing is designed for demonstrating the formal proof of the Goldbach theorem.

Keywords: Number theory, Goldbach conjecture, proof, mirror primes, mirror prime decomposition, recursive sequence, numerical algorithm

Received: September 26, 2021. Revised: May 24, 2022. Accepted: June 26, 2022. Published: July 18, 2022.

1. Introduction

Prime numbers are fundamental mathematical objects in number theory [1, 2, 3, 4, 5, 6]. One of the challenging questions in number theories yet to be answered is the *Goldbach's conjecture* [7] that queried by Christian Goldbach in a letter to Leonhard Euler in 1742 [4, 8, 9, 10]. A typical and informal expression of the Goldbach conjecture may be stated as follows.

Definition 1. The *Goldbach conjecture* queries whether every even integer greater than 2 may be expressed as the sum of two primes.

Key milestones towards the proof of Goldbach conjecture in the past 278 years and beyond includ: 1) The Euclid's *Fundamental Theorem of Arithmetic* (FTA) that revealed there is always a unique prime factorization for any integer [1, 3]; 2) The Legendre's *Sieve of Eratosthenes* (1808) that provided a foundation for modern sieve theories [2, 11]; 3) The *Prime Number Theorem* (PNT) $\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \log n} = 1$ that proved by

Hadamard and de la Vallee Poussin in 1896, independently [4]; 4) Vinogradov's theorem (1937) that stated all large odd numbers may be expressed by n (large) = $p_1 + p_2 + p_3$ with triple primes [12]; 5) A finding that the number of positive even integers less than n which are not representable as a sum of two primes grows slower than $\frac{n}{(\log n)^r}$ for any positive r

[13]; 6) There are some integer k such that every sufficiently large even number is the sum of two primes and the k th powers of 2 [9]; 7) The refined Linnik's theorem for $k = 8$ [10]; 8) The proof that every sufficiently large even number is the sum of a prime and a number with at most two prime factors [14]; 9) T. Tao explored obstructions to uniformity of primes and their arithmetic patterns [15]; 10) Every odd number (≥ 7) can be written as the sum of three primes known as the ternary Goldbach conjecture [16]; 11) Numerical algorithms for testing the Goldbach conjecture in a certain scope [17]; 12) Every odd number greater than 1 is the sum of at most five primes [18]; and 13) Every positive integer can be written as the sum of a prime number and a square free number [19]. However, there is no formal proof for the *Goldbach conject* yet that may hold in all cases because the nature of its complexity.

It is revealed in this work that the key to proof Goldbach conjecture is the missing of a *prime decomposition theory* for arbitrary even numbers as a counterpart of Euclid's FTA on *prime factorization* [1]. This work intends to present a formal proof of the Goldbach conjecture based on the finding of the set of mirror primes $\mathbb{P}_\mu \subset \mathbb{P} \times \mathbb{P}$ where the set of primes $\mathbb{P} \subset \mathbb{N}_o$ (odd integers) $\subset \mathbb{N}$ except 2 as well as the theorem of *mirror-prime decomposition*. A formal model and the recursive properties of the set of primes \mathbb{P} are described in Section 2. The concept of *mirror primes* \mathbb{P}_μ is introduced in Section 3 that leads to the proof of the Theorem of Mirror-

Prime Decomposition for arbitrary even numbers. These preparations lead to the proof of the Goldbach conjecture as formally presented in Section 4 by the universal existence of mirror primes and the inductive rule of mirror-prime decomposition. A set of experiments based on an Algorithm of *Goldbach Theorem verification* is provided for visualizing the proven Goldbach conjecture.

2. The Big-R Calculus for Manipulating Recursive Structures and Functions

The set of prime numbers \mathbb{P} is a subset of special odd integers supplement by 2 in natural numbers \mathbb{N} , i.e., $\mathbb{P} \subset \mathbb{N}_o \cup \{2\} \setminus \{1\} \subset \mathbb{N}$. Since \mathbb{N} is infinite, so is \mathbb{P} according to its *countability* with respect to \mathbb{N} . Therefore, \mathbb{P} shares the generic properties of \mathbb{N}_o as a *necessary* condition, but also obeys special primality properties as their *sufficient* conditions as described in this section.

In order to efficiently denote and manipulate infinite sets and sequences as well as functions operating on them, a general recursive notation known as the *big-R* calculus [20] is introduced. As shown in Section 2.1, a suitable notation may significantly reduce the complexity of problem modeling and solving. It may also increase the efficiency in recursive inferences for hard problems and long-chain reasoning for mathematical induction and deduction.

2.1 Mathematical Models of Recursive Structures and Properties of Primes

Definition 2. The *big-R calculus* is a recursive operator for neatly modeling finite or infinite sequences of recurrent structures and manipulating a series of embedded functions such as:

$$\left\{ \begin{array}{l} \text{a) Infinite sequence: } \mathcal{Q} \triangleq \left(\bigoplus_{i=0}^{\infty} q_i \right) = (q_0, q_1, q_2, \dots, q_k, \dots) \\ \text{b) Infinite set: } \mathcal{S} \triangleq \left\{ \bigoplus_{i=0}^{\infty} n_i \right\} = \{n_0, n_1, n_2, \dots, n_k, \dots\} \\ \text{c) Infinitely inductive functions: } \mathbb{F}_i \triangleq \bigoplus_{k=1}^{\infty} f^k(f^{k-1}) \\ \qquad \qquad \qquad = f^k(f^{k-1}(\dots f^1(f^0)\dots)), \exists f^0 \\ \text{d) Infinitely deductive functions: } \mathbb{F}_d \triangleq \bigoplus_{k=\infty}^1 f^k(f^{k-1}) \\ \qquad \qquad \qquad = f^k(f^{k-1}(\dots f^1(f^0)\dots)), \exists f^0 \end{array} \right. \quad (1)$$

Example 1. The set of even integers \mathbb{N}_e and the recursive structures of a series of deductively embedded functions \mathbb{F}_d

may be formally described by the *big-R* notation, respectively, as follows:

$$\begin{aligned} \mathbb{N}_e &= \left\{ \bigoplus_{n=0}^{\infty} 2n+2 \right\} = \{2, 4, 6, 8, \dots, 2n+2, 2(n+1)+2, \dots\} \\ \mathbb{F}_d &= \bigoplus_{k=n}^1 f^k(f^{k-1}) = f^n(f^{n-1}(\dots f^1(f^0)\dots)), \exists f^0 = \text{constant} \end{aligned} \quad (2)$$

Definition 3. The *set of natural numbers* \mathbb{N} is all positive integers in the scope of $[1, \infty)$ with a uniform step of increment that may be denoted by the *big-R* calculus:

$$\mathbb{N} \triangleq \left\{ 1, \bigoplus_{n=1}^{\infty} n+1 \right\} = \{1, 2, 3, \dots, n+1, n+2, \dots\} \quad (3)$$

Similarly, the sets of *even* and *odd integers* \mathbb{N}_e and \mathbb{N}_o , $\mathbb{N}_e \cup \mathbb{N}_o = \mathbb{N}$, are denoted, respectively, by:

$$\begin{aligned} \mathbb{N}_e &\triangleq \left\{ \bigoplus_{n=1}^{\infty} 2n \right\} = \{2, 4, 6, \dots, 2n, 2(n+1), 2(n+2), \dots\} \\ \mathbb{N}_o &\triangleq \left\{ \bigoplus_{n=1}^{\infty} 2n-1 \right\} = \{1, 3, 5, \dots, 2n-1, 2(n+1)-1, 2(n+2)-1, \dots\} \end{aligned} \quad (4)$$

Definition 4. A *prime number* p , except 2, is an odd positive integer $p > 1 \in \mathbb{N}_o \subset \mathbb{N}$ that is not a product of two smaller integers:

$$p \triangleq (n \mid \bigoplus_{m=2}^{\lfloor \sqrt{n} \rfloor} n \not\equiv 0 \pmod{m}), \forall n \in \mathbb{N}_o \cup \{2\} \setminus \{1\} \quad (5)$$

Any prime may be verified based on Definition 4 though more efficient sieve methods and algorithms exist [21, 22, 24, 25, 26, 27]. A generic method for primality testing may be formally described as follows.

Definition 5. The *primality testing function* $\rho(n)$ determines whether n is prime $\forall n \in \mathbb{N}_o \cup \{2\} \setminus \{1\}$:

$$\rho(n) \triangleq \begin{cases} 0, & \bigoplus_{m=2, m \in \mathbb{P}}^{\lfloor \sqrt{n} \rfloor} n \equiv 0 \pmod{m} \quad // n \notin \mathbb{P} \\ 1, & \text{otherwise} \quad // n \in \mathbb{P} \end{cases} \quad (6)$$

where $\rho(n)$ results in a positive verification *iff* $n \not\equiv 0 \pmod{m}$ for all $2 \leq m \leq \lfloor \sqrt{n} \rfloor \in \mathbb{P}$. Otherwise, as a shortcut, any negative result $n \equiv 0 \pmod{m}$ will terminate the testing by returning false.

In classic number theory, the set of prime numbers $\mathbb{P} \subset \mathbb{N}$ is used to be perceived as a random set. However, according to Definitions 4 and 5, \mathbb{P} may be rationally perceived as a recursively determinable sequence as follows.

Definition 6. The *generic pattern of primes* \mathbb{P} is a recursive and infinite sequence of monotonously increasing odd integers (except 2) validated by the primality checker $\rho(n)$:

$$\mathbb{P} \triangleq \{R p_i\}_{i=1}^{\infty}$$

$$= \{p_1 = 2, p_2 = 3, R_{i=3}^{\infty} [R_{k=1}^{p_{i-1}} (p_i = p_{i-1} + 2k) \mid \rho(p_i) = 1]\}, k \in \mathbb{N}$$
(7)

Example 2. The following subset of primes may be recursively derived by Eq. (7) following the first two known primes $p_1 = 2$ and $p_2 = 3$ in \mathbb{P} .

$$p_3 = (p_2 + 2) = (3 + 2) = 5 \in \mathbb{P} \Rightarrow \mathbb{P}_3 = \{2, 3, 5, \dots\}$$

$$p_4 = (p_3 + 2) = (5 + 2) = 7 \in \mathbb{P} \Rightarrow \mathbb{P}_4 = \{2, 3, 5, 7, \dots\}$$

$$p_5 = (p_4 + 2) = (7 + 2) \notin \mathbb{P}$$

$$\rightarrow (p_4 + 4) = (7 + 4) = 11 \in \mathbb{P} \Rightarrow \mathbb{P}_5 = \{2, 3, 5, 7, 11, \dots\}$$

...

$$p_{25} = (p_{24} + 2) = (89 + 2) \notin \mathbb{P}$$

$$\rightarrow (89 + 4) \notin \mathbb{P}$$

$$\rightarrow (89 + 6) \notin \mathbb{P}$$

$$\rightarrow (89 + 8) = 97 \in \mathbb{P} \Rightarrow \mathbb{P}_{25} = \{2, 3, 5, 7, 11, \dots, 97\}$$

$$p_{26} = (97 + 2) \notin \mathbb{P}$$

$$\rightarrow (97 + 4) = 101 \in \mathbb{P} \Rightarrow \mathbb{P}_{26} = \{2, 3, 5, 7, 11, \dots, 97, 101\}$$

...

$$p_n = (p_{n-1} + 2) = ((2996863034895 \cdot 2^{1290000} - 1) + 2) \in \mathbb{P}$$

$$\Rightarrow \mathbb{P}_n = R_{n=1}^{\infty} p_i = \{2, 3, 5, 7, 11, \dots, 97, 101, \dots,$$

$$2996863034895 \cdot 2^{1290000} - 1, 2996863034895 \cdot 2^{1290000} + 1,$$

$$\dots\} \subset \mathbb{P}$$

where the largest twin primes, $2996863034895 \cdot 2^{1290000} \mp 1$, have been found in 2016 [29]. The largest prime number as known in 2020 is $2^{82,589,933} - 1$ which has been revealed by Patrick Laroche from the group of Great Internet Mersenne Prime Search (GIMPS) [6].

2.2 Recursive Properties of the Sequence of Primes

The generic pattern of prime numbers described in Section 2.1 reveals the analytic and distribution properties of the set of primes \mathbb{P} . According to Definition 6, all primes

$p_i \in \mathbb{P}$ are derived from a recursive sequence that provides a new perspective on the nature of primes and their manipulations.

Theorem 1 (Recursiveness of the Prime Sequence, RPS). Primes in \mathbb{P} are a *recursive sequence* where prime p_{n+1}

is derived from and constrained by the preceding ones $R_{i=1}^n p_i$ based on the following *necessary* and *sufficient* conditions:

$$R_{n=2}^{\infty} p_{n+1} (R_{i=1}^n p_i) = R_{n=2}^{\infty} \left\{ \begin{array}{l} \text{(a) The necessary condition } n \in \mathbb{N} \\ p_{n+1} = p_n + 2k, k \in \mathbb{N} \\ \text{(b) The sufficient condition} \\ \lfloor \sqrt{p_n} \rfloor \\ R_{m=2, m \in \mathbb{P}} p_{n+1} \not\equiv 0 \pmod{m} \end{array} \right.$$
(8)

where $n, m, i, k \in \mathbb{N}$, $p_1 = 2$, and $p_2 = 3$

Proof. Theorem 1 holds based on the inherent properties of primes as a special sequence of particular odd integers, except 2, according to Definition 6:

a) Condition (a) is necessary because

$$\forall n, k \in \mathbb{N}, n \geq 2, p_1, p_n, p_{n+1} \in \mathbb{P}, p_1 = 2, \text{ and } p_2 = 3,$$

$$p'_{n+1} \neq R_{k=1}^{\leq p_n} (p_n + 2k)$$

results in either $\rho(p'_{n+1}) \neq 1$ or some of the potential p'_{n+1} would be missed. Thus, any eligible prime p_{n+1} must be at one of the positions:

$$p_{n+1} = R_{k=1}^{\leq p_n} (p_n + 2k) \text{ as necessary.}$$

b) Condition (b) is sufficient based on (a) because

$$R_{m=2, m \in \mathbb{P}}^{\lfloor \sqrt{p_n} \rfloor} p_{n+1} \not\equiv 0 \pmod{m} = \bigwedge_{m=2, m \in \mathbb{P}}^{\lfloor \sqrt{p_n} \rfloor} p_{n+1} \not\equiv 0 \pmod{m}$$

eliminates all potential prime divisors among preceding

primes $R_{n=2, n \in \mathbb{P}}^{\lfloor \sqrt{p_n} \rfloor} (p_n < p_{n+1})$ in \mathbb{P} , such that each

$p_{n+1} = R_{n=2}^{\infty} p_{n+1}(p_n)$ is recursively determined by

previously known primes validated by

$$2 \leq m \in \mathbb{P} \leq \lfloor \sqrt{p_n} \rfloor \text{ or } R_{k=1}^{\leq p_n} \rho(p_n + 2k) \equiv 1.$$

Theorem 1 reveals the nature of primality and the *recursive property* of the infinite sequence of primes. It also indicates that p_{n+1} would remain indeterminable until the preceding $p_{\lfloor \sqrt{p_{n+1}} \rfloor}$ have been acquired by any inexhaustive prime sieve method. ■

3. Formal Models and Properties of Oktqt'Rt kogu'P_μ

Based on the preparations in Section 2, a key concept of mirror primes is introduced in this section to model an important distribution pattern of primes towards the proof of Goldbach conjecture.

Definition 7. The *mirror primes* $p_{\mu}^{n_e/2}$ with respect to a pivotal even number $n_e \in \mathbb{N}_e \subset \mathbb{N}$ are pairwise primes symmetrically adjacent to the central e_n within finite $\pm k \in \mathbb{N}$ distances:

$$p_{\mu}^{n_e/2} \triangleq \left\{ \prod_{k=1}^{\frac{n_e-2}{2}} (p_{\mu^-}^{n_e/2} = \frac{n_e}{2} - k, p_{\mu^+}^{n_e/2} = \frac{n_e}{2} + k) \mid \rho(p_{\mu^-}^{n_e/2}) \wedge \rho(p_{\mu^+}^{n_e/2}) = 1 \right\} \quad (9)$$

where k is called the *half interval* and the primality validation function $\rho(\frac{n_e}{2} \mp k)$, $1 \leq k \in \mathbb{N} \leq \frac{n_e}{2} - 2$ as given in Definition 5 eliminates any potential decomposition that is not a pair of mirror primes.

Example 3. The following sets of mirror primes are derived according to Definition 7 where the sum of each pair is always equal to their corresponding pivotal n_e :

Based on Definition 7, the entire set of mirror primes \mathbb{P}_{μ} may be recursively derived as given in Definition 8.

Definition 8. The *set of mirror primes* \mathbb{P}_{μ} is all valid pairs of mirror primes with respect to each pivotal even number $4 \leq n_e/2 \in \mathbb{N}_e$ in finite distance $1 \leq k \leq \frac{n_e}{2} - 2$:

$$\begin{aligned} p_{\mu}^4 &= \left\{ \prod_{k=1}^{\frac{n_e-2}{2}} \left(\frac{n_e}{2} \mp k \mid \rho\left(\frac{n_e}{2} \mp k\right) = 1 \right) \right\} = \left\{ \prod_{k=1}^2 (4 \mp k) \mid \rho(4 \mp k) = 1 \right\} \\ &= \{(3, 5), (2, 6) \mid \rho(4 \mp k) = 1\} = \{(3, 5)\} \\ &\Rightarrow k_{\min}(p_{\mu}^4) = 1 \text{ for mirror-prime decomposing } n_e = 8 = 3 + 5 \\ p_{\mu}^5 &= \left\{ \prod_{k=1}^3 (5 \mp k) \mid \rho(5 \mp k) = 1 \right\} \\ &= \{(4, 6), (3, 7), (2, 8) \mid \rho(5 \mp k) = 1\} = \{(3, 7)\} \\ &\Rightarrow k_{\min}(p_{\mu}^5) = 2 \text{ for } n_e = 10 = 3 + 7 \\ \dots \\ p_{\mu}^{50} &= \left\{ \prod_{k=1}^{48} (50 \mp k) \mid \rho(50 \mp k) = 1 \right\} \\ &= \{(49, 51), (48, 52), (47, 53), (46, 54), (45, 55), (44, 56), (43, 57), (42, 58), (41, 59), (40, 60), \\ &\quad (39, 61), (38, 62), (37, 63), (36, 64), (35, 65), (34, 66), (33, 67), (32, 68), (31, 69), (30, 70), \\ &\quad (29, 71), (28, 72), (27, 73), (26, 74), (25, 75), (24, 76), (23, 77), (22, 78), (21, 79), (20, 80), \\ &\quad (19, 81), (18, 82), (17, 83), (16, 84), (15, 85), (14, 86), (13, 87), (12, 88), (11, 89), (10, 90), \\ &\quad (9, 91), (8, 92), (7, 93), (6, 94), (5, 95), (4, 96), (3, 97), (2, 98) \mid \rho(50 \mp k) = 1\} \\ &= \{(47, 53), (41, 59), (29, 71), (11, 89), (3, 97)\} \\ &\Rightarrow k_{\min}(p_{\mu}^{50}) = 3 \text{ for } n_e = 100 = 47 + 53 \\ \dots \end{aligned}$$

$$\begin{aligned} \mathbb{P}_{\mu} &\triangleq \left\{ \prod_{n_e/2=4}^{\infty} p_{\mu}^{n_e/2} \right\} \subset (\mathbb{P} \times \mathbb{P}) \\ &= \left\{ \prod_{n_e/2=4}^{\infty} \left[\prod_{k=1}^{\frac{n_e-2}{2}} \left(p_{\mu^-}^{n_e/2} = \frac{n_e}{2} - k, p_{\mu^+}^{n_e/2} = \frac{n_e}{2} + k \right) \mid \rho(p_{\mu^-}^{n_e/2}) \wedge \rho(p_{\mu^+}^{n_e/2}) = 1 \right] \right\} \quad (10) \end{aligned}$$

where all pairs of mirror primes $p_{\mu}^{n_e/2} \in \mathbb{P}_{\mu}$ in the scope $8 \leq n_e < \infty$ are determined by Definition 7.

It is noteworthy that the set of mirror primes represents all symmetric pairs of adjacent primes with respect to any pivotal even number $n_e/2$ in equal distances. Based on the generic model of mirror primes, the classic *twin primes* $p_{\tau}^{n_e}$ may be formally derived as a special subset of \mathbb{P}_{μ} where the half interval $k \equiv 1$. For instances:

$$\begin{aligned} p_{\tau}^4 &= p_{\mu}^4(8/2 \mid k=1) = \{(4 \mp 1) \mid \rho(4 \mp 1) = 1\} = \{(3, 5)\} \\ p_{\tau}^6 &= p_{\mu}^6(12/2 \mid k=1) = \{(6 \mp 1) \mid \rho(6 \mp 1) = 1\} = \{(5, 7)\} \\ p_{\tau}^8 &= p_{\mu}^8(16/2 \mid k=1) = \{(8 \mp 1) \mid \rho(8-1) = 1 \wedge \rho(8+1) = 0\} \\ &= \{(7, \emptyset)\} = \{\emptyset\}, \text{ while } p_{\mu}^8 = \{(5, 11 \mid k=3), (3, 13 \mid k=5)\} \\ p_{\tau}^{10} &= p_{\mu}^{10}(20/2 \mid k=1) = \{(10 \mp 1) \mid \rho(9) = 0 \wedge \rho(11) = 1\} \\ &= \{(\emptyset, 11)\} = \{\emptyset\}, \text{ while } p_{\mu}^{10} = \{(7, 13 \mid k=3), (3, 17 \mid k=7)\} \\ p_{\tau}^{12} &= p_{\mu}^{12}(24/2 \mid k=1) = \{(12 \mp 1) \mid \rho(12 \mp 1) = 1\} = \{(11, 13)\} \\ \dots \end{aligned}$$

According to Definition 8, although the number of mirror primes with respect to different n_e is proportional to its value, i.e., $(n_e/2) - 2$, but at least one pair of mirror primes exists in finite steps for mirror-prime decomposition. This discovery

of the interesting properties of mirror primes is formalized in the following theorem.

Theorem 2 (Mirror Prime Decomposition, MPD). Any even integer $n_e / 2 \geq 4 \in \mathbb{N}_e$ may be decomposed to the sum of at least a pair of mirror primes $p_{\mu}^{n_e/2} = (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) = (\frac{n_e}{2} - k, \frac{n_e}{2} + k) \in \mathbb{P}_{\mu}$ adjacent to $n_e/2$ as the pivot within $1 \leq k \leq \frac{n_e}{2} - 2$ steps:

$$\forall n_e / 2 \geq 4 \in \mathbb{N}_e \subset \mathbb{N}, k \in \mathbb{N}:$$

$$n_e \equiv p_{\mu^-}^{n_e/2} + p_{\mu^+}^{n_e/2} = (\frac{n_e}{2} - k) + (\frac{n_e}{2} + k) \text{ bounded} \quad (11)$$

by $1 \leq k \leq \frac{n_e}{2} - 2$

where $p_{\mu}^{n_e/2} = (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) \in \mathbb{P}_{\mu}$

$$\in \bigcap_{n_e/2=4}^{\infty} \left\{ \bigcap_{k=1}^{\frac{n_e}{2}-2} \left(p_{\mu^-}^{n_e/2} = \frac{n_e}{2} - k, p_{\mu^+}^{n_e/2} = \frac{n_e}{2} + k \right) \mid \rho(p_{\mu^-}^{n_e/2}) \wedge \rho(p_{\mu^+}^{n_e/2}) = 1 \right\}.$$

Proof. Theorem 1 holds according to the principle of mathematical induction throughout the entire set of mirror primes $\mathbb{P}_{\mu} \subset \mathbb{P} \times \mathbb{P}$ as follows:

$$\forall n_e / 2 \geq 4 \in \mathbb{N}_e \subset \mathbb{N}, k \in \mathbb{N}, \text{ and } (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) \in \mathbb{P}_{\mu}:$$

Applying rules of mathematical induction based on Def. 6:

$$\mathbb{P}_{\mu} = \left\{ \bigcap_{n_e/2=4}^{\infty} \left[\bigcap_{k=1}^{\frac{n_e}{2}-2} \left(p_{\mu^-}^{n_e/2} = \frac{n_e}{2} - k, p_{\mu^+}^{n_e/2} = \frac{n_e}{2} + k \right) \mid \rho(p_{\mu^-}^{n_e/2}) \wedge \rho(p_{\mu^+}^{n_e/2}) = 1 \right] \right\}$$

a) The statement for the base case $n_e = 8$ (or $n_e/2 = 4$) is true:

$$\mathbb{P}_{\mu}^8 = \left\{ \bigcap_{k=1}^{(8/2)-2} ((4-k, 4+k) \mid \rho(4 \mp k) = 1) \right\}$$

$$= \{(3, 5), (2, 6) \mid \rho(4 \mp 1) = 1\} = \{(3, 5)\}$$

\Rightarrow The prime decomposition is $n_e = 8 = 3 + 5$
 determined within the minimum half interval
 $k_{\min} = 1 \leq (n_e/2) - 2 = 2;$

b) Assume the statement true $\forall n_e = 1,000$, i.e., $n_e/2 = 500$:

$$\mathbb{P}_{\mu}^{1000} = \left\{ \bigcap_{k=1}^{498} ((500-k, 500+k) \mid \rho(500 \mp k) = 1) \right\}$$

$$= \{(499, 501), (498, 502), \dots, (491, 509), \dots \mid \rho(500 \mp 9) = 1\}$$

$$= \{(491, 509), \dots\}$$

$\Rightarrow n_e = 1000 = 491 + 509$ with
 $k_{\min} = 9 \leq (n_e/2) - 2 = 498;$

c) Then, the next pair of mirror primes for $n_e = 1000 + 2 = 1002$ is also true:

$$\mathbb{P}_{\mu}^{1002} = \left\{ \bigcap_{k=1}^{499} ((501-k, 501+k) \mid \rho(501 \mp k) = 1) \right\}$$

$$= \{(500, 502), (499, 503), \dots \mid \rho(501 \mp 2) = 1\}$$

$$= \{(499, 503), \dots\}$$

$\Rightarrow n_e = 1002 = 499 + 503$ with $k_{\min} = 2 \leq (n_e/2) - 2 = 499;$

Thus, it has been inductively proven that $\forall n_e \geq 8 \in \mathbb{N}_e \subset \mathbb{N}$,

$$\exists \text{ at least a pair of mirror primes } p_{\mu}^{n_e/2} = (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2})$$

$$= (\frac{n_e}{2} - k, \frac{n_e}{2} + k) \in \mathbb{P}_{\mu}$$

that satisfies the MPD theorem $n_e \equiv p_{\mu^-}^{n_e/2} + p_{\mu^+}^{n_e/2}$ bounded in
 $1 \leq k \leq \frac{n_e}{2} - 2$ steps. ■

The Theorem of MPD is a coherent counterpart of Euclid's FTA on *prime factorization* in number theory [1]. It provides a general theory and methodology for finding all pairs of mirror primes, including twin primes, on both sides of

any arbitrary even number in the scope of $4 \leq \frac{n_e}{2} < \infty$, except

the special case $\frac{n_e}{2} = 2$ where the mirror primes regress to a

pair of *reflexive* primes $p_{\nu}^4 = (2, 2), k = 0$. The proven existence of at least a symmetric pair of mirror primes to any pivotal even numbers according to the MPD theorem paves a way to formally prove Goldbach conjecture in the following section.

4. Proof of the Goldbach Conjecture

The classic expression of *Goldbach* conjecture has been described in Definition 1. Although in his letter to Euler [7], Goldbach demonstrated alternative prime compositions for a few small even integers, he could not go very far perhaps because of the extreme complexity to deal with both infinite sets of \mathbb{N} and \mathbb{P} . More fundamentally, we now understand that the yet to be proven conjecture was mainly due to the lack of a formal *prime decomposition* theory for even numbers representation as revealed in Theorem 2 supplement to Euclidean FTA [1] for prime factorization in number theory.

Goldbach conjecture as given in Definition 1 may be formally described as a hypothesis of general prime decomposition for even numbers as follows.

Hypothesis 1. *Goldbach Conjecture* states that any arbitrary even number n_e as equal to or greater than 4 may be expressed by the sum of two primes p_i and p_j :

$$n_e = p_i + p_j, p_i, p_j \in \mathbb{P}, n_e \in \mathbb{N}_e \subset \mathbb{N}, n_e \geq 4 \quad (12)$$

On the basis of the MPD theorem, Goldbach conjecture may be deduced to a general prime decomposition problem for even numbers. Therefore, the establishment of Theorem 2 has provided the necessary and sufficient conditions for proving the Goldbach conjecture based on the mathematical model of mirror primes \mathbb{P}_μ .

Theorem 3 (The Goldbach Theorem). Given any arbitrary even integer $n_e / 2 \geq 4 \in \mathbb{N}_e \subset \mathbb{N}$, there exist at least a pair of mirror primes $(p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) \in \mathbb{P}_\mu \subset \mathbb{P} \times \mathbb{P}$ that satisfy:

$$\bigcap_{n_e/2=4}^{\infty} [n_e \equiv (p_{\mu^-}^{n_e/2} + p_{\mu^+}^{n_e/2}) \mid (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) \in \mathbb{P}_\mu] \quad (13)$$

where $p_{\mu^-}^{n_e/2} = \frac{n_e}{2} - k$, $p_{\mu^+}^{n_e/2} = \frac{n_e}{2} + k$, in finite distance $1 \leq k \leq \frac{n_e}{2} - 2$.

Proof. The Goldbach theorem is proven based on the recursive symmetric property of mirror-prime decomposition as established in Theorem 2:

$$\forall \frac{n_e}{2} \geq 4 \in \mathbb{N}_e \subset \mathbb{N} \text{ and } k \in \mathbb{N}:$$

Theorem 2 ensures that

at least a pair of valid mirror primes is in

$$\bigcap_{k=1}^{\frac{n_e}{2}-2} \{(p_{\mu^-}^{n_e/2} = \frac{n_e}{2} - k, p_{\mu^+}^{n_e/2} = \frac{n_e}{2} + k) \mid (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) \in \mathbb{P}_\mu\}$$

pinpointable by $1 \leq k \leq \frac{n_e}{2} - 2$ steps where

$$\left| \bigcap_{k=1}^{\frac{n_e}{2}-2} (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) \in \mathbb{P}_\mu \right| \geq 1,$$

that satisfies:

$$\bigcap_{n_e/2=4}^{\infty} [n_e \equiv (p_{\mu^-}^{n_e/2} + p_{\mu^+}^{n_e/2}) = (\frac{n_e}{2} - k) + (\frac{n_e}{2} + k)]$$

without exception. ■

Example 4. Applying the Goldbach Theorem to the largest twin primes $p_{\tau}^{n_e} = 2996863034895 \cdot 2^{1290000} \mp 1$ discovered in 2016 [29], $n_e = 2996863034895 \cdot 2^{1290000}$ is surely decomposable by the pair of known twin primes as a special case of the mirror primes where $k = 1$:

$$\exists n_e = 2996863034895 \cdot 2^{1290000}, \text{ and}$$

$$\rho(2996863034895 \cdot 2^{1290000} \mp 1) = 1,$$

according to Theorem 3:

$$n_e = 2996863034895 \cdot 2^{1290000}$$

$$= p_{\mu^-}^{n_e} + p_{\mu^+}^{n_e} = p_{\tau}^{n_e} + p_{\tau}^{n_e} = (\frac{n_e}{2} - 1) + (\frac{n_e}{2} + 1), k = 1$$

$$= (\frac{2996863034895 \cdot 2^{1290000}}{2} - 1) + (\frac{2996863034895 \cdot 2^{1290000}}{2} + 1)$$

The proven Goldbach conjecture in Theorem 3 may be numerically explained by an infinitively inductive sequence in \mathbb{P}_μ . An algorithm for numerically implementing the Goldbach theorem is derived for prime decomposition of arbitrary even numbers. It is formally described using *Real-Time Process Algebra* (RTPA) [28] known as a form of Intelligent Mathematics (IM) [5, 23] for AI programming.

Algorithm 1. The *Algorithm of Goldbach Theorem Verification* (AGTV) is designed based on Theorem 3 as a numerical verification tool for mirror-prime decompositions of arbitrary even integers. The AGTV algorithm treats the Goldbach theorem as a recursive function $\bigcap_{n_e/2=4}^{\infty} f(p_{\mu^-}^{n_e}, p_{\mu^+}^{n_e})$

according to Eq. (13), which links the hard problem in number theory to a deterministic numerical solution. The AGTV algorithm as a process model (PM) in RTPA, *AGTV*|PM, is shown in Fig. 1.

The AGTV algorithm is a computational implementation of the mathematical models obtained in Theorem 3. The input (*I*) of *AGTV*|PM is the maximum expected prime decomposition for $\bigcap_{n_e=8}^{n_e^{\max}|\mathbb{N}_e} (p_{\mu^-}^{n_e}, p_{\mu^+}^{n_e}) \in \mathbb{P}_\mu$. The output (*O*) of

AGTV|PM is a set of verified results represented by $\bigcap_{n_e=8}^{n_e^{\max}|\mathbb{N}_e} \mathbb{R}(n_e|\mathbb{N}_e = p_{\mu^-}^{n_e}|\mathbb{P} + p_{\mu^+}^{n_e}|\mathbb{P})$. The *Hyperstructure* (*H*)

denotes underpinning Structure Models (SMs) to be operated by the algorithm. *AGTV*|PM is implemented by a recursive

process in the loop $\bigcap_{n_e/2|\mathbb{N}_e=8}^{n_e^{\max}|\mathbb{N}_e} (\dots)$ after the upper limit for

iteration is validated by the if-then-(else) structure (◆). It then determines the first or nearest mirror-prime decomposition for each $n_e|\mathbb{N}_e = p_{\mu^-}|\mathbb{P} + p_{\mu^+}|\mathbb{P}$ guaranteed by

Theorem 3 within $k \leq \frac{n_e}{2} - 2$ iterations. Once a validate pair of

mirror-prime decomposition for a given even number $n_e|\mathbb{N}_e$ is found, the algorithm exits ($\rightarrow \emptyset$) and enter the next iteration until all $n_e^{\max}|\mathbb{N}_e$ cases of Goldbach decompositions are completed.

The time complexity of *AGTV*|PM is $O(n_e^{\max} \cdot \frac{n_e^{\max}}{2} \cdot \left\lceil \sqrt{n_e^{\max}} \right\rceil) \simeq O(\frac{1}{2}(n_e^{\max})^{\frac{5}{2}})$. The space requirement for AGTV is constrained by the memory size of the underpinning computer platform.

```

AGTV|PM(<I:: nemax |Ne>; <O:: ∃ Rne/2=4nemax |Ne [(pμ-ne/2, pμ+ne/2)]|Pμ ⇒  $\frac{n_e |N_e}{2} = p_{\mu^-}^{n_e/2} |P + p_{\mu^+}^{n_e/2} |P$ >;
<H:: Pμ|E ⊂ P|E × P|E = Rne/2|Ne=4∞- [(pμ-ne/2, pμ+ne/2)]|Pμ, ρ(pμ-ne/2, pμ+ne/2) = 1]> ≜
{→ ♦ nemax |Ne ≥ 8
→ Rne/2|Ne=4nemax |Ne (→ Find|B := F|B
→ Rk|N=1ne |Ne-2 (→ pμ-ne/2 |No =  $\frac{n_e |N_e}{2} - k$ 
→ pμ+ne/2 |No =  $\frac{n_e |N_e}{2} + k$ 
→ ( ♦ √m|N=2, m∈Ppμ-ne/2 |No [pμ-ne/2 |No ≡ 0 (mod m|N) ∧ pμ+ne/2 |No ≡ 0 (mod m|N)] // Primality test fail
→ ∅ // Exit
| ~ // The nτth+1 Pτ find
→ Print("ne |Ne = pμ-ne/2 |P + pμ+ne/2 |P")
→ ∅
)
)
}
    
```

Fig. 1. The algorithm for Goldbach Theorem verification (AGTV)

The AGTV algorithm may be implemented in any programming language for enabling empirical testing by readers as illustrated in Experiment 1. A set of numerical experiments based on AGTV is tested in MATLAB that provides empirical evidence for demonstrating the nature of the proven Goldbach theorem.

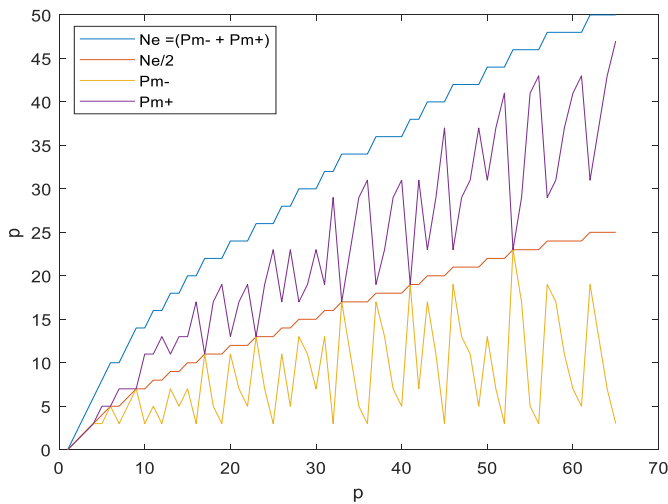


Fig. 2. Experimental results of Goldbach theorem for $P_{\mu}^{66} = P_{\mu}^{66} \times P_{\mu}^{66}$ by Algorithm 1

Experiment 1. Applying the AGTV algorithm, a set of experimental results has been obtained as illustrated in Figures 2 and 3 in the two-dimensional space . Figure 2

demonstrates the proven decompositions of the first 66 samples in the scope of $4 \leq N_e / 2 \leq 66$. It shows that any even number N_e can be expressed as the sum of a pair of mirror primes, $N_e \equiv P_{m^-} + P_{m^+}$, as predicated by the proven Goldbach theorem. It is noteworthy that the curve of $N_e/2$ functions as a divider for separating the pairs of both sets of symmetric mirror numbers. The cases where the mirror primes almost touch the $N_e/2$ curve indicate those of twin primes ($k = 1$) decomposition as special cases of mirror primes.

Similarly, the proven decompositions of the set of 100 even numbers in the scope of $4 \leq N_e / 2 \leq 100$ is autonomously generated as illustrated in Figure 3 in a neat form where every $N_e \equiv (P_{m^-} + P_{m^+})/2$ is determined based on the proven Goldbach theorem. Any large set of experiments may serve as additional instances to demonstrate the Goldbach theorem in general. The only constraint for the processing capability of AGTT is the limit of computer speed and memory space towards exhaustively decomposing the infinite sequence of mirror primes. Therefore, the inductive theorem and mathematical inferences as proven in Theorems 2 and 3 play more generic and rigorous roles for manipulating the infinite scope of mirror-prime decompositions problem beyond any empirical experiment towards infinite.

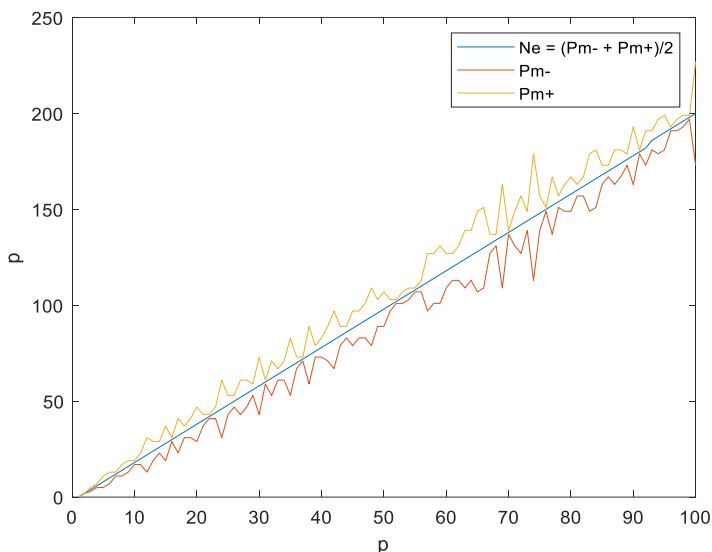


Fig. 3. Experimental results of Goldbach theorem for $\mathbb{P}_\mu^{100} = \mathbb{P}^{100} \times \mathbb{P}^{100}$ by Algorithm 1

The experiments have provided a visualization of the Goldbach Theorem, which empirically explain the nature of Goldbach conjecture. Figures 1 and 2 demonstrate there always exist at least one pair of mirror primes to decompose arbitrary even numbers in most of the testing cases according to Theorem 3. It is found that the expected pair of primes for satisfying the Goldbach theorem is not arbitrary primes, but merely those belong to the set of mirror primes. The Goldbach theorem and MPD theorem proven in this work have found many interesting applications including a deepened understanding of the nature and the recursive distribution patterns of primes, an expected fast recursive algorithm for primality testing, and a formal proof of the twin prime conjecture [30].

5. Summary

This work has presented a formal proof of Goldbach conjecture based on a discovery of mirror primes and their recursive properties. A theorem of mirror-prime decomposition for arbitrary even numbers has been established towards the formal proof of the Goldbach conjecture. The work has led to a new perception on the Goldbach theorem as an infinite recursive sequence in

$$\forall n_e \in \mathbb{N}_e \subset \mathbb{N} \text{ and } 1 \leq (k \in \mathbb{N}) \leq \frac{n_e}{2} - 1:$$

$$\mathbb{P}_\mu \subset \mathbb{P} \times \mathbb{P}$$

$$\exists p_{\mu^-}^{n_e/2} = (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) \in \mathbb{P}_\mu$$

$$= \bigcup_{n_e/2=4}^{\infty} \left\{ \bigcup_{k=1}^{\frac{n_e}{2}-2} \left(p_{\mu^-}^{n_e/2} = \frac{n_e}{2} - k, p_{\mu^+}^{n_e/2} = \frac{n_e}{2} + k \right) \mid (p_{\mu^-}^{n_e/2}, p_{\mu^+}^{n_e/2}) \in \mathbb{P}_\mu \right\}$$

satisfies $n_e \equiv p_{\mu^-}^{n_e/2} + p_{\mu^+}^{n_e/2} = \left(\frac{n_e}{2} - k\right) + \left(\frac{n_e}{2} + k\right).$

such that there exist at least a pair of mirror primes for any $n_e/2 \geq 4$ bounded by $1 \leq k \leq (n_e/2) - 2$ steps. Experiments using the algorithm of Goldbach theorem testing have empirically and visually demonstrated the Goldbach theorem in analytic number theory.

Acknowledgement

This work is supported by the Intelligent Mathematics Initiative of the International Institute of Cognitive Informatics and Cognitive Computing (I2CICI), the IEEE SMC Society Technical Committee on Brain-Inspired Cognitive Systems (TC-BCS) and the AutoDefence project of DND, Canada. The author would like to thank the anonymous reviewers for their valuable suggestions and comments.

References

- [1] Euclid (325-265 BC), *The Thirteen Books of Euclid's Elements*, Translated by T.L. Heath (1928), Dover, London, UK.
- [2] M. Kline (1972), *Mathematical Thought from Ancient to Modern Times*, Oxford Univ. Press, Oxford, UK.
- [3] M.D. Hendy (1975), Euclid and the Fundamental Theorem of Arithmetic, *Historia Mathematica*, 2:189–191.
- [4] T. Gowers, J. Barrow-Green and I. Leader eds. (2008), *The Princeton Companion to Mathematics*, Princeton University Press, NJ, USA.
- [5] Y. Wang (2021), Keynote: Emergence of Contemporary Abstract Sciences: From Intelligence, Knowledge, Information, Data Sciences to Intelligent Mathematics, *4th International Tokyo Conference on Innovative Studies of Contemporary Sciences* (TokyoSummit-IV), July, Tokyo, Japan, p.2.
- [6] GIMPS (2021), The Great Internet Mersenne Prime Search (GIMPS), <https://www.mersenne.org/>.
- [7] C. Goldbach (1742), A Letter to Leonhard Euler, https://en.wikipedia.org/wiki/Goldbach%27s_conjecture.
- [8] G.H. Hardy and J.E. Littlewood (1923), Some problems of 'Partitio numerorum'; III: On the Expression of a Number as a Sum of Primes, *Acta Math*, 44:1-70.
- [9] Y.V. Linnik (1951), Prime Numbers and Powers of Two, *Trudy Math. Isnt. Steklov*, 38(151): 152–169.
- [10] J. Pintz and I.Z. Ruzsa (2003), On Linnik's Approximation to Goldbach's Problem, I. *Acta Arith.*,109:169–194.
- [11] I. Henryk (1997), The Sieve of Eratosthenes – Legendre, *Annali della Scuola Normale Superiore di Pisa – Classe di Scienze*, Sér. 4(2):257–268. MR 453676.
- [12] K. Ramachandra and A. Sankaranarayanan (1997), Vinogradov's Three Primes Theorem, *Math. Student*, 66:1-4/27-72.
- [13] T. Estermann (1938), On Goldbach's Problem: Proof that Almost all Even Positive Integers are Sums of Two Primes, *Proceedings of the London Mathematical Society*, 2(44): 307-314.

- [14] J.R. Chen (1973), On the Representation of a Larger Even Integer as the Sum of a Prime and the Product of at Most Two Primes, *Sci. Sinica*, 16:157-176.
- [15] T. Tao (2006), Obstructions to Uniformity and Arithmetic Patterns in the Primes, *Pure Appl. Math.* 2: 199–217.
- [16] H.A. Helfgott (2014), *The Ternary Goldbach Conjecture is True*, arXiv:1312.7748, 1-79.
- [17] M.K. Sinisalo (1993), Checking the Goldbach Conjecture up to 4×10^{11} , *Mathematics of Computation*, American Mathematical Society, 61(204): 931–934.
- [18] T. Tao (2014), Every Odd Number Greater than 1 is the Sum of at most Five Primes, *Mathematics of Computation*, March, 83(286):997–1038.
- [19] A.W. Dudek (2017), On the Sum of a Prime and a Square-free Number, *The Ramanujan J.*, 42:233–240.
- [20] Y. Wang (2008), On the Big-R Notation for Describing Iterative and Recursive Behaviors, *International Journal of Cognitive Informatics and Natural Intelligence*, Jan., 2(1): 17-28.
- [21] V. Brun (1915), Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare, *Archiv for Mathematik og Naturvidenskab* (in German), 34 (8): 3–19.
- [22] H.G. Mairson (1977), Some New Upper Bounds on the Generation of Prime Numbers, *Communications of the ACM*, 20(9):664–669.
- [23] Y. Wang, F. Karray, S. Kwong, K.N. Plataniotis, H. Leung, M. Hou, E. Tunstel, I.J. Rudas, L. Trajkovic, O. Kaynak, J. Kacprzyk, M. Zhou, M.H. Smith, P. Chen, and S. Patel (2021), On the Philosophical, Cognitive and Mathematical Foundations of Symbiotic Autonomous Systems, *Phil. Trans. Royal Society (A): Math, Phys & Engg Sci.*, 379(219x), Oxford, UK.
- [24] D. Gries and J. Misra (1978), A Linear Sieve Algorithm for Finding Prime Numbers, *Communications of the ACM*, 21(12):999-1003.
- [25] P. Pritchard (1987), Linear Prime-Number Sieves: A Family Tree, *Sci. Compt. Program*, 9(1):17-35.
- [26] G. Greaves (2001), *Sieves in Number Theory*, Springer, Berlin: Springer.
- [27] B. Green and T. Tao (2006), Restriction Theory of the Selberg Sieve, with applications, *J. Theor. Nombres Bordeaux* 18(1):147–182.
- [28] Y. Wang (2008), RTPA: A Denotational Mathematics for Manipulating Intelligent and Computational Behaviors, *International Journal of Cognitive Informatics and Natural Intelligence*, April, 2(2):44-62.
- [29] PrimeBios (2021), <https://primes.utm.edu/bios/home.php>.
- [30] Y. Wang (2021), A Formal Proof of Twin Prime Conjecture in the $\mathbb{P} \times \mathbb{P}$ Space, *Communications of the American Mathematical Society*, submitted.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US