# New Understanding of Fundamental Theorem of Algebra and Goldbach's Conjecture

B. Zhang
Department of Mechanical Engineering, Saga University
1 Honjo-machi, Saga-shi, Saga 840-8502, Japan
e-mail: zhang@me.saga-u.ac.jp

**Abstract**

Goldbach's conjecture is proved through the new understanding of the fundamental theorem of algebra.

keywords: Fundamental theorem of algebra, Polynomial ideal, Polynomial equations, Hilbert's nullstellensatz, Bézout's identity, Goldbach's conjecture.

## 1 Introduction

I knew Goldbach's conjecture through the report about Chen Jingrun by Xu Chi [8] just before entering university. Goldbach's conjecture is one of the most beautiful problems in the history of mathematics. Constant effort has been being devoted to proof of the conjecture since it was proposed in 1742 [6, 5] , but not until 2013 was the weak conjecture proved[7], which is, however, not a peer-reviewed publication. It has been proved that the conjecture is true with quite high confidence [9, 4]. As a mechanical engineer, I cannot fully understand its importance and its difficulty as well. It is the ignorance that makes me challenge the task. Unlike engineering, mathematics is a solitary science which constantly makes me feel powerlessness. I like mathematics very much. I became an engineer only because I failed my entry examination of university in mathematics. Over 40 years' experiences in mechanical engineering encourage me to try the millennium problem.

Goldbach's conjecture states that every even integer greater than 4 can be expressed as the sum of two primes [6]. Goldbach's conjecture is beautiful because of its simplicity and the simpler the intension, the greater the extension. We can express primes [10], but the expression is so inefficient in computation that it is almost worthless. Because primes are not computable, Chen's theorem [2] may be the best result by using the sieve theory. The precision limitation of the sieve theory is destined not to give a complete proof of Goldbach's conjecture. A different method from the sieve theory is necessary to fully prove Goldbach's conjecture. The new path to proof of Goldbach's conjecture emerged of polynomial equations soon after I started to tackle the problem, but it spent a long time for me to find that the path is unpaved because I am nearsighted mathematically. The new understanding of fundamental theorem of algebra paves the path.

# 2 New Understanding of Fundamental Theorem of Algebra

## 2.1 Degrees of freedom

Let $k$ be a field, and $k[X] = k[x_1, \cdots, x_n]$ be the ring of polynomials in indeterminates $x_1, x_2, \cdots, x_n$ with coefficients in field $k$, which is written as follows

$$k[x_1, \cdots, x_n] = \sum_{e_1 e_2 \cdots e_n} a_{e_1 e_2 \cdots e_n} x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}, \tag{1}$$

where $a_{e_1 e_2 \cdots e_n}$ are numbers in $k$, and $e_j \in \mathbb{Z}_+$; $j = 1, 2, \cdots, n$. The exponent $e_j$ on an indeterminate $x_j$ in a term is called the order (to avoid confusion, instead of term "degree" , we use term "order" in the paper) of that indeterminate in that term; the order of the term is the sum of the orders of the indeterminates in that term, and the order of a polynomial is the largest order of terms in that polynomial.

$0[X]$ is the zero polynomial which is denoted by $0_p$. The zero polynomial is the only polynomial of which the order is undefined. For all polynomials $f(X) \in k[X]$ we have

$$f(X) = f(X) + 0_p. \tag{2}$$

Proper polynomials are the polynomials with defined order. $0_p$ is the only improper polynomial. The indeterminates of $0_p$ are also undefined. With no confusion, proper polynomials are simply called polynomials in the text.

Unit polynomial $1_p$ is unique, and is the only zero order polynomial except the difference in a proportional factor. Unit polynomial $1_p$ is also the only polynomials without zero, which is equivalent to the fundamental theorem of algebra. Also, for all polynomials $f(X) \in k[X]$ we have

$$f(X) = f(X)1_p. \tag{3}$$

Degrees of freedom (to avoid confusion, instead of term "dimension" , we use term "freedom" in the paper) of polynomial $f \in k[x_1, \cdots, x_n]$ are the set of indeterminates $x_1, \cdots, x_n$. The number of degrees of freedom of polynomial $f \in k[x_1, \cdots, x_n]$ is the number of indeterminates in the polynomial. $0_p$ has neither the defined degree of freedom, nor the defined number of degree of freedom. The number of degree of freedom for $1_p$ is zero. In other words, the degree of freedom for $1_p$ is null.

**Definition 2.1** (Constraint)**.** *For a polynomial $f(X) \in k[X] - \{0_p\}$, equation $f(X) = 0$ is a constraint.*

The number of degrees of freedom of a polynomial equation is the number of degrees of freedom of the polynomial subtracted by the number of the constraint. Therefore, the number of degrees of freedom of polynomial $f(x_1, x_2, \cdots, x_n)$ is $n$, while the number of degrees of freedom of polynomial $f(x_1, x_2, \cdots, x_n) = 0$ is $n - 1$.

The following statements hold.

1. The number of degrees of freedom of $0_p$ is not defined.
2. The number of constraint of $0_p = 0$ is zero.
3. The number of degrees of freedom of equation $0_p = 0$ is not defined.
4. The number of degrees of freedom of $1_p$ is zero.
5. The number of constraint of $1_p = 0$ is 1.
6. The number of degrees of freedom of equation $1_p = 0$ is $-1$.
7. Equation $1_p = 0$ has no solution.

## 2.2 New understanding of fundamental theorem of algebra

**Theorem 2.1** (Fundamental Theorem of Algebra [3, 1]). *Every polynomial $f(x) \in k[x]$ of order $\geq 1$ has a root in $\mathbb{C}$.*

There are several equivalent formulations of the theorem[3] as follows.

1. Every univariate polynomial of positive order with real coefficients has at least one complex root.
2. Every univariate polynomial of positive order with complex coefficients has at least one complex root.
3. Every univariate polynomial of positive order $n$ with complex coefficients can be factorized as $c(x - r_1) \cdots (x - r_n)$ where $c, r_1, \ldots, r_n$ are complex numbers.
4. Every univariate polynomial with real coefficients of order larger than 2 has a factor of order 2 with real coefficients.
5. Every univariate polynomial with real coefficients of positive order can be factored as $cp_1 \cdots p_k$ where $c$ is a real number and each $p_i$ is a monic polynomial of order at most 2 with real coefficients. Moreover, one can suppose that the factors of order 2 do not have any real root.

The new understanding of the fundamental theorem of algebra is as follows

**Corollary 2.1** (Fundamental Theorem of Algebra). *Polynomial $1_p$ is the only polynomial that has no root in $\mathbb{C}$.*

**Corollary 2.2.** *Improper polynomial $0_p$ is the only polynomial that has no constraint.*

## 2.3 Polynomial ideal

A polynomial ideal $I$ is a subset of a polynomial ring $k[X]$ such that
(a) if $h(X) \in k[X]$ and $f(X) \in I$ then $h(X)f(X) \in I$;
(b) if $f(X), g(X) \in I$ then $f(X) + g(X) \in I$.

**Definition 2.2** (Ideals of Polynomials). *Let polynomials $f_1(X), f_2(X), \cdots, f_m(X)$ be in $k[X]$. Ideal $I$ is a linear combination of $f_1(X), f_2(X), \cdots, f_m(X)$, which is written as follows*

$$I = \langle f_1(X), f_2(X), \cdots, f_m(X) \rangle = h_1(X)f_1(X) + h_2(X)f_2(X) + \cdots + h_m(X)f_m(X), \tag{4}$$

*where $h_1(X), h_2(X), \cdots, h_m(X) \in k[X]$ are arbitrary. The polynomials $f_1(X), f_2(X), \cdots, f_m(X)$ are called the generators of ideal $I$.*

All polynomial equations $f_j(X) = 0$ are the zeros of ideal $I$. $f_j(X) = 0$ are constraints, but the constraints may be pseudo.

Variety $V(f(X))$ of polynomial $f(X)$ is defined by

$$V(f(X)) = \{X | f(X) = 0\}, \tag{5}$$

and variety $V(I)$ of polynomial ideal $I = \langle f_1, f_2, \cdots, f_m \rangle \in k[X]$ is defined by

$$V(I) = \{X | g(X) = 0, \forall g(X) \in I\}. \tag{6}$$

It has been proved that

$$V(I) = \{X | f_j(X) = 0; j = 1, 2, \cdots, m\}. \tag{7}$$

The variety $V(I)$ of an ideal $I$ is definite by the ideal $I$, but the number of the member of the ideal $I$ is infinite. We may define the members of an ideal $I$ determining the variety $V(I)$ as the bases of the ideal. The bases of an ideal are definite. The ideal bases are always square free because multiplying a polynomial by itself does not change the variety. It seems absurd that the ideal bases may not be in the ideal because the generators of the ideal may not be square free. An ideal formed by square free generators is radical which is denoted by $\sqrt{I}$. We have $V\left(\sqrt{I}\right) = V(I)$ and $I\left(V\left(\sqrt{I}\right)\right) = \sqrt{I}$. Radical ideal and the variety are bijective. Square free generators are equivalent to the bases. The ideal $I$ generated by square free generators is equivalent to the radical ideal $\sqrt{I}$, that is, $I = \sqrt{I}$.

Let $V(f)$ and $V(I)$ be the varieties of polynomial $f(X) \in k[X]$ and polynomial ideal $I$, respectively. Then the following statements are true.

1.
$$V(f_1, f_2, \cdots, f_m) = V(f_1) \cap V(f_2) \cap \cdots V(f_m). \tag{8}$$

2.
$$V(f, 0_p) = V(f) \cap V(0_p) = V(f). \tag{9}$$

3. The variety of $0_p$ is not defined
$$V(0_p) = \forall, \tag{10}$$
where $\forall$ is for any set.

4.
$$V(f, 1_p) = V(f) \cap V(1_p) = \emptyset. \tag{11}$$
This is the weak Hilbert's Nullstellensatz.

5.
$$V(f_1 * f_2 * \cdots f_m) = V(f_1) \cup V(f_2) \cup \cdots V(f_m). \tag{12}$$

6.
$$V(f) = V(f * 1_p) = V(f) \cup V(1_p). \tag{13}$$

7. $1_p$ is the only polynomial without zeros. This is the fundamental theorem of algebra.
$$V(1_p) = \emptyset. \tag{14}$$

8. Let $\langle f_1, f_2, \cdots, f_m \rangle \in k[X]$ be an ideal. If $1_p \in \{f_1, f_2, \cdots, f_m\}$, then $\langle f_1, f_2, \cdots, f_m \rangle = \langle 1_p \rangle$.

9. Let $N_F(I)$ be the number of degrees of freedom of ideal $I$. If $N_F(I) = -1$, then $V(I) = \emptyset$ in $\mathbb{C}$. If $N_F(I) = 0$, $V(I)$ is finite in number in $\mathbb{C}$. If $N_F(I) \geq 1$, $V(I) \in C^{N_F(I)}$ in $\mathbb{R}$.

10. The minimum degrees of freedom of all polynomial ideals $I \in k[X]$ is $N_F(I)_{min} = -1$ in $\mathbb{C}$.

## 2.4 Hilbert's nullstellensatz

**Theorem 2.2** (Hilbert's Nullstellensatz [11]). *Let $k$ be a field. Consider ideal $I =< f_1, f_2, \cdots, f_m >\in k[x_1, \ldots, x_n]$ and variety $\mathrm{V}(I)$. Hilbert's Nullstellensatz states that if $f \in k[x_1, \ldots, x_n]$ that $\mathrm{V}(I) \subseteq V(f)$, then there exists a natural number $\mu$ such that $f^\mu \in I$.*

*Proof.* Let $s(X) \in I$. If $V(s(X)) = V(f(X))$, then the radicals of $s(X)$ and $f(X)$ are equal. That is to say

$$s(X) = \prod_{\forall j} u_j(X)^{\lambda_j}, \tag{15}$$

and

$$f(X) = \prod_{\forall j} u_j(X)^{\beta_j}, \tag{16}$$

where $\lambda_j \in \mathbb{N}$ and $\beta_j \in \mathbb{N}$, and $u_j(X)$ is prime polynomial over field $k$. If

$$\mu = \mathrm{lcm}_{\forall j}(\lambda_j), \tag{17}$$

then $f^\mu \in I$. □

**Theorem 2.3** (Weak Hilbert's Nullstellensatz). *Let $k$ be a field. Consider the polynomial ring $k[x_1, \ldots, x_n]$ and let $I$ be an ideal in this ring and $\mathrm{V}(I)$ be the variety of $I$. $1_p \in I$ if and only if $V(I) = \emptyset$.*

*Proof.* The new understanding of the fundamental theorem of algebra states that $V(I) = \emptyset \Leftrightarrow 1_p \in I$. □

## 2.5 Bézout's identity

**Theorem 2.4** (Bézout's Identity for Polynomials with Degree 1 [12, 13]). *Let $f(x)$ and $g(x)$ be any two polynomials with degree 1. The greatest common divisor (common zeros) $d(x)$ of $f(x)$ and $g(x)$ may be expressed by a linear combination of $f(x)$ and $g(x)$.*

*Proof.* That $f(x)/d(x)$ and $g(x)/d(x)$ are prime to each other means that $f(x)/d(x)$ and $g(x)/d(x)$ have no common zeros. According to the fundamental theorem of algebra, $1_p \in \langle f(x)/d(x), g(x)/d(x)\rangle$. □

**Corollary 2.3** (Bézout's Identity for Polynomials with Degree 1). *Let $f(x)$ and $g(x)$ be any two polynomials with degree 1. $f(x)$ and $g(x)$ are prime to each other if and only if $1_p \in \langle f(x), g(x)\rangle$.*

If there exists the greatest common divisor in $f(x)$ and $g(x)$, the two equations are combined into one equation of the common divisor $d(x) = 0$, and the number of the constraint is reduced from 2 to 1. If $f(x)$ and $g(x)$ are prime to each other, the two equations are contradictory equations. There are no common zeros for contradictory equations.

**Theorem 2.5** (Inverse Bézout's Identity for Polynomials with Degree 1). *Let $f(x)$, $g(x)$, $d(x)$, $a(x)$ and $b(x)$ be polynomials of degree 1 in $k[x]$ and $d(x) = a(x)f(x) + b(x)g(x)$. If $\max(N_a + N_f, N_b + N_g) < 2N_d \leq 2\min(N_f, N_g)$ then $d(x)$ is the greatest common divisor of $f(x)$ and $g(x)$, where $N_f, N_g, N_d, N_a$ and $N_b$ are the orders of polynomials $f(x)$, $g(x)$, $d(x)$, $a(x)$ and $b(x)$, respectively .*

*Proof.* $d(x)$ is a linear combination of $f(x)$ and $g(x)$ as follows

$$d(x) = a(x)f(x) + b(x)g(x). \tag{18}$$

Because the order of $d(x)$ is not greater than that of $f(x)$ and $g(x)$, we have

$$f(x) = q_f(x)d(x) + r_f(x), \tag{19}$$

and

$$g(x) = q_g(x)d(x) + r_g(x). \tag{20}$$

Substituting equations into equation gives

$$\begin{aligned} d(x) &= a(x)\left[q_f(x)d(x) + r_f(x)\right] + b(x)\left[q_g(x)d(x) + r_g(x)\right] \\ &= \left[a(x)q_f(x) + b(x)q_g(x)\right]d(x) + a(x)r_f(x) + b(x)r_g(x). \end{aligned} \tag{21}$$

Because the order of $a(x)r_f(x) + b(x)r_g(x)$ is lower than the order of $d(x)$, $a(x)r_f(x) + b(x)r_g(x)$ is the remainder. Therefore, there must be

$$a(x)r_f(x) + b(x)r_g(x) = 0_p. \tag{22}$$

$d(x)$ is the greatest common divisor of $f(x)$ and $g(x)$.

□

Bézout's identity may be extended to polynomials with degree $n > 1$. Let $f(X)$ and $g(X)$ be any two polynomials with degree $n > 1$.

Before discussing polynomials with degree $n > 1$, we would like to introduce a rational function which is defined as

$$r(X) = \frac{f(X)}{g(X)}, \tag{23}$$

where $f(X)$ and $g(X)$ are polynomials in $k[X]$. Rational functions constitute a field $k(X)$.

**Theorem 2.6** (Bézout's Identity for Polynomials with Degree $n > 1$)**.** *Let $f(X)$ and $g(X)$ be any two polynomials in a polynomial ring $k[X]$ with degree n, and $d(X)$ is the greatest common divisor of $f(X)$ and $g(X)$. There exists a linear combination of $f(X)$ and $g(X)$ so that $d(X) = a(X)f(X) + b(X)g(X)$ where $a(X)$ and $b(X)$ are in $k(X - \{x_i\})[x_i]$.*

*Proof.* For polynomials $f(X)$ and $g(X)$ in $k[X]$, we have

$$k[X] = k[X - \{x_i\}][x_i] \subset k(X - \{x_i\})[x_i]. \tag{24}$$

□

Equations with the greatest common divisor $d(X)$ are combined into one constraint $d(X) = 0$.

**Theorem 2.7** (Bézout's Identity for Polynomials with Degree $n > 1$)**.** *Let $f(X)$ and $g(X)$ be any two polynomials in a polynomial ring $k[X]$ with degree n. At least one indeterminate $x_i$ can be eliminated by a linear combination of $f(X)$ and $g(X)$, that is, there is $c(X - \{x_i\}) = a(X)f(X) + b(X)g(X)$, if $f(X)$ and $g(X)$ are prime to each other.*

*Proof.* For coprime polynomials $f(X)$ and $g(X)$ in $k[X]$, we have

$$1_p = u(X)f(X) + u(X)g(X). \tag{25}$$

Let $c(X - \{x_i\})$ be the least common denominator of $u(X) \in k(X - \{x_i\})[x_i]$ and $v(X) \in k(X - \{x_i\})[x_i]$. We have

$$c(X - \{x_i\}) = \left[u(X)c(X - \{x_i\})\right] f(X) + \left[v(X)c(X - \{x_i\})\right] g(X). \tag{26}$$

Now, $a(X) = u(X)c(X - \{x_i\})$, $b(X) = v(X)c(X - \{x_i\}) \in k[X]$. $x_i$ is eliminated in $c(X - \{x_i\})$. □

Unsquare the greatest common multiple $c(X - \{x_i\})$, and then add it into the basis of the ideal $\langle f(X), g(X)\rangle$. If $c(X - \{x_i\}) = c(\emptyset)$, then the polynomials have no common zeros.

Now let us consider the pair-wise prime polynomials with degree 3 $(X) = (x_1, x_2, x_3)$ as follows

$$\begin{aligned} f_1(X) &= 0, \\ f_2(X) &= 0, \\ f_3(X) &= 0. \end{aligned} \tag{27}$$

The first elimination gives

$$\begin{aligned} c_1(x_1, x_2) &= a_1(X)f_1(X) + b_1(X)f_2(X), \\ c_2(x_1, x_2) &= a_2(X)f_1(X) + b_2(X)f_3(X). \end{aligned} \tag{28}$$

If there is $c_1(x_1, x_2) = c_1(\emptyset)$ or $c_2(x_1, x_2) = c_2(\emptyset)$, there are no common zeros among $f_1, f_2$ and $f_3$. If there is $c_1(x_1, x_2) = c_1(x_1)$ or $c_2(x_1, x_2) = c_2(x_1)$, the elimination is terminated and the solution is completed. $c_1(x_1, x_2)$ and $c_2(x_1, x_2)$ must be prime to each other. Otherwise, if $c_1(x_1, x_2)$ and $c_2(x_1, x_2)$ have the greatest common multiple $d(x_1, x_2)$, then equations (28) become

$$\begin{aligned} d(x_1, x_2)h_1(x_1, x_2) &= a_1(X)f_1(X) + b_1(X)f_2(X), \\ d(x_1, x_2)h_2(x_1, x_2) &= a_2(X)f_1(X) + b_2(X)f_3(X). \end{aligned} \tag{29}$$

From equations (29), we have

$$\begin{aligned} &d(x_1, x_2)h_1(x_1, x_2)b_2(X)f_3(X) - d(x_1, x_2)h_2(x_1, x_2)b_1(X)f_2(X) \\ &\quad = a_1(X)f_1(X)b_2(X)f_3(X) \\ &\qquad - a_2(X)f_1(X)b_1(X)f_2(X). \end{aligned} \tag{30}$$

That is

$$\begin{aligned} &d(x_1, x_2)\left[h_1(x_1, x_2)b_2(X)f_3(X) - h_2(x_1, x_2)b_1(X)f_2(X)\right] \\ &\quad = f_1(X)\left[a_1(X)b_2(X)f_3(X)\right. \\ &\qquad \left. -a_2(X)b_1(X)f_2(X)\right]. \end{aligned} \tag{31}$$

Because $f_2(X)$ and $f_3(X)$ are coprime, there is uniquely

$$c_3(x_1, x_2) = a_3(X)f_2(X) + b_3(X)f_3(X). \tag{32}$$

If the order of $x_1$ or $x_2$ in $d(x_1, x_2)$ is not zero, then

$$d(x_1, x_2) = c_3(x_1, x_2) \tag{33}$$

and

$$f_1(X) = h_1(x_1, x_2)b_2(X)f_3(X) - h_2(x_1, x_2)b_1(X)f_2(X). \tag{34}$$

Equation (34) contradicts that $f_1(X)$, $f_2(X)$ and $f_3(X)$ are pair-wise prime. Therefore, there must be $d(x_1, x_2) = d(\emptyset)$. $c_1(x_1, x_2)$ and $c_2(x_1, x_2)$ are coprime.

The elimination is contiued as follows

$$g(x_1) = u(x_1, x_2)c_1(x_1, x_2) + v(x_1, x_2)c_2(x_1, x_2). \tag{35}$$

The elimination is terminated. This leads to the following theorem.

**Theorem 2.8** (Effective Constraint)**.** *For a polynomial equation system, the pair-wise prime polynomials or the greatest common multiples are the effective constraints.*

# 3 Goldbach's Conjecture

Let $\mathbb{P}_n$ be prime number set not larger than a given positive number $n$, and $\pi(n)$ be the number of elements of $\mathbb{P}_n$.

Let $\mathbb{M}_n$ be the prime factors of number $n$, and $\omega(n)$ be the number of element of $\mathbb{M}_n$.

Let $\mathbb{M}_n^d = \mathbb{P}_n$ - $\mathbb{M}_n$, and $\rho(n)$ be the number of elements of the difference set $\mathbb{M}_n^d$.

**Theorem 3.1** (The Fundamental Theorem of Arithmetic[14])**.** *Every number $n > 1$ can be written uniquely as a product of primes as follows*

$$n = \prod_{i=1}^{\omega(n)} p_i^{\alpha_i} \qquad \alpha_i \geq 1 \qquad p_i \in \mathbb{M}_n. \tag{36}$$

The fundamental theorem of arithmetic leads to the following partition lemma.

**Corollary 3.1** (Prime Partition of Number)**.** *Let the difference set $\mathbb{M}_n^d$ be $\{q_1, q_2, \cdots, q_{\rho(n)}\}$. Then every number $n \geq 3$ is uniquely partitioned into a given prime $q_k \in \mathbb{M}_n^d \neq \emptyset$ and a production of primes as follows*

$$n = \prod_{\substack{i=1 \\ \sigma_i \neq k}}^{\rho(n-q_k)} q_{\sigma_i}^{\beta_{k,\sigma_i}} + q_k \qquad q_{\sigma_i}, q_k \in \mathbb{M}_n^d, \qquad \beta_{k,\sigma_i} \geq 1 \qquad k = 1, 2, \cdots, \rho(n). \tag{37}$$

*Proof.* For $q_k \in \mathbb{M}_n^d$ and $n - q_k > 1$, the fundamental theorem of arithmetic tells that the number $n - q_k$ is uniquely expressed as

$$n - q_k = \prod_{i=1}^{\rho(n-q_k)} t_i^{\alpha_i} \qquad t_i \in \mathbb{P}_{n-q_k} \subseteq \mathbb{P}_n. \tag{38}$$

Now we prove that $\forall t_i \in \mathbb{M}_n^d$. By contradiction presume that $\exists t_i \in \mathbb{M}_n$, say $t_*$. This means that $t_*$ divides $n$. On the other hand, we have

$$n - q_k = t_*^{\alpha_*} \prod_{i=1, i\neq *}^{\rho(n-q_k)} t_i^{\alpha_i}, \tag{39}$$

which leads to that $t_*$ divides $q_k$. This is not true because $q_k$ is a prime. Therefore equation (37) holds.

Equation (37) may include that

$$n = \prod_{i=1}^{\rho(n-1)} q_{\sigma_i}^{\beta_{k,\sigma_i}} + 1. \tag{40}$$

For $n - q_k = 1$ we have

$$n = 1 + q_k. \tag{41}$$

□

Goldbach's conjecture states that

**Conjecture 3.1** (Goldbach's Conjecture)**.** *Even number* $2n \geq 4$ *can be partitioned as follows*

$$2n = r_i + q_i \qquad i = 1, 2, \cdots, \rho^*, \tag{42}$$

*where*

$$r_i = \prod_{\substack{l=1 \\ \sigma_l \neq i}}^{\rho(2n-q_i)} q_{\sigma_l}^{\gamma_{i,\sigma_l}}, \qquad q_{\sigma_l}, q_i \in \mathbb{M}_n^d \setminus 2, \qquad \sum_{\sigma_l} \gamma_{i,\sigma_l} \geq 2, \tag{43}$$

*which is call remainder term, and at least for one* $q_i$

$$r_i = q^*, \tag{44}$$

*where* $q^* > n$ *is a prime, and*

$$\rho^* = \rho(n) - (1 - (-1)^n)/2. \tag{45}$$

Now let us prove Goldbach's conjecture (3.1).

*Proof.* By contradiction, we assume that, for all $q_i$, we have

$$2n = \prod_{\substack{l=1 \\ \sigma_l \neq i}}^{\rho(2n-q_i)} q_{\sigma_l}^{\gamma_{i,\sigma_l}} + q_i \qquad i = 1, 2, \cdots, \rho^*, 2 < q_i < n, \tag{46}$$

where $\rho(2n - q_i) \geq 2$.

In addition, as a special case $q_0 = 1$, we have

$$2n = \prod_{l=1}^{\rho(2n-1)} q_{\sigma_l}^{\gamma_{0,\sigma_l}} + 1. \tag{47}$$

We now take equations (46) and (47) as an equation system for indeterminates $q_i$ with known exponents $\gamma_{i,\sigma_l}$.

Without confusion, equations (47) and (46) may be rewritten as follows,

$$f_i = \prod_{\substack{l=1 \\ l \neq i}}^{K} q_l^{\gamma_{i,l}} + q_i - 2n \;\; i = 1, 2, \cdots, K, \tag{48}$$

$$f_0 = \prod_{l=1}^{K} q_l^{\gamma_{0,l}} + 1 - 2n, \tag{49}$$

where $K = \rho^* \geq 2$. Here we have

$$\begin{gathered} \sum_{l=1, l \neq i}^{K} \gamma_{i,l} \geq 2, \\ q_1 < q_2 < \cdots q_{K-1} < q_K. \end{gathered} \tag{50}$$

Zeros of polynomials (48, 49) are the anti-Goldbach conjecture equations.

Because we can always eliminate $q_k$ from two different polynomials $f_i, f_j$ including indeterminate $q_k$, $f_i$ and $f_j$ are coprime. The number of effective constrains is $K+1$, and the number of degrees of freedom of ideal $\langle f_0, f_1, \ldots, f_K \rangle$ is -1. There are no common zeros in the ideal $\langle f_0, f_1, \ldots, f_K \rangle$. Goldbach's conjecture is proved.

□

# 4 Conclusion

Goldbach's conjecture has been proved through the new understanding of the fundamental theorem of algebra.

# References


[1] Campesato J-B. 14 - Zeroes of analytic functions (PDF). MAT334H1-F – LEC0101, Complex Variables, University of Toronto, 2020-9, retrieved 2024-09-05.

[2] Chen J R. 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, 1973, 157–176.

[3] Dunham W. Euler and the fundamental theorem of algebra (PDF). The College Journal of Mathematics, 22 (4), 1991-9, 282–293, doi:10.2307/2686228, JSTOR 2686228.

[4] Estermann T. On Goldbach's problem: proof that almost all even positive integers are sums of two primes. Proc. London Math. Soc.. 2 44, 1938, 307–314. doi:10.1112/plms/s2-44.4.307.

[5] Euler L. Letter XLIV, Euler to Goldbach (PDF). Correspondence of Leonhard Euler. Mathematical Association of America. 30 June 1742. Retrieved 2025-01-19.

[6] Goldbach C. Letter XLIII, Goldbach to Euler. Correspondence of Leonhard Euler. Mathematical Association of America. 7 June 1742. Retrieved 2025-01-19.

[7] Helfgott H A. Major arcs for Goldbach's theorem. arXiv:1305.2897 [math.NT], 2013.

[8] Shi Xingze. China Writers' Association. Retrieved 4 October 2019.

[9] Van der Corput J G. Sur l'hypothèse de Goldbach. Proc. Akad. Wet. Amsterdam 41, 1938, 76–80.

[10] Willans C P. On formulae for the nth prime number. The Mathematical Gazette 48 (366), 1964-12, 413-415, doi:10.2307/3611701, ISSN 0025-5572, JSTOR 3611701.

[11] Zariski O, Samuel P. Commutative Algebra, Vol. II, Springer Berlin, Heidelberg, 1960, Ch. VII, Theorem 14, doi:10.1007/978-3-662-29244-0, ISSN 0072-5285.

[12] Bézout É. Théorie générale des équations algébriques. Paris, France: Ph. D. Pierres, 1779.

[13] Tignol J-P. Galois' Theory of Algebraic Equations. Singapore: World Scientific, 2001. ISBN 981-02-4541-6.

[14] Hardy G H, Wright E M. An Introduction to the Theory of Numbers. 5th ed. Oxford, England: Clarendon Press, 1979, pp. 2-3.