Proceedings of CONF-CIAP 2026 Symposium: Applied Mathematics and Statistics
DOI: 10.54254/2753-8818/2026.CH30671

Analysis of the Related Corollaries, Concepts, and Impacts of the Fundamental Theorem of Arithmetic in Number Theory and Abstract Algebra

Wenbo Tang

Soochow Foreign Language School, Suzhou, China
wenbotang@appmail.cn

Abstract. The Fundamental Theorem of Arithmetic (FTA), first formalized in Euclid's Elements around 300 BCE, established the foundation for classical number theory, composed around 300 BCE. The principle of unique factorization later became central to the rise of modern mathematics. In the mid-19th century, mathematicians such as J.W.R. Dedekind and D. Hilbert extended number-theoretic questions into quadratic fields and rings of algebraic integers, creating the foundations of algebraic number theory. Steinitz's work in the early twentieth century of 1910 further generalized algebraic structures, marking the beginning of abstract algebra as an independent field. The purpose of this essay is to examine the Fundamental Theorem of Algebra's proof. and applies it to several representative problems in elementary number theory. It then extends to related corollaries and conceptual developments of unique factorization, including notable cases in non-unique factorization rings where the property does not hold. Finally, it introduces approaches grounded in properties of the FTA that have been applied to the ongoing study of major open problems, including the Goldbach Conjecture. Overall, through both review and mathematical analysis, the paper shows that the structural foundation provided by the FTA underlies the verification and proof of many of the most difficult results and open conjectures in mathematics, including Fermat's Last Theorem and the Goldbach Conjecture.

Keywords: FTA, Algebraic Number Theory, Abstract Algebra, Dedekind's Unique Factorization Theorem, Goldbach Conjecture

1. Introduction

The Fundamental Theorem of Arithmetic (FTA) can be stated as follows: For every integer $a > 1$, if a is composite, then a can be uniquely expressed as a product of a finite number of prime numbers., that is

$$\alpha = \exists \prod_{i=1}^{n} p_i^{b_i} \tag{1}$$

DOI: 10.54254/2753-8818/2026.CH30671

and $P_1 < P_2 < P_3 < \ldots\ldots < P_n$ where each piis a prime number and each exponent biis a positive integer, and $1 \le i \le n$

However, in the set $Z\left[\sqrt{-5}\right] = \left\{\alpha = a + b\sqrt{-5} : a, b \in Z\right\}$ the FTA does not hold, and the detailed derivation will be presented later in this paper. The strong Goldbach Conjecture can be stated as: For any even integer β with $\beta > 2$, it is equal to the sum of two prime numbers. As for the weak Goldbach conjecture, it is merely a corollary of the former and thus will not be elaborated upon here. Since 1966, when Chinese mathematician Chen Jingrun proved the "1+2" result, there have been few major breakthroughs [1]. On the other hand, the weak Goldbach conjecture was proven in 2013 by Peruvian mathematician Harald Helfgott [2]. In this paper, following a review and mathematical summary of the relevant concepts, corollaries, and theorems of the FTA in number theory and abstract algebra, we draw on the unique factorization property to provide insights that may assist scholars in their study of the strong Goldbach Conjecture. This work may thus offer a new perspective for future researchers on the strong Goldbach conjecture.

2. Different proofs of the FTA and the problems they resolve

2.1. Proof of the FTA and basic consequences

To prove the FTA, it demonstrate the existence and uniqueness of the factorization

$$\int(P) = \alpha = \exists \prod_{i=1}^{n} p_i^{b_i} \tag{2}$$

We begin by proving its existence.

Prove:

Assume, for contradiction, that the FTA fails $\alpha = \min\{Z\} \Rightarrow$ FTA. Then regarding every composite integer α :

$$\exists n, \frac{\alpha}{n} \in Z \wedge 1 < n, \frac{\alpha}{n} < \alpha \Rightarrow \alpha = n \times \frac{\alpha}{n} \tag{3}$$

By the assumption, its proper divisors n and $\frac{\alpha}{n}$ can each be included in a prime number product. Substituting these prime factorizations into the product expression for $\alpha = n \times \frac{\alpha}{n}$, we obtain a prime factorization of α as well. This contradicts the assumption that α cannot be written as a primary product. Hence the proof is complete.

Theorem 1. For any integer $\alpha \in \mathbb{Z}$ with $\alpha > 1$ can be expressed as a prime or as a product of a finite number of primes.

Lemma 1. If P is a number which is prime and $P|mn$ then P | m or P | n.

On the basis of Theorem 1 and Lemma 1, We can now demonstrate the prime factorization's uniqueness in the FTA.

Assume that there exist:

$$a = min\{Z\} \Rightarrow a = p_1 \times p_2 \times p_3 \times \ldots\ldots \times p_n = q_1 \times q_2 \times q_3 \times \ldots\ldots \times q_m, q, p \tag{4}$$

is a prime number

DOI: 10.54254/2753-8818/2026.CH30671

$$p_1|(q_1)(q_2q_3.....q_m) \tag{5}$$

Follow by lemma 2.1 we know that

$$p_1|q_1 \vee p_1|q_2q_3.....q_m \tag{6}$$

Thus,

$$p_1 = q_1 \vee p_1 = q_i(2 \leq i \leq m, i \in k) \tag{7}$$

In either case, this implies that there exists a smaller integer β which can be stated in two different ways as a product of primes.The idea that α is the smallest such integer is refuted by this.. Hence the proof is complete.

There are multiple methods for proving the existence of an FTA [3-5]. This paper discusses only focuses on proof by contradiction, though the overall objective remains to demonstrate both its existence and uniqueness. The following sections present several corollaries related to the FTA.

Corollary 1.

Let any

$$\alpha = \exists \prod_{i=1}^{n} p_i^{b_i}, a > 1 \wedge a \in Z \tag{8}$$

be the prime factorization of α . Then any divisor d of α can be written as

$$d =, b_i \geq \gamma_i \geq 0 \tag{9}$$

2.2. Applications of the FTA

2.2.1. Using the FTA to determine the most common factor and smallest common multiple

The most common factor and smallest common multiple can be calculated in a number of ways, such as Euclidean algorithm and its variants. Here, adopting the Fundamental Theorem of Arithmetic and its corollaries to carry out these computations. We begin by stating the relevant theorem.

Corollary 2.

Let

$$m, n \in \mathbb{Z}^+, m = \prod_{i=1}^{n} P_i^{a_i}, n = \prod_{i=1}^{n} P_i^{b_i} \wedge a_i, b_i \geq 0 \tag{10}$$

Then,

$$(m, n) = \prod_{i=1}^{n} p_i^{min(a_i, b_i)}, [m, n] = \prod_{i=1}^{n} p_i^{max(a_i, b_i)} \tag{11}$$

DOI: 10.54254/2753-8818/2026.CH30671

Lemma 2.

$$m,n \in Z^+, (m,n) = p \wedge [m,n] = q \Leftrightarrow mn = pq \tag{12}$$

With this preparation, we can now compute the biggest common factor and the least common multiple, which results the Theorem 2.

Proof. Let $\gamma_i = \min(a_i, b_i)$ and $\delta_i = \max(a_i, b_i)$. Obviously,

$$\prod_{i=1}^{n} p_i^{a_i} \mid mand \prod_{i=1}^{n} p_i^{b_i} \mid n \Rightarrow \prod_{i=1}^{n} p_i^{\gamma_i} \mid (m,n) \tag{13}$$

Thus,

$$\prod_{i=1}^{n} p_i^{\gamma_i} \leq (m,n) \tag{14}$$

Assume

$$(m,n) = \prod_{i=1}^{n} p_i^{s_i} \Rightarrow s_i \leq min(a_i, b_i) \Rightarrow (m,n) \leq \prod_{i=1}^{n} p_i^{\gamma_i} \tag{15}$$

Therefore,

$$(m,n) = \prod_{i=1}^{n} p_i^{\gamma_i} \tag{16}$$

Based on the presumption,

$$\gamma_i + \delta_i = a_i + b_i \Rightarrow min(a_i, b_i) + max(a_i, b_i) = a_i + b_i \tag{17}$$

Since

$$mn = \prod_{i=1}^{n} p_i^{a_i + b_i} \tag{18}$$

Lemma 2 gives us

$$\prod_{i=1}^{n} p_i^{\delta_i} = [m,n] \tag{19}$$

2.2.2. Using the FTA to prove the infinitude of primes

We adopt the classical method of proof by contradiction.

Proof. It is clear that $2 = \min\{p\}$ is prime, so there is at least one prime number. Suppose, for contradiction, that there are only finitely many primes, and list as p1, p2, …, pn.

Consider the natural number

DOI: 10.54254/2753-8818/2026.CH30671

$$N = 1 + p_1 p_2 \cdots p_n \tag{20}$$

Since $N > 1$, it must have a prime divisor m. Then $m \mid N$, and because m is among the primes $p_1, p_2, \ldots, p_n$, we also have $m \mid p_1 p_2 \cdots p_n$. Hence

$$m \mid (N - p_1 p_2 \cdots p_n) = 1 \tag{21}$$

which is impossible because any prime $m \geq 2$. This contradiction shows that the primes cannot be finite in number. Hence the proof is complete.

3. Concepts, theorems, and corollaries derived from the FTA

3.1. Definition, properties, and applications of unique factorization domains

We begin with the definition of a unique factorization domain (UFD). A ring R is called a UFD if R is an integral domain in which factorization exists and is a unique properties that closely parallel those in the Fundamental Theorem of Arithmetic.

More precisely, the existence property states that every nonzero non-unit element $m \in R$ can be expressed as an irreducible element's finite product:

$$m = p_1 p_2 \cdots p_n, p_i irreducible \tag{22}$$

Such a factorization is unique up to ordering and associates, according to the uniqueness property; that is, if

$$m = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_s \tag{23}$$

then $s = n$, and after reordering, each p_i is associated to the corresponding q_i (i.e., $p_i \sim q_i$ for all i).

$$m = p_1 \times p_2 \times p_3 \times \ldots\ldots \times p_n = q_1 \times q_2 \times q_3 \times \ldots\ldots \times q_n, p_n \sim q_n \tag{24}$$

About UFD, A unique factorization domain R possesses the three important properties:

1). Every prime element in R is irreducible. However, the converse does not necessarily hold in a general integral domain that is not a UFD. For instance, the ring $Z\left[\sqrt{-5}\right] = \left\{\alpha = a + b\sqrt{-5} : a, b \in Z\right\}$ provides a counterexample in which irreducible elements need not be prime.

2). For any two elements that are nonzero in R, a greatest common divisor exists (unique up to associates).

3). The $R[x]$ is a UFD polynomial ring, if R is likewise a UFD.

The simplest application of a UFD arises in the ring of integers, where the Fundamental Theorem of Arithmetic provides one foundational tool in number-theoretic arguments. More generally, when the algebraic integers' ring in a number field happens to be a UFD, a natural extension of $\mathbb{Z}$, many simplifications familiar from elementary number theory continue to hold. For example, questions

DOI: 10.54254/2753-8818/2026.CH30671

concerning common divisors or factorization in classical Diophantine problems, including those related to Fermat-type equations, can be handled by applying prime factorization's uniqueness.

However, in most number fields, the ring of integers fails to be a UFD, and the distinction between prime and irreducible elements becomes problematic. Consequently, factorization at the level of elements is no longer a reliable tool. To address this obstruction, Dedekind introduced the unique factorization of ideals, allowing the restoration of a factorization theory in these settings. This ideal-theoretic approach will be examined in the following sections.

3.2. Euclidean domains: definition, properties, and applications

Compared with unique factorization domains, Euclidean domains (EDs) are particularly effective for computation because they support a generalized form of division with remainder. Formally, if a Euclidean function exists, an integral domain R is referred to be a Euclidean domain.

$$\varphi : R \setminus 0 \to \mathrm{N} \tag{25}$$

such that for any $\mathrm{m}, \mathrm{n} \in \mathrm{R}$ with $\mathrm{n} \neq 0$, one can write

$$m = nq + r \tag{26}$$

where either $\mathrm{r} = 0$ or $\varphi(\mathrm{r}) < \varphi(\mathrm{n})$.

In other words, Euclidean domains generalize the familiar modular division of integers to broader algebraic settings. Typical examples include the ring of integers $\mathbb{Z}$, the polynomial ring $\mathrm{F}[\mathrm{x}]$ over a field F, and the Gaussian integers $\mathbb{Z}[\mathrm{i}]$, where the Euclidean function is chosen in a way compatible with the division algorithm in each context. These settings illustrate how the computational strengths of EDs naturally extend from integers to polynomials and certain complex integer rings.

Euclidean domains also satisfy a key structural hierarchy:

$$\text{Euclidean domain} \Rightarrow \text{principal ideal domain (PID)} \Rightarrow \text{unique factorization domain (UFD)}$$

Therefore, every Euclidean domain is both a PID and, consequently, a UFD. All benefits of unique factorization discussed in Section 3.1 naturally apply here, while the additional presence of a division algorithm further enhances practical computation in number-theoretic and algebraic settings.

4. Situations where the FTA fails

4.1. The ring $\mathbb{Z}[\sqrt{-5}]$

In the ordinary ring of integers $\mathbb{Z}$, the FTA has no counterexamples. Therefore, to see the failure of unique factorization one must pass to other number rings. A classical example is the ring: $\mathrm{R} = \mathbb{Z}\left[\sqrt{-5}\right] = \left\{\mathrm{a} + \mathrm{b}\sqrt{-5} \ : \ \mathrm{a}, \mathrm{b} \in \mathbb{Z}\right\}$. Here we call an element irreducible if it cannot be expressed as the product of two nonunits. (parallels the notion of a prime number in $\mathbb{Z}$). In R we

DOI: 10.54254/2753-8818/2026.CH30671

have the factorization $6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$, which already suggests non-uniqueness. In order to turn this into a proof, it suffices to show that the four factors $2,\ 3,\ 1+\sqrt{-5},\ 1-\sqrt{-5}$ are irreducible and that no two of them are associates. Consider the norm $N : R \to \mathbb{N}$ given by $N\left(a+b\sqrt{-5}\right) = a^2+5b^2$. It is multiplicative: $N(xy) = N(x)N(y)$, and $N(u) = 1$ iff u is a unit (± 1). We compute $N\left(2\right) = 4, N\left(3\right) = 9, N\left(1\pm\sqrt{-5}\right) = 6$. If $2 = xy$ with both x, y nonunits, then $N(x), N(y) > 1$ and $N(x)N(y) = 4$.

The only possibility is $(2,2)$, which would force $N(x) = N(y) = 2$, impossible because the norm takes values $a^2+5b^2 \neq 2$. Hence 2 is irreducible.The same argument with 9 shows 3 is irreducible (there are no elements of norm 3). If $1+\sqrt{-5} = xy$ with nonunits x, y, then $N(x), N(y) > 1$ and $N(x)N(y) = 6$. The only factor pairs are $(2,3)$ or $(3,2)$. But there are no elements of norm 2 or 3 in R, so $1+\sqrt{-5}$ is irreducible, likewise for $1-\sqrt{-5}$. Moreover, none of $2,3,1+\sqrt{-5},1-\sqrt{-5}$ are associates since their norms $4,9,6,6$ are not equal up to units (units preserve norm). Consequently, we obtain two factorizations of 6 into irreducibles that are pairwise non-associate: $6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$, so the element-wise unique factorization property fails in R.

A basic example of applying UFD theory appears in the integer ring, where the FTA itself plays a central role. More generally, when the ring of algebraic integers in a number field is a UFD, a natural extension of $\mathbb{Z}$ preserving unique factorization—the same simplifications used in elementary number theory can be carried over. For instance, one may use the uniqueness of factorization to determine whether two elements share a common divisor or to address classical Diophantine problems such as Fermat-type equations.

However, in most cases relevant to number theory, the ring of algebraic integers is not a UFD. This reintroduces the difficulty already mentioned in Section 3.1, the distinction between prime and irreducible elements, which prevents direct, element-level analysis of factorization questions. To overcome these obstacles, one employs Dedekind's theory of ideal factorization, which will be discussed in detail in the following section.

4.2. Dedekind ideal theory

To resolve the issue mentioned in Section 4.1, we employ Dedekind's unique factorization theorem, which converts the factorization problem of elements into one concerning ideals. This approach can be extended to many rings that are not UFDs.

An integral domain that is Noetherian, integrally closed, and in which each nonzero prime ideal is maximum is called a Dedekind domain. Equivalently, one may describe it using fractional ideals: for a Dedekind domain R with field of fractions K, a fractional ideal A is an R-submodule of K for which there exists a nonzero $m \in R$ such that $mA \subseteq R$. Every fractional ideal in a Dedekind domain can be uniquely factored as a prime-ideal product, which is a crucial structural truth. As a result, under ideal multiplication, the set of nonzero fractional ideals of a Dedekind domain, generated by the nonzero prime ideals, forms a free abelian group.

Theorem 3. Every nonzero fractional ideal in a Dedekind domain can be broken down into a finite product of prime fractional ideals; this factorization is unique up to the factors' order.

DOI: 10.54254/2753-8818/2026.CH30671

In the example of 4.1, the counterexample to the uniqueness of factorization is the element 6 in the ring $\mathbb{Z}\left[\sqrt{-5}\right]$. Here, we will instead study the corresponding principal ideal (6) . Next, consider the ideal (2) . It can be factored into the product of a prime ideal generated by 2 and $1+\sqrt{-5}$, and the ideal (2) itself, that is, $(2)=\mathrm{M}^2$. Similarly, the ideal (3) can also be decomposed into the product of two prime ideals, i.e., $(3)=\mathrm{PQ}$, where $\mathrm{P}=\left(3,1+\sqrt{-5}\right)$ and $\mathrm{Q}=\left(3,1-\sqrt{-5}\right)$ .Finally, we observe that the factorization of the principal ideal (6) is unique, namely $(6)=\mathrm{M}^2\mathrm{PQ}$.

Thus, the issue of the factorization uniqueness not holding for elements in the ring is resolved.

4.3. Unique factorization property and the strong Goldbach conjecture

The strong Goldbach conjecture states that the sum of two prime numbers can be used to represent any even number larger than two. The concept of a prime itself is closely tied to the property of unique factorization. As mentioned earlier, in rings without unique factorization, prime elements are not necessarily identical to irreducible elements. Therefore, the unique factorization property ensures the precise definition of primes in the ring of integers that primes are irreducible numbers, thus providing a clear mathematical foundation for the strong Goldbach conjecture.

Current research on the conjecture mainly focuses on methods in analytic number theory, particularly the circle method and sieve method [4–5]. To elaborate, the circle method relies on Fourier analysis, using characteristic functions of primes and number-theoretic functions such as the Riemann ζ-function. Its core idea is to transform problems in additive number theory into estimates of integrals over the unit circle, essentially representing additive combinations through analytic integrals. The main difficulty lies in estimating sums over the remaining intervals. The first step involves quantifying the conjecture and defining an appropriate counting function

Let

$$r(N)=\sum_{\substack{p+q=N\\ p,qprime}} \tag{27}$$

After applying Fourier analysis, it can be converted into an integral estimate on the unit circle. Let the prime exponential sum be

$$S(\alpha)=\sum_{pprime} e^{2\pi ip\alpha} \tag{28}$$

Then

$$r(N)=\int_0^1 S(\alpha)^2\, e^{-2\pi i\alpha N}\, d\alpha \tag{29}$$

Using Dirichlet character decomposition and its orthogonality relations, we have the approximation

DOI: 10.54254/2753-8818/2026.CH30671

$$S\left(\frac{\alpha}{q}+\beta\right) \approx \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(\alpha)} \sum_{pprime} \chi(p)\, e^{2\pi i p\beta} \tag{30}$$

Then by applying the Riemann zeta function, Perron's formula, and the Dirichlet prime number theorem, the contribution from the major arcs is

$$\int_{MajorArcs} S(\alpha)^2\, e^{-2\pi i\alpha N}\, d\alpha \sim \sigma(N)\, \frac{N}{(logN)^2} \tag{31}$$

where σ(N) is the Goldbach singular series.

The main interval is not the difficult part of the problem, the real challenge lies in proving the results for the remaining intervals.

$$\left| \int_{remaining} S(a)^2 e^{-2\pi i\alpha N} d\alpha \right| = o\frac{N}{log^2 N} \tag{32}$$

A clear and rigorous upper bound is required to ensure that the estimated integral error remains small, so that the contribution of the remainder interval is less than that of the main interval. This is the fundamental issue in solving the strong Goldbach conjecture. The core idea behind the circle method, including the use of the Riemann zeta function, ultimately originates from the unique factorization theorem.

5. Conclusion

This paper mainly discusses the generalization of the unique factorization property from the ring of integers to general number fields through Dedekind's theory of ideals and its intrinsic mathematical connection to the strong Goldbach conjecture. The study leads to the conclusion that the essence of the FTA is fundamentally the unique factorization property. This property holds significant importance for the formulation of numerous theorems and concepts in abstract algebra, number theory, and related fields. Attempts to study many difficult problems and conjectures necessitate establishing the premise that the unique factorization theorem holds.

While this paper does not provide an in-depth investigation into specific methods for resolving the Strong Goldbach Conjecture, it focuses on the core mathematical difficulty underlying the problem. Future research may further concentrate on the estimation and control of the integral contribution of the counting function over the remainder interval.

References

[1] Chen, J. (1966). On the representation of a large even integer as the sum of a prime and the product of at most two primes. Science Bulletin (English Edition), (9), 385–386.
[2] Helfgott, H. A. (2012). Minor arcs for Goldbach's problem. arXiv: 1205.5252.
[3] Griffiths, M. (2013). Intuiting the Fundamental Theorem of Arithmetic. Educational Studies in Mathematics, 82(1), 75–96.
[4] Sabihi, A. (2016). An approach towards the proof of the Strong Goldbach's Conjecture for sufficiently large even integers. arXiv: 1605.08938.
[5] Song, F. G. (2006). The ethereal sieve method for the Goldbach conjecture. Far East Journal of Mathematical Sciences, 21(2), 223–234.