EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 4, Article Number 6781
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Classification and Enumeration of Primitive Eisenstein Triples using Prime Factorization Techniques

Somphong Jitman[1], Mohd Sham Mohammad[2], Ekkasit Sangwisut[3,*]

[1] *Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom, Thailand*
[2] *Centre for Mathematical Sciences, Universiti Malaysia Pahang Al-Sultan Abdullah, Lebuh Persiaran Tan Khalil Yaakob, Kuantan, Pahang, Malaysia*
[3] *Department of Mathematics and Statistics, Faculty of Science and Digital Innovation, Thaksin University, Phattalung, Thailand*

Abstract. This study delves into the concept of primitive Eisenstein triples, defined as positive integer solutions (a, b, c) to the quadratic equation $a^2 - ab + b^2 = c^2$, subject to the condition $a < c < b$ and $\gcd(a, b, c) = 1$. We classify these triples according to the prime factorization of the integer c, elucidating how their existence is intricately linked to specific congruence conditions imposed on the prime divisors of c. Furthermore, we establish a bijective correspondence between these triples and a certain subset of the unit circle. This correspondence enables a comprehensive enumeration of the triples and precisely characterizes the conditions under which such solutions exist.

2020 Mathematics Subject Classifications: 11D09, 11D45, 20K25

Key Words and Phrases: Eisenstein triples, Eisenstein integers, abelian groups, prime number

1. Introduction

The study of positive integer solutions to the equation $a^2 + b^2 = c^2$, known as Pythagorean triples, has fascinated mathematicians for centuries. Equivalently, the integers a, b and c are the lengths of a right-angled triangle. These triples, characterized by positive integers a, b and c satisfying the equation, serve as a cornerstone of number theory and geometry. Beyond their classical role in mathematics, Pythagorean triples have deep connections to algebraic structures, modular forms, and applications in modern cryptography and coding theory.

In [1], W. Sierpinski remarked that "It would be more difficult to prove the existence of an arbitrary number of primitive Pythagorean triples with the same hypotenuse."

[*] Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i4.6781

Email addresses: sjitman@gmail.com (S. Jitman), mohadsham@umpsa.edu.my (M. Sham), ekkasit@tsu.ac.th (E. Sangwisut)

Subsequently, in [2], Ch. L. Shedd demonstrated that there are precisely 64 primitive Pythagorean triples with the hypotenuse $c = 2,576,450,045 = 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37 \cdot 41 \cdot 53$. Twenty-two years later, this question was revisited by E. J. Eckert in [3], the group structure of the set of primitive Pythagorean triples was investigated. Eckert provided necessary and sufficient conditions for the existence of primitive Pythagorean triples with a given hypotenuse. Alternatively, the set of primitive Pythagorean triples can be identified with the group of rational points on the unit circle. As discussed in [4, 5], this group can be decomposed into a direct sum of the unit group of the group of rational points on the unit circle and a free abelian group. This group-theoretic framework enables both the characterization and enumeration of primitive Pythagorean triples with a given hypotenuse (see [5]).

In a similar manner, Eisenstein triples (60-degree triples) arise from the analogous equation $a^2 - ab + b^2 = c^2$. These triples correspond to triangles with sides of integer lengths a, b, and c, where the angle opposite the side of length c is 60°. A general method for constructing all such triples have been established (see [6]). Previous studies, including [7], [8], and [9], have explored parametric equations and have established relationships between 120-degree triples and 60-degree triples. Fundamental properties of Eisenstein triples have been presented in [10].

This paper focuses on the characterization and enumeration of primitive Eisenstein triples for a fixed hypotenuse. In particular, the one-to-one correspondence between these triples and the ω-rational points (see (3) for the definition) in the second sextant of the unit circle. The paper is organized as follows. In Section 2, the concept and basic properties of (primitive) Eisenstein triples are recalled. In Section 3, the concept of the ω-rational unit circle is introduced together with a link between Eisenstein triples and points on the ω-rational unit circle. The group structure of the ω-rational unit circle is presented in Section 4. Based on this group structure, the characterization and enumeration of primitive Eisenstein triples with a fixed hypotenuse are established in Section 5. The summary is given in Section 6.

2. Eisenstein Triples

In this section, some properties and geometric interpretation of Eisenstein triples are recalled in terms of triangles with a 60° angle. Key results from [10] concerning the classification of these triples and the constraints on the values of c are presented. In addition, a useful partition of the set of all primitive Eisenstein triples is introduced.

An **Eisenstein triple** is a triple (a, b, c) of positive integers with $a < c < b$, that satisfies the equation

$$a^2 - ab + b^2 = c^2. \tag{1}$$

The Eisenstein triple is said to be **primitive** if $\gcd(a, b, c) = 1$.

The law of cosines states that for any triangle with sides a, b and c, and θ is the angle θ opposite side c, the following equation holds:

$$a^2 - 2ab\cos\theta + b^2 = c^2. \tag{2}$$

When θ is $60°$, (2) simplifies the form given in (1), which is the equation of an Eisenstein triple (see Figure 1).

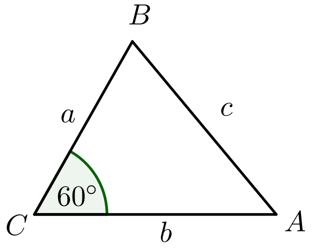

Figure 1: Triangles containing a 60° angle.

For examples:

- The triples $(3, 8, 7)$ and $(5, 8, 7)$ are primitive Eisenstein triples.
- The Eisenstein triples $(6, 16, 14)$ and $(10, 16, 14)$ are not primitive.

We note that every non-primitive Eisenstein triple can be expressed as a positive multiple of a primitive one. It is therefore sufficient to focus primarily on the study of primitive Eisenstein triples. The concept of conjugate Eisenstein triples is given as follows.

Theorem 1 ([10]). *If (a, b, c) is a primitive Eisenstein triple, then $(b - a, b, c)$ is also a primitive Eisenstein triple.*

A primitive Eisenstein triple $(b - a, b, c)$ is called a **conjugate** of the primitive Eisenstein triple (a, b, c) (see Figure 2).

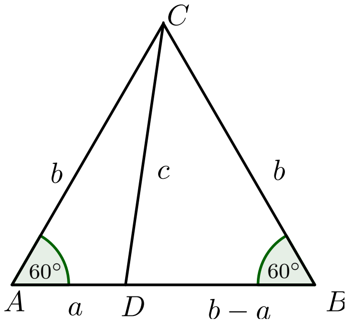

Figure 2: An Eisenstein triple and its conjugate

The length of the side c of a primitive Eisenstein triple (a, b, c) is subject to the following restriction.

Theorem 2 ([10, Theorem 1]). *If (a, b, c) is a primitive Eisenstein triple, then c is neither a multiple of 2 nor 3. More generally, the only prime factors of c are primes of the form $6k + 1$.*

Based on Theorem 2, we introduce the following useful partition on the set of primitive Eisenstein triples. Let ET denote the set of all primitive Eisenstein triples. For each positive integer c, let ET_c denote the subset of ET containing triples whose side opposite an angle 60° is c. From Theorem 2, the integer c in every primitive Eisenstein triple must have only prime factors of the form $6k+1$ for some non-negative integer k. This yields the following partition

$$\mathrm{ET} = \bigsqcup_{c>1} \mathrm{ET}_c = \mathrm{ET}_7 \sqcup \mathrm{ET}_{13} \sqcup \mathrm{ET}_{19} \sqcup \dots,$$

where the union is taken over all values of c whose prime factors are congruence to 1 modulo 6.

3. From Eisenstein Triples to the ω-Rational Unit Circle

This section presents a connection between Eisenstein triples and points on the ω-rational unit circle (see (3) for the definition). Using the unique factorization property of Eisenstein integers, we demonstrate how each primitive Eisenstein triple is mapped to an ω-rational point in the unit circle in the complex plane. This mapping not only highlights the geometric structure of Eisenstein triples but also establishes a link between their algebraic and geometric representations.

Eisenstein integers are complex numbers of the form $z = a + b\omega$, where $a, b \in \mathbb{Z}$, and $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{3}i}{2}$ is a primitive cube root of unity. We note that ω and $\overline{\omega}$ are roots of the polynomial $x^2 + x + 1$, where $\overline{\omega}$ is the complex conjugate of ω. It is easily seen that $\omega^3 = \overline{\omega}^3 = 1, \omega^2 = \overline{\omega} = -1 - \omega, \omega \cdot \overline{\omega} = 1$ and $\omega + \overline{\omega} = -1$. The set of all Eisenstein integers, denoted $\mathbb{Z}[\omega]$, forms a commutative ring with identity under the usual addition and multiplication of complex numbers. The unit group of $\mathbb{Z}[\omega]$ is

$$U = \left\{1, \omega, \omega^2, -1, -\omega, -\omega^2\right\} = \langle -\omega \rangle,$$

which is isomorphic to the cyclic group of order 6. The norm of an Eisenstein integer $z = a + b\omega$ is defined by

$$N(z) = \sqrt{z\overline{z}} = \sqrt{(a+b\omega)(a+b\overline{\omega})} = \sqrt{a^2 - ab + b^2}.$$

For two Eisenstein integers z and z', the norm satisfies $N(zz') = N(z)N(z')$. Two Eisenstein integers z and z' are said to be **associates** if $z = \delta \cdot z'$ for some unit $\delta \in U$. The ring $\mathbb{Z}[\omega]$ is a unique factorization domain (UFD), meaning every nonzero, non-unit element has a unique factorization into a product of irreducible elements, up to the rearrangement of the factors and the replacement of any irreducible element with one of its associates. For more information on Eisenstein integers, the reader may refer to [11–13] and [14].

Let $\mathcal{G}(\mathbb{R})$ denote the unit circle in the complex plane. Since $N(z)$ equals the Euclidean norm of z for all complex numbers z, the elements in $\mathcal{G}(\mathbb{R})$ can be viewed as their ω-expansions. Precisely,

$$\mathcal{G}(\mathbb{R}) := \left\{ \zeta = u + v\omega \in \mathbb{C} \,\middle|\, u, v \in \mathbb{R},\ N(\zeta) = \sqrt{u^2 - uv + v^2} = 1 \right\}.$$

The set $\mathcal{G}(\mathbb{R})$ forms an abelian group under the standard multiplication in $\mathbb{C}$. Moreover, $N(1) = 1, N(\zeta_1\zeta_2) = N(\zeta_1)N(\zeta_2),$ and $N(\zeta^{-1}) = N(\zeta)^{-1}$. Let $\mathcal{G}(\mathbb{Q})$ be the subset of $\mathcal{G}(\mathbb{R})$ of the form

$$\mathcal{G}(\mathbb{Q}) := \left\{ \zeta = u + v\omega \,\middle|\, u, v \in \mathbb{Q},\ N(\zeta) = \sqrt{u^2 - uv + v^2} = 1 \right\}. \tag{3}$$

The set $\mathcal{G}(\mathbb{Q})$ is called the **ω-rational unit circle** and each element in $\mathcal{G}(\mathbb{Q})$ is called an **ω-rational point**. We observe that although $i \in \mathcal{G}(\mathbb{R})$ but it is not in $\mathcal{G}(\mathbb{Q})$. It is interesting to investigate properties further.

Proposition 1. *The set $\mathcal{G}(\mathbb{Q})$ is a subgroup of $\mathcal{G}(\mathbb{R})$.*

Proof. It is easy to see that $1 = 1 + 0 \cdot \omega \in \mathcal{G}(\mathbb{Q})$ which implies that $\mathcal{G}(\mathbb{Q}) \neq \emptyset$. For elements $u_1 + v_1\omega, u_2 + v_2\omega \in \mathcal{G}(\mathbb{Q})$, the product $(u_1 + v_1\omega)(u_2 + v_2\omega)^{-1} = \frac{u_1+v_1\omega}{u_2+v_2\omega}$ can be expressed as $\frac{u_1+v_1\omega}{u_2+v_2\omega} = \frac{(u_1+v_1\omega)(u_2+v_2\overline{\omega})}{u_2^2-u_2v_2+v_2^2}$. Simplifying the numerator and denominator yields $\frac{(u_1u_2+v_1v_2-u_1v_2)+(v_1u_2-u_1v_2)\omega}{u_2^2-u_2v_2+v_2^2}$. This can be written as $\frac{u_1u_2+v_1v_2-u_1v_2}{u_2^2-u_2v_2+v_2^2} + \frac{v_1u_2-u_1v_2}{u_2^2-u_2v_2+v_2^2}\omega$. Since $u_1, v_1, u_2, v_2 \in \mathbb{Q}$, the result is in $\mathcal{G}(\mathbb{Q})$.

For a given primitive Eisenstein triple (a, b, c), define the associated Eisenstein integer

$$z := a + b\omega,$$

whose norm is given by $N(z) = \sqrt{a^2 - ab + b^2} = c$. It follows immediately that $2a \neq b$. Otherwise, we would have $c = \sqrt{3}a$, which contradicts the assumption that c is an integer. The corresponding point in the unit circle is the normalized complex number

$$\zeta := \frac{z}{N(z)} = \frac{a}{c} + \frac{b}{c}\omega = \frac{2a-b}{2c} + \frac{b\sqrt{3}}{2c}i \in \mathcal{G}(\mathbb{R}).$$

Since $\frac{a}{c}$ and $\frac{b}{c}$ are rational numbers, ζ is an ω-rational point in $\mathcal{G}(\mathbb{Q})$. Consequently, each primitive Eisenstein triple in ET gives rise to an ω-rational point in the ω-rational unit circle $\mathcal{G}(\mathbb{Q})$ illustrated in Figure 3.

Next, we show that ζ lies in the second sextant. Since $\mathrm{Im}(\zeta) > 0$, it follows that ζ lies in the upper half plane. We note that the slope of the line from the origin to ζ is

$$m = \frac{b\sqrt{3}}{2a-b}$$

which implies that $m > \sqrt{3}$ if $2a > b$, or $m < -\sqrt{3}$ if $2a < b$. In both cases, ζ lies in the second sextant.

Let $\zeta := u + v\omega \in \mathcal{G}(\mathbb{Q}) \setminus \{\omega, -\overline{\omega}\}$ be in the second sextant. Let d denote the least common multiple of the denominators of u and v. Then $d\zeta = du + dv\omega \in \mathbb{Z}[\omega]$ which ensures that the coordinates of the associated Eisenstein triple (du, dv, d) are integral. Alternatively, we may consider the primitive representation of the triple (du, dv, d) by dividing by the greatest common divisor.

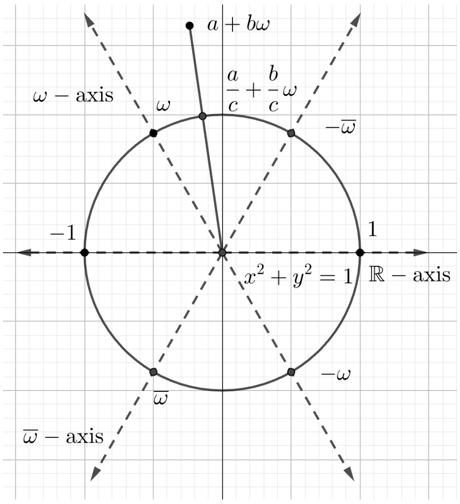

Figure 3: Geometric projection of the Eisenstein integer $a + b\omega$ into the ω-rational unit circle by normalization.

For example, take $\zeta = \frac{18}{42} + \frac{120}{105}\omega \in \mathcal{G}(\mathbb{Q})$. Then the least common multiple of the denominators is $d = \operatorname{lcm}(42, 105) = 210$ which implies that

$$210\zeta = 90 + 240\omega \in \mathbb{Z}[\omega].$$

Hence, the corresponding Eisenstein triple is $(90, 240, 210)$ whose primitive representative (after dividing by the greatest common divisor 30) is $(3, 8, 7) \in \mathrm{ET}$.

The set of associate elements of $\zeta \in \mathcal{G}(\mathbb{Q})$ is denoted by

$$U\zeta = \{\zeta, (-\omega)\zeta, (-\omega)^2\zeta, (-\omega)^3\zeta, (-\omega)^4\zeta, (-\omega)^5\zeta\} \tag{4}$$

which represents six distinct points on $\mathcal{G}(\mathbb{Q})$, each located in a different sextant (see Figure 4). In other words, multiplying ζ by $-\omega$ results in a 60° clockwise rotation of ζ.

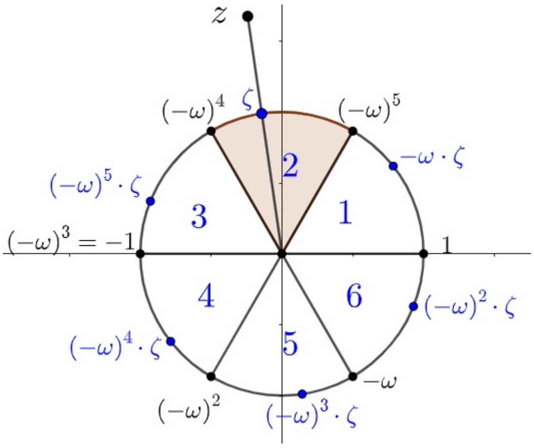

Figure 4: The associate elements of ζ in $\mathcal{G}(\mathbb{Q})$.

Let ζ be a point in $\mathcal{G}(\mathbb{Q}) \setminus U$. Let f br a function responsible for rotating ζ clockwise into the second sextant. Precisely,

$$f(\zeta) = (-\omega)^{i-2}\zeta$$

for all ζ in the ith sextant (for $1 \leq i \leq 6$). This operation ensures that $f(\zeta)$ locates in the second sextant. Next, let g be a function that maps points on the second sextant to the set of Eisenstein triples ET. Finally, let

$$\mathrm{et} = g \circ f \tag{5}$$

be a composite function that maps any point $\zeta \in \mathcal{G}(\mathbb{Q}) \setminus U$ to ET by first rotating ζ clockwise into the second sextant and then applying g.

We demonstrate the infinitude of the set of primitive Eisenstein triples by showing that $\mathcal{G}(\mathbb{Q})$ contains infinitely many points.

Proposition 2. *The set of primitive Eisenstein triples is infinite.*

Proof. From (5), it is not difficult to see that the function

$$\mathrm{et} : \mathcal{G}(\mathbb{Q}) \setminus U \to \mathrm{ET}$$

is surjective and it is a 6-to-1 map. To complete the proof, it suffices to show that $\mathcal{G}(\mathbb{Q})$ has infinite order. For each element $m \in \mathbb{Q}$, let $z_m = \frac{1-2m}{1-m+m^2} + \frac{1-m^2}{1-m+m^2}\omega$. Then $\frac{1-2m}{1-m+m^2}, \frac{1-m^2}{1-m+m^2} \in \mathbb{Q}$ and

$$N(z_m) = \sqrt{\left(\tfrac{1-2m}{1-m+m^2}\right)^2 - \left(\tfrac{1-2m}{1-m+m^2}\right)\left(\tfrac{1-m^2}{1-m+m^2}\right) + \left(\tfrac{1-m^2}{1-m+m^2}\right)^2} = 1.$$

It follows that $z_m \in \mathcal{G}(\mathbb{Q})$ for all $m \in \mathbb{Q}$. Since $z_m \neq z_n$ for all $m \neq n \in \mathbb{Q}$, $G(\mathbb{Q})$ contains infinitely many ω-rational points. Hence, $\mathcal{G}(\mathbb{Q})$ has infinite order.

Table 1 illustrates a behavior of the element $\zeta = \frac{3}{7} + \frac{8}{7}\omega$ in $\mathcal{G}(\mathbb{Q})$ and their successive powers ζ^n for all integers $-3 \leq n \leq 3$.

- The corresponding values of ζ^n in the second column.
- The associated Eisenstein triples $\mathrm{et}(\zeta^n) = (a_n, b_n, c_n)$ in the third column.

4. Prime Numbers and the Abelian Group Structure

This section examines the structure of prime numbers in the ring $\mathbb{Z}[\omega]$, focusing on their factorization and classification based on residue classes modulo 3. Based on the unique factorization in this ring, it can be shown that the group $\mathcal{G}(\mathbb{Q})$ can be decomposed as a direct sum of the unit group and a free abelian group.

n	ζ^n	$\mathrm{et}(\zeta^n) = (a_n, b_n, c_n)$
-3	$\frac{323}{343} + \frac{360}{343}\omega$	$(323, 360, 343)$
-2	$\frac{-39}{49} + \frac{16}{49}\omega$	$(16, 55, 49)$
-1	$-\frac{5}{7} - \frac{8}{7}\omega$	$(5, 8, 7)$
1	$\frac{3}{7} + \frac{8}{7}\omega$	$(3, 8, 7)$
2	$-\frac{55}{49} - \frac{16}{49}\omega$	$(39, 55, 49)$
3	$-\frac{37}{343} - \frac{360}{343}\omega$	$(37, 360, 343)$

Table 1: Powers of $\zeta = \frac{3}{7} + \frac{8}{7}\omega$ in $\mathcal{G}(\mathbb{Q})$ and their associated primitive Eisenstein triples.

Let P denote the set of positive prime numbers. For $i \in \{1, 2, 3\}$, let P_i denote the set of prime numbers congruence i modulo 3. Then P can be partitioned into residue classes modulo 3 as follows:

$$P = P_1 \sqcup P_2 \sqcup P_3 = \{7, 13, 19, 31, \dots\} \sqcup \{2, 5, 11, 17, \dots\} \sqcup \{3\}. \tag{6}$$

While P_3 is a singleton, it can be seen that P_1 and P_2 are infinite sets,

For each $p \in P_1$, we have $p \equiv 1 \pmod 3$ which can be expressed as $p = a^2 - ab + b^2$ for some integers a and b (see [15]). This allows us to express the factorization $p = (a + b\omega)(a + b\overline{\omega})$ (see [11, 12]). Let $q := a + b\omega$. Then the conjugate of q is $\overline{q} = a + b\overline{\omega}$. Let ζ_p be the complex number of the form

$$\zeta_p = \frac{q}{\overline{q}} = \frac{a + b\omega}{a + b\overline{\omega}}. \tag{7}$$

Since ζ_p has rational coordinates and its norm satisfies $N(\zeta_p) = \frac{N(a+b\omega)}{N(a+b\overline{\omega})} = \frac{\sqrt{a^2-ab+b^2}}{\sqrt{a^2-ab+b^2}} = 1$, it follows that ζ_p belongs to the group $\mathcal{G}(\mathbb{Q})$.

Example 1. *Let $p = 7$. Then $7 = (1 + 3\omega) \cdot (1 + 3\overline{\omega}) = q \cdot \overline{q}$, where $q = 1 + 3\omega$ and $\overline{q} = 1 + 3\overline{\omega}$. It follows that*

$$\zeta_7 = \frac{q}{\overline{q}} = \frac{1 + 3\omega}{1 + 3\overline{\omega}}$$

is an element in $\mathcal{G}(\mathbb{Q})$. Similarly, for $p = 13$, we write $13 = (1 + 4\omega)(1 + 4\overline{\omega})$, where $q = 1 + 4\omega$ and $\overline{q} = 1 + 4\overline{\omega}$. Hence,

$$\zeta_{13} = \frac{1 + 4\omega}{1 + 4\overline{\omega}} \in \mathcal{G}(\mathbb{Q}).$$

We note that $\mathbb{Z}[\omega]$ is a unique factorization domain with the unit group $U = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$. The classification of the irreducible elements in $\mathbb{Z}[\omega]$ is recalled as follows. For more information on irreducible elements in $\mathbb{Z}[\omega]$, the reader may refer to [14] and [12, p. 110]. Based on the partition in (6) of P, there are of three types of partitions.

- For each $p \in P_1$, the irreducible factorization of p in $\mathbb{Z}[\omega]$ is given by $p = (a + b\omega)(a + b\overline{\omega})$, where $a + b\omega$ and $a + b\overline{\omega}$ are not associated. In this case, we have $U(a + b\omega) \neq U(a + b\overline{\omega})$ and $N(a + b\omega) = N(a + b\overline{\omega}) = \sqrt{p}$.

- For each $p \in P_2$, p is an irreducible element in $\mathbb{Z}[\omega]$ and $N(p) = p$.
- For the positive prime integer $p = 3$, its factorization is $3 = (1 + 2\omega)(1 + 2\overline{\omega}) = -(1 + 2\omega)^2$. In this case, $1 + 2\omega$ and $1 + 2\overline{\omega}$ are associated and $1 + 2\omega$ is irreducible in $\mathbb{Z}[\omega]$. Furthermore, $N(1 + 2\omega) = \sqrt{3}$.

As the ring $\mathbb{Z}[\omega]$ contains the ring $\mathbb{Z}$, this implies that prime integers in P_1 and P_3 can be factored further. Define an equivalence relation on the set $\mathbb{Z}[\omega]$ by $z \sim z'$ if and only if z and z' are associated. Each equivalence class under the relation $\sim$ consists of all elements in $\mathbb{Z}[\omega]$ that are associated elements of z. Precisely, the equivalence class containing z is

$$Uz = \left\{z, (-\omega)z, (-\omega)^2 z, (-\omega)^3 z, (-\omega)^4 z, (-\omega)^5 z\right\},$$

which represents points on the circle of radius $N(z)$ in different sextants (see Figure 4). Consequently, the partition of P in (6) is defined as follows.

Let Q denote the set of irreducible elements in the ring $\mathbb{Z}[\omega]$. The Q has a partition of the form

$$Q := Q_1 \sqcup \overline{Q}_1 \sqcup Q_2 \sqcup Q_3 \tag{8}$$

with the following conditions.

(i) For each $p \in P_1$, if the factorization of p in $\mathbb{Z}[\omega]$ is $p = q \cdot \overline{q}$, the elements q and $\overline{q}$ are assigned to the sets Q_1 and $\overline{Q}_1$, respectively.

(ii) $Q_2 := P_2$.

(iii) $Q_3 := \{1 + 2\omega\}$.

It follows that every nonzero element $z \in \mathbb{Z}[\omega]$ can be uniquely expressed in the form

$$z = \delta \cdot \prod_{i=1}^{k} q_i^{e_i}, \tag{9}$$

where $\delta \in U$, $k \geq 0$, q_i is an irreducible element in Q, and $e_i \geq 1$ is an integer. This factorization is unique up to the rearrangement of the factors and the replacement of any irreducible element with one of its associates.

Next, the decomposition of $\mathcal{G}(\mathbb{Q})$ will be presented using the field of fractions of $\mathbb{Z}[\omega]$. Let

$$\mathbb{Q}[\omega] = \{u + v\omega \mid u, v \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

Then $\mathbb{Q}[\omega]$ is the field of fractions of $\mathbb{Z}[\omega]$. Analogous to (9), each element $z \in \mathbb{Q}[\omega] \setminus \{0\}$ can be uniquely expressed in the form

$$z = \delta \cdot \prod_{i=1}^{k} q_i^{e_i}, \tag{10}$$

where $\delta \in U$, $k \geq 0$, q_i is an irreducible element in Q, and $e_i \in \mathbb{Z} \setminus \{0\}$. The following theorem describes the decomposition of $\mathcal{G}(\mathbb{Q})$.

Theorem 3. *The abelian group $\mathcal{G}(\mathbb{Q})$ is decomposed as an internal direct sum:*

$$\mathcal{G}(\mathbb{Q}) = U \oplus F,$$

where $U = \left\{1, \omega, \omega^2, -1, -\omega, -\omega^2\right\}$ is the unit group of $\mathbb{Z}[\omega]$, and F is a free abelian group with basis given by the collection $\{\zeta_p \mid p \in P_1\}$, where P_1 is the set of prime integers congruent to $1 \pmod 3$.

Proof. Let $z \in \mathcal{G}(\mathbb{Q})$. Then $z \in \mathbb{Q}[\omega]$ which has a unique factorization in the form of (10). Rearrange the factorization using the set of irreducible elements Q in (8), we have

$$z = \delta \cdot \left(\prod_{i=1}^{r} q_i^{c_i} \overline{q}_i^{d_i}\right) \cdot \left(\prod_{i=1}^{s} \widetilde{q_j}^{e_j}\right) \cdot (1+2\omega)^t, \tag{11}$$

where $\delta \in U, q_1, \ldots, q_r \in Q_1, \overline{q}_1, \ldots, \overline{q}_r \in \overline{Q}_1, \widetilde{q_1}, \ldots, \widetilde{q_s} \in Q_2$, and the exponents $c_1, \ldots, c_r$, $d_1, \ldots, d_r, e_1, \ldots, e_s$ and t are integers. Since z is an ω-rational point in the ω-rational unit circle, we have $N(z) = 1$. Expanding $N(z)$ using its factorization, it follows that

$$\begin{aligned} 1 &= N(z) \\ &= N(\delta) \cdot N\left(\prod_{i=1}^{r} q_i^{c_i} \overline{q}_i^{d_i}\right) \cdot N\left(\prod_{i=1}^{s} \widetilde{q_j}^{e_j}\right) \cdot N(1+2\omega)^t \\ &= \left(\prod_{i=1}^{r} N(q_i)^{c_i} N(\overline{q}_i)^{d_i}\right) \left(\prod_{i=1}^{s} N\left(\widetilde{q_j}\right)^{e_j}\right) \cdot \left(\sqrt{3}\right)^t \\ &= \left(\prod_{i=1}^{r} N(q_i)^{c_i} N(q_i)^{d_i}\right) \left(\prod_{i=1}^{s} N\left(\widetilde{q_j}\right)^{e_j}\right) \cdot \left(\sqrt{3}\right)^t. \end{aligned}$$

We note that $N(q_i) = N(\overline{q}_i)$ for $q_i \in Q_1$ and $\overline{q}_i \in \overline{Q}_1$. Since $N(z) = 1$, we deduce that $c_i = -d_i$, and e_j and t are zero. Substituting these constrains into (11), it can be concluded that

$$z = \delta \cdot \left(\prod_{i=1}^{r} q_i^{c_i} \overline{q}_i^{-c_i}\right) = \delta \cdot \prod_{i=1}^{r} \left(\frac{q_i}{\overline{q}_i}\right)^{c_i}.$$

By setting $\zeta_i = \frac{q_i}{\overline{q}_i}$ as in (7), we further deduced that

$$z = \delta \cdot \prod_{i=1}^{r} \zeta_i^{c_i} \in U \oplus F.$$

This completes the proof.

5. Characterization and Enumeration of Primitive Eisenstein Triples

In this section, we focus on the characterization and enumeration of primitive Eisenstein triples. We begin with a formula for the hypotenuse c of an Eisenstein triple. Next, we present necessary and sufficient conditions for the existence of primitive Eisenstein triples with a given hypotenuse c, highlighting the relationship between the prime factorization of c and the structure of the corresponding triples. This allows us to establish the enumeration of primitive Eisenstein triples with a given hypotenuse c. Finally, we provide examples that demonstrate how these results can be applied to specific values of c, illustrating the number of primitive Eisenstein triples associated with particular integers.

Lemma 1. *For a positive integer k, distinct primes $p_1, \dots, p_k$ in P_1, nonzero integers $n_1, \dots, n_k$, and signs $\epsilon_1, \dots, \epsilon_k \in \{\pm 1\}$, define*

$$(a, b, c) := \mathrm{et}\left(\prod_{i=1}^{k} \zeta_{p_i}^{\epsilon_i \cdot n_i}\right) \in \mathrm{ET}\,.$$

Then $c = p_1^{n_1} \dots p_k^{n_k}$.

Proof. Let $\zeta = \prod_{i=1}^{k} \zeta_{p_i}^{\epsilon_i \cdot n_i}$. By the defining $\zeta_{p_i} = \frac{q_i}{\overline{q}_i}$ given in (7), it can be rewritten in the form of

$$\zeta = \prod_{i=1}^{k} \zeta_{p_i}^{\epsilon_i \cdot n_i} = \prod_{i=1}^{k} \left(\frac{q_i}{\overline{q}_i}\right)^{\epsilon_i \cdot n_i}.$$

Since $p_1, \dots, p_k$ are in P_1, we have the factorization $p_i = q_i \cdot \overline{q}_i$ over $\mathbb{Z}[\omega]$ for all $i = 1, \dots, k$. It follows that

$$c = \prod_{i=1}^{k} p_i^{n_i} = \prod_{i=1}^{k} (q_i \cdot \overline{q}_i)^{n_i}.$$

Let

$$z := \zeta \cdot c = \prod_{i=1}^{k} \left(\frac{q_i}{\overline{q}_i}\right)^{\epsilon_i \cdot n_i} \cdot (q_i \cdot \overline{q}_i)^{n_i} = \prod_{i=1}^{k} \frac{q_i^{(\epsilon_i+1)\cdot n_i}}{\overline{q}_i^{(\epsilon_i-1)\cdot n_i}} = \prod_{i=1}^{k} \widetilde{q_i}^{2n_i},$$

where $\widetilde{q_i}$ is defined to be

$$\widetilde{q_i} = \begin{cases} q_i & \text{if} \quad \epsilon_i = 1, \\ \overline{q}_i & \text{if} \quad \epsilon_i = -1. \end{cases}$$

Hence, $z \in \mathbb{Z}[\omega]$ and its norm satisfies $N(z) = N\left(\prod_{i=1}^{k} \widetilde{q_i}^{2n_i}\right) = \prod_{i=1}^{k} p_i^{n_i} = c$. We can choose $\delta \in U$ such that the associate $\delta z = a + b\omega$ is in the second sextant. Hence, (a, b, c) forms an Eisenstein triple.

Next, we show that the Eisenstein triple (a, b, c) is primitive. For contrary, we suppose that there exists p_i such that $p_i \mid a$ and $p_i \mid b$. Then $a = p_i a'$ and $b = p_i b'$ for some integers a' and b'. Substituting these expressions into δz, we obtain $\delta z = a + b\omega = p_i a' + p_i b' \omega = p_i\,(a' + b'\omega)$ which implies that $p_i \mid z$. Since $z = \prod_{i=1}^{k} \widetilde{q_i}^{2n_i}$ and $p_i = q_i \cdot \overline{q}_i$, q_i and $\overline{q}_i$ appear as factors in z. This is a contradiction. Consequently, there a and b has no common prime divisors. As a result, the Eisenstein triple (a, b, c) must be primitive.

The following theorem provides a classification of primitive Eisenstein triples based on the prime factorization of the hypotenuse c.

Theorem 4. *Let $c > 1$ be an integer with prime factorization*

$$c = p_1^{n_1} \dots p_k^{n_k},$$

where k is a positive integer, $p_1, \dots, p_k$ are distinct prime numbers, and $n_1, \dots, n_k$ are positive exponents. Then exactly one of the following statements holds:

(i) If $p_i \equiv 1 \pmod 3$ for all $i = 1, \dots, k$, then the map

$$\mathrm{et}_{|_Z} : Z \to \mathrm{ET}_c$$

is a bijection, where $Z = \left\{\prod_{i=1}^k \zeta_{p_i}^{\epsilon_i \cdot n_i} \mid \epsilon_1, \dots, \epsilon_k \in \{\pm 1\}\right\}$, and ζ_{p_i} is a complex number defined in (7) for the prime p_i.

(ii) Otherwise, the set ET_c is empty.

Proof. To prove 1), assume the notations as in Section 3. Consider the surjective function

$$\mathrm{et} : \mathcal{G}(\mathbb{Q}) \setminus U \to \mathrm{ET}$$

defined in (5). Let Ω be a relation on $\mathcal{G}(\mathbb{Q}) \setminus U$ given by $\zeta_1 \Omega \zeta_2$ if and only if $\zeta_1^{-1}\zeta_2 \in U$. Then Ω is an equivalence relation and we denote the corresponding quotient set by $(\mathcal{G}(\mathbb{Q}) \setminus U)/\Omega$. Consequently, the induced function

$$\mathrm{et} : (\mathcal{G}(\mathbb{Q}) \setminus U)/\Omega \to \mathrm{ET}$$

is bicjective. By the Theorem 3, we have $\mathcal{G}(\mathbb{Q}) = U \oplus F$, which implies that

$$\mathcal{G}(\mathbb{Q}) \setminus U = (U \oplus F) \setminus U = U \oplus (F \setminus \{1\}).$$

Since every element in $U \oplus F$ is uniquely of the form uf with $u \in U$ and $f \in F$, the elements *not in* U are exactly those with $f \neq 1$. Hence, $(U \oplus F) \setminus U = \{uf \mid u \in U,\ f \in F \setminus \{1\}\} = U \oplus (F \setminus \{1\})$. Thus, the quotient sets are identical:

$$(\mathcal{G}(\mathbb{Q}) \setminus U)/\Omega = (U \oplus (F \setminus \{1\}))/\Omega = F \setminus \{1\}.$$

This establishes the one-to-one correspondence

$$\mathrm{et} : F \setminus \{1\} \to \mathrm{ET}\,.$$

Now, let $p_1, \dots, p_k$ be distinct primes in P_1 and let $n_1, \dots, n_k$ be positive integers. Let

$$Z := \left\{ \prod_{i=1}^{k} \zeta_{p_i}^{\epsilon_i \cdot n_i} \mid \epsilon_1, \dots, \epsilon_k \in \{\pm 1\} \right\}.$$

Then $Z \subseteq F \smallsetminus \{1\}$ and the restriction map

$$\text{et}\,|_Z \colon Z \to \text{ET}$$

is injective, and the image of Z is ET_c (see Lemma 1). Therefore, $\text{et}\,|_Z \colon Z \to \text{ET}_c$ is a bijection.

From Theorem 2, 2) follows immediately.

Corollary 1. *Let $c > 1$ be an integer with prime factorization as described in Theorem 4. Then, exactly one of the following holds:*

(i) If $p_i \equiv 1 \pmod 6$ for all $i = 1, \ldots, k$, then there are 2^k primitive Eisenstein triples with hypotenuse c.

(ii) Otherwise, there are no primitive Eisenstein triples with hypotenuse c.

Proof. The first statement follows form the one-to-one correspondence established in 1) of Theorem 4. Precisely,

$$|\text{ET}_c| = \left| \left\{ \prod_{i=1}^{k} \zeta_{p_i}^{\epsilon_i \cdot n_i} \mid \epsilon_1, \ldots, \epsilon_k \in \{\pm 1\} \right\} \right| = 2^k.$$

The second statement can be deduced directly from 2) of Theorem 4.

The following examples illustrate the application of Theorem 4 and Corollary 1 to determine the primitive Eisenstein triples for specific hypotenuses.

Example 2. *Let $c = 49$. The prime factorization is $c = 7^2$ which $7 \in P_1$. By Example 1, we have $\zeta_7 = \frac{1+3\omega}{1+3\overline{\omega}} = -\frac{8}{7} - \frac{3}{7}\omega$ and $\zeta_7^{-1} = \frac{1+3\overline{\omega}}{1+3\omega} = -\frac{5}{7} + \frac{3}{7}\omega$. We have the set $Z = \left\{\zeta_7^{\epsilon \cdot 2} \mid \epsilon \in \{\pm 1\}\right\} = \left\{\zeta_7^2, \zeta_7^{-2}\right\}$. By Theorem 4, there are two cases:*
Case $\epsilon_1 = 1$: We compute ζ_7^2:

$$\zeta_7^2 = \left(-\frac{8}{7} - \frac{3}{7}\omega\right)^2 = \frac{55}{49} + \frac{39}{49}\omega.$$

This lies in the sixth sextant. Its associate in the second sextant is $\frac{16}{49} + \frac{55}{49}\omega$. The corresponding primitive Eisenstein triples is $\text{et}\left(\frac{16}{49} + \frac{55}{49}\omega\right) = (16, 55, 49)$.
Case $\epsilon_1 = -1$: We compute ζ_7^{-2}:

$$\zeta_7^{-2} = \left(-\frac{5}{7} + \frac{3}{7}\omega\right)^2 = \frac{16}{49} - \frac{39}{49}\omega.$$

This lies in the fifth sextant. Its associate in the second sextant is $\frac{39}{49} + \frac{55}{49}\omega$. The corresponding primitive Eisenstein triples is $\text{et}\left(\frac{39}{49} + \frac{55}{49}\omega\right) = (39, 55, 49)$.

Consequently, $\text{ET}_{49} = \{(16, 55, 49), (39, 55, 49)\}$.

Example 3. *Let $c = 91$. Then the prime factorization is $c = 7 \cdot 13$, where $7, 13 \in P_1$. From Example 1, we have*

$$\zeta_7 = \frac{1+3\omega}{1+3\overline{\omega}}, \text{ and } \zeta_{13} = \frac{1+4\omega}{1+4\overline{\omega}}.$$

Then $Z = \{\zeta_7^{\epsilon_1}\zeta_{13}^{\epsilon_2} \mid \epsilon_1, \epsilon_2 \in \{\pm\}\} = \{\zeta_7\zeta_{13}, \zeta_7^{-1}\zeta_{13}, \zeta_7\zeta_{13}^{-1}, \zeta_7^{-1}\zeta_{13}^{-1}\}$. By Theorem 4, we analyze the following four cases:
Case 1: $\epsilon_1 = 1, \epsilon_2 = 1$. Compute $\zeta_7 \cdot \zeta_{13}$:

$$\zeta_7 \cdot \zeta_{13} = \frac{1+3\omega}{1+3\overline{\omega}} \cdot \frac{1+4\omega}{1+4\overline{\omega}} = \frac{96}{91} + \frac{85}{91}\omega.$$

This lies in the sixth sextant. Its associate in the second sextant is $\frac{11}{91} + \frac{96}{91}\omega$. The corresponding primitive Eisenstein triples is et $\left(\frac{11}{91} + \frac{96}{91}\omega\right) = (11, 96, 91)$.
Case 2: $\epsilon_1 = -1, \epsilon_2 = 1$. Compute $\zeta_7^{-1} \cdot \zeta_{13}$:

$$\zeta_7^{-1} \cdot \zeta_{13} = \frac{1+3\overline{\omega}}{1+3\omega} \cdot \frac{1+4\omega}{1+4\overline{\omega}} = \frac{99}{91} + \frac{19}{91}\omega.$$

This lies in the sixth sextant. Its associate in the second sextant is $\frac{80}{91} + \frac{99}{91}\omega$. The corresponding primitive Eisenstein triples is et $\left(\frac{80}{91} + \frac{99}{91}\omega\right) = (80, 99, 91)$.
Case 3: $\epsilon_1 = 1, \epsilon_2 = -1$. Compute $\zeta_7 \cdot \zeta_{13}$:

$$\zeta_7 \cdot \zeta_{13}^{-1} = \frac{1+3\omega}{1+3\overline{\omega}} \cdot \frac{1+4\overline{\omega}}{1+4\omega} = \frac{80}{91} - \frac{19}{91}\omega.$$

This lies in the fifth sextant. Its associate in the second sextant is $\frac{19}{91} + \frac{99}{91}\omega$. The corresponding primitive Eisenstein triples is et $\left(\frac{19}{91} + \frac{99}{91}\omega\right) = (19, 99, 91)$.
Case 4: $\epsilon_1 = -1, \epsilon_2 = -1$. Compute $\zeta_7 \cdot \zeta_{13}$:

$$\zeta_7^{-1} \cdot \zeta_{13}^{-1} = \frac{1+3\overline{\omega}}{1+3\omega} \cdot \frac{1+4\overline{\omega}}{1+4\omega} = \frac{11}{91} - \frac{85}{91}\omega.$$

This lies in the fifth sextant. Its associate in the second sextant is $\frac{85}{91} + \frac{96}{91}\omega$. The corresponding primitive Eisenstein triples is et $\left(\frac{85}{91} + \frac{96}{91}\omega\right) = (85, 96, 91)$.

Therefore, $\mathrm{ET}_{49} = \{(11, 96, 91), (85, 96, 91), (80, 99, 91), (19, 99, 91)\}$.

6. Conclusion

This paper develops a unified framework for primitive Eisenstein triples, those integer triangles with a 60–degree angle and side lengths satisfying the classical Eisenstein relation. The key idea is to translate triples into points on the ω–rational unit circle and back. Using unique factorization in the ring of Eisenstein integers, we show that the ω–rational unit circle splits cleanly into two parts: a finite set of six units and a free abelian group with basis given by the collection $\{\zeta_p \mid p \in P_1\}$, where P_1 is the set of primes congruent to one modulo three. Every ω–rational point can be written uniquely as a unit times a product of these generators. Choosing a canonical representative in the second sextant and clearing denominators gives a direct and lossless way to pass from points to primitive triples. This perspective yields sharp existence and counting results for a fixed hypotenuse. Write the hypotenuse as a product of rational primes. Primitive Eisenstein triples exist exactly when every prime factor is congruent to one modulo three. In that case, if there are k distinct such primes, the number of primitive triples with that hypotenuse is exactly two to the power k. Practically, the test for existence reduces to a single inspection of the prime factorization, and enumeration follows immediately. Algorithmically, recovering the side lengths from a chosen omega–rational point—or directly from the factorization of the hypotenuse—enables efficient generation at scale.

It would be interesting to investigate whether the distribution and averaging of counts for a fixed hypotenuse admit a generating-function treatment in which Stirling numbers of the second kind or Whitney numbers arise naturally; we leave this as future work (see, e.g., [16, 17]).

Acknowledgements

S. Jitmam was supported by the National Research Council of Thailand and Silpakorn University under Research Grant N42A650381.

References

[1] Wacław Sierpiński. *Pythagorean Triangles.* Dover Publications, Mineola, NY, 2011.

[2] Charles L. Shedd. A hypotenuse common to 64 primitive right triangles. *Scripta Mathematica*, 15:131–132, 1949.

[3] E. Eckert. The group of primitive Pythagorean triangles. *Mathematics Magazine*, 57:22–27, 1984.

[4] Lin Tan. The Group of Rational Points on the Unit Circle. *Mathematics Magazine*, 69(3):163–171, 1996.

[5] Amnon Yekutieli. Pythagorean Triples, Complex Numbers, Abelian Groups and Prime Numbers. *The American Mathematical Monthly*, 130(4):321–334, 2023.

[6] Bob Burn. 87.23 Triangles with a 60° Angle and Sides of Integer Length. *The Mathematical Gazette*, 87(508):148–153, 2003.

[7] John Gilder. Integer-sided triangles with an angle of 60°. *The Mathematical Gazette*, 66:261–266, 1982.

[8] Emrys Read. On integer-sided triangles containing angles of 120° or 60°. *The Mathematical Gazette*, 90:299–305, 2006.

[9] Keith Selkirk. Integer-Sided Triangles with an Angle of 120°. *The Mathematical Gazette*, 67(442):251–255, 1983.

[10] Russell A. Gordon. Properties of Eisenstein triples. *Mathematics Magazine*, 85:12–25, 2012.

[11] J. H. Conway and R. Guy. *The Book of Numbers.* Springer, New York, NY, 2012.

[12] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, New York, NY, 2 edition, 1990.

[13] R. Takloo-Bighash. *A Pythagorean Introduction to Number Theory: Right Triangles, Sums of Squares, and Arithmetic.* Undergraduate Texts in Mathematics. Springer International Publishing, 2018.

[14] Philip P. West and Brian D. Sittinger. A Further Stroll into the Eisenstein Primes. *The American Mathematical Monthly*, 124:609–620, 2017.

[15] Kamal Bahmanpour. Prime numbers p with expression $p = a^2 \pm ab \pm b^2$. *Journal of Number Theory*, 166:208–218, 2016.

[16] D. S. Kim and T. Kim. Moment Representations of Fully Degenerate Bernoulli and Degenerate Euler Polynomials. *Russian Journal of Mathematical Physics*, 32(31):682–690, 2024.

[17] T. Kim and D. S. Kim. Spivey-Type Recurrence Relations for Degenerate Bell and Dowling Polynomials. *Russian Journal of Mathematical Physics*, 32(2):288–296, 2025.