entropy

MDPI

Article

On Algebraic Properties of Primitive Eisenstein Integers with Applications in Coding Theory

Abdul Hadi [1,2], Uha Isnaini [1], Indah Emilia Wijayanti [1] and Martianus Frederic Ezerman [3,*]

[1] Department of Mathematics, Universitas Gadjah Mada, Sekip Utara Bulaksumur 21, Yogyakarta 55281, Indonesia; abdulhadi1989@mail.ugm.ac.id or abdulhadi@lecturer.unri.ac.id (A.H.); isnainiuha@ugm.ac.id (U.I.); ind_wijayanti@ugm.ac.id (I.E.W.)
[2] Department of Mathematics, Universitas Riau, Tampan, Pekanbaru 28293, Indonesia
[3] School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Singapore
* Correspondence: fredezerman@ntu.edu.sg

Abstract: An even Eisenstein integer is a multiple of an Eisenstein prime of the least norm. Otherwise, an Eisenstein integer is called odd. An Eisenstein integer that is not an integer multiple of another one is said to be primitive. Such integers can be used to construct signal constellations and complex-valued codes over Eisenstein integers via a carefully designed modulo function. In this work, we establish algebraic properties of even, odd, and primitive Eisenstein integers. We investigate conditions for the set of all units in a given quotient ring of Eisenstein integers to form a cyclic group. We perform set partitioning based on the multiplicative group of the set. This generalizes the known partitioning of size a prime number congruent to 1 modulo 3 based on the multiplicative group of the Eisenstein field in the literature.

Keywords: Eisenstein integers; unit group; set partitioning; signal constellation

check for updates

Academic Editor: Lu Wei

Received: 27 February 2025
Revised: 17 March 2025
Accepted: 17 March 2025
Published: 24 March 2025

Citation: Hadi, A.; Isnaini, U.; Wijayanti, I.E.; Ezerman, M.F. On Algebraic Properties of Primitive Eisenstein Integers with Applications in Coding Theory. *Entropy* **2025**, *27*, 337. https://doi.org/10.3390/e27040337

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Eisenstein integers, named after the mathematician Ferdinand Gotthold Max Eisenstein, are complex numbers that can be expressed as $\alpha := a + b\rho$, where a and b are integers and $\rho = e^{2\pi i/3} = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ such that $\rho^3 = 1$ in $\mathbb{C}$ and $i^2 = -1$. The integers a and b are the *real part* and the *rho part*, respectively. Since the set of all Eisenstein integers, denoted by $\mathbb{Z}[\rho]$, forms a commutative ring with identity, it is commonly referred to as *the ring of Eisenstein integers* [1]. Occasionally, it is also called *the ring of Eisenstein–Jacobi integers*. The integers possess remarkable geometric properties. They form a hexagonal lattice in the complex plane, making them particularly useful in coding theory, cryptography, and signal processing. They allow for optimal packing and minimal energy configurations in various practical setups. The ring $\mathbb{Z}[\rho]$ is a Euclidean domain and, hence, is also a principal ideal domain and a unique factorization domain. Inspired by the algebraic properties of Gaussian integers discussed in, e.g., [2,3], many researchers have discovered properties of $\mathbb{Z}[\rho]$ by generalizing important properties of the ring of integers $\mathbb{Z}$ and the ring of Gaussian integers $\mathbb{Z}[i]$. We know of fundamental concepts such as the factor ring, the unit structure of the factor ring, and the Euler-Totient function on Eisenstein integers from results presented in [4–7].

Gullerud and Mbirika in [7] introduced the notion of even and odd numbers in $\mathbb{Z}[\rho]$. Revisiting their motivation, the prime number 2 has the least norm, in this case defined as the absolute value, in $\mathbb{Z}$. The quotient by the ideal generated by the even prime 2 has two cosets that partition $\mathbb{Z}$ into even and odd integers. Since $1 - \rho$ and its *associates* are primes

with the least norm, to be formally defined below, in $\mathbb{Z}[\rho]$, we can pick $1-\rho$ to play the role of an even prime in $\mathbb{Z}[\rho]$, just like 2 in $\mathbb{Z}$. Unlike in $\mathbb{Z}$, however, the quotient by the ideal generated by $1-\rho$ is the set whose elements partition $\mathbb{Z}[\rho]$ into three sets, which we call *even*, *odd of Type 1*, and *odd of Type 2* sets. Some of their properties were investigated based on the norm and the sum of the real and the rho parts in [7].

In $\mathbb{Z}[\rho]$, an Eisenstein integer that is not an integer multiple of another is called *primitive*. Such an integer can be used to construct signal constellations and complex-valued codes over Eisenstein integers. These codes are obtained through a modulo function. Complex-valued codes are mathematical representations of coded symbols in communication systems, where codewords are constructed from complex numbers rather than real-valued symbols. These codes are particularly useful in digital communication for efficient modulation and error correction. We have provided a necessary and sufficient condition for an Eisenstein integer to be primitive in [8]. In that same work, we also constructed signal constellations for codes over $\mathbb{Z}[\rho]$ by studying primitive and non-primitive Eisenstein integers. In communication systems, a *signal constellation* is a physical diagram that depicts all possible symbols used by a signaling system to transmit data better. Mathematically, a signal constellation is a set of the residual class rings obtained by taking some modulo. Eisenstein integers have been used in designing denser and more efficient patterns in signal transmission. Such patterns have been shown to be beneficial in modern approaches, such as multiple input multiple output (MIMO) in [9], physical-layer network coding in [10–13], and compute and forward in [14].

Primitive Eisenstein integers exhibit excellent algebraic and number theoretic properties for applications in cryptography and error-correcting codes. There is an isomorphism between $\mathbb{Z}[\rho]$ modulo a primitive Eisenstein integer and $\mathbb{Z}$ modulo an integer, based on Theorem 8 below. In this work, we focus on discovering further algebraic properties of primitive Eisenstein integers as well as even and odd Eisenstein integers.

The multiplicative group of units in the quotient ring of Eisenstein integers has applications in coding theory. It has been used as QAM signals in [15,16], for enhanced spatial modulation in [17], and as a tool for set partitioning and multilevel-coded modulation in [18]. The set partitioning method leverages on the cyclic group structure of the units in the Eisenstein field $\mathbb{Z}[\rho]/\langle\psi\rangle$ such that the norm of ψ is a prime integer $q \equiv 1 \pmod 3$.

Constructions of codes over a number of other rings based on their primitive elements have been proposed in the literature. They utilize an isomorphism between a quotient ring induced by a primitive element and the ring of integers modulo the norm of a primitive element. The isomorphism sends a one-dimensional signal to a higher-dimensional signal. This general approach has been successfully performed to obtain codes. Examples include codes over $\mathbb{Z}[i]$ built based on primitive Gaussian integers in [19], codes over Lipschitz integers based on primitive Lipschitz integers in [20], and codes over Hurwitz integers, again using the primitive Lipschitz integers in [21–23]. The properties of primitive Lipschitz integers that are beneficial for encoding can be found in [24].

Li, Gan, and Ling in [25] provided a necessary and sufficient condition for two Eisenstein integers to be relatively prime.

Theorem 1 ([25]). *Two arbitrary Eisenstein integers α and θ are relatively prime if and only if*

$$\gcd\left(N_\rho(\alpha), N_\rho(\theta), \frac{2}{\sqrt{3}}\operatorname{Im}(\alpha\bar{\theta})\right) = 1,$$

with $\bar{\theta}$ being the conjugate of θ, or, equivalently,

$$\gcd\left(N_\rho(\alpha), N_\rho(\theta), \operatorname{Re}(\alpha\bar{\theta}) - \frac{1}{\sqrt{3}}\operatorname{Im}(\alpha\bar{\theta})\right) = 1.$$

We also know, this time from [26] that, if a Gaussian integer α and its conjugate $\bar{\alpha}$ are relatively prime, then $\alpha^{-1} \pmod{\bar{\alpha}}$ is an integer. This fact is useful in constructing multi-channel modulo samplers from Gaussian integers. It seems that no one has checked if the analogue of the fact and its application work over $\mathbb{Z}[\rho]$.

Freudenberger and Shavgulidze in [18] considered finite sets of Eisenstein integers $\mathcal{E}_\eta = \{\mu_\eta(\alpha) : \alpha \in \mathbb{Z}_{N_\rho(\eta)}\}$. They paid special attention to the case of $\eta = \psi$, which is a primitive and prime Eisenstein integer whose norm is a prime $q \equiv 1 \pmod 3$, as a two-dimensional signal constellation. Computing $\mu_\psi(\alpha)$ according to (2) below, the set of all units in $\mathcal{E}_\eta$, denoted by $(\mathcal{E}_\psi)^*$, can then be considered as a signal constellation for the general spatial modulation. In general, $\mathcal{E}_\eta$ is a representation of the quotient ring of Eisenstein integers only when η is primitive. In such a case, we can then partition $(\mathcal{E}_\psi)^*$ into $n = \frac{\varphi(\psi)}{6}$ subsets, indexed by $j \in \{0, 1, \ldots, n-1\}$, as

$$(\mathcal{E}_\psi)^*_{(j)} = \{\alpha^{n+j}, \alpha^{2n+j}, \alpha^{3n+j}, \alpha^{4n+j}, \alpha^{5n+j}, \alpha^{6n+j}\} = \{\pm\alpha^j, \pm\rho\alpha^j, \pm(1+\rho)\alpha^j\},$$

with α being a generator of the cyclic group $(\mathcal{E}_\psi)^*$ that corresponds to the generator of the cyclic group $(\mathbb{Z}[\rho]/\langle\psi\rangle)^*$. We can perform set partitioning on $(\mathcal{E}_\psi)^*_{(j)}$ according to the following theorem to obtain a larger minimum distance in each subset.

Theorem 2 (Proposition 1 in [18]). *Let $j \in \{0, 1, \ldots, n-1\}$. The minimum Euclidean distance in $(\mathcal{E}_\psi)^*_{(j)}$ is $\|\alpha^j\|$. We can partition $(\mathcal{E}_\psi)^*_{(j)}$ further into three subsets*

$$(\mathcal{E}_\psi)^*_{(j)} = \{\pm\alpha^j\} \cup \{\pm\rho\alpha^j\} \cup \{\pm(1+\rho)\alpha^j\},$$

each with minimum Euclidean distance $2\|\alpha^j\|$. We can also partition $(\mathcal{E}_\psi)^*_{(j)}$ into two subsets

$$(\mathcal{E}_\psi)^*_{(j)} = \{\alpha^j, \rho\alpha^j, -(1+\rho)\alpha^j\} \cup \{-\alpha^j, -\rho\alpha^j, (1+\rho)\alpha^j\},$$

each with minimum Euclidean distance $\sqrt{3}\|\alpha^j\|$.

In this paper, we gladly report the following contributions.

1. We establish further algebraic properties of primitive, even, and odd Eisenstein integers. We then answer Question 6.1 in [7]. Let ψ be an Eisenstein prime such that $N_\rho(\psi) = q$ is a prime integer and $q \equiv 1 \pmod 3$.
   a. Are the (non-associate) distinct pairs of primes ψ and $\bar{\psi}$ always of the same odd class? The answer is *yes, they are*.
   b. Does the corresponding q predict the odd class of ψ and $\bar{\psi}$? The answer is *no, it does not*.
2. Taking advantage of Theorem 1, our Theorem 22 confirms that, if Eisenstein integers α and $\bar{\alpha}$ are relatively prime, then $\alpha^{-1} \pmod{\bar{\alpha}}$ is in $\mathbb{Z}$. This result leads to a construction of multi-channel modulo samplers.
3. We prove important properties of the set of all units in a quotient ring of $\mathbb{Z}[\rho]$ when the set forms a cyclic group. The multiplicative group of the set leads to a nice set partitioning that generalizes Theorem 2 by using the modulo function in (1), which differs from the original modulo function in (2).

In terms of organization, Section 2 reviews known properties of Eisenstein integers. Section 3 presents our new results. We establish the algebraic properties of Eisenstein integers related to their being even, odd, or primitive. We look into the cyclic groups in the quotient ring. Set partitioning based on the multiplicative group of units in the quotient ring is the focus of Section 4. Section 5 highlights the role of primitive Eisenstein

integers in the relevant code constructions. Section 6 contains a summary and several concluding remarks.

2. Preliminaries

This section recalls known properties of Eisenstein integers related to their being prime, primitive, odd or even. We also recall useful results on the quotient rings and and the unit group in a quotient ring.

2.1. Ring of Eisenstein Integers

Since $\rho = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ is a complex primitive third root of unity, we have $\rho^3 = 1$ and $(\rho - 1)(\rho^2 + \rho + 1) = 0$ implies $\rho^2 + \rho + 1 = 0$. Addition and multiplication in $\mathbb{Z}[\rho]$ are defined, respectively, by

$$\begin{aligned}(a + b\rho) + (c + d\rho) &= (a + c) + (b + d)\rho \\ (a + b\rho) \cdot (c + d\rho) &= (ac - bd) + (ad + bc - bd)\rho.\end{aligned}$$

The *conjugate* and *norm* of $\alpha = a + b\rho \in \mathbb{Z}[\rho]$ for $a, b \in \mathbb{Z}$ are defined, respectively, as

$$\bar{\alpha} = (a - b) - b\rho \text{ and } N_\rho(\alpha) = N_\rho(\bar{\alpha}) = \alpha\,\bar{\alpha} = a^2 + b^2 - ab \in \mathbb{Z}.$$

By definition, $N_\rho(\alpha) = \|\alpha\|^2$, where $\|\cdot\|$ denotes the Euclidean distance, and the norm is multiplicative since $N_\rho(\alpha\theta) = N_\rho(\alpha)\,N_\rho(\theta)$ for all $\alpha, \theta \in \mathbb{Z}[\rho]$.

The division algorithm works over $\mathbb{Z}[\rho]$, i.e., for $\alpha, \eta \neq 0 \in \mathbb{Z}[\rho]$, there exists a unique quotient θ and a remainder δ in $\mathbb{Z}[\rho]$ such that $\alpha = \theta\eta + \delta$ and $N_\rho(\delta) < N_\rho(\eta)$. Since $\mathbb{Z}[\rho]$ is a Euclidean domain (ED), it is a principal ideal domain (PID) and a unique factorization domain (UFD).

In $\mathbb{Z}[\rho]$, an element η divides α, denoted by $\eta \mid \alpha$, if there exists $\theta \in \mathbb{Z}[\rho]$ such that $\alpha = \theta\eta$. We say that α is a *unit* in $\mathbb{Z}[\rho]$ if $\alpha\lambda = 1$ for some $\lambda \in \mathbb{Z}[\rho]$. A unit has a unique multiplicative inverse. It is known that α is a unit if and only if $N_\rho(\alpha) = 1$ and that $\mathbb{Z}[\rho]$ has 6 units. These are $\pm 1, \pm\rho$, and $\pm(1 + \rho)$. We say that α and β are *associates*, denoted by $\alpha \sim \eta$, if $\alpha = \theta\,\eta$ for some unit $\theta \in \mathbb{Z}[\rho]$. The associates of $\alpha = a + b\rho$ are $\pm\alpha$, $\pm\rho\alpha$, and $\pm(1 + \rho)\alpha$, with $\rho\alpha = -b + (a - b)\,\rho$ and $(1 + \rho)\alpha = (a - b) + a\,\rho$.

The *greatest common divisor* (GCD) ω of $\alpha, \theta \in \mathbb{Z}[\rho]$, denoted by $\omega := \gcd(\alpha, \theta)$, is the largest Eisenstein integer in terms of modulus, up to multiplication by any unit, that divides *both* α and θ. Every common divisor of α and θ divides ω.

Let $Q(\cdot)$ denote the quantization to the closest Eisenstein integer in as [27,28]. Fixing a nonzero $\eta \in \mathbb{Z}[\rho]$, we can define a *modulo function* $\mu_\eta(\cdot)$ as

$$\mu_\eta(\alpha) := \alpha \pmod{\eta} = \alpha - Q(\tfrac{\alpha}{\eta}) \cdot \eta. \tag{1}$$

Algorithm 1, which computes a remainder $\mu_\eta(\alpha)$ when α is divided by η, is a slight adaptation of the version in [11,27].

We highlight that the modulo function μ_η in (1) is different from the modulo function

$$\mu_\eta(\alpha) = \alpha - \lfloor \tfrac{\alpha}{\eta} \rceil \eta, \tag{2}$$

with $\lfloor \cdot \rceil$ denoting the rounding to the nearest integer as defined in [29]. For avoidance of doubt, we choose to define $\lfloor x \rceil := \lfloor x + 0.5 \rfloor$ for all $x \in \mathbb{R}$ in this paper. Our choice is somewhat arbitrary. If so desired, one can define $\lfloor x \rceil := \lceil x - 0.5 \rceil$ for all $x \in \mathbb{R}$.

Algorithm 1: Finding a remainder $\delta := \alpha \pmod{\eta}$ on input a given α and a fixed η.

1. $z \leftarrow \frac{\alpha}{\eta} = \mathrm{Re}(z) + \mathrm{Im}(z)i$ and $z - \rho \leftarrow \mathrm{Re}(z-\rho) + \mathrm{Im}(z-\rho)i$.
2. The nearest Eisenstein integers $\theta_1 \in \mathbb{Z}[\sqrt{3}i]$ and $\theta_2 \in \rho + \mathbb{Z}[\sqrt{3}i]$ are

$$\theta_1 \leftarrow \lfloor \mathrm{Re}(z) \rceil + \left\lfloor \frac{\mathrm{Im}(z)}{\sqrt{3}} \right\rceil \sqrt{3}i$$
$$\theta_2 \leftarrow \lfloor \mathrm{Re}(z-\rho) \rceil + \left\lfloor \frac{\mathrm{Im}(z-\rho)}{\sqrt{3}} \right\rceil \sqrt{3}i + \rho.$$

3. $\delta_1 \leftarrow \alpha - \theta_1 \eta$ and $\delta_2 \leftarrow \alpha - \theta_2 \eta$.
4. Output $\delta := \alpha \pmod{\eta}$ based on

$$\delta \leftarrow \delta_1, \text{ if } N_\rho(\delta_1) < N_\rho(\delta_2), \text{ or } N_\rho(\delta_1) = N_\rho(\delta_2) \text{ and } \mathrm{Re}(\theta_1) < \mathrm{Re}(\theta_2),$$
$$\delta \leftarrow \delta_2, \text{ otherwise.}$$

We use the modulo function in (1) because it gives us $N_\rho(\mu_\eta(\alpha)) = N_\rho(\delta) \leq N_\rho(\alpha)$ for every $\alpha \in \mathbb{Z}[\rho]$. In contrast, using (2) over $\mathbb{Z}[\rho]$ implies the existence of $\eta \in \mathbb{Z}[\rho]$ such that $N_\rho(\mu_\eta(\alpha)) > N_\rho(\alpha)$ for some $\alpha \in \mathbb{Z}[\rho]$.

Example 1. *Let* $\eta = -6 + 5\rho$ *and* $\alpha = 5$. *Since*

$$\frac{5}{-6+5\rho} = \frac{5(-11-5\rho)}{(-6+5\rho)(-11-5\rho)} = \frac{-55}{91} + \frac{-25}{91}\rho,$$

we have

$$\left\lfloor \frac{5}{-6+5\rho} \right\rceil = \left\lfloor \frac{-55}{91} \right\rceil + \left\lfloor \frac{-25}{91} \right\rceil \rho = -1 + 0\rho = -1.$$

Applying (2), *we obtain*

$$\mu_\eta(5) = 5 - (-1)(-6+5\rho) = -1 + 5\rho \text{ and}$$
$$N_\rho(\mu_\eta(5)) = N_\rho(-1+5\rho) = 31 > 25 = N_\rho(5).$$

2.2. Prime and Primitive Eisenstein Integers

An $\alpha \in \mathbb{Z}[\rho]$ is called *(Eisenstein) prime* if α cannot be expressed as $\alpha = \theta\eta$ where θ and η are not units in $\mathbb{Z}[\rho]$. In other words, α is Eisenstein prime if *all* of its divisors are of the form $u\,\alpha$ with $u \in \{\pm 1, \pm\rho, \pm(1+\rho)\}$. Otherwise, α is *(Eisenstein) composite*. An $\alpha = a + b\rho$ is primitive if $\gcd(a, b) = 1$.

Eisenstein primes are classified as follows:

1. The prime $1 - \rho$ and its associates.
2. The prime $c + d\,\rho$, with $N_\rho(c + d\,\rho) = q$ such that q is a prime in $\mathbb{Z}$, with $q \equiv 1 \pmod 3$, and its associates.
3. The prime $p \in \mathbb{Z}$ such that $p \equiv 2 \pmod 3$ and its associates.

For the rest of this paper, let $\beta := 1 - \rho$ and let p and q be prime integers such that $p \equiv 2 \pmod 3$ and $q = \psi\,\bar{\psi} \equiv 1 \pmod 3$, where ψ and $\bar{\psi}$ are non-associate Eisenstein primes. We denote a generic Eisenstein prime by γ.

Remark 1. *Units as well as Eisenstein primes* β *and* ψ *up to associates are primitive Eisenstein integers. Any prime integer* $p \equiv 2 \pmod 3$ *and its associates are* not *primitive Eisenstein integers. We note that* $5 + 4\rho$ *is primitive but not an Eisenstein prime since* $5 + 4\rho = (1-\rho)(2+3\rho)$.

Theorem 3 ([30]). *If γ_1 and γ_2 are Eisenstein primes such that $N_\rho(\gamma_1) = N_\rho(\gamma_2)$, then $\gamma_1 \sim \gamma_2$ or $\gamma_1 \sim \overline{\gamma_2}$. If $N_\rho(\gamma_1) = 3$, then $\gamma_1 \sim \beta$. If $N_\rho(\gamma_1) = p^2$, with $p \equiv 2 \pmod 3$, then $\gamma_1 \sim \overline{\gamma_1}$. Lastly, if q is a prime integer such that $N_\rho(\gamma_1) = q \equiv 1 \pmod 3$, then $\gamma_1 \not\sim \overline{\gamma_1}$.*

Theorem 4 ([8]). *Given any two elements $\alpha, \theta \in \mathbb{Z}[\rho]$, we have $N_\rho(\alpha) = N_\rho(\theta) \in \mathbb{Z}$ if and only if $\alpha \sim \theta$ or $\alpha \sim \bar{\theta}$.*

Gullerud and Mbirika stated in Theorem 5.8 of [7] that any power of an Eisenstein prime ψ is a primitive element. To prove this valid claim, they had assumed that if the norms of two Eisenstein integers are the same, then they are associates. This *assumption is invalid*. Theorem 4 states that it does *not* hold in general. We reproduce the original theorem and supply a proof in Appendix A. Our proof uses Theorem 4.

Theorem 5 (Theorem 5.8 in [7]). *Let $\psi = x + y\rho$ be a prime in $\mathbb{Z}[\rho]$. If $N_\rho(\psi) = q \equiv 1 \pmod 3$ be such that q is a prime in $\mathbb{Z}$, then ψ^n is a primitive Eisenstein integer for all $n \in \mathbb{N}$.*

Proof. See Appendix A. □

In another recent work, we have established a necessary and sufficient condition for an Eisenstein integer to be primitive.

Theorem 6 ([8]). *An Eisenstein integer η is primitive if and only if $\eta \sim \beta^r \psi_1^{r_1} \cdots \psi_m^{r_m}$, with*

- *$r \in \{0, 1\}$, m, and r_i are nonnegative integers,*
- *$N_\rho(\psi_i) = q_i \in \mathbb{Z}$ is a prime such that $q_i \equiv 1 \pmod 3$ for $0 \le i \le m$,*
- *$q_i \neq q_j$ for $i, j \in \{0, 1, \ldots, m\}$ such that $i \neq j$.*

2.3. On the Quotient Ring of Eisenstein Integers

Since $\mathbb{Z}[\rho]$ is a PID, any ideal is of the form $\langle \eta \rangle$ for some $\eta \in \mathbb{Z}[\rho]$. A congruence in $\mathbb{Z}[\rho]$ modulo $\langle \eta \rangle$ can then be defined. For any $\alpha, \theta \in \mathbb{Z}[\rho]$, we have $\alpha \equiv \theta \pmod \eta$ if and only if $\alpha - \theta \in \langle \eta \rangle$. For any $\alpha \in \mathbb{Z}[\rho]$, the *equivalence class* of α with respect to η, denoted by $[\alpha]_\eta$, is defined to be

$$[\alpha]_\eta = \{\theta \in \mathbb{Z}[\rho] \, : \, \theta \equiv \alpha \pmod \eta\}.$$

The set $\{[\alpha]_\eta \, : \, \alpha \in \mathbb{Z}[\rho]\}$ forms the *quotient ring* $\mathbb{Z}[\rho]/\langle \eta \rangle$.

We will soon make use of three results from [4].

Theorem 7 ([4]). *If $\eta \in \mathbb{Z}[\rho] \setminus \{0\}$ is such that $\eta = a + b\rho = t(m + n\rho)$, with $\gcd(a, b) = t$ and $\gcd(m, n) = 1$, then the complete residue system is*

$$\mathbb{Z}[\rho]/\langle \eta \rangle = \{[x + y\rho]_\eta \, : \, 0 \le x < tN_\rho(m + n\rho), \; 0 \le y < t\},$$

with $[x + y\rho]_\eta := x + y\rho + \langle \eta \rangle$.

Theorem 8 ([4]). *If η is a primitive Eisenstein integer, then $\mathbb{Z}[\rho]/\langle \eta \rangle \cong \mathbb{Z}_{N_\rho(\eta)}$.*

Theorem 9 ([4]). *If $n \in \mathbb{N}$, then $\mathbb{Z}[\rho]/\langle n \rangle \cong \mathbb{Z}_n[\rho]$.*

The ring $\mathbb{Z}_n[\rho]$ is known as *the ring of Eisenstein integers modulo n*.

2.4. Even and Odd Eisenstein Integers

By Theorem 7, for $\beta = 1 - \rho \in \mathbb{Z}[\rho]$, we have $\mathbb{Z}[\rho]/\langle\beta\rangle = \{[0]_\beta,\ [1]_\beta,\ [2]_\beta\}$, with

$$\begin{aligned}[0]_\beta &= \{x + y\rho \in \mathbb{Z}[\rho] \ : \ x + y\rho \equiv 0 \pmod{\beta}\},\\ [1]_\beta &= \{x + y\rho \in \mathbb{Z}[\rho] \ : \ x + y\rho \equiv 1 \pmod{\beta}\},\\ [2]_\beta &= \{x + y\rho \in \mathbb{Z}[\rho] \ : \ x + y\rho \equiv 2 \pmod{\beta}\}.\end{aligned}$$

An Eisenstein integer α is *even* if $\alpha \in [0]_\beta$. An Eisenstein integer α is *odd* if α is in $[1]_\beta \cup [2]_\beta$. More precisely, α is *odd of Type-1* if $\alpha \in [1]_\beta$. It is *odd of Type-2* if $\alpha \in [2]_\beta$. We denote the respective sets of all even, odd Type-1, and odd Type-2 Eisenstein integers by E, O_1, and O_2.

Remark 2. *By Theorem 6, an Eisenstein integer of the form $(1+\rho)^\ell \beta \psi_1^{r_1} \cdots \psi_m^{r_m}$ is even primitive and an Eisenstein integer of the form $(1+\rho)^\ell \psi_1^{r_1} \cdots \psi_m^{r_m}$ is odd primitive.*

We have a simple characterization based on the sum of the real and the rho parts.

Theorem 10 ([7])**.** *For any $x + y\rho \in \mathbb{Z}[\rho]$, we have*

i. $x + y\rho \in E$ *if and only if* $x + y \equiv 0 \pmod 3$ *if and only if* $N_\rho(x + y\rho) \equiv 0 \pmod 3$.
ii. $x + y\rho \in O_1$ *if and only if* $x + y \equiv 1 \pmod 3$, *which implies* $N_\rho(x + y\rho) \equiv 1 \pmod 3$.
iii. $x + y\rho \in O_2$ *if and only if* $x + y \equiv 2 \pmod 3$, *which implies* $N_\rho(x + y\rho) \equiv 1 \pmod 3$.

Example 2. *A prime β, its associates and multiples are even Eisenstein integers. The other primes are odd Eisenstein integers. The prime $\psi_1 = 2 + 3\rho$ is an odd Eisenstein integer of Type-2. The prime $\psi_2 = 3 + 4\rho$ is an odd Eisenstein integer of Type-1. Any prime integer $p \equiv 2 \pmod 3$ is an odd Eisenstein integer of Type-2.*

Theorem 11 ([7])**.** *If α, θ, τ, τ', σ, and σ' are in $\mathbb{Z}[\rho]$ such that $\theta \in E$, $\tau, \tau' \in O_1$, and $\sigma, \sigma' \in O_2$, then*

$$\alpha \cdot \theta \in E, \quad \tau \cdot \sigma \in O_2, \quad \tau \cdot \tau' \text{ and } \sigma \cdot \sigma' \in O_1.$$

2.5. Unit Group in the Quotient Ring of Eisenstein Integers

The set of all units in $\mathbb{Z}[\rho]/\langle\eta\rangle$, formally defined to be

$$(\mathbb{Z}[\rho]/\langle\eta\rangle))^* = \{[\alpha]_\eta \in \mathbb{Z}[\rho]/\langle\eta\rangle \ : \ \gcd(\alpha, \eta) = 1\},$$

is a group under multiplication. The Euler-Totient function with respect to $\eta \in \mathbb{Z}[\rho]$ is the order of unit group $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$,

$$\varphi_\rho(\eta) = |(\mathbb{Z}[\rho]/\langle\eta\rangle)^*|.$$

If η and 1 are associates, then $\varphi_\rho(\eta) = 1$.

Recall that γ denotes a generic Eisenstein prime. We have the following easy way to determine the units in $\mathbb{Z}[\rho]/\langle\gamma^n\rangle$.

Theorem 12 ([4])**.** *The set of all units in $\mathbb{Z}[\rho]/\langle\gamma^n\rangle$ are*

$$\begin{aligned}(\mathbb{Z}[\rho]/\langle\beta^n\rangle)^* &= \{[x + y\rho]_{\beta^n} \in \mathbb{Z}[\rho]/\langle\beta^n\rangle \ : \ x + y \not\equiv 0 \pmod 3\},\\ (\mathbb{Z}[\rho]/\langle\psi^n\rangle)^* &= \{[x]_{\psi^n} \in \mathbb{Z}[\rho]/\langle\psi^n\rangle \ : \ \gcd(x, q) = 1\},\\ (\mathbb{Z}[\rho]/\langle p^n\rangle)^* &= \{[x + y\rho]_{p^n} \in \mathbb{Z}[\rho]/\langle p^n\rangle \ : \ \gcd(x, p) = 1 \text{ or } \gcd(y, p) = 1\}.\end{aligned}$$

The unit group $\mathbb{Z}_n^*$ in $\mathbb{Z}$ is cyclic if and only if $n \in \{2, 4, p^k, 2p^k\}$, where p is an odd prime and k is a positive integer. A necessary and sufficient condition for the unit group $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$ to be cyclic is known.

Theorem 13 ([31,32]). *A unit group $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$ is cyclic if and only if*

$$\eta \text{ is an element or an associate of an element in } \{\beta, \beta^2, 2\beta, \psi^k, p\},$$

where $k \in \mathbb{N}$, ψ is an Eisenstein prime such that $N_\rho(\psi) = q \equiv 1 \pmod 3$, and p is a prime integer such that $p \equiv 2 \pmod 3$.

Theorem 14 ([7]). *If $\eta \in \mathbb{Z}[\rho] \setminus \{0\}$, then $\varphi_\rho(\eta)$ is even, except when η is a unit, or η and 2 are associates.*

Theorem 15 ([33]). *Let $\eta \in \mathbb{Z}[\rho] \setminus \{0\}$ be such that η is not a unit. If $\beta \not\sim \eta \not\sim 2$, then $6 \mid \varphi_\rho(\eta)$.*

Theorem 16 ([33]). *If $\eta \sim n$ for an $n \in \mathbb{Z}$, then $\varphi(n) \mid \varphi_\rho(\eta)$ and $\varphi(\varphi(n)) \leq \varphi(\varphi_\rho(\eta))$. In particular, for any positive integer k,*

$$\varphi_\rho(\eta) = \begin{cases} \varphi(n), & \text{if } n = 1, \\ n\varphi(n), & \text{if } n = 3^k, \\ (\varphi(n))^2, & \text{if } n = q^k, \text{ with } q \equiv 1 \pmod 3 \text{ being a prime integer}, \\ \left(n + \frac{n}{p}\right)\varphi(n), & \text{if } n = p^k, \text{ with } p \equiv 2 \pmod 3 \text{ being a prime integer}. \end{cases}$$

3. Further Properties of Eisenstein Integers

We discuss further properties of primitive, even, and odd Eisenstein integers in the first subsection. The second subsection centers on the cyclic group of units in the quotient rings of Eisenstein integers.

3.1. On Even, Odd, and Primitive Eisenstein Integers

Theorem 17. *Let $\alpha, \theta \in \mathbb{Z}[\rho]$. The following statements hold:*

i. *If $\alpha, \theta \in E$, then $\alpha + \theta \in E$.*
ii. *If $\alpha, \theta \in O_1$, then $\alpha + \theta \in O_2$.*
iii. *If $\alpha, \theta \in O_2$, then $\alpha + \theta \in O_1$.*
iv. *If $\alpha \in O_1$ and $\theta \in O_2$, then $\alpha + \theta \in E$.*
v. *If $\alpha \in E$ and $\theta \in O_1$, then $\alpha + \theta \in O_1$.*
vi. *If $\alpha \in E$ and $\theta \in O_2$, then $\alpha + \theta \in O_2$.*

Proof. A straightforward application of Theorem 10 confirms the assertions. □

Theorem 18. *Let $\alpha, \theta \in \mathbb{Z}[\rho]$.*

i. *If $\alpha \in E$ and $\alpha \sim \theta$, then $\theta, \bar{\alpha} \in E$.*
ii. *If $\alpha \in O_1$ and $\alpha \sim \theta$, then $\theta = \alpha, \rho\alpha, -(1+\rho)\alpha \in O_1$, and $-\theta \in O_2$.*
iii. *If $\alpha \in O_2$ and $\alpha \sim \theta$, then $\theta = \alpha, \rho\alpha, -(1+\rho)\alpha \in O_2$, and $-\theta \in O_1$.*
iv. *If $\alpha \in O_1$, then $\bar{\alpha} \in O_1$.*
v. *If $\alpha \in O_2$, then $\bar{\alpha} \in O_2$.*

Proof. We proceed by items as listed.

i. Let $\alpha = a + b\rho \in E$ and $\theta \sim \alpha$. By Theorems 4 and 10, $N_\rho(\alpha) \equiv 0 \pmod 3$ and $N_\rho(\theta) = N_\rho(\alpha) = N_\rho(\bar{\alpha}) \equiv 0 \pmod 3$, affirming $\theta, \bar{\alpha} \in E$.

ii. Assuming $\alpha = a + b\rho \in O_1$ and $\alpha \sim \theta$, Theorem 10 yields $(a+b) \equiv 1 \pmod 3$. Hence,

$$\begin{aligned} -\alpha &= -a - b \equiv 2(a+b) \equiv 2 \pmod 3, \\ \rho\alpha &= -b + (a-b) \equiv a - 2b \equiv a + b \equiv 1 \pmod 3, \\ -\rho\alpha &= b + (b-a) \equiv 2b - a \equiv 2b + 2a \equiv 2(a+b) \equiv 2 \pmod 3, \\ -(1+\rho)\alpha &= (-a+b) - a \equiv b - 2a \equiv b + a \equiv 1 \pmod 3, \\ (1+\rho)\alpha &= a - b + a \equiv 2a - b \equiv 2(a+b) \equiv 2 \pmod 3. \end{aligned}$$

Thus, $\theta \in O_1$ and $-\theta \in O_2$ whenever $\theta \in \{\alpha, \rho\alpha, -(1+\rho)\alpha\}$.

iii. Assuming $\alpha = a + b\rho \in O_2$ and $\alpha \sim \theta$, Theorem 10 yields $(a+b) \equiv 2 \pmod 3$. Hence,

$$\begin{aligned} -\alpha &= -a - b \equiv 2(a+b) \equiv 4 \equiv 1 \pmod 3, \\ \rho\alpha &= -b + (a-b) \equiv a - 2b \equiv a + b \equiv 2 \pmod 3, \\ -\rho\alpha &= b + (b-a) \equiv 2b - a \equiv 2b + 2a \equiv 2(a+b) \equiv 4 \equiv 1 \pmod 3, \\ -(1+\rho)\alpha &= (-a+b) - a \equiv b - 2a \equiv b + a \equiv 2 \pmod 3, \\ (1+\rho)\alpha &= a - b + a \equiv 2a - b \equiv 2(a+b) \equiv 4 \equiv 1 \pmod 3. \end{aligned}$$

Thus, $\theta \in O_2$ and $-\theta \in O_1$ whenever $\theta \in \{\alpha, \rho\alpha, -(1+\rho)\alpha\}$.

iv. Assuming $\alpha = a + b\rho \in O_1$, Theorem 10 gives us $a + b \equiv 1 \pmod 3$. Hence, $a - b - b \equiv a - 2b \equiv a + b \equiv 1 \pmod 3$, ensuring $\bar{\alpha} \in O_1$

v. Assuming $\alpha = a + b\rho \in O_2$, we obtain $a + b \equiv 2 \pmod 3$ by Theorem 10. Hence, $a - b - b \equiv a - 2b \equiv a + b \equiv 2 \pmod 3$ and $-a - b \equiv 2(a+b) \equiv 4 \equiv 1 \pmod 3$, which means $\bar{\alpha} \in O_2$.

□

We can now answer Question 6.1 in [7].

- By Theorem 18 iv. and v., we conclude that distinct primes ψ and $\overline{\psi}$ which are non-associates always belong to the the same odd class. Both are in O_1 or both are in O_2.
- Any prime $q \equiv 1 \pmod 3$ is always in O_1. By Theorem 11, however, both ψ and $\overline{\psi}$ are in O_1 or both are in O_2. We note, for example, that both $\psi_1 = 2 + 3\rho$ and $\overline{\psi_1} = -1 - 3\rho$ are in O_2. Both $\psi_2 = 3 + \rho$ and $\overline{\psi_2} = 2 - \rho$ are in O_1, with $q = N_\rho(\psi_1) = N_\rho(\psi_2) = 7 \equiv 1 \pmod 3$ being in O_1. Without further investigation, the q that corresponds to a given ψ does not automatically identify which odd class both ψ and $\overline{\psi}$ belong to.

The next result is a corollary to Theorem 11.

Corollary 1. *Given an odd Eisenstein integer*

$$\eta = \prod_{\psi_i \in O_1} \psi_i^{r_i} \prod_{\psi_j \in O_2} \psi_j^{s_j} \prod_{p_k \in O_2} p_k^{t_k},$$

if $(\sum s_j + \sum t_k) \equiv 0 \pmod 2$, *then* $\eta \in O_1$. *Otherwise,* $\eta \in O_2$.

Proof. By Theorem 11, if $(\sum s_j + \sum t_k) \equiv 0 \pmod 2$, then

$$\prod_{\psi_i \in O_1} \psi_i^{r_i} \in O_1 \text{ and } \prod_{\psi_j \in O_2} \psi_j^{s_j} \prod_{p_k \in O_2} p_k^{t_k} \in O_1,$$

ensuring $\eta \in O_1$. If $(\sum s_j + \sum t_k) \equiv 1 \pmod 2$, then $\prod_{\psi_j \in O_2} \psi_j^{s_j} \prod_{p_k \in O_2} p_k^{t_k} \in O_2$. Since $\prod_{\psi_i \in O_1} \psi_i^{r_i} \in O_1$, we confirm that $\eta \in O_2$. □

Theorem 19. *The associates and conjugates of a primitive Eisenstein integer are also primitive Eisenstein integers.*

Proof. If $\eta = a + b\rho$ such that $\gcd(a, b) = 1$, then

$$\gcd(a - b, -b) = \gcd(b - a, b) = \gcd(-a, -b) = \gcd(a - b, a) = \gcd(b - a, -a) = 1.$$

Hence, its conjugate $\bar{\eta} = a - b - b\rho$ and associates $\pm\alpha, \pm\rho\alpha$ and $\pm(1 + \rho)\alpha$, with $\rho\alpha = -b + (a - b)\rho$ and $(1 + \rho)\alpha = (a - b) + a\rho$, are primitives. □

We know from Corollary 3 in [34] that an Eisenstein integer $\alpha = a + b\rho$ and its conjugate $\bar{\alpha}$ are relatively prime if and only if $\gcd(a - b, b) = 1$ and $\gcd(a - 2b, 3) = 1$. Since $\gcd(a - b, b) = 1$ is equivalent to $\gcd(a, b) = 1$, and $\gcd(a - 2b, 3) = 1$ is equivalent to $a + b \equiv \pm 1 \pmod 3$, we can use the following equivalent expression of the corollary.

Proposition 1. *An Eisenstein integer $\alpha = a + b\rho$ and its conjugate $\bar{\alpha}$ are relatively prime if and only if $\gcd(a, b) = 1$ and $a + b \equiv \pm 1 \pmod 3$. In short, an Eisenstein integer and its conjugate are relatively prime if and only if the Eisenstein integer is odd and primitive.*

The next result is a direct consequence of Proposition 1.

Corollary 2. *If an odd primitive Eisenstein integer η is not a unit, then η and $\bar{\eta}$ are not associates.*

Proof. Let η be an odd primitive Eisenstein integer such that η is not a unit. If η and $\bar{\eta}$ are associates, then $\gcd(\eta, \bar{\eta}) = \eta$, which contradicts Proposition 1. □

Theorem 20. *Let $\eta = \prod_{\psi_i \in O_1} \psi_i^{r_i} \prod_{\psi_j \in O_2} \psi_j^{s_j}$ be an odd primitive Eisenstein integer. If $\sum s_j \equiv 0 \pmod 2$, then $\eta \in O_1$. Otherwise, $\eta \in O_2$.*

Proof. By Theorem 11, if $\sum s_j \equiv 0 \pmod 2$, then

$$\prod_{\psi_i \in O_1} \psi_i^{r_i} \in O_1 \text{ and } \prod_{\psi_j \in O_2} \psi_j^{s_j} \in O_1,$$

implying $\eta \in O_1$. On the other hand, if $\sum s_j \equiv 1 \pmod 2$, then $\prod_{\psi_j \in O_2} \psi_j^{s_j} \in O_2$. Since $\prod_{\psi_i \in O_1} \psi_i^{r_i} \in O_1$, it is clear that $\eta \in O_2$. □

Theorem 21. *Let η be a non-unit primitive Eisenstein integer.*

i. If η is even, then $\gcd(\eta, \bar{\eta}) = \beta$.
ii. If η and β are not associates, then η and $\bar{\eta}$ are also not associates.

Proof. We prove the assertions according to their order of appearance.

i. Let $u \in \mathbb{Z}[\rho]$ be a unit and let $\eta = u\beta\psi_1^{r_1} \cdots \psi_k^{r_k}$. Since $\bar{\beta} = (1 + \rho)\beta$, we have

$$\bar{\eta} = (1 + \rho)u\beta\overline{\psi_1^{r_1}} \cdots \overline{\psi_k^{r_k}}.$$

By Proposition 1, we have $\gcd(\psi_1^{r_1} \cdots \psi_k^{r_k}, \overline{\psi_1^{r_1}} \cdots \overline{\psi_k^{r_k}}) = 1$. Thus, $\gcd(\eta, \bar{\eta}) = \beta$.

ii. For a contradiction, let us assume that η and $\bar{\eta}$ are associates. Let $u \in \mathbb{Z}[\rho]$ be a unit such that $\eta = u\psi_1^{r_1} \cdots \psi_k^{r_k}$. Then,

$$\psi_1^{r_1} \cdots \psi_k^{r_k} \sim \overline{\psi_1}^{r_1} \cdots \overline{\psi_k}^{r_k}, \text{ contradicting Corollary 2.}$$

If $\eta = u\beta\psi_1^{r_1}\cdots\psi_k^{r_k}$ for some unit $u \in \mathbb{Z}[\rho]$, then

$$\begin{aligned}\beta\psi_1^{r_1}\cdots\psi_k^{r_k} &\sim \bar{\beta}\overline{\psi_1}^{r_1}\cdots\overline{\psi_k}^{r_k},\\ \beta\psi_1^{r_1}\cdots\psi_k^{r_k} &\sim (1+\rho)\beta\overline{\psi_1}^{r_1}\cdots\overline{\psi_k}^{r_k},\\ \psi_1^{r_1}\cdots\psi_k^{r_k} &\sim \overline{\psi_1}^{r_1}\cdots\overline{\psi_k}^{r_k}, \text{ contradicting Corollary 2.}\end{aligned}$$

□

Theorem 22. *If an Eisenstein integer $\alpha = a + b\rho$ and its conjugate $\bar{\alpha}$ are relatively prime, then the modular multiplicative inverse $c \equiv \alpha^{-1} \pmod{\bar{\alpha}}$ is an integer.*

Proof. By Theorem 1 and recalling that $N_\rho(\alpha) = N_\rho(\bar{\alpha})$, we have

$$\begin{aligned}1 &= \gcd\left(N_\rho(\alpha), \frac{2}{\sqrt{3}}\operatorname{Im}(\alpha^2)\right) = \gcd(a^2+b^2-ab, b(2a-b))\\ &= \gcd(a^2+b^2-ab, b) = \gcd(a^2+b^2-ab, 2a-b).\end{aligned}$$

Hence, there are integers c and d such that

$$c(2a-b) + d(a^2+b^2-ab) = c(\alpha+\bar{\alpha}) + d\alpha\bar{\alpha} = 1.$$

We verify that $c\alpha \equiv 1 \pmod{\bar{\alpha}}$ and confirm that $c \equiv \alpha^{-1} \pmod{\bar{\alpha}}$. □

Corollary 3. *If η is an odd primitive Eisenstein integer, then the modular multiplicative inverse $c \equiv \eta^{-1} \pmod{\bar{\eta}}$ is an integer.*

Proof. By Proposition 1, $\gcd(\eta, \bar{\eta}) = 1$. Applying Theorem 22 settles the claim. □

Theorem 23. *An Eisenstein integer α is an associate of $\bar{\alpha}$ if and only if α is an associate of n or $k\beta$ for some $n, k \in \mathbb{Z}$.*

Proof. If $\alpha \sim n$ then $\bar{\alpha} \sim \bar{n}$ and $n \sim \alpha$. If $\alpha \sim k\beta$ for some $k \in \mathbb{Z}$, then $\bar{\alpha} \sim k\bar{\beta} \sim k\beta \sim \alpha$. Conversely, if $\alpha = a + b\rho$ and $\alpha \sim \bar{\alpha}$, then $\alpha = u\bar{\alpha}$ for some unit u in $\mathbb{Z}[\rho]$.

- If $u = 1$, then $a + b\rho = (a-b) - b\rho$. In this case, $b = 0$, which implies $\alpha = a$.
- If $u = \rho$, then $a + b\rho = b + a\rho$. Hence, $a = b$, implying $\alpha = a + a\rho = a(1+\rho)$.
- If $u = -(1+\rho)$, then $a + b\rho = -a + (b-a)\rho$. Hence, $a = 0$, which yields $\alpha = b\rho$.
- If $u = -1$, then $a + b\rho = (b-a) + b\rho$. We obtain $b = 2a$ and, hence, $\alpha = a + 2a\rho = a(1+2\rho)$.
- If $u = -\rho$, then $a + b\rho = -b - a\rho$. We obtain $b = -a$ and, therefore, $\alpha = a - a\rho = a(1-\rho)$.
- If $u = 1+\rho$, then $a + b\rho = a + (a-b)\rho$. We have $a = 2b$, which means $\alpha = 2b + b\rho = b(2+\rho)$.

Having covered all cases, we confirm that α is an associate of n or $k\beta$ for some $n, k \in \mathbb{Z}$. □

Recalling Theorem 3, we know that $\psi \not\sim \overline{\psi}$ whenever ψ is an Eisenstein prime.

Corollary 4. *If α is a primitive Eisenstein integer such that α is not a unit and α is neither β nor any of its associates, then α and $\bar{\alpha}$ are not associates.*

Proof. Given the conditions on α, it is neither an associate of any $n \in \mathbb{Z}$ nor a multiple $k\beta$ of β with $k \in \mathbb{Z}$. The conclusion follows by Theorem 23. □

3.2. The Group of Units as a Cyclic Group

If α is a generator element of a cyclic group G of order n, then α^i is also a generator of G if and only if $\gcd(i, n) = 1$. The number of generators of such a G is $\varphi(n)$. Moreover, an $\alpha \in G$ is a generator of G if and only if $\alpha^{\frac{n}{q}} \neq 1$ for each prime divisor q of n.

The cyclic group $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$ of order $\varphi_\rho(\eta)$ have $\varphi(\varphi_\rho(\eta))$ generators. Our next result shows that the probability of successfully selecting one generator in the cyclic group $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$ at random is smaller than doing so in the cyclic group $\mathbb{Z}_n^*$.

Theorem 24. *If η is an associate of some $n \in \mathbb{N}$, then* $\dfrac{\varphi(\varphi_\rho(\eta))}{\varphi_\rho(\eta)} \leq \dfrac{\varphi(\varphi(n))}{\varphi(n)}$.

Proof. By Theorem 16, we know that $\varphi(n) \mid \varphi_\rho(\eta)$ whenever η and $n \in \mathbb{N}$ are associates. For $a, b \in \mathbb{N}$, it is well known that, if $a \mid b$, then $\frac{\varphi(b)}{\varphi(a)} \leq \frac{b}{a}$. Hence, we have

$$\frac{\varphi(\varphi_\rho(\eta))}{\varphi(\varphi(n))} \leq \frac{\varphi_\rho(\eta)}{\varphi(n)}, \text{ which implies} \frac{\varphi(\varphi_\rho(\eta))}{\varphi_\rho(\eta)} \leq \frac{\varphi(\varphi(n))}{\varphi(n)}.$$

□

Example 3. *For the Eisenstein prime $p = 5$, the order of the cyclic group $(\mathbb{Z}[\rho]/\langle 5\rangle)^* \cong (\mathbb{Z}_5[\rho])^*$ is $\varphi_\rho(5) = 5^2 - 1 = 24$ whose prime factorization is $\varphi_\rho(5) = 2^3 \cdot 3$. Let α be a generator of $(\mathbb{Z}_5[\rho])^*$. It suffices to show that*

$$\alpha^{\frac{\varphi_\rho(5)}{3}} = \alpha^8 \neq 1 \pmod 5 \text{ and } \alpha^{\frac{\varphi_\rho(5)}{2}} = \alpha^{12} \neq 1 \pmod 5.$$

We can select $\alpha := 2 + \rho$ to generate $(\mathbb{Z}_5[\rho])^*$, since $\alpha^8 = 4 + 4\rho \pmod 5$ and $\alpha^{12} = 4 \pmod 5$. The other seven generators are

$$\begin{aligned} &\alpha^5 = 1 + 4\rho, && \alpha^7 = 1 + 3\rho, && \alpha^{11} = 3 + 2\rho, && \alpha^{13} = 3 + 4\rho, \\ &\alpha^{17} = 4 + \rho, && \alpha^{19} = 4 + 2\rho, && \alpha^{23} = 2 + 3\rho. \end{aligned}$$

The group $\mathbb{Z}_5^*$ has $\varphi(\varphi(5)) = \varphi(4) = 2$ generators, namely, 2 and 3. It is clear that

$$\frac{\varphi(\varphi_\rho(5))}{\varphi_\rho(5)} = \frac{8}{24} < \frac{2}{4} = \frac{\varphi(\varphi(5))}{\varphi(5)}.$$

Theorem 25. *If $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$ is a cyclic group, then*

$$\prod_{\alpha \in (\mathbb{Z}[\rho]/\langle\eta\rangle)^*} \alpha \equiv -1 \pmod \eta.$$

Proof. Let $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$ be a cyclic group. By Theorem 13, η is an element in the set $\{\beta, \beta^2, 2\beta, \psi^k\}$, a prime $p \equiv 2 \pmod 3$, or any of their associates. We investigate by the values that η takes.

If $\gamma = \beta$, then, by Theorem 12, we get $(\mathbb{Z}[\rho]/\langle\beta\rangle)^* = \{[1]_\beta, [2]_\beta\}$. Hence,

$$\prod_{\alpha \in (\mathbb{Z}[\rho]/\langle\beta\rangle)^*} \alpha \equiv 1 \cdot 2 \equiv 2 \equiv -1 \pmod \beta.$$

If $\gamma = 2$, then $(\mathbb{Z}[\rho]/\langle 2\rangle)^*$ is a cyclic group of order $\varphi_\rho(2) = 3$. Letting θ be a generator,

$$\prod_{\alpha \in (\mathbb{Z}[\rho]/\langle 2\rangle)^*} \alpha \equiv \prod_{0 \leq t \leq 2} \theta^t \equiv \theta^3 \pmod 2.$$

Since the generators of $(\mathbb{Z}[\rho]/\langle 2\rangle)^*$ are ρ and $1+\rho$, we have $\theta^3 \equiv 1 \equiv -1 \pmod 2$.

If $\gamma \in \{\beta^2, 2\beta, \psi^k\}$ or $\gamma = p \equiv 2 \pmod 3$ such that $p \neq 2$, then $\varphi_\rho(\gamma)$ is an even number, by Theorem 14. Letting θ be a generator of $(\mathbb{Z}[\rho]/\langle\gamma\rangle)^*$,

$$\prod_{\alpha \in (\mathbb{Z}[\rho]/\langle\gamma\rangle)^*} \alpha \equiv \prod_{0 \leq t \leq \varphi_\rho(\gamma)-1} \theta^t \equiv \theta^{\frac{\varphi_\rho(\gamma)(\varphi_\rho(\gamma)-1)}{2}} \pmod \gamma.$$

The order of θ is an even number $\varphi_\rho(\gamma)$. Hence, $\theta^{\frac{\varphi_\rho(\gamma)}{2}} \in (\mathbb{Z}[\rho]/\langle\gamma\rangle)^*$ must be -1 because -1 is the only element of order 2 in $(\mathbb{Z}[\rho]/\langle\gamma\rangle)^*$. Since $\varphi_\rho(\gamma) - 1$ is an odd number,

$$\theta^{\frac{\varphi_\rho(\gamma)(\varphi_\rho(\gamma)-1)}{2}} = \left(\theta^{\frac{\varphi_\rho(\gamma)}{2}}\right)^{\varphi_\rho(\gamma)-1} \pmod \gamma = (-1)^{\varphi_\rho(\gamma)-1} \pmod \gamma = -1 \pmod \eta.$$

□

The Wilson Theorem over $\mathbb{Z}$ had been generalized to Gaussian integers in [35], but not to Eisenstein integers in the prior literature. We highlight that we have achieved this as a special case of Theorem 25.

Theorem 26 (Wilson Theorem for Eisenstein Integers). *If $\gamma \in \mathbb{Z}[\rho]$ is an Eisenstein prime, then*

$$\prod_{\alpha \in (\mathbb{Z}[\rho]/\langle\gamma\rangle)^*} \alpha \equiv -1 \pmod \gamma.$$

4. Set Partitioning Based on the Multiplicative Group

In a recent work [8], we proposed a number of Eisenstein constellations $\mathcal{E}_\eta$ as two-dimensional signal constellations by using the modulo function in (1). The setup, given a suitable η, has

$$\begin{aligned} \mathcal{E}_\eta &= \{\mu_\eta(\alpha) \,:\, \alpha \in \mathcal{R}_\eta\} \text{ with} \\ \mathcal{R}_\eta &= \{x + y\rho \,:\, 0 \leq x < tN_\rho(m + n\rho) \text{ and } 0 \leq y < t\}. \end{aligned} \tag{3}$$

In that work, we also introduced set partitioning of Eisenstein integers based on *additive* subgroups. In this section, we focus on set partitioning based on the *multiplicative* group.

We now propose Eisenstein constellations $(\mathcal{E}_\eta)^*$, corresponding to the cyclic group $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$, with $\eta \in \{\beta^2, 2\beta, \psi^k \,:\, k \in \mathbb{N}\}$ or η being an odd prime integer $p \equiv 2 \pmod 3$. In doing this, we generalize Proposition 1 in [18], which covers the case of $\eta = \psi$. Our set partitioning technique for signal constellation $(\mathcal{E}_\eta)^*$ benefits from the facts that $(\mathbb{Z}[\rho]/\langle\eta\rangle)^*$ is a cyclic group of order $\varphi_\rho(\eta)$, by Theorem 13, and $\varphi_\rho(\eta) \equiv 0 \pmod 6$, by Theorem 15. The elements of $(\mathcal{E}_\eta)^*$ can be expressed as powers of a generator α as

$$(\mathcal{E}_\eta)^* = \left\{\alpha^0, \alpha^1, \ldots, \alpha^{\varphi_\rho(\eta)-1}\right\}.$$

Letting $n := \frac{\varphi_\rho(\eta)}{6}$, the set of all unit (see [29] for $\eta = \psi$) is

$$\{\alpha^n, \alpha^{2n}, \alpha^{3n}, \alpha^{4n}, \alpha^{5n}, \alpha^{6n}\} = \{\pm 1, \pm\rho, \pm(1+\rho)\}.$$

We can then partition $(\mathcal{E}_\eta)^*$ into n subsets, indexed by $j \in \{0, 1, \ldots, n-1\}$, as

$$(\mathcal{E}_\eta)^*_{(j)} = \{\alpha^{n+j}, \alpha^{2n+j}, \alpha^{3n+j}, \alpha^{4n+j}, \alpha^{5n+j}, \alpha^{6n+j}\} = \{\pm\alpha^j, \pm\rho\alpha^j, \pm(1+\rho)\alpha^j\}.$$

All elements of $(\mathcal{E}_\eta)^*$ can be found by calculating α^j for $j \in \{0, 1, \ldots, n-1\}$ using the modulo function in (1), followed by multiplying each α^j by the units.

Our next result extends Theorem 2 to the cases $\eta \in \{2\beta, \beta^2, \psi^k : k \in \mathbb{N}\}$ or η being an odd prime integer $p \equiv 2 \pmod 3$.

Theorem 27. *Let $\eta \in \{2\beta, \beta^2, \psi^k : k \in \mathbb{N}\}$ or $\eta = p$, with $p \equiv 2 \pmod 3$ being an odd prime. If α is a generator of $(\mathcal{E})^*_\eta$, then the minimum Euclidean distance in the subset $(\mathcal{E}_\eta)^*_{(j)}$ is $\|\alpha^j\|$. Furthermore, $(\mathcal{E}_\eta)^*_{(j)}$ can be partitioned into three subsets*

$$(\mathcal{E}_\eta)^*_{(j)} = \{\pm\alpha^j\} \cup \{\pm\rho\alpha^j\} \cup \{\pm(1+\rho)\alpha^j\},$$

each with minimum Euclidean distance $2\|\alpha^j\|$. We also can partition $(\mathcal{E}_\eta)^*_{(j)}$ into two subsets

$$(\mathcal{E}_\eta)^*_{(j)} = \{\alpha^j, \rho\alpha^j, -(1+\rho)\alpha^j\} \cup \{-\alpha^j, -\rho\alpha^j, (1+\rho)\alpha^j\},$$

each with minimum Euclidean distance $\sqrt{3}\|\alpha^j\|$.

Proof. Two neighboring points in $(\mathcal{E}_\eta)^*_{(j)}$ have a phase difference of $\pi/3$. Hence, the pair together with the origin form an equilateral triangle whose sides are of length $\|\alpha^j\|$, confirming that the minimum Euclidean distance is $\|\alpha^j\|$.

The sets $\{\pm\alpha^j\}, \{\pm\rho\alpha^j\}$ and $\{\pm(1+\rho)\alpha^j\}$ contain points whose pairwise phase difference is π, ensuring the minimum distance $2\|\alpha^j\|$. The sets $\{\alpha^j, \rho\alpha^j, -(1+\rho)\alpha^j\}$ and $\{-\alpha^j, -\rho\alpha^j, (1+\rho)\alpha^j\}$ contain points whose pairwise phase difference is $2\pi/3$, yielding the minimum distance of $\sqrt{3}\|\alpha^j\|$. □

Example 4. *(Primitive but not prime) Given a primitive Eisenstein $\psi^2 = -5+3\rho$, with $\psi = 2+3\rho$, we have the cyclic group $(\mathbb{Z}[\rho]/\langle -5+3\rho\rangle)^* \cong (\mathcal{E}_{-5+3\rho})^*$ generated by $\alpha = 3$. Since $\varphi_\rho(\psi^2) = 42$, we can partition $(\mathcal{E}_{\psi^2})^*$ into 7 subsets defined as*

$$(\mathcal{E}_{\psi^2})^*_{(j)} = \{\pm\alpha^j, \pm\rho\alpha^j, \pm(1+\rho)\alpha^j\} \text{ with } j \in \{0,1,2,3,4,5,6\}.$$

Since $\alpha = 3$, by using the modulo function (1), we have

$$\alpha^2 = -4-2\rho, \quad \alpha^3 = -4-\rho, \quad \alpha^4 = 1-\rho, \quad \alpha^5 = -2, \quad \alpha^6 = -1-3\rho.$$

We rely on Theorem 27 to partition $(\mathcal{E}_{\psi^2})^*_{(j)}$ into three subsets and two subsets, each with respective minimum Euclidean distances $2\|\alpha^j\|$ and $\sqrt{3}\|\alpha^j\|$ for $j \in \{0,1,2,3,4,5,6\}$ as follows:

$$\begin{aligned}
(\mathcal{E}_{\psi^2})^*_{(0)} &= \{1,\ \rho,\ 1+\rho,\ -1,-\rho,\ -1-\rho\},\\
&= \{1,\ -1\} \cup \{\rho,\ -\rho\} \cup \{-1-\rho,\ 1+\rho\},\\
&= \{1,\ \rho,\ -1-\rho\} \cup \{-1,-\rho,1+\rho\},\\
(\mathcal{E}_{\psi^2})^*_{(1)} &= \{3,\ 3+3\rho,\ 3\rho,\ -3,\ -3-3\rho,\ -3\rho\},\\
&= \{3,\ -3\} \cup \{3\rho,\ -3\rho\} \cup \{-3-3\rho,\ 3+3\rho\},\\
&= \{3,\ 3\rho,\ -3-3\rho\} \cup \{-3,\ -3\rho,\ 3+3\rho\},\\
(\mathcal{E}_{\psi^2})^*_{(2)} &= \{4+2\rho,\ 2+4\rho,\ -2+2\rho,\ -4-2\rho,\ -2-4\rho,\ 2-2\rho\},\\
&= \{4+2\rho,\ -4-2\rho\} \cup \{2+4\rho,\ -2-4\rho\} \cup \{-2+2\rho,\ 2-2\rho\},\\
&= \{4+2\rho,\ -2-4\rho\ -2+2\rho\} \cup \{\ -4-2\rho,\ 2+4\rho,\ 2-2\rho\},
\end{aligned}$$

$$
\begin{aligned}
(\mathcal{E}_{\psi^2})^*_{(3)} &= \{4+\rho,\ 3+4\rho,\ -1+3\rho,\ -4-\rho,\ -3-4\rho,\ 1-3\rho\},\\
&= \{4+\rho,\ -4-\rho\} \cup \{3+4\rho,\ -3-4\rho\} \cup \{-1+3\rho,\ 1-3\rho\},\\
&= \{4+\rho,\ -1+3\rho,\ -3-4\rho\} \cup \{-4-\rho,,\ 1-3\rho,\ 3+4\rho\},\\
(\mathcal{E}_{\psi^2})^*_{(4)} &= \{2+\rho,\ 1+2\rho,\ -1+\rho,\ -2-\rho,\ -1-2\rho,\ 1-\rho\},\\
&= \{2+\rho,\ -2-\rho\} \cup \{-1+\rho,\ 1-\rho\} \cup \{-1-2\rho,\ 1+2\rho\},\\
&= \{2+\rho,\ -1-2\rho,\ -1+\rho\} \cup \{-2-\rho,\ 1+2\rho,\ 1-\rho\},\\
(\mathcal{E}_{\psi^2})^*_{(5)} &= \{2,\ 2+2\rho,\ 2\rho,\ -2,\ -2-2\rho,\ -2\rho\},\\
&= \{2,\ -2\} \cup \{2\rho,\ -2\rho\} \cup \{-2-2\rho,\ 2+2\rho\},\\
&= \{2,\ 2\rho,\ -2-2\rho,\} \cup \{-2,\ 2+2\rho,\ -2\rho\},\\
(\mathcal{E}_{\psi^2})^*_{(6)} &= \{3+2\rho,\ 1+3\rho,\ -2+\rho,\ -3-2\rho,\ -1-3\rho,\ 2-\rho\},\\
&= \{3+2\rho, -3-2\rho\} \cup \{1+3\rho,\ -1-3\rho\} \cup \{-2+\rho,\ 2-\rho\},\\
&= \{3+2\rho,\ -1-3\rho,\ -2+\rho\} \cup \{-3-2\rho,\ 1+3\rho,\ 2-\rho\}.
\end{aligned}
$$

Figures 1–3 visualize the Eisenstein constellations $(\mathcal{E}_{\psi^2})^*$ *and its signal partitions in* $\mathbb{C}$.

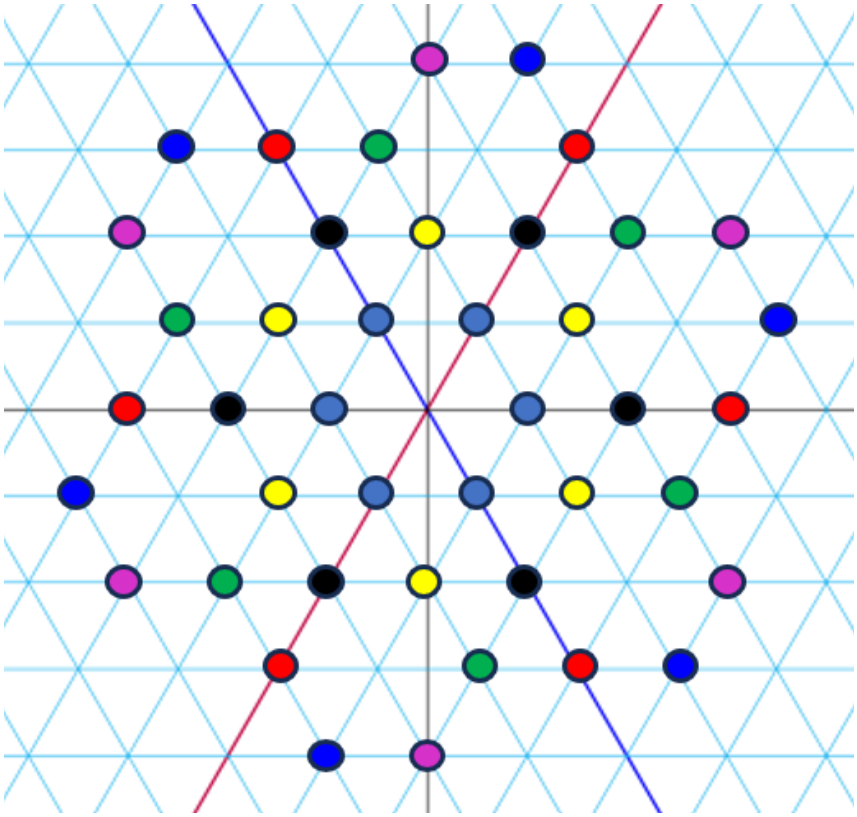

Figure 1. Set partitioning of $(\mathcal{E}_{\psi^2})^*$ into seven subsets. Circles represent the integers, with colours corresponding to indices.

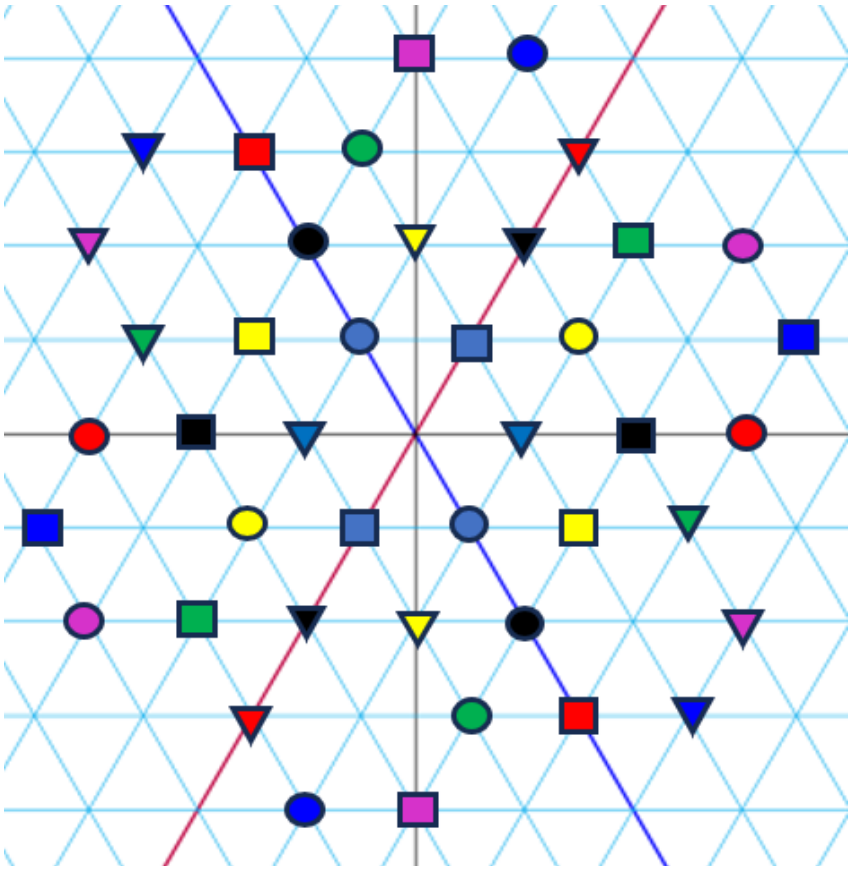

Figure 2. Set partitioning of $(\mathcal{E}_{\psi^2})^*_{(j)}$ into three subsets. Colours correspond to indices. Forms (circle, square, and triangle) correspond to subsets.

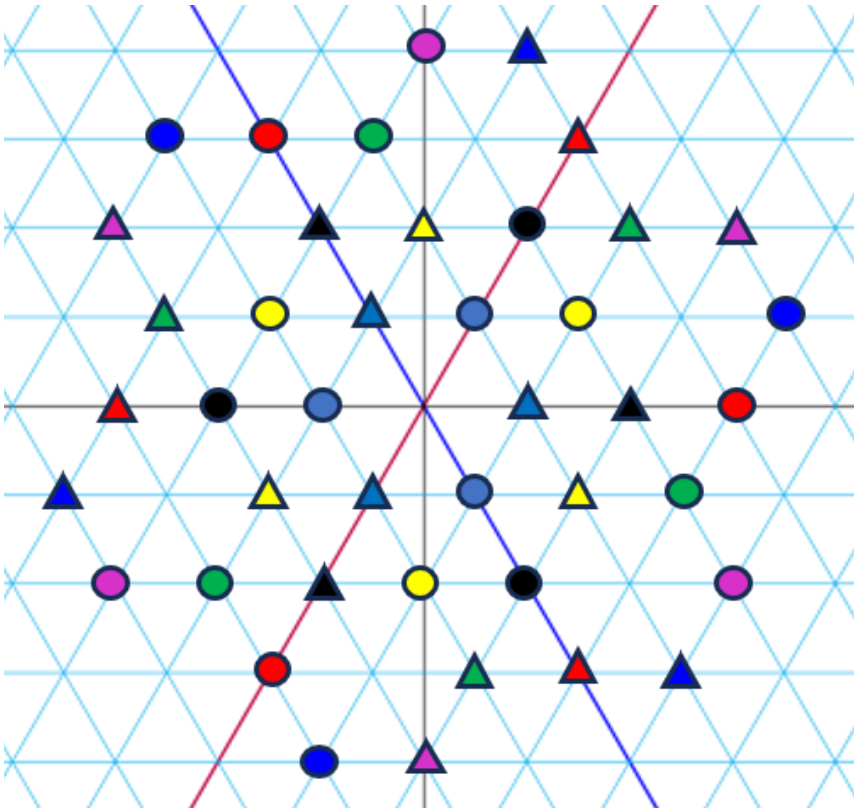

Figure 3. Set partitioning of $(\mathcal{E}_{\psi^2})^*_{(j)}$ into two subsets. Colours correspond to indices. Forms (circle and triangle) correspond to subsets.

Example 5. *(Prime but not primitive) Given an Eisenstein prime $p = 5$, we have the cyclic group $(\mathbb{Z}[\rho]/\langle 5\rangle)^* \cong (\mathcal{E}_5)^*$ generated by $\alpha = 2+\rho$. Since $\varphi_\rho(5) = 24$, we can partition $(\mathcal{E}_5)^*$ into 4 subsets as*

$$(\mathcal{E}_5)^*_{(j)} = \{\pm\alpha^j, \pm\rho\alpha^j, \pm(1+\rho)\alpha^j\}, \text{ with } j \in \{0,1,2,3\}.$$

Since $\alpha = 2+\rho$, the modulo function in (1) gives us $\alpha^2 = -2-2\rho$ and $\alpha^3 = -2+\rho$. By Theorem 27, we partition $(\mathcal{E}_5)^*_{(j)}$ into three and two subsets each with respective minimum Euclidean distances $2\|\alpha^j\|$ and $\sqrt{3}\|\alpha^j\|$ for $j \in \{0,1,2,3\}$ as follows:

$$\begin{aligned}
(\mathcal{E}_5)^*_{(0)} &= \{1,\ \rho,\ 1+\rho,\ -1, -\rho,\ -1-\rho\},\\
&= \{1,\ -1\} \cup \{\rho,\ -\rho\} \cup \{-1-\rho,\ 1+\rho\},\\
&= \{1,\ \rho,\ -1-\rho\} \cup \{-1, -\rho, 1+\rho\},\\
(\mathcal{E}_5)^*_{(1)} &= \{2+\rho,\ 1+2\rho,\ -1+\rho,\ -2-\rho,\ -1-2\rho,\ 1-\rho\},\\
&= \{2+\rho,\ -2-\rho\} \cup \{-1+\rho,\ 1-\rho\} \cup \{-1-2\rho,\ 1+2\rho\},\\
&= \{2+\rho,\ -1-2\rho,\ -1+\rho\} \cup \{-2-\rho,\ 1+2\rho,\ 1-\rho\},\\
(\mathcal{E}_5)^*_{(2)} &= \{2,\ 2+2\rho,\ 2\rho,\ -2,\ -2-2\rho,\ -2\rho\},\\
&= \{2,\ -2\} \cup \{2\rho,\ -2\rho\} \cup \{-2-2\rho,\ 2+2\rho\},\\
&= \{2,\ -2-2\rho,\ 2\rho\} \cup \{-2,\ 2+2\rho,\ -2\rho\},\\
(\mathcal{E}_5)^*_{(3)} &= \{3+2\rho,\ -3-2\rho,\ -2+\rho,\ 2-\rho,\ -1-3\rho,\ 1+3\rho\},\\
&= \{3+2\rho,\ -3-2\rho\} \cup \{-2+\rho,\ 2-\rho\} \cup \{-1-3\rho,\ 1+3\rho\},\\
&= \{3+2\rho,\ -1-3\rho,\ -2+\rho\} \cup \{-3-2\rho,\ 2-\rho,\ 1+3\rho\}.
\end{aligned}$$

Figures 4–6 visualize the constellation $(\mathcal{E}_5)^*$ and its signal partitions in $\mathbb{C}$.

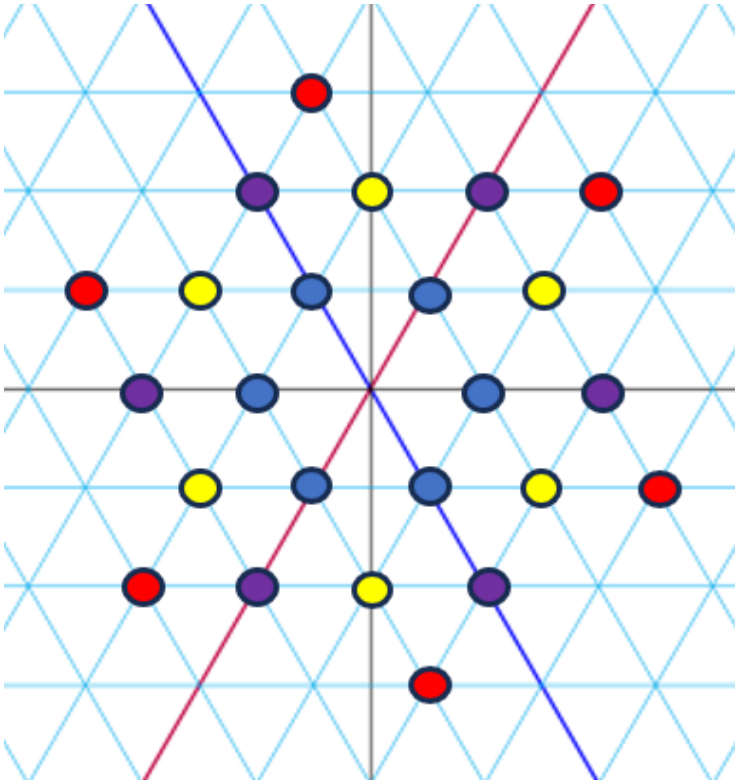

Figure 4. Set partitioning of $(\mathcal{E}_5)^*$ into four subsets. Circles represent the integers, with colours corresponding to indices.

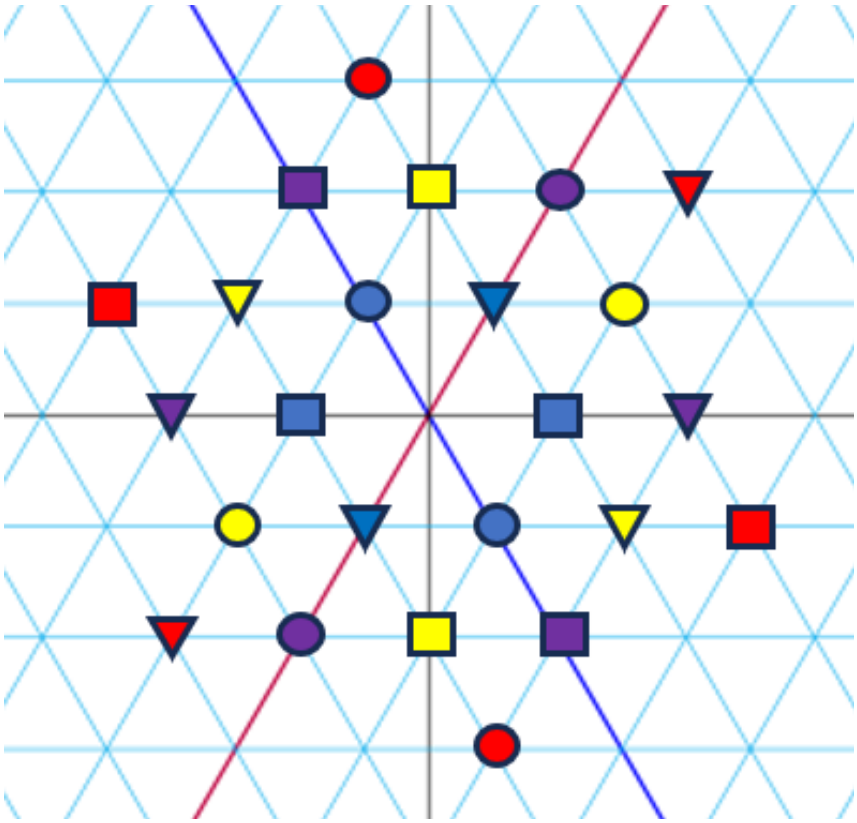

Figure 5. Set partitioning of $(\mathcal{E}_5)^*_{(j)}$ into three subsets. Forms (circle, square, and triangle) correspond to subsets. Colours correspond to indices.

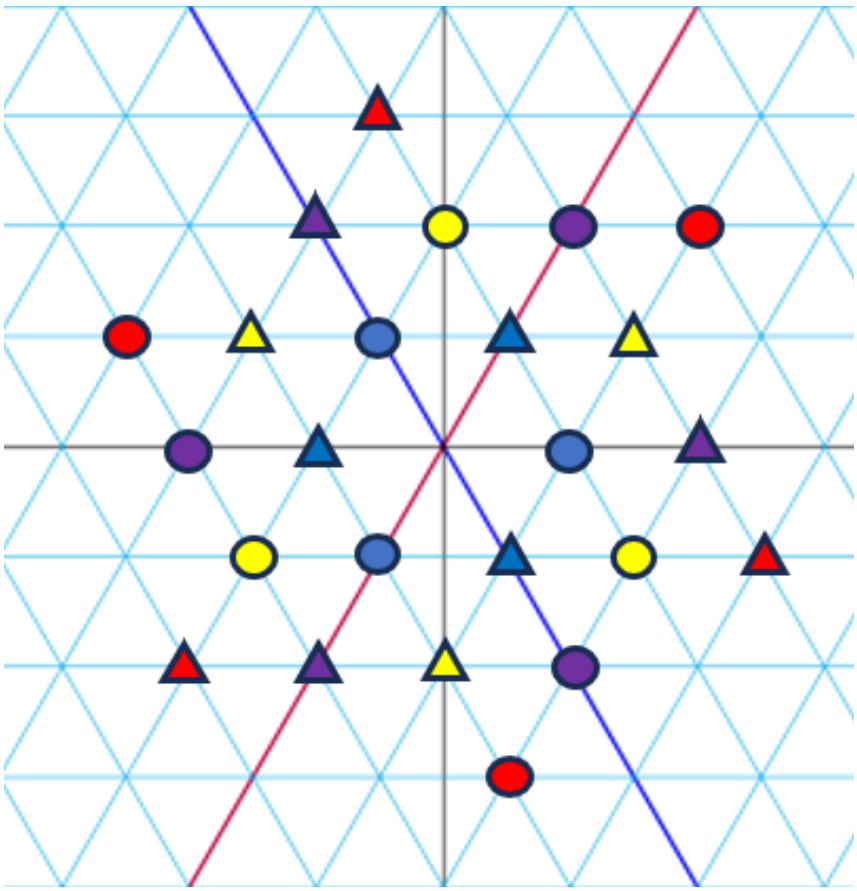

Figure 6. Set partitioning of $(\mathcal{E}_5)^*_{(j)}$ into two subsets. Form (circle and triangle) correspond to subsets. Colours correspond to indices.

5. Discussion

We can use a primitive Eisenstein integer η to construct signal constellations and complex-valued codes over Eisenstein integers. We consider the sets $\mathcal{R}_\eta$ and $\mathcal{E}_\eta$ in (3) as code alphabets, where $\mathcal{E}_\eta$ is obtained through the modulo function in (1), based on an isomorphism between $\mathbb{Z}[\rho]$ modulo a primitive Eisenstein integer η and $\mathbb{Z}$ modulo a norm of the primitive Eisenstein as in Theorem 8. Codes over Eisenstein integers whose alphabet set $\mathcal{E}_\psi$ is an Eisenstein field of cardinality a prime $q \equiv 1 \pmod 3$ were investigated in [29] and [36]. The Eisenstein field corresponds to a quotient ring of Eisenstein integers over an ideal generated by a prime and a primitive Eisenstein integer ψ. More generally, a recent code construction via a quotient ring of Eisenstein integers induced by an ideal generated by a primitive but not a prime Eisenstein integer can be found in [8]. Table 1 provides an example. The alphabet set $\mathcal{E}_{\psi^2}$ is obtained from the quotient ring $\mathbb{Z}[\rho]/\langle\psi^2\rangle$ with primitive Eisenstein $\psi^2 = -5 + 3\rho$ and $\psi = 2 + 3\rho$ via the modulo function in (1).

Table 1. Elements in $Z[\rho]/\langle\psi^2\rangle \cong \mathbb{Z}_{49}$ and $\mathcal{E}_{\psi^2}$.

$\mathbb{Z}[\rho]/\langle\psi^2\rangle$	$\mathcal{E}_{\psi^2}$	$\mathbb{Z}[\rho]/\langle\psi^2\rangle$	$\mathcal{E}_{\psi^2}$	$\mathbb{Z}[\rho]/\langle\psi^2\rangle$	$\mathcal{E}_{\psi^2}$
$[0]_{\psi^2}$	0	$[17]_{\psi^2}$	$-1+\rho$	$[34]_{\psi^2}$	$-2+2\rho$
$[1]_{\psi^2}$	1	$[18]_{\psi^2}$	ρ	$[35]_{\psi^2}$	$-1+2\rho$
$[2]_{\psi^2}$	2	$[19]_{\psi^2}$	$1+\rho$	$[36]_{\psi^2}$	2ρ
$[3]_{\psi^2}$	3	$[20]_{\psi^2}$	$2+\rho$	$[37]_{\psi^2}$	$1+2\rho$
$[4]_{\psi^2}$	$-1+3\rho$	$[21]_{\psi^2}$	$3+\rho$	$[38]_{\psi^2}$	$2+2\rho$
$[5]_{\psi^2}$	3ρ	$[22]_{\psi^2}$	$4+\rho$	$[39]_{\psi^2}$	$3+2\rho$
$[6]_{\psi^2}$	$1+3\rho$	$[23]_{\psi^2}$	$-3-4\rho$	$[40]_{\psi^2}$	$4+2\rho$
$[7]_{\psi^2}$	$2+3\rho$	$[24]_{\psi^2}$	$-2-4\rho$	$[41]_{\psi^2}$	$-3-3\rho$
$[8]_{\psi^2}$	$3+3\rho$	$[25]_{\psi^2}$	$2+4\rho$	$[42]_{\psi^2}$	$-2-3\rho$
$[9]_{\psi^2}$	$-4-2\rho$	$[26]_{\psi^2}$	$3+4\rho$	$[43]_{\psi^2}$	$-1-3\rho$
$[10]_{\psi^2}$	$-3-2\rho$	$[27]_{\psi^2}$	$-4-\rho$	$[44]_{\psi^2}$	-3ρ
$[11]_{\psi^2}$	$-2-2\rho$	$[28]_{\psi^2}$	$-3-\rho$	$[45]_{\psi^2}$	$1-3\rho$
$[12]_{\psi^2}$	$-1-2\rho$	$[29]_{\psi^2}$	$-2-\rho$	$[46]_{\psi^2}$	-3
$[13]_{\psi^2}$	-2ρ	$[30]_{\psi^2}$	$-1-\rho$	$[47]_{\psi^2}$	-2
$[14]_{\psi^2}$	$1-2\rho$	$[31]_{\psi^2}$	$-\rho$	$[48]_{\psi^2}$	-1
$[15]_{\psi^2}$	$2-2\rho$	$[32]_{\psi^2}$	$1-\rho$		
$[16]_{\psi^2}$	$-2+\rho$	$[33]_{\psi^2}$	$2-\rho$		

A *code* is a nonempty subset $C \subseteq \mathcal{E}_\eta^n$ whose elements are called *codewords*. A *linear code* C of length n over $\mathcal{E}_\eta$ is a submodule of $\mathcal{E}_\eta^n$. Since $\mathcal{E}_\eta$ and $\mathcal{E}_\eta^n$ are abelian groups, we say that C is a *group code* if it is a subgroup of $\mathcal{E}_\eta^n$. When $\mathcal{E}_\eta$ is a finite field, that is, $\mathcal{E}_\eta^n$ is a vector space of dimension n over $\mathcal{E}_\eta$, a linear code C is a subspace of $\mathcal{E}_\eta^n$. We call C an (n, k) code if C has exactly $|\mathcal{E}_\eta|^k$ codewords.

By Corollaries 2 and 4, odd primitives η and $\bar{\eta}$ are not associates. Hence, $\langle\eta\rangle \neq \langle\bar{\eta}\rangle$ and, therefore, $\mathbb{Z}[\rho]/\langle\eta\rangle \neq \mathbb{Z}[\rho]/\langle\bar{\eta}\rangle$. By Proposition 1, odd primitives $\psi_1^{r_1}\cdots\psi_k^{r_k}$ and $\overline{\psi_1^{r_1}\cdots\psi_k^{r_k}}$ are relatively prime. By the Chinese Remainder Theorem (CRT) with $N_\rho(\psi_i) = q_i$ being a prime integer such that $q_i \equiv 1 \pmod 3$, we have

$$\mathbb{Z}[\rho]/\langle q_1^{r_1}\cdots q_k^{r_k}\rangle \cong \mathbb{Z}[\rho]/\langle\psi_1^{r_1}\cdots\psi_k^{r_k}\rangle \times \mathbb{Z}[\rho]/\langle\overline{\psi_1^{r_1}\cdots\psi_k^{r_k}}\rangle.$$

For an even primitive Eisenstein integer η, however, the CRT does not hold. Hence,

$$\mathbb{Z}[\rho]/\langle n\rangle \ncong \mathbb{Z}[\rho]/\langle\eta\rangle \times \mathbb{Z}[\rho]/\langle\bar{\eta}\rangle \text{ with } N_\rho(\eta) = n.$$

Set partitioning based on an *additive* subgroup is structurally *not feasible* on the Eisenstein field $\mathcal{E}_\psi$ due to its cardinality being a prime integer. Hence, set partitioning based

on a *multiplicative* group of the Eisenstein field $\mathcal{E}_\psi$ was proposed in [18]. The investigation leveraged on the fact that a multiplicative group of the Eisenstein field is cyclic to perform set partitioning. Theorem 27 is an insightful generalization. It extends set partitioning to a multiplicative group of a quotient ring of Eisenstein integers when the group is designed to be cyclic.

Given a primitive Eisenstein integer η, the quotient ring $\mathbb{Z}[\rho]/\langle\eta\rangle \cong \mathbb{Z}_{N_\rho(\eta)}$ defines a finite set of representative elements that form the signal constellation

$$\mathcal{E}_\eta = \{\mu_\eta(\alpha) : \alpha \in \mathbb{Z}_{N_\rho(\eta)}\}.$$

This constitutes a special case of (3), where $\mu_\eta(\alpha)$ denotes the modulo function in (1) applied to an Eisenstein integer α. Such a structure is fundamental in designing multidimensional lattice codes. It enables efficient encoding and decoding procedures. By integrating Eisenstein constellations into coding theory, we establish a direct link between complex-valued codes and structured lattice-based signal constellations. The resulting codes benefit from increased minimum Euclidean distances, enhancing signal robustness in noisy communication channels.

6. Summary and Concluding Remarks

We have just reported properties of primitive, even, or odd Eisenstein integers. For the odd ones, we investigated whether they are of Type 1 or 2 and their implied properties according to the type.

Given an Eisenstein prime ψ such that $N_\rho(\psi) = q$ is a prime integer equivalent to $1 \pmod 3$, we settled the question posed as Question 6.1 in [7]. If ψ and $\bar{\psi}$ are distinct Eisenstein primes which are not associates, then they belong to the same odd class. If one of them is of Type 1, then the other is also of Type 1. The same goes for Type 2. The corresponding q, however, is insufficient to conclude which odd class ψ and $\bar{\psi}$ belong to.

We have confirmed that, if Eisenstein integers α and $\bar{\alpha}$ are relatively prime, then $\alpha^{-1} \pmod{\bar{\alpha}}$ is in $\mathbb{Z}$. We also managed to prove that the multiplicative group of the set of all units in a quotient ring of $\mathbb{Z}[\rho]$ forms a cyclic group. This leads to a nice set partitioning, allowing us to propose Eisenstein signal constellations. Some examples were given to further illustrate the insights.

Many algebraic signal constellations have been known to enhance the performance of communication systems. Studying use cases and measuring the optimality of certain families of constellations form an important topic in modern communications. Constructing good constellations and benchmarking their performance against previously best-known ones, either in general or for specific setups, are interesting directions to consider.

Author Contributions: Conceptualization, A.H.; investigation—mostly A.H., helped by U.I., I.E.W., and M.F.E.; validation, A.H., U.I., I.E.W., and M.F.E.; writing—original draft, A.H.; writing—review and editing, M.F.E.; visualization, A.H.; supervision, U.I. and I.E.W. All authors have read and agreed to the submitted version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The data is contained within the article.

Acknowledgments: A. Hadi is supported by the Indonesian Education Scholarship (BPI), provided by the Center for Higher Education Funding and Assessment of the Indonesian Ministry of Higher Education, Science, and Technology, No. 00082/J5.2.3./BPI.06/9/2022. His studies benefit from the Indonesia Endowment Fund for Education (LPDP).

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Proof of Theorem 5

We prove by induction. Starting with $n = 1$, we have

$$\psi^n = \psi = x + y\rho \text{ and } N_\rho(\psi) = q = x^2 + y^2 - xy.$$

Let us assume that $\gcd(x, y) = r \geq 1$. Hence, $r \mid x$ and $r \mid y$, implying $r \mid (x^2 + y^2 - xy)$, that is $r \mid q$. Since q is prime integer, $r = 1$ or $r = q$. If $r = q$, then $x = rs = qs$ and $y = rt = qt$ for some $s, t \in \mathbb{Z}$. Observing that

$$q = x^2 + y^2 - xy = q^2 N_\rho(s + t\rho),$$

we obtain $1 = q\, N_\rho(s + t\rho)$, which is impossible since q is a prime integer. Thus, we conclude that $r = \gcd(x, y) = 1$.

Next, we assume $\psi^k = c + d\rho$, where $\gcd(c, d) = 1$ for some $k \geq 1$. We have

$$\begin{aligned} \psi^{k+1} &= (x + y\rho)^{k+1} = (x + y\rho)^k (x + y\rho) \\ &= (c + d\rho)(x + y\rho) = (xc - yd) + (xd + yc - yd)\rho. \end{aligned} \tag{A1}$$

Letting $A = xc - yd$ and $B = xd + yc - yd$, it now suffices to show that $\gcd(A, B) = 1$. For a contradiction, suppose that $\gcd(A, B) = r > 1$. We have $r \mid A$ and $r \mid B$. Since $q^{k+1} = N_\rho(\psi^{k+1}) = A^2 + B^2 - AB$, we are sure that $r \mid (A^2 + B^2 - AB)$, implying $r \mid q^{k+1}$. Since q is a prime integer, $r = 1$ or $r = q^m$ for some $m \in \{1, \ldots, k+1\}$. We show that having $r = q^m$ is impossible. Again, since $r \mid A$ and $r \mid B$, we can write $A = q^m s$ and $B = q^m t$ for some $s, t \in \mathbb{Z}$. Using the expression

$$q^{k+1} = A^2 + B^2 - AB = q^{2m} N_\rho(s + t\rho), \tag{A2}$$

we consider three cases, namely, $2m > k + 1$, $2m = k + 1$, and $2m < k + 1$.

Case A1. If $2m > k + 1$, then $q^{2m-(k+1)} \geq q > 1$. Hence, $q^{2m-(k+1)} N_\rho(s + t\rho) > 1$, which contradicts (A2).

Case A2. If $2m < k + 1$, then $N_\rho(s + t\rho) = q^{k+1-2m} = N_\rho(\psi^{k+1-2m})$. By Theorem 4,

$$s + t\rho \sim \psi^{k+1-2m} \text{ or } s + t\rho \sim \bar{\psi}^{k+1-2m}.$$

If $s + t\rho \sim \psi^{k+1-2m}$, then

$$A + B\rho = q^m (s + t\rho) \sim q^m \psi^{k+1-2m}.$$

Since $\psi^{k+1} = A + B\rho$ by Equation (A1), we obtain $\psi^{2m} \sim q^m = \psi^m \bar{\psi}^m$, which means that $\psi \sim \bar{\psi}$. This contradicts Theorem 3, in which $\psi \nsim \bar{\psi}$. Similarly, if $s + t\rho \sim \bar{\psi}^{k+1-2m}$, then $\psi \sim \bar{\psi}$, which is a contradiction.

Case A3. If $2m = k + 1$, then, by Equation (A2), $N_\rho(s + t\rho) = 1$, meaning $s + t\rho$ is a unit in $\mathbb{Z}[\rho]$. Since $\psi^{k+1} = A + B\rho = q^m (s + t\rho)$, we know that $\psi^{k+1} = \psi^{2m} \sim q^m = \psi^m \bar{\psi}^m$ and, hence, $\psi \sim \bar{\psi}$, which is a contradiction.

Thus, $\gcd(A, B) = r = 1$ and the proof is now complete.

References

1. Ireland, K.; Rosen, M.I.; Rosen, M. *A Classical Introduction to Modern Number Theory*, 2nd ed.; Springer Science & Business Media: New York, NY, USA, 1990; ISBN 978-1-4757-2103-4.

2. Cross, J.T. The Euler φ-function in the Gaussian Integers. *Am. Math. Mon.* **1983**, *90*, 518–528. [CrossRef]
3. Dresden, G.; Dymacek, W.M. Finding factors of factor rings over the Gaussian integers. *Am. Math. Mon.* **2005**, *112*, 602–611. [CrossRef]
4. Ozkan, E.; Ozturk, R.; Aydogdu, A. On the factor rings of Eisenstein integers. *Erzincan Univ. J. Sci. Technol.* **2013**, *6*, 165–174.
5. Misaghian, M. Factor rings and their decompositions in the Eisenstein integers ring $\mathbb{Z}[\omega]$. *Armen. J. Math.* **2013**, *5*, 58–68.
6. Bucaj, V. Finding factors of factor rings over Eisenstein integers. *Int. Math. Forum* **2013**, *9*, 1521–1537. [CrossRef]
7. Gullerud, E.; Mbirika, A. An Euler phi function for the Eisenstein integers and some applications. *Integers* **2020** Art. No. A20. Available online: https://math.colgate.edu/~integers/u20/u20.pdf (accessed on 26 February 2025).
8. Hadi, A.; Isnaini, U.; Wijayanti, I.E.; Ezerman, M.F. On codes over Eisenstein integers. *arXiv* **2024**. [CrossRef]
9. Stern, S.; Rohweder, D.; Freudenberger, J.; Fischer, R.F.H. Binary multilevel coding over Eisenstein integers for MIMO broadcast transmission. In Proceedings of the International ITG Workshop Smart Antennas (WSA 2019), Vienna, Austria, 24–26 April 2019; pp. 1–8.
10. Feng, C.; Silva, D.; Kschischang, F.R. An algebraic approach to physical-layer network coding. *IEEE Trans. Inf. Theory* **2013**, *59*, 7576–7596.
11. Sun, Q.T.; Yuan, J.; Huang, T.; Shum, K.W. Lattice network codes based on Eisenstein integers. *IEEE Trans. Commun.* **2013**, *61*, 2713–2725. [CrossRef]
12. Sun, Q. T.; Yuan, J.; Huang, T. On lattice-partition-based physical-layer network coding over GF(4). *IEEE Commun. Lett.* **2013**, *17*, 1988–1991.
13. Fang, D.; Burr, A.; Wang, Y. Eisenstein integer based multi-dimensional coded modulation for physical-layer network coding over $\mathbb{F}_4$ in the two-way relay channels. In Proceedings of the European Conference on Networks and Communications (EuCNC 2014), Bologna, Italy, 23–26 June 2014; pp. 1–5.
14. Tunali, N.E.; Huang, Y.C.; Boutros, J.J.; Narayanan, K.R. Lattices over Eisenstein integers for compute-and-forward. *IEEE Trans. Inf. Theory* **2015**, *61*, 5306–5321.
15. Dong, X.; Soh, C.B.; Gunawan, E.; Tang, L. Groups of algebraic integers used for coding QAM signals. *IEEE Trans. Inf. Theory* **1998**, *44*, 1848–1860. [CrossRef]
16. Dong, X.; Soh, C.B.; Gunawan, E. Multiplicative groups used for coding QAM signals. *IMA J. Math. Control Inform.* **2002**, *19*, 229–243. [CrossRef]
17. Goutham Simha, G.D.; Raghavendra M.A.N.S.; Shriharsha, K.; Acharya, U.S. Signal constellations employing multiplicative groups of Gaussian and Eisenstein integers for enhanced spatial modulation. *Phys. Commun.* **2017**, *25*, 546–554.
18. Freudenberger, J.; Shavgulidze, S. Signal constellations based on Eisenstein integers for generalized spatial modulation. *IEEE Commun. Lett.* **2017**, *21*, 556–559. [CrossRef]
19. Freudenberger, J.; Ghaboussi, F.; Shavgulidze, S. New coding techniques for codes over Gaussian integers. *IEEE Trans. Commun.* **2013**, *61*, 3114–3124. [CrossRef]
20. Freudenberger, J.; Ghaboussi, F.; Shavgulidze, S. New four-dimensional signal constellations from Lipschitz integers for transmission over the Gaussian channel. *IEEE Trans. Commun.* **2015**, *63*, 2420–2427.
21. Rohweder, D.; Stern, S.; Fischer, R.F.; Shavgulidze, S.; Freudenberger, J. Four-dimensional Hurwitz signal constellations, set partitioning, detection, and multilevel coding. *IEEE Trans. Commun.* **2021**, *69*, 5079–5090.
22. Güzeltepe, M. On some perfect codes over Hurwitz integers. *Math. Adv. Pure Appl. Sci.* **2018**, *1*, 39–45.
23. Duran, R.; Guzeltepe, M. An algebraic construction technique for codes over Hurwitz integers. *Hacet. J. Math. Stat.* **2023**, *52*, 652–672. [CrossRef]
24. Duran, R.; Guzeltepe, M. Encoder Lipschitz integers: The Lipschitz integers that have the "division with small remainder" property. In *Rendiconti del Circolo Matematico di Palermo Series 2*; Springer: Berlin/Heidelberg, Germany, 2024; Volume 73, pp. 1–15.
25. Li, C.; Gan, L.; Ling, C. Coprime sensing via Chinese remaindering over quadratic fields—Part II: Generalizations and applications. *IEEE Trans. Signal Process.* **2019**, *67*, 2911–2922. [CrossRef]
26. Gong, Y.; Gan, L.; Liu, H. Multi-channel modulo samplers constructed from Gaussian integers. *IEEE Signal Process. Lett.* **2021**, *28*, 1828–1832. [CrossRef]
27. Jarvis, K.; Nevins, M. ETRU: NTRU over the Eisenstein integers. *Des. Codes Cryptog.* **2013**, *74*, 219–242.
28. Conway, J.H.; Sloane, N.J.A. *Sphere Packings, Lattices and Groups*, 3rd ed.; Springer: New York, NY, USA, 2019, ISBN 9780387985855.
29. Huber, K. Codes over Eisenstein-Jacobi integers. *AMS. Contemp. Math.* **1994**, *168*, 165–179.
30. Löfgren, S. *The Eisenstein Integers and Cubic Reciprocity*; Technical Report; Uppsala University: Uppsala, Sweden, 2022.
31. Vargas, J.D. Recillas, H.T. *La función de Euler en Los Enteros de Eisenstein-Jacobi*; Reportes de Investigación; Departamento de Matemáticas, Universidad Autónoma Metropolitana-Iztapalapa: Mexico City, Mexico, 1989.
32. Vargas, J.D.; Barrios, C.J.R.; Recillas, H.T. The Euler totient function on quadratic fields. *JP J. Algebra Number Theory Appl.* **2021**, *52*, 17–94.

33. Hadi, A.; Isnaini, U.; Wahyudi, E.E.; Wijayanti, I.E.; Ezerman, M.F. RSA-like schemes over Eisenstein integers. 2024, *under review*.
34. Li, C.; Gan, L.; Ling, C. Coprime sensing via Chinese remaindering over quadratic fields—Part I: Array designs. *IEEE Trans. Signal Process.* **2019**, *67*, 2898–2910.
35. Awad, Y.; El-Kassar, A.N.; Kadri, T. Rabin public-key cryptosystem in the domain of Gaussian integers. In Proceedings of the 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 25–26 August 2018; pp. 336–340.
36. da Nobrega Neto, T.P.; Interlando, J.C.; Favareto, O.M.; Elia, M.; Palazzo, R. Lattice constellations and codes from quadratic number fields. *IEEE Trans. Inf. Theory* **2001**, *47*, 1514–1527.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.