

2022-2023 Power Round

Rules

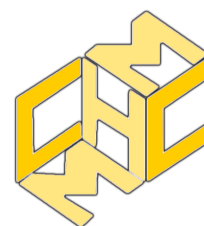
1. **DO NOT FLIP THIS PAGE UNTIL THE GROUP ROUND BEGINS.**
2. You have **135 minutes** to work on the **Power Round**, concurrently with the **Team Round**.
3. You may collaborate with your other teammates during the Group Round. Otherwise, **no other collaboration, computers, calculators, or other outside aid is permitted.**
4. You are permitted to use ruler and compass but **not** a protractor.
5. This round will count towards 5/9 of your team's Group Round score, the Team Round being worth the other 4/9. The Group Round score, in turn, is worth half the overall team score.

General Power Round Conventions

1. Every **Problem** is labeled with a point value. For multi-part problems, each part is labeled with a point value, and the multi-part problem itself is labeled with the sum of the point values of its parts. The point value indicates the general difficulty of each problem/part.
2. A problem worded with "compute" will always call for an **exact numerical answer or algebraic expression**. In this case, credit will be awarded only based on providing a correct answer. Answers are still expected to be *reasonably simplified* as in the Team and Individual Rounds.
3. Problems not worded with "compute" will **require explanation or proof**, unless otherwise specified.
 - Explanations/proofs will be graded on *correctness* and not *readability*. However, unreadable submissions/parts of submissions will be assumed incorrect and lose you credit, so we encourage you to write proofs clearly and carefully!
 - For problems that call for a final answer (and an explanation), no credit will be earned for a submission providing a final answer without an explanation.
4. In your solution to a given problem or part, you may cite the results of **earlier** problems, parts, theorems, etc. (but not **later** ones), without additional justification, even if you have not solved them. You may also cite any "standard" results used in AMC/AIME/USA(J)MO/IMO as long as they do not completely trivialize the problem.

Directions

1. There are **5 Sections** of problems in this round, worth a total of **100 Points**. The sections are of approximately **increasing order** of difficulty, and some later sections may depend on earlier ones.
2. Start your work on each section at the **top of a new page**, on a new sheet of blank, loose leaf paper. You must write on *only one side* of each page you submit.
3. Each page you submit must contain the **section number** (i.e. 1, 2, etc.) and **team name**, written clearly at the top of the page. If you have multiple pages for a section, number them and write the total number of pages for the section (e.g. 1/3, 2/3, 3/3).
4. You must indicate clearly the *start* and *end* of your work on each **problem** that you submit. You must submit your solution to a problem on page(s) of the corresponding section, i.e. the solution to Problem 2.1 must be on a page labeled Section 2.
5. After the end of 135 minute time limit, your team will be granted **5 minutes** to **organize** your submission to the Power Round by section, stacking the pages of each section together in the numbered order. Your submission may not be graded if it is poorly organized.



Eisenstein Number System

Author: Brian Yang

Throughout this Power Round, let \mathbb{Z} be the integers, \mathbb{Q} be the rational numbers, and \mathbb{C} be the complex numbers.

All throughout your lives, you have been intimately familiar with the number system \mathbb{Z} , the integers. You have taken for granted the many fundamental facts about the integers, such as division with remainder, the unique factorization of integers into primes, and Bezout's identity. It turns out, however, there are many number systems that share such properties of the integers! These number systems are some of the essential examples in the modern study of *algebraic number theory*. One of the most famous examples of such a number system are the *Gaussian integers*, denoted by $\mathbb{Z}[i]$, consisting of the set of all complex numbers $a + bi$ where a, b are integers. Today we will be studying another integer-like number system, called the *Eisenstein integers*.

IMPORTANT Notation: For the remainder of this Power Round, set the complex number

$$\omega = \frac{-1 + i\sqrt{3}}{2} = \cos(120^\circ) + i\sin(120^\circ).$$

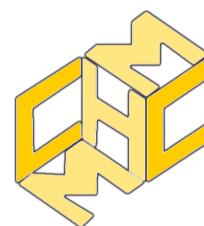
Here, ω is the Greek letter "omega."

Overview

1	Introduction (19 Points)	3
2	Euclidean Division (15 Points)	7
3	Eisenstein Primes (27 Points)	9
4	Diophantine Equations (20 Points)	14
5	Integral Dependence (19 Points)	17

Please read: Section 1 presents the basics of the Eisenstein integers, and is crucial for the remainder of this round. Section 2 defines the Euclidean division algorithm for the Eisenstein integers, and Section 3 aims to understand the Eisenstein primes, leveraging the theory developed in Section 2. Section 4 poses some contest-styled number theory problems that may be tackled by applying the main results of Section 3. Finally, Section 5 explores some (abstract) algebraic aspects of the Eisenstein integers, and as such depends mostly on Section 1 and not 2 or 3.

Some problem statements may contain hints. Every hint is labeled with square brackets [] at the end of the problem statement.



1 Introduction (19 Points)

Definition 1.1. The *Eisenstein integers*, denoted by $\mathbb{Z}[\omega]$, is a subset of the complex numbers, given by the set of all finite sums of the form

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_n\omega^n \tag{1}$$

for integers a_0, a_1, \dots, a_n . We may also refer to $\mathbb{Z}[\omega]$ as the *Eisenstein numbers* or the *Eisenstein number system*.

Note that two choices of coefficients a_0, a_1, \dots, a_n and b_0, b_1, \dots, b_m , as in the above definition, may give rise to the same Eisenstein integer (i.e., the same number in \mathbb{C}). We can make this definition more precise.

Problem 1.1 (2 Points). Prove that any Eisenstein integer $z \in \mathbb{Z}[\omega]$ may be written in the form $z = a + b\omega$ for integers a, b [Show that $\omega^2 + \omega + 1 = 0$].

Solution. By the quadratic formula, one of the solutions of the equation $x^2 + x + 1 = 0$ is precisely ω . Given Eisenstein integer $z := a_0 + a_1\omega + a_2\omega^2 + \cdots + a_n\omega^n$ of “degree” $n \geq 2$, we note $\omega^n = -\omega^{n-1} - \omega^{n-2}$, so that

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_n\omega^n = a_0 + a_1\omega + \cdots + (a_{n-2} - a_n)\omega^{n-2} + (a_{n-1} - a_n)\omega^{n-1}$$

We have written z as an Eisenstein integer of degree at most $n - 1$. Applying this method inductively allows us to write z in the desired form. □

In fact, it is true for any $z \in \mathbb{Z}[\omega]$, there exist *unique* integers a, b such that $z = a + b\omega$. This follows from the following general fact (not hard to prove):

Proposition 1.2. For any complex $z \in \mathbb{C}$, there exist *unique* real numbers c, d such that $z = c + d\omega$.

So from now on, we shall write Eisenstein integers in this form unless otherwise specified. For instance, whenever we say something like “let $z = a + b\omega$ be an Eisenstein integer,” the coefficients a, b are integers.

In light of these notions, here is a plot of the Eisenstein integers around the origin of the complex plane. As we can see, the Eisenstein integers form a *lattice* inside \mathbb{C}^1 :

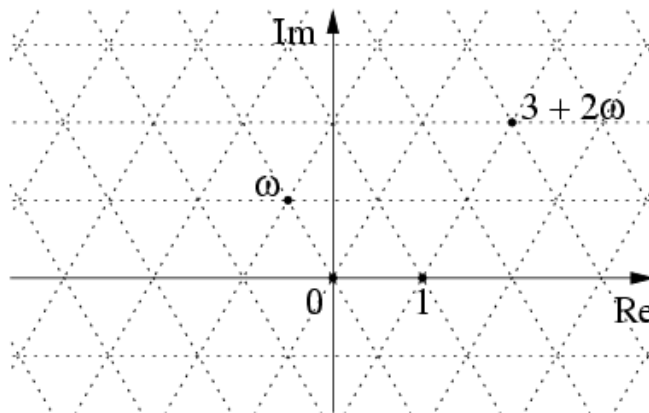


Figure 1: Eisenstein Lattice in \mathbb{C}

¹Source: https://en.wikipedia.org/wiki/Eisenstein_integer



Notice that the sum or difference of any two Eisenstein integers is again an Eisenstein integer. In other words, $\mathbb{Z}[\omega]$ is *closed* under addition or subtraction. However, $\mathbb{Z}[\omega]$ is also closed under multiplication:

Problem 1.2 (1 Point). Let $a_1 + b_1\omega, a_2 + b_2\omega$ be Eisenstein integers. Expand $(a_1 + b_1\omega)(a_2 + b_2\omega)$ and express it (explicitly) in the form $a + b\omega$. Deduce that the product of any two Eisenstein integers is again an Eisenstein integer [Again, $\omega^2 + \omega + 1 = 0$].

Remark. Formally speaking, one says that the Eisenstein integers $\mathbb{Z}[\omega]$ are a *ring* under the usual addition $+$ and multiplication \cdot operations.

Solution. Using $\omega^2 = -1 - \omega$, we have

$$(a_1 + b_1\omega)(a_2 + b_2\omega) = a_1a_2 + (a_1b_2 + b_1a_2)\omega + b_1b_2\omega^2 = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2 - b_1b_2)\omega$$

which is in the form $a + b\omega$. □

Definition 1.3. Let $z = a + b\omega$ be an Eisenstein integer. The *norm* of z is defined to be the following integer:

$$N(z) = N(a + b\omega) := a^2 - ab + b^2 \tag{2}$$

The norm of an Eisenstein integer is the analogue of the absolute value of an integer.

Problem 1.3 (2 Points). Suppose $a + b\omega$ is an Eisenstein integer. Prove that

1. (1 Point) $N(a + b\omega) = |a + b\omega|^2$, where $|\cdot|$ is the usual magnitude for \mathbb{C} (hence, the norm function is non-negative, and $N(z) = 0$ only when $z = 0$).
2. (1 Point) $N(a + b\omega) = (a + b\omega)(a + b\omega^2)$.

Solution 1. Using $\omega = \frac{-1+i\sqrt{3}}{2}$, we have

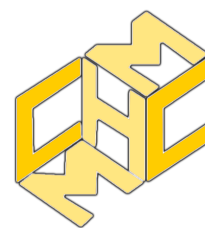
$$|a + b\omega|^2 = \left| \left(a - \frac{b}{2} \right) + \left(\frac{bi\sqrt{3}}{2} \right) \right|^2 = \left(a - \frac{b}{2} \right)^2 + \left(\frac{b\sqrt{3}}{2} \right)^2 = a^2 - ab + \frac{b^2}{4} + \frac{3b^2}{4} = a^2 - ab + b^2$$

as requested. □

Solution 2. Notice $\omega^2 = \frac{-1-i\sqrt{3}}{2} = \bar{\omega}$, so $\overline{a + b\omega^2} = a + b\omega$. Thus, $(a + b\omega)(a + b\omega^2) = (a + b\omega)\overline{(a + b\omega)} = |a + b\omega|^2 = N(a + b\omega)$. □

Problem 1.4 (2 Points). Prove that the norm function for $\mathbb{Z}[\omega]$ is multiplicative. Spelled out: let $z_1, z_2 \in \mathbb{Z}[\omega]$. Prove that $N(z_1z_2) = N(z_1)N(z_2)$.

Solution. Since complex magnitude is multiplicative, for $z_1, z_2 \in \mathbb{Z}[\omega]$ we have $N(z_1)N(z_2) = |z_1|^2|z_2|^2 = |z_1z_2|^2 = N(z_1z_2)$. □



Problem 1.5 (2 Points). Compute the norms $N(-1 + 2\omega), N(3 + 4\omega), N(1 + 5\omega)$.

Solution. We have $N(-1 + 2\omega) = (-1)^2 - (-1)(2) + 2^2 = 7$, $N(3 + 4\omega) = 3^2 - 3 \cdot 4 + 4^2 = 13$, $N(1 + 5\omega) = 1^2 - 1 \cdot 5 + 5^2 = 21$. \square

In the integers \mathbb{Z} , we have a basic notion of *unit*; namely, a unit u is a number such that any integer a may be “safely” divided by u . A more precise definition is:

Definition 1.4. Let a be an integer. An integer b is said to be a *multiplicative inverse* of a if $ab = 1$. The number a is said to be a *unit* of \mathbb{Z} if there exists a multiplicative inverse to a .

It is clear the units of \mathbb{Z} are precisely ± 1 . Here is the analogous definition in $\mathbb{Z}[\omega]$:

Definition 1.5. Let α be an Eisenstein integer. An Eisenstein integer $\beta \in \mathbb{Z}[\omega]$ is said to be a *multiplicative inverse* of α if $\alpha\beta = 1$. The number α is said to be an *Eisenstein unit*, or *unit* of $\mathbb{Z}[\omega]$, if there exists a multiplicative inverse to α .

Problem 1.6 (5 Points). Let $\alpha \in \mathbb{Z}[\omega]$ be an Eisenstein integer.

1. (1 Point) Prove that the product of any two units of $\mathbb{Z}[\omega]$ is again a unit of $\mathbb{Z}[\omega]$.
2. (2 Points) Suppose α is a unit of $\mathbb{Z}[\omega]$, and that $z \in \mathbb{Z}[\omega]$ is another Eisenstein integer. The number $\frac{z}{\alpha}$ is a complex number. Prove that it is in fact an Eisenstein integer.
3. (2 Points) If α is a unit of $\mathbb{Z}[\omega]$, prove that $N(\alpha) = 1$.

Solution 1. If $\alpha_1, \alpha_2 \in \mathbb{Z}[\omega]$ are Eisenstein units, then there exists $\beta_1, \beta_2 \in \mathbb{Z}[\omega]$ such that $\alpha_1\beta_1 = \alpha_2\beta_2 = 1$. Then, $(\alpha_1\alpha_2)(\beta_1\beta_2) = 1$, so by definition $\alpha_1\alpha_2$ is also an Eisenstein unit. \square

Solution 2. By definition, let $\beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = 1$. Then, $\frac{1}{\alpha} = \beta$ in $\mathbb{Z}[\omega]$. Hence, $\frac{z}{\alpha} = z \cdot \beta$ is an Eisenstein integer: we proved in Problem 1.2 that $\mathbb{Z}[\omega]$ is closed under multiplication. \square

Solution 3. Suppose there exists $\beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = 1$. Then, $1 = N(\alpha\beta) = N(\alpha)N(\beta)$ by multiplicativity of norm. Since norm is integral and non-negative, we have $N(\alpha) = 1$. \square

We are ready to classify the units of $\mathbb{Z}[\omega]$:

Problem 1.7 (5 Points). Prove that the units of $\mathbb{Z}[\omega]$ are precisely $\pm 1, \pm\omega, \pm\omega^2$ [Use the third part of the previous problem].

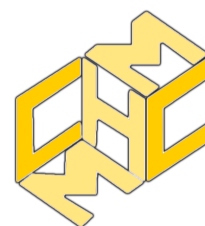
Solution. By the third part of Problem 1.6, we want to find those Eisenstein integers of norm 1. For any fixed integer b and varying real number a , the expression $a^2 - ab + b^2$ is minimized when $a = \frac{b}{2}$, achieving the minimum value of $\frac{3b^2}{4} \geq 0$. When b is even and nonzero, the minimum value of $a^2 - ab + b^2$ is $\frac{3b^2}{4}$, which is at least 3. When b is odd and nonzero, then the integral values of a that minimize $a^2 - ab + b^2$ are $a = \frac{b \pm 1}{2}$. In these cases, $a^2 - ab + b^2$ achieves the value $\frac{3b^2}{4} + \frac{1}{4}$, which is exactly 1 if $|b| = 1$ and at least 7 if $|b| \geq 3$. Hence, for any



integers a, b , we have $N(a + b\omega) = 1$ only if $b \in \{-1, 0, 1\}$ (by symmetry, this means $N(a + b\omega) = 1$ only if $a, b \in \{-1, 0, 1\}$). Thus, there are at most 9 units of $\mathbb{Z}[\omega]$.

The cases $(a, b) \in \{(\pm 1, 0), (0, \pm 1), (\mp 1, \mp 1)\}$ correspond to the Eisenstein integers $\pm 1, \pm\omega, \pm\omega^2$, and $N(a + b\omega) = 1$ in each of these cases. On the other hand, $N(0) = 0$ (in case $(a, b) = (0, 0)$) and $N(1 - \omega) = N(-1 + \omega) = 3$ (in case $(a, b) \in \{(\pm 1, \mp 1)\}$). Recalling the fact $\omega^3 = 1$, the Eisenstein integers $\pm 1, \pm\omega, \pm\omega^2$ have multiplicative inverses $\pm 1, \pm\omega^2, \pm\omega$, respectively, completing the proof. \square

Notice in particular the Eisenstein units are precisely those Eisenstein integers of norm 1.



2 Euclidean Division (15 Points)

The only integers that divide *any* element of \mathbb{Z} are by are the units ± 1 . For every other integer divisor, we can only settle for a division algorithm with remainder. In particular, we say that the integers \mathbb{Z} have the *Euclidean division property*.

Theorem 2.1 (Euclidean division algorithm for \mathbb{Z}). For any integers a, b with $b \neq 0$, there exist integers q, r such that

$$a = qb + r \quad \text{and} \quad 0 \leq |r| < |b|. \quad (3)$$

This is the equation you would usually write when performing “integer division with remainder” (except that we drop the assumption that the remainder is positive). This property of \mathbb{Z} is essential, as one may prove that it implies the *Fundamental Theorem of Arithmetic*, which says all positive integers may be factored, uniquely, into a product of positive primes.

We want to ask whether there is an analogous *Euclidean division property* for the Eisenstein integers. If we can answer in the affirmative, then it would imply that there is an analogue of the Fundamental Theorem of Arithmetic in $\mathbb{Z}[\omega]$. We should state what we want in a precise way. Let α, β be Eisenstein integers with $\beta \neq 0$. We are asking whether there exist Eisenstein integers γ, ρ such that

$$\alpha = \gamma\beta + \rho \quad \text{and} \quad 0 \leq N(\rho) < N(\beta). \quad (4)$$

It turns out we can answer this question in the affirmative. The following problem describes a Euclidean division algorithm for the Eisenstein integers:

Problem 2.1 (6 Points). (*Euclidean division property of $\mathbb{Z}[\omega]$*) Let α, β be Eisenstein integers with $\beta \neq 0$. Put $z = \frac{\alpha}{\beta}$. Recall that there exist *unique* real numbers c, d such that $z = c + d\omega$.

1. (3 Points) Suppose c' and d' are the integers given by rounding c and d , respectively, to the nearest integer. Define $\gamma = c' + d'\omega \in \mathbb{Z}[\omega]$. Prove that $N(\gamma - z) \leq \frac{3}{4}$.
2. (3 Points) Let $\rho = \alpha - \gamma\beta$, where γ is defined previously. Explain why ρ is an Eisenstein integer. Prove that $N(\rho) < N(\beta)$, concluding that $\alpha, \beta, \gamma, \rho$ satisfy Equation (4) (hence, the Eisenstein integers have Euclidean division).

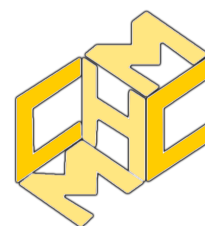
Solution 1. Notice $\gamma - z = (c' - c) + (d' - d)\omega$. Thus,

$$N(\gamma - z) = (c' - c)^2 - (c' - c)(d' - d) + (d' - d)^2 \leq (c' - c)^2 + |c' - c||d' - d| + (d' - d)^2 \leq \frac{3}{4}$$

as $|c' - c|, |d' - d| \leq \frac{1}{2}$ by rounding. □

Solution 2. Since γ, β are Eisenstein integers, $\gamma\beta$ is as well. Thus, the difference $\alpha - \gamma\beta$ is again an Eisenstein integer. Since $z = \frac{\alpha}{\beta}$, we have $\alpha - \gamma\beta = \alpha - z\beta + (z - \gamma)\beta = (z - \gamma)\beta$, and we have $N(\rho) = N(z - \gamma)N(\beta) \leq \frac{3}{4}N(\beta) < N(\beta)$, as requested. Hence, the Eisenstein integers have Euclidean division. □

In fact, by choosing γ more carefully, the above bound $N(\rho) \leq \frac{3}{4}N(\beta)$ may be further tightened. But this Euclidean division algorithm suffices for our purposes. Now, let's introduce the notion of an *ideal* of \mathbb{Z} (resp. $\mathbb{Z}[\omega]$), which is, somewhat informally speaking, a subset of \mathbb{Z} (resp. $\mathbb{Z}[\omega]$) closed under addition and “scalar” multiplication. This is a concept typically introduced in the context of abstract algebra.



Definition 2.2. Let R be either \mathbb{Z} or $\mathbb{Z}[\omega]$. A nonempty subset $I \subset R$ is called an *ideal* of R if for every $z, z_1, z_2 \in I$ and $\alpha \in R$, we have $z_1 + z_2 \in I$ and $\alpha z \in I$.

Let $I \subset R$ be an ideal. If there exists $\beta \in I$ such that every element $z \in I$ is of the form $z = \alpha\beta$ for some $\alpha \in R$, then we say I is a *principal ideal* of R and that its *generator* is β .

Example 2.3. The set $\{0\}$ is an ideal of both \mathbb{Z} and $\mathbb{Z}[\omega]$, called the *zero ideal*. The set of all $\mathbb{Z}[\omega]$ -multiples of 2022 is an ideal of $\mathbb{Z}[\omega]$. This ideal strictly contains the set of all integer multiples of 2022, which is an ideal of \mathbb{Z} . All of these examples are principal ideals.

With the definition of an ideal, we can prove the following important consequence of the Euclidean division property. It is actually one of the key steps to proving the Fundamental Theorem of Arithmetic (in generality for either \mathbb{Z} or $\mathbb{Z}[\omega]$)!

Remark. Formally speaking, \mathbb{Z} and $\mathbb{Z}[\omega]$ are called *principal ideal domains*.

Problem 2.2 (4 Points). Prove that every ideal of the integers \mathbb{Z} and of the Eisenstein integers $\mathbb{Z}[\omega]$ is principal.

Solution. Here is the proof for an ideal $I \subset \mathbb{Z}[\omega]$. If $I = \{0\}$ then there is nothing to prove. Otherwise, let $\beta \in I$ be any nonzero element of minimum norm². By definition of ideal, the principal ideal generated by β , denoted by (β) , is contained in I . Assume on the contrary there exists $\alpha \in I, \alpha \notin (\beta)$. By Euclidean division, write $\alpha = \gamma\beta + \rho$ for some $\gamma, \rho \in \mathbb{Z}[\omega]$ such that $N(\rho) < N(\beta)$. Since $\rho = \alpha - \gamma\beta$ and $\alpha, \gamma\beta \in I$, we have $\rho \in I$. By the minimality of the norm of β , we must have $\rho = 0$, completing the proof.

The proof for \mathbb{Z} is exactly the same as above, using the Euclidean division property of \mathbb{Z} and replacing the Eisenstein norm with the usual absolute value. □

Now let's try some examples.

Problem 2.3 (2 Points). Find Eisenstein integers γ, ρ such that

$$13 = \gamma(2 + \omega) + \rho \quad \text{and} \quad 0 \leq N(\rho) < N(2 + \omega). \quad (5)$$

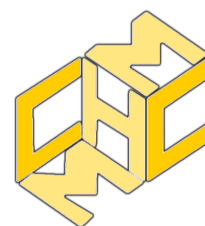
Solution. We apply Euclidean division. We have $\frac{13}{(2+\omega)} = \frac{13(2+\omega^2)}{(2+\omega)(2+\omega^2)} = \frac{26}{3} + \frac{13}{3}\omega^2 = \frac{13}{3} - \frac{13}{3}\omega$. Rounding, we obtain $\gamma = (4 - 4\omega)$. To finish, we have $\rho = 13 - (4 - 4\omega)(2 + \omega) = 13 - (8 - 4\omega - 4\omega^2) = 13 - 12 = 1$. □

Problem 2.4 (3 Points). Show that there are unique Eisenstein integers γ, ρ such that

$$19 = \gamma(3 - 2\omega) + \rho \quad \text{and} \quad 0 \leq N(\rho) < N(3 - 2\omega). \quad (6)$$

Solution. In this case notice $19 = (3 - 2\omega)(3 - 2\omega^2)$. Hence, set $\gamma = 3 - 2\omega^2$ and $\rho = 0$. Now, for any other choice of γ , the unique value of ρ satisfying the first equation must be $(3 - 2\omega)(3 - 2\omega^2 - \gamma)$. Hence, $N(\rho) \geq N(3 - 2\omega)$ by multiplicativity of norm. Thus, our original choice of γ, ρ is unique. □

²Such an element exists since the set of norms of nonzero elements of I has a minimum element by the well-ordering of \mathbb{Z} .



3 Eisenstein Primes (27 Points)

As alluded to in Section 2, there exists a Fundamental Theorem of Arithmetic for the Eisenstein number system. We will state this Fundamental Theorem in short order. But we can't go about factoring the Eisenstein integers until we know something about the primes in the Eisenstein integers! Finding prime numbers in \mathbb{Z} is not easy: there is no big classification theorem that tells us what every prime integer is. What about primes in $\mathbb{Z}[\omega]$? Well, actually, the primes in \mathbb{Z} already give us tons of information on the primes in $\mathbb{Z}[\omega]$. This section focuses on solving this problem.

We shall start with a review on the notions of divisibility and primes in the integers.

Definition 3.1. Let a, b be integers. Then, b divides a , or b is said to be a *divisor* of a (denoted by $b \mid a$), in \mathbb{Z} , if there exists an integer k such that $kb = a$.

Definition 3.2. An integer p , not equal to 0 or ± 1 , is called a *rational prime* if whenever we have integers a, b such that $ab = kp$ for some integer k (i.e., p divides ab), either p divides a or p divides b . If $p > 0$ we say p is a *positive rational prime*.

In other words, a positive integer p is a (positive) rational prime if and only if it is a prime number in the usual sense: its only positive divisors are 1 and itself. We can think of the rational primes, including the negative ones, as a generalization of the usual prime numbers to all of \mathbb{Z} . For the remainder of this power round, the term "prime" without any qualifiers refers to "positive rational prime," i.e. the usual prime numbers. Now, let's state the analogous definitions in the Eisenstein integers. First, we define "divisibility."

Definition 3.3. Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be Eisenstein integers. Then, β divides α , or β is said to be a *divisor* of α (denoted by $\beta \mid \alpha$), in $\mathbb{Z}[\omega]$, if there exists $\kappa \in \mathbb{Z}[\omega]$ such that $\kappa\beta = \alpha$.

Notice any Eisenstein integer divides 0. Moreover, for any $a, b \in \mathbb{Z}$, observe $a \mid b$ in \mathbb{Z} if and only if $a \mid b$ in $\mathbb{Z}[\omega]$. Some standard properties of divisibility in \mathbb{Z} are unchanged when moving to $\mathbb{Z}[\omega]$, such as reflexivity and transitivity. Now onto the definition of *Eisenstein prime*.

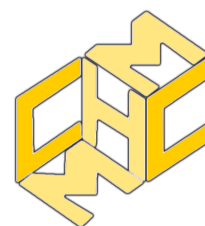
Definition 3.4. A nonzero Eisenstein integer $\pi \in \mathbb{Z}[\omega]$ is said to be an *Eisenstein prime* if it is not a unit and whenever we have Eisenstein integers $\alpha, \beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = \kappa\pi$ for some $\kappa \in \mathbb{Z}[\omega]$ (i.e., π divides $\alpha\beta$), either π divides α or π divides β .

We can see the Eisenstein primes are to the Eisenstein integers as the rational primes (including negative ones) are to the usual integers. Here is a basic fact on Eisenstein primes:

Problem 3.1 (2 Points). Let $\pi \in \mathbb{Z}[\omega]$ be an Eisenstein integer and $u \in \mathbb{Z}[\omega]$ a unit. Prove that π is an Eisenstein prime if and only if $u\pi$ is an Eisenstein prime.

Solution. Pick $v \in \mathbb{Z}[\omega]$ such that $uv = 1$. Note v is a unit.

Suppose π is an Eisenstein prime, and $\alpha, \beta \in \mathbb{Z}[\omega]$ such that $u\pi$ divides $\alpha\beta$. Since π divides $u\pi$, transitivity of divisibility implies π divides $\alpha\beta$. Hence, π divides α or β . Since π divides $v\pi$, we see $u\pi$ divides $uv\pi = \pi$. Hence, $u\pi$ divides α or β , so $u\pi$ is an Eisenstein prime.



Conversely, suppose $u\pi$ is an Eisenstein prime. Repeating the above proof with the unit v , we conclude $vu\pi = \pi$ is an Eisenstein prime. \square

This leads us to the following definition:

Definition 3.5. An Eisenstein integer z_1 is said to be *associate* to z_2 if there exists a unit $u \in \mathbb{Z}[\omega]$ such that $z_1 = uz_2$. In particular, an Eisenstein prime π_1 is said to be *associate* to π_2 if there exists a unit $u \in \mathbb{Z}[\omega]$ such that $\pi_1 = u\pi_2$.

We shall conduct the following discussion to clarify some important details about the above definition. For $z_1, z_2, z_3 \in \mathbb{Z}[\omega]$:

- z_1 is always associate to itself.
- If z_1 is associate to z_2 , then z_2 is associate to z_1 .
- If z_1 is associate to z_2 , and z_2 is associate to z_3 , then z_1 is associate to z_3 .

In particular, sometimes we will call z_1, z_2 *associates* rather than spelling out “ z_1 is associate to z_2 .” Now, the above three properties imply the following proposition:

Proposition 3.6. There exists a partition of $\mathbb{Z}[\omega]$ into a family of pairwise disjoint nonempty subsets: $\mathbb{Z}[\omega] = \bigsqcup_{\alpha} C_{\alpha}$, such that two Eisenstein integers belong in the same C_{α} if and only if they are associates. Each set C_{α} is called an *equivalence class*.

Remark. The expression $\bigsqcup_{\alpha} C_{\alpha}$ denotes the *disjoint union* of all C_{α} ’s. Namely, the statement $\mathbb{Z}[\omega] = \bigsqcup_{\alpha} C_{\alpha}$ says: the union of all equivalence classes C_{α} ’s is $\mathbb{Z}[\omega]$, and for any two distinct classes C_{α}, C_{β} , we have $C_{\alpha} \cap C_{\beta} = \emptyset$.

Remark. In the situation of the above Proposition, each equivalence class has exactly 6 elements, since there are 6 units in $\mathbb{Z}[\omega]$. In other words, each Eisenstein integer $z \in \mathbb{Z}[\omega]$ is associate to exactly 6 other Eisenstein integers, namely $\pm z, \pm\omega z, \pm\omega^2 z$.

We are at last ready to state the Fundamental Theorem of Arithmetic (the proof of which we omit):

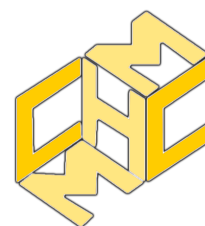
Theorem 3.7 (Fundamental Theorem of Arithmetic). Let $z \in \mathbb{Z}[\omega]$ be an Eisenstein integer. Then, z may be factored as a product of Eisenstein primes $z = \pi_1 \dots \pi_r$, and if $z = \pi'_1 \dots \pi'_s$ is another factorization into Eisenstein primes, then $r = s$ and there is some renumbering of the factors π'_1, \dots, π'_s such that the Eisenstein primes π_j, π'_j are associates for all $1 \leq j \leq r$.

Note in particular that if $\alpha, \beta \in \mathbb{Z}[\omega]$ are associate to $\pi_1^{a_1} \dots \pi_r^{a_r}, \pi_1^{b_1} \dots \pi_r^{b_r}$, respectively (where the exponents a_j, b_j are non-negative), then $\alpha\beta$ is associate to $\pi_1^{a_1+b_1} \dots \pi_r^{a_r+b_r}$.

With the Fundamental Theorem of Arithmetic on hand, we are ready to begin the classification of Eisenstein primes. The classification theorem is proven from Problem 3.2 to to Problem 3.7.

Problem 3.2 (3 Points). Let z be an Eisenstein integer such that $N(z)$ is a positive rational prime. Prove that z is an Eisenstein prime [Use the Euclidean division property].

Solution. Let $\alpha, \beta \in \mathbb{Z}[\omega]$ such that $z \mid \alpha\beta$. By Euclidean division, there exist $\gamma_1, \gamma_2, \rho_1, \rho_2$ such that $\alpha = \gamma_1 z + \rho_1, \beta = \gamma_2 z + \rho_2$ and $0 \leq N(\rho_1), N(\rho_2) < N(z)$.



Assume on the contrary $z \nmid \alpha, z \nmid \beta$. Thus, ρ_1, ρ_2 are both nonzero, so $N(\rho_1), N(\rho_2)$ are also nonzero. Hence, by multiplicativity of norm, $N(\rho_1\rho_2)$ is not a multiple of $N(z)$. On the other hand, $\rho_1\rho_2 = (\alpha - \gamma_1z)(\beta - \gamma_2z)$, so in fact $z \mid \rho_1\rho_2$. This means we can write $\rho_1\rho_2 = \kappa z$ for some $\kappa \in \mathbb{Z}[\omega]$, i.e. $N(\rho_1\rho_2) = N(\kappa)N(z)$, a contradiction. It follows z is an Eisenstein prime. \square

Problem 3.3 (4 Points). Let p be a positive rational prime satisfying $p \equiv 2 \pmod{3}$.

1. (1 Point) Let $a + b\omega$ be an Eisenstein integer. Prove that $N(a + b\omega) \equiv 0 \pmod{3}$ or $N(a + b\omega) \equiv 1 \pmod{3}$.
2. (3 Points) Using the previous result, prove that p is an Eisenstein prime.

Solution 1. Recall $N(a + b\omega) = a^2 - ab + b^2$. By a direct computation, we observe that modulo 3 residue pairs $(a, b) \in \{(0, 0), (1, 2), (2, 1)\} \subset (\mathbb{Z}/3\mathbb{Z})^2$ satisfy the congruence $a^2 - ab + b^2 \equiv 0 \pmod{3}$ while all other modulo 3 residue pairs (a, b) satisfy the congruence $a^2 - ab + b^2 \equiv 1 \pmod{3}$. \square

Solution 2. Let $\alpha, \beta \in \mathbb{Z}[\omega]$ such that $p \mid \alpha\beta$. By Euclidean division, there exists $\gamma_1, \gamma_2, \rho_1, \rho_2$ such that $\alpha = \gamma_1p + \rho_1, \beta = \gamma_2p + \rho_2$ and $0 \leq N(\rho_1), N(\rho_2) < N(p) = p^2$. Since $\rho_1 = \alpha - \gamma_1p, \rho_2 = \beta - \gamma_2p$ we have that $p \mid \rho_1\rho_2$. We can write $\rho_1\rho_2 = \kappa p$ for some $\kappa \in \mathbb{Z}[\omega]$, i.e. $N(\rho_1\rho_2) = N(\kappa)N(p)$.

Assume on the contrary $p \nmid \alpha, p \nmid \beta$. Thus, ρ_1, ρ_2 are both nonzero, so $N(\rho_1), N(\rho_2)$ are also nonzero. However, $N(\rho_1\rho_2) = N(\rho_1)N(\rho_2)$ is a multiple of $N(p) = p^2$, so we must have $N(\rho_1), N(\rho_2) = p$. This is a contradiction of part 1. \square

Problem 3.4 (2 Points). Prove that 3 is not an Eisenstein prime by finding two Eisenstein primes π_1, π_2 such that $3 = \pi_1\pi_2$. For your choice of π_1, π_2 : show that π_1, π_2 are associates (thus, by the Fundamental Theorem of Arithmetic, 3 is the “square” of an Eisenstein prime).

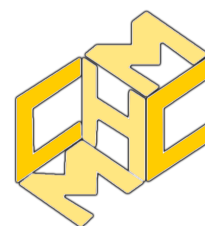
Solution. One possible factorization is $3 = (-1 + \omega)(-1 + \omega^2)$. We can check by direct computation that $N(-1 + \omega) = N(-1 + \omega^2) = 3$ is prime, implying by Problem 3.2 that the two factors are prime. In this case we have $-\omega^2(-1 + \omega) = -1 + \omega^2$, i.e. $-1 + \omega$ times the unit $-\omega^2$ is $-1 + \omega^2$. \square

Problem 3.5 (6 Points). Let p be a positive rational prime satisfying $p \equiv 1 \pmod{3}$. Prove the following two facts in any order you wish. Circular reasoning will not earn credit.

- (a) Prove that p factors as a product of two Eisenstein primes.
- (b) Prove there exist $a, b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$.

Solution. First, let's give a proof of (a) and then deduce (a) \implies (b). Note p is an odd prime, so $6 \mid p - 1$. Then, by the primitive root theorem there exists an integer s such that $s^3 \equiv -1 \pmod{p}, s \not\equiv -1 \pmod{p}$. By sum of cubes factorization this means $s^2 - s + 1 \equiv 0 \pmod{p}$. Then, p divides $s^2 - s + 1 = (s + \omega)(s + \omega^2)$ in $\mathbb{Z}[\omega]$. Assume on the contrary p is an Eisenstein prime. Then, it divides one of $s + \omega, s + \omega^2$ in $\mathbb{Z}[\omega]$ —WLOG there exists $\kappa \in \mathbb{Z}[\omega]$ such that $p\kappa = s + \omega$. Since $s + \omega^2$ is the complex conjugate of $s + \omega$, we use the fact p is real to observe $p\bar{\kappa} = s + \omega^2$. Hence, p divides both $s + \omega, s + \omega^2$, hence divides $\omega - \omega^2 = i\sqrt{3}$, a contradiction.

Since p is not an Eisenstein prime, the Fundamental Theorem of Arithmetic gives a factorization of p as a product of r primes. In particular, notice $N(p) = p^2$ and every Eisenstein prime has norm greater than 1; applying



multiplicativity of norm, the prime factorization must be of the form $p = \pi_1 \pi_2$ for two Eisenstein primes π_1, π_2 satisfying $N(\pi_1) = N(\pi_2) = p$. This proves (a). Writing $\pi_1 = a + b\omega$, we conclude $p = N(\pi_1) = a^2 - ab + b^2$, which is (b).

Alternatively, here is a direct proof of (b) using the Pigeonhole principle. Again, since $3 \mid p - 1$, by the primitive root theorem there exists an integer s such that $s^3 \equiv 1 \pmod{p}, s \not\equiv 1 \pmod{p}$. By difference of cubes factorization this means $s^2 + s + 1 \equiv 0 \pmod{p}$.

Note that the set $P := \{(x, y) : 0 \leq x, y \leq \lfloor \sqrt{p} \rfloor\}$ has $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$ pairs. Thus, by the Pigeonhole principle, we have the following result: for any integer s , in particular the s fixed above, there are two distinct pairs $(x_1, y_1), (x_2, y_2) \in P$ such that

$$x_1 - sy_1 \equiv x_2 - sy_2 \pmod{p}.$$

Writing $a = x_1 - x_2, b = y_2 - y_1$ we have that $a \equiv -sb \pmod{p}$. Of course, a, b are nonzero, as the pairs $(x_1, y_1), (x_2, y_2)$ are distinct. Thus, $a^2 \equiv s^2 b^2 \equiv (-s - 1)b^2 \pmod{p}$. Simplifying, we get $a^2 - ab + b^2 \equiv 0 \pmod{p}$. However, $a^2 - ab + b^2 = N(a + b\omega)$ is nonzero, yet $a^2 - ab + b^2 \leq |a^2| + |ab| + |b^2| < 3p$. The case $a^2 - ab + b^2 = 2p$ is impossible as the RHS is congruent to $2 \pmod{3}$. It follows $a^2 - ab + b^2 = p$ as requested. Now, notice $(a + b\omega)(a + b\omega^2) = a^2 - ab + b^2 = p$, proving (b). Since $N(a + b\omega) = p, N(p) = p^2$, by multiplicativity of norm we have $N(a + b\omega^2) = p$. Thus, $p = (a + b\omega)(a + b\omega^2)$ is a product of two Eisenstein primes (cf. Problem 3.2: an Eisenstein integer of prime norm is Eisenstein prime). This is (a). \square

Remark. In the situation of Problem 3.5, p is in fact a product of two *non-associate* Eisenstein primes. The proof of this fact is a matter of tedious casework and will be omitted.

We have exhibited a lot of Eisenstein primes! Formally speaking, the positive rational primes $p \equiv 2 \pmod{3}$ are said to be *inert* in $\mathbb{Z}[\omega]$ whereas the positive rational primes $p \equiv 1 \pmod{3}$ are said to be *split* in $\mathbb{Z}[\omega]$. The prime $p = 3$ is said to be *ramified* in $\mathbb{Z}[\omega]$. Now, we contend Problems 3.2, 3.3, 3.4, 3.5 classify the set of *all* Eisenstein primes. To do so, we must show that any Eisenstein prime $\pi \in \mathbb{Z}[\omega]$ is “closely” related to the usual (positive) primes in \mathbb{Z} . We shall tackle this in the following two problems.

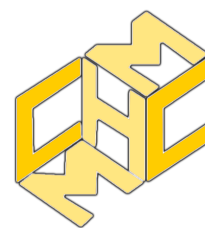
Problem 3.6 (4 Points). Let $\pi \in \mathbb{Z}[\omega]$ be an Eisenstein prime, and let I be the principal ideal of $\mathbb{Z}[\omega]$ generated by π .

1. (1 Point) Show that $I \cap \mathbb{Z}$ is an ideal of \mathbb{Z} .
2. (1 Point) Prove that the ideal $I \cap \mathbb{Z}$ of \mathbb{Z} satisfies the following property: if a, b are integers such that $ab \in I \cap \mathbb{Z}$, then either $a \in I \cap \mathbb{Z}$ or $b \in I \cap \mathbb{Z}$ (this property says $I \cap \mathbb{Z}$ is a *prime ideal* of \mathbb{Z}).
3. (2 Points) Conclude that $I \cap \mathbb{Z}$ is a principal ideal of \mathbb{Z} generated by a positive rational prime p . Deduce p is a multiple of π in $\mathbb{Z}[\omega]$.

Solution 1. For $z_1, z_2 \in I \cap \mathbb{Z}$, we have $z_1 + z_2 \in I \cap \mathbb{Z}$ by definition of ideal and the fact the integers are closed under addition. Moreover, for $z \in I \cap \mathbb{Z}, a \in \mathbb{Z}$, we have $az \in I$ (again by definition of ideal) and $az \in \mathbb{Z}$ since integers are closed under multiplication. Hence, $I \cap \mathbb{Z}$ is an ideal of \mathbb{Z} . \square

Solution 2. By definition of (Eisenstein) prime: for any $a, b \in \mathbb{Z}$ such that $ab \in I$, either π divides a or π divides b . Hence, either $a \in I \cap \mathbb{Z}$ or $b \in I \cap \mathbb{Z}$. \square

Solution 3. Since every ideal of \mathbb{Z} is principal, suppose $I \cap \mathbb{Z}$ is the principal ideal of \mathbb{Z} generated by some integer n . We may assume n is non-negative, as the principal ideal of \mathbb{Z} generated by n is the same as that generated by



$-n$. Notice n is a multiple of π in $\mathbb{Z}[\omega]$, as $n \in I$ and π generates I , so $n \neq 1$: it is not an Eisenstein unit. Moreover, since $N(\pi) = \pi\bar{\pi} \in I \cap \mathbb{Z}$ is non-zero, n must also be non-zero. Thus, n is either a prime or composite number in \mathbb{N} (in the usual sense). But the case where n is composite is a contradiction of the previous part. Hence, n is a positive rational prime p (that is a multiple of π in $\mathbb{Z}[\omega]$). \square

In particular, every Eisenstein prime is a divisor of a *unique* positive rational prime p .

Problem 3.7 (3 Points). (*Classification of primes in $\mathbb{Z}[\omega]$*) Suppose $\pi \in \mathbb{Z}[\omega]$ is an Eisenstein prime that divides some positive rational prime p in $\mathbb{Z}[\omega]$. Prove that $N(\pi)$ is either p or p^2 . Deduce that the Eisenstein primes are exactly the following list:

- An associate of a positive rational prime congruent to 2 (mod 3)
- Eisenstein integers of norm 3
- Eisenstein integers of prime norm congruent to 1 (mod 3)

Solution. Since Problem 3.6 proved that π divides p in $\mathbb{Z}[\omega]$, $N(\pi)$ divides $N(p) = p^2$. However, π is not a unit, meaning $N(\pi)$ is not equal to 1. Hence, $N(\pi) \in \{p, p^2\}$.

Problems 3.2, 3.3, 3.4, 3.5 showed that the above list of Eisenstein integers are indeed Eisenstein primes. Conversely, by the above, any Eisenstein prime π has norm p or p^2 for some positive rational prime p such that π divides p . The $N(\pi) = p$ case implies that either $p = 3$ or $p \equiv 1 \pmod{3}$, because Problem 3.3 excludes the possibility of $p \equiv 2 \pmod{3}$. In the $N(\pi) = p^2$ case, the divisibility condition says $u\pi = p$ for some $u \in \mathbb{Z}[\omega]$. Then, u is a unit, since $N(p) = p^2$. Hence, p is an Eisenstein prime; by Problem 3.3 that means it is a positive rational prime congruent to 2 (mod 3). \square

Remark. Thus, if $\pi \in \mathbb{Z}[\omega]$ is an Eisenstein prime of norm p or p^2 , where p is a positive rational prime, then π divides p . For π divides a unique positive rational prime q , so $N(\pi)$ equals q or q^2 . If $q \neq p$, then $N(\pi)$ does not equal either p or p^2 .

This concludes the classification of Eisenstein primes. Let's try some example problems.

Problem 3.8 (3 Points). Find Eisenstein prime factorizations of the following Eisenstein integers z :

1. (1 Point) $z = 91$
2. (2 Points) $z = 15\omega^2 - 25$.

Solution 1. Since 13 is prime and $13 \equiv 1 \pmod{3}$, an Eisenstein prime factorization of 13 is of the form $13 = (a + b\omega)(a + b\omega^2)$ by Problem 3.5, where $a^2 - ab + b^2 = 13$. We check $a = 4, b = 1$ works. Likewise, since 7 is prime and $7 \equiv 1 \pmod{3}$, an Eisenstein prime factorization of 7 is given by $7 = (2 - \omega)(2 - \omega^2)$. Thus, the desired factorization is $91 = (2 - \omega)(2 - \omega^2)(4 + \omega)(4 + \omega^2)$. \square

Solution 2. First note $15\omega^2 - 25 = \omega^2(15 - 25\omega) = 5\omega^2(3 - 5\omega)$ and $5 \equiv 2 \pmod{3}$, so $5\omega^2$ is an Eisenstein prime. Notice $N(3 - 5\omega) = 3^2 + 3 \cdot 5 + 5^2 = 49 = 7^2$ and that it is not an Eisenstein prime as $7 \equiv 1 \pmod{3}$ (cf. Problem 3.7). This suggests we look to write $3 - 5\omega$ as a product of two Eisenstein primes of norm 7. Indeed: $(2 - \omega)(2 - \omega) = 4 - 4\omega + \omega^2 = 3 - 5\omega$. Thus, the desired factorization is $15\omega^2 - 25 = 5\omega^2(2 - \omega)(2 - \omega)$. \square



4 Diophantine Equations (20 Points)

The Eisenstein integers are invaluable to solving certain classical Diophantine equations, particularly those involving expressions of the form $a^2 - ab + b^2, a^2 + ab + b^2$. Namely, the properties $N(a + b\omega) = a^2 - ab + b^2$, $N(a - b\omega) = a^2 + ab + b^2$ give an immediate relation between these Diophantine expressions and the Eisenstein integers. The problems in this section are *best approached using the Eisenstein integers and primes* especially using the machinery developed in Section 3. See in particular Theorem 3.7 the Fundamental Theorem of Arithmetic in $\mathbb{Z}[\omega]$ and Problem 3.7 the classification theorem on Eisenstein primes. You are welcome to attempt solving these problems without these techniques, however, although we do not recommend this.

We begin with the following warm-up problem, which may be readily approached with our knowledge of Eisenstein primes.

Problem 4.1 (3 Points). List all ordered pairs (a, b) of positive integers such that $a^2 - ab + b^2 = 2023$. You do not need to give justification [Compare to the equation $a^2 - ab + b^2 = 7$].

Solution. We have $N(a + b\omega) = a^2 - ab + b^2$, for any Eisenstein integer $a + b\omega$, so the equivalent problem is to find Eisenstein integers $a + b\omega$ of norm 2023 with $a, b \in \mathbb{N}$. Suppose $a + b\omega$ is an Eisenstein integer of norm 2023. Writing $a + b\omega = \pi_1\pi_2 \dots \pi_r$ as a product of Eisenstein primes, we have $N(a + b\omega) = N(\pi_1)N(\pi_2) \dots N(\pi_r)$. Since $2023 = 7 \cdot 17^2$, the classification theorem (cf. Problem 3.7) implies that $r = 2$ and $a + b\omega$ is the product of an Eisenstein prime of norm 7 and an Eisenstein prime associate to the rational prime 17. In particular, since $7 = (2 - \omega)(2 - \omega^2)$, every Eisenstein prime of norm 7 is associate to either $2 - \omega$ or $2 - \omega^2$. Hence, the Eisenstein integers of norm 2023 are precisely $17(2 - \omega)$ or $17(2 - \omega^2)$ up to multiplication by a unit. Among those Eisenstein integers $a + b\omega$ where a, b are *positive* integers, we obtain the positive integer solution set $(a, b) = \{(17, 51), (34, 51), (51, 34), (51, 17)\}$ to the original Diophantine equation. \square

Problem 4.1 admits the following generalization:

Problem 4.2 (5 Points). Let n be a positive integer with prime factorization $n = 3^k p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$, where p_1, \dots, p_r are distinct (positive rational) primes congruent to 1 (mod 3) and q_1, \dots, q_s are distinct primes congruent to 2 (mod 3). Consider the Diophantine equation $a^2 - ab + b^2 = n$.

1. (2 Points) Prove that the equation $a^2 - ab + b^2 = n$ has a solution in integers (a, b) if and only if the exponents b_1, \dots, b_s are even.
2. (3 Points) In the situation in which the condition of the previous problem holds (b_1, \dots, b_s are even), find, in terms of the parameters $k, a_1, \dots, a_r, b_1, \dots, b_s$, the number of solutions to $a^2 - ab + b^2 = n$ in integers (a, b) [Examine Proposition 3.6 and its following remark].

Solution 1. Since $N(a + b\omega) = a^2 - ab + b^2$, the solutions to the Diophantine equation $a^2 - ab + b^2 = n$ are in one-to-one correspondence with Eisenstein integers of norm $n = 3^k p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$. Suppose $a + b\omega$ is an Eisenstein integer of norm n . Writing $a + b\omega = \pi_1\pi_2 \dots \pi_t$ as a product of Eisenstein primes, we have $N(a + b\omega) = N(\pi_1)N(\pi_2) \dots N(\pi_t)$. By the classification theorem (cf. Problem 3.7), for each $1 \leq j \leq t$ we either have $N(\pi_j) = p$ for $p = 3$ or $p \equiv 1 \pmod{3}$ or $N(\pi_j) = p^2$ for $p \equiv 2 \pmod{3}$ (where p is a positive rational prime). Hence, each of the exponents b_1, \dots, b_s of the positive rational primes congruent to 2 (mod 3) in the prime factorization $n = 3^k p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$ must be even. Conversely, if b_1, \dots, b_s are even, then the classification



theorem supplies Eisenstein primes of norms $3, p_1, \dots, p_r, q_1^2, \dots, q_s^2$ and thus (combining these Eisenstein primes appropriately) an Eisenstein integer of norm $3^k p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$. \square

Solution 2. Assume b_1, \dots, b_s are even. For each prime p_j congruent to 1 (mod 3), there exist non-associate Eisenstein primes $\pi_j, \bar{\pi}_j \in \mathbb{Z}[\omega]$ such that $p_j = \pi_j \bar{\pi}_j$ by Problem 3.5, and in fact these are the only Eisenstein prime divisors of p_j . If $a + b\omega$ is an Eisenstein integer of norm n , then by examining norms as before, the factorization of $a + b\omega$ into Eisenstein primes is precisely of the form

$$a + b\omega = (1 - \omega)^k \left(\prod_{j=1}^r \pi_j^{c_j} \bar{\pi}_j^{a_j - c_j} \right) \left(\prod_{j=1}^s q_j^{b_j/2} \right) \quad \text{for non-negative integers } 0 \leq c_j \leq a_j$$

up to a multiplication by a unit of $\mathbb{Z}[\omega]$. The parameter c_j has $a_j + 1$ choices, so any element of $\mathbb{Z}[\omega]$ of norm n is associate to one of the above $(a_1 + 1) \dots (a_r + 1)$ choices. Finally, each element of $\mathbb{Z}[\omega]$, corresponding to a choice of c_1, \dots, c_r , is associate to 6 elements of $\mathbb{Z}[\omega]$ (cf. the remark after Proposition 3.6). Therefore, there are $6(a_1 + 1) \dots (a_r + 1)$ solutions to $a^2 - ab + b^2 = n$ in integers (a, b) . \square

Recall that Euclid's formula says that for any *primitive Pythagorean triple*, namely, an ordered triple (a, b, c) of relatively prime positive integers (i.e., $\gcd(a, b, c) = 1$) such that a, b, c are the side lengths of a right triangle with c opposite the right angle (assume b is even), that there exists relatively prime positive integers m, n , not both odd, such that

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2 \tag{7}$$

For example, the primitive Pythagorean triple $(3, 4, 5)$ admits $m = 2, n = 1$.

With our knowledge of the Eisenstein integers, we shall develop a "Euclid's formula" for triangles with an angle of 120° :

Problem 4.3 (12 Points). Let a, b, c be positive integers, $\gcd(a, b, c) = 1$, that are the sides of a (non-degenerate) triangle such that c is opposite an angle of 120° .

1. (1 Point) Explain why $a^2 + ab + b^2 = c^2$.
2. (2 Points) Show that $\gcd(a, b) = 1$ and that either $a - b$ or $b - a$ is congruent to 1 (mod 3).
3. (9 Points) ("*Euclid's*" formula) Assume $a - b \equiv 1 \pmod{3}$. Show that there exist relatively prime positive integers m, n , with $m \not\equiv n \pmod{3}$, such that

$$a = m^2 - n^2, \quad b = 2mn + n^2, \quad c = m^2 + mn + n^2. \tag{8}$$

Solution 1. Since $\cos(120^\circ) = -\frac{1}{2}$, the equation $a^2 + ab + b^2 = c^2$ holds by the Law of cosines. \square

Solution 2. Suppose $d > 1$ is a common divisor of a, b , so $a = a'd, b = b'd$. Then, $a^2 + ab + b^2 = d^2(a'^2 + a'b' + b'^2) = c^2$. Hence, $d \mid c$, a contradiction of $\gcd(a, b, c) = 1$.

Now, if $3 \mid a - b$, i.e. $a \equiv b \pmod{3}$, then a^2, ab, b^2 are all congruent to 0 or 1 (mod 3); hence, $a^2 + ab + b^2 = c^2 \equiv 0 \pmod{3}$. Thus, $9 \mid c^2$. Writing $b = a + 3k$ for $k \in \mathbb{Z}$, we have

$$a^2 + a(a + 3k) + (a + 3k)^2 \equiv 0 \pmod{9} \implies 3a^2 + 9ak + 9k^2 \equiv 0 \pmod{9} \implies 3a^2 \equiv 0 \pmod{9}.$$

In particular, $a^2 \equiv 0 \pmod{3}$, so $a \equiv 0 \pmod{3}$. That means $b \equiv 0 \pmod{3}$, as well, a contradiction of $\gcd(a, b, c) = 1$. Thus, either $a - b$ or $b - a$ is congruent to 1 (mod 3). \square



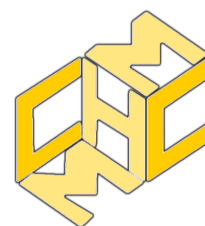
Solution 3. Notice $c \not\equiv 0 \pmod{3}$, otherwise $a^2 + ab + b^2 \equiv c^2 \equiv 0 \pmod{9}$, which means $(a-b)^2 \equiv a^2 - 2ab + b^2 \equiv -3ab \pmod{9}$ and thus $a-b \equiv 0 \pmod{3}$. Notice $c^2 = N(a-b\omega) = (a-b\omega)(a-b\bar{\omega})$. We claim that $\alpha = a-b\omega, \bar{\alpha} = a-b\bar{\omega}$ are relatively prime in $\mathbb{Z}[\omega]$, i.e. that they do not share any Eisenstein prime divisors. Assume on the contrary $\pi \in \mathbb{Z}[\omega]$ is an Eisenstein prime dividing both $\alpha, \bar{\alpha}$ in $\mathbb{Z}[\omega]$. Then, π divides $\bar{\alpha} - \alpha = b\omega(1-\omega)$ in $\mathbb{Z}[\omega]$. On the one hand, if π divides $1-\omega$ (equiv. π is associate to the *unique* Eisenstein prime associated to 3), then $3 = \pi\bar{\pi}$ divides $\alpha\bar{\alpha} = c^2$ in $\mathbb{Z}[\omega]$, a contradiction of $c \not\equiv 0 \pmod{3}$. On the other hand, if π divides $b\omega$ in $\mathbb{Z}[\omega]$, then π also divides a in $\mathbb{Z}[\omega]$. Then, by Bezout's lemma, π divides $\gcd(a,b) = 1$ in $\mathbb{Z}[\omega]$, a contradiction as Eisenstein primes never divide units. This completes the proof of the claim.

Remark c^2 is associate to an Eisenstein prime factorization $\pi_1^{2a_1} \dots \pi_r^{2a_r}$ for non-negative a_1, \dots, a_r . By “relatively-primeness” (in $\mathbb{Z}[\omega]$), α is associate to a square $\pi_1^{2a_1} \dots \pi_s^{2a_s}$ for some $0 < s < r$ in $\mathbb{Z}[\omega]$ (rearranging the primes π_1, \dots, π_r as appropriate). Hence,

$$a - b\omega = u(m - n\omega)^2 \quad \text{for some Eisenstein unit } u \in \{\pm 1, \pm\omega, \pm\omega^2\} \text{ and } m, n \in \mathbb{Z}.$$

Then, note that $a - b\omega^2 = \overline{a - b\omega} = \bar{u}(m - n\omega^2)^2$, so $c^2 = (m - n\omega)^2(m - n\omega^2)^2$, implying $c = m^2 + mn + n^2$. That means $m \not\equiv n \pmod{3}$, as $c \not\equiv 0 \pmod{3}$.

We may suppose $u = \pm 1$, because $\omega = \omega^4$ (e.g., $\omega(m - n\omega)^2 = \omega^4(m - n\omega)^2$ may be rewritten as $(m\omega^2 - n\omega^3)^2$ and simplifying $m\omega^2 - n\omega^3$ into the $a' + b'\omega$ form). Thus, $a - b\omega = \pm((m^2 - n^2) - (2mn + n^2)\omega)$. Hence, m, n are both nonzero, because a, b are both positive. The negative case of the expression $\pm((m^2 - n^2) - (2mn + n^2)\omega)$ cannot hold, because then $a - b \equiv -(m^2 - n^2 - 2mn - n^2) \equiv -((m - n)^2 - 3n^2) \equiv 2 \pmod{3}$ as $m \not\equiv n \pmod{3}$. Hence, $a = m^2 - n^2, b = 2mn + n^2$. We may replace m, n by $-m, -n$, if necessary, so that n is positive. Then, since $|m| > n$, m must be positive for $2mn + n^2 > 0$. Finally, m, n are relatively prime—for any common divisor d of m, n , the number d^2 is a common divisor of a, b, c . This completes the proof. \square



5 Integral Dependence (19 Points)

As already mentioned in Section 1, the only units, i.e. elements of \mathbb{Z} with a multiplicative inverse, are ± 1 . One way to “remedy” this situation is to consider the *rational numbers* \mathbb{Q} , which, as we know, are fractions $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. We can always add, subtract, and multiply any two fractions. But most importantly, we can divide any rational number by any other non-zero rational number. In particular, we can divide any integer by any non-zero integer to obtain a rational number. Hence, any non-zero element of \mathbb{Q} has a multiplicative inverse.

The natural question to ask, now, is the analogue of this concept for the Eisenstein number system $\mathbb{Z}[\omega]$. Indeed, one may define the *Eisenstein rationals* as follows.

Definition 5.1. The *Eisenstein rationals*, denoted by $\mathbb{Q}(\omega)$ or $\mathbb{Q}[\omega]$, is a subset of the complex numbers, given by the set of all finite sums of the form

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_n\omega^n \quad (9)$$

for rational numbers a_0, a_1, \dots, a_n .

Problem 5.1 (3 Points). Let $z \in \mathbb{Q}(\omega)$ be an Eisenstein rational.

1. (1 Point) Prove that z may be written in the form $z = a + b\omega$ for unique rational numbers a, b . Also prove that z may be written in the form $z = c + di\sqrt{3}$ for unique rational numbers c, d .
2. (2 Points) Prove that for any Eisenstein rationals $\alpha, \beta \in \mathbb{Q}(\omega)$ where $\beta \neq 0$, the complex number $\frac{\alpha}{\beta}$ is an Eisenstein rational. Conversely, show that any Eisenstein rational equals $\frac{\alpha}{\beta}$ for some Eisenstein integers $\alpha, \beta \in \mathbb{Z}[\omega]$.

Solution 1. Apply the argument in Problem 1.1, which holds without further restriction, to show existence of a representation $z = a + b\omega$. The uniqueness of a, b holds due to Proposition 1.2. Suppose $z = a + b(\frac{-1+i\sqrt{3}}{2})$ is a unique representation. Then, $z = c + di\sqrt{3}$ for $c = a - \frac{b}{2}$, $d = \frac{b}{2}$, as needed. Conversely, if $z = c + di\sqrt{3}$ is a representation, then $z = (c + d) + 2d(\frac{-1+i\sqrt{3}}{2})$, and the system of equations $a = c + d, b = 2d$ has a unique rational solution in c, d , proving uniqueness. \square

Solution 2. Write $\alpha = a + b\omega, \beta = c + d\omega \in \mathbb{Z}[\omega]$. Then,

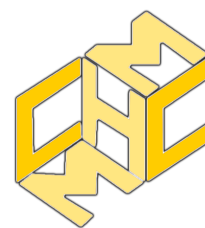
$$\frac{\alpha}{\beta} = \frac{a + b\omega}{c + d\omega} = \frac{(a + b\omega)(c + d\omega^2)}{(c + d\omega)(c + d\omega^2)} = \frac{1}{c^2 - cd + d^2} ((ac + bd - ad) + (bc - ad)\omega) \in \mathbb{Q}(\omega).$$

Here, note that the denominator $N(c + d\omega) = c^2 - cd + d^2$ is positive, since $c + d\omega \neq 0$. We are carrying over the norm function for $\mathbb{Z}[\omega]$ to $\mathbb{Q}(\omega)$; the properties of Problem 1.3 hold.

Conversely, for $\frac{a}{b} + \frac{c}{d}\omega \in \mathbb{Q}(\omega)$, note $\frac{ad + bc\omega}{bd} = \frac{a}{b} + \frac{c}{d}\omega$ and the numerator and denominator of the LHS are Eisenstein integers. \square

Hence, the Eisenstein rationals are closed under addition, subtraction, multiplication (cf. Problem 1.2), and division (by non-zero values).

Remark. Formally speaking, one says that the Eisenstein rationals $\mathbb{Q}(\omega)$ are a *field* under the usual addition $+$ and multiplication \cdot operations and the property of non-zero multiplicative inverses. Every *field* is a *ring* (cf. Section 1).



Problem 5.2 (1 Point). Prove that $z = \sqrt{2} + i\sqrt{5}$ is not an Eisenstein rational.

Solution. Suppose for sake of contradiction z is an Eisenstein rational. Then, $z^2 = -3 + 2i\sqrt{10}$ is an Eisenstein rational as well. Adding 3 and dividing by $2i\sqrt{3}$, that means $\sqrt{\frac{10}{3}}$ is an Eisenstein rational. In fact, if $\sqrt{\frac{10}{3}} = a + b\omega \in \mathbb{Q}(\omega)$, then $b = 0$ as the LHS is a real number. Hence, $\sqrt{\frac{10}{3}} \in \mathbb{Q}$.

From here the argument is standard, we include it for completion. Namely, suppose $\frac{a}{b} = \sqrt{\frac{10}{3}}$ is a rational number and a, b are coprime. Then, $\frac{a^2}{b^2} = \frac{10}{3}$, so $10b^2 = 3a^2$. Since $10b^2$ is a multiple of 3 and $\gcd(10, 3) = 1$, b is a multiple of 3. Dividing by 3 on both sides, we also conclude a is a multiple of 3, a contradiction. \square

Now, consider the following “pointless” way of defining the integers. For every rational number $r \in \mathbb{Q}$, there exists a unique nonzero monic (recall: monic = leading coefficient is 1) polynomial with rational coefficients, of minimal degree, which has r as one of its roots—namely, $x - r$. Let’s call this the *minimal polynomial* of r . The integers \mathbb{Z} are precisely those rational numbers whose minimal polynomials have *integer* coefficients. However, this definition becomes not so pointless when we move to $\mathbb{Z}[\omega]$ and $\mathbb{Q}(\omega)$. From now on, let $\mathbb{Z}[x], \mathbb{Z}[\omega][x]$, and $\mathbb{Q}[x]$ be the set of all polynomials with integer, Eisenstein integer, and rational coefficients, respectively, in the single variable x .

Definition 5.2. Let $\alpha \in \mathbb{Q}(\omega)$ be an Eisenstein rational. We say that α is *algebraic* (over \mathbb{Q}) if there exists a nonzero polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$.

Clearly every rational number $r \in \mathbb{Q}$ is algebraic.

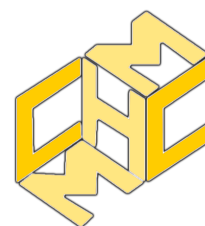
Problem 5.3 (3 Points). Prove that every $\alpha \in \mathbb{Q}(\omega)$ is algebraic. In fact, prove the following stronger statement: for each $\alpha \in \mathbb{Q}(\omega)$, there exists a *unique* nonzero monic polynomial $m_\alpha(x) \in \mathbb{Q}[x]$, of minimal degree, such that α is a root of $m_\alpha(x)$. By minimal, we mean that there is no nonzero polynomial in $\mathbb{Q}[x]$ of degree lesser than that of $m_\alpha(x)$ that contains α as a root.

Solution. First note that nonzero degree 0 polynomials in $\mathbb{Q}[x]$ do not have roots. Assume $\alpha \in \mathbb{Q}$ is a rational number. Then, the polynomial $x - \alpha \in \mathbb{Q}[x]$ is nonzero monic of degree 1, hence of minimal degree. Thus, $m_\alpha(x) = x - \alpha$.

Now, assume $\alpha = a + b\omega \in \mathbb{Q}(\omega)$ is irrational non-real (i.e. $b \neq 0$). The polynomial $f(x) = x^2 - (2a - b)x + (a^2 - ab + b^2) \in \mathbb{Q}[x]$ factors as $(x - (a + b\omega))(x - (a + b\omega^2))$; hence, α is algebraic. We claim $f(x) = m_\alpha(x)$. To do so, note $m_\alpha(x)$ cannot be degree 1, as any linear polynomials in $\mathbb{Q}[x]$ has a unique rational root. Now, any degree 2 polynomial in $\mathbb{Q}[x]$ with $a + b\omega$ as one of its (nonreal) roots must also have the complex conjugate $\overline{a + b\omega} = a + b\omega^2$ as its other root (this is a well-known general property for all polynomials with *real* coefficients). Hence, any degree 2 monic polynomial containing α as one of its roots is uniquely determined, so we conclude $m_\alpha(x) = f(x)$. \square

Definition 5.3. For any $\alpha \in \mathbb{Q}(\omega)$, the polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ corresponding to α as defined in Problem 5.3 is called its *minimal polynomial* (over \mathbb{Q}).

The relation between $\mathbb{Z}[\omega]$ and $\mathbb{Q}(\omega)$ involves the concept of *integral dependence*:



Definition 5.4. An Eisenstein rational $\alpha \in \mathbb{Q}(\omega)$ is said to be *integral* over \mathbb{Z} (resp. $\mathbb{Z}[\omega]$) if there exists a nonzero monic polynomial $f(x) \in \mathbb{Z}[x]$ (resp. $f(x) \in \mathbb{Z}[\omega][x]$) such that α is a root of $f(x)$.

Note that the definition of “algebraic” and “integral” are analogous: each instance of \mathbb{Q} is replaced by \mathbb{Z} (or $\mathbb{Z}[\omega]$). The reason for the different terminology is the fundamental difference between the structures of \mathbb{Q} and \mathbb{Z} : in \mathbb{Q} , every non-zero element of \mathbb{Q} is a unit (carrying over Definition 1.4 in the obvious way), whereas the only units in \mathbb{Z} and $\mathbb{Z}[\omega]$, respectively, are ± 1 and $\pm 1, \pm \omega, \pm \omega^2$, respectively. It thus turns out that the properties of “algebraic” and “integral” are studied in different contexts in the overarching field of abstract algebra.

Here is a useful characterization of integral dependence:

Problem 5.4 (3 Points). Prove that $\alpha \in \mathbb{Q}(\omega)$ is integral over \mathbb{Z} if and only if the minimal polynomial of α lies in $\mathbb{Z}[x]$.

Solution. Assume $f(x) \in \mathbb{Z}[x]$ is a monic polynomial containing α as a root. Recall that $f(x)$ may be factored into monic irreducible divisors in $\mathbb{Z}[x]$. One of these irreducible divisors $g(x)$ contains α as a root. By Gauss’s lemma, $g(x)$ is also irreducible in $\mathbb{Q}[x]$. Now, consider the minimal polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ of α . By polynomial division in $\mathbb{Q}[x]$, there are polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that $g(x) = q(x)m_\alpha(x) + r(x)$ and $\deg r(x) < \deg m_\alpha(x)$. By substituting α into this equation, we deduce $r(\alpha) = 0$. But by minimality of the degree of $m_\alpha(x)$, we must have $r(x) = 0$ identically. Now, since $g(x)$ is irreducible monic, we have $q(x) = 1$ identically and $g(x) = m_\alpha(x)$. Hence, $m_\alpha(x) \in \mathbb{Z}[x]$. The converse is obvious by the definition of integral dependence. \square

The following Problem gives a definition of the Eisenstein integers $\mathbb{Z}[\omega]$ in terms of the Eisenstein rationals $\mathbb{Q}(\omega)$ (and \mathbb{Z}), instead of the other way around, as we did in Section 1 and the beginning of Section 4.

Problem 5.5 (5 Points). Prove that the subset of elements of $\mathbb{Q}(\omega)$ integral over \mathbb{Z} is precisely the Eisenstein integers $\mathbb{Z}[\omega]$. We call $\mathbb{Z}[\omega]$ the *integral closure* of \mathbb{Z} in $\mathbb{Q}(\omega)$. This explains the term “integral dependence!”

Solution. First note that $\mathbb{Z}[\omega]$ is integral over \mathbb{Z} , as any $a \in \mathbb{Z}$ has minimal polynomial $x - a \in \mathbb{Z}[x]$ and any nonreal Eisenstein integer $a + b\omega$ has minimal polynomial $x^2 - (2a - b)x + (a^2 - ab + b^2) \in \mathbb{Z}[x]$. For any rational number $q \in \mathbb{Q}$ that is not an integer, the minimal polynomial $x - q$ clearly does not lie in $\mathbb{Z}[x]$. Thus, it suffices to prove for $a + b\omega = c + di\sqrt{3} \in \mathbb{Q}(\omega)$, $b \neq 0$, that $x^2 - (2a - b)x + (a^2 - ab + b^2) \in \mathbb{Z}[x]$ implies $a, b \in \mathbb{Z}$.

Perform the substitutions $a = c + d, b = 2d$ and note $a, b \in \mathbb{Z}$ if and only if $2c, 2d$ are integers of the same parity. Thus, suppose $2c = 2a - b, c^2 + 3d^2 = a^2 - ab + b^2 \in \mathbb{Z}$; we must show that $c = \frac{m}{2}, d = \frac{n}{2}$ for $m, n \in \mathbb{Z}$ both even or both odd. Since $2c, 2d \in \mathbb{Z}$, we have $4(c^2 + 3d^2) = (2c)^2 + 3(2d)^2 \in \mathbb{Z}$, so $3(2d)^2 \in \mathbb{Z}$. Since 3 is squarefree, it follows $2d \in \mathbb{Z}$. Thus, write $c = \frac{m}{2}, d = \frac{n}{2}$ for $m, n \in \mathbb{Z}$. Since $c^2 + 3d^2 \in \mathbb{Z}$, we have $m^2 + 3n^2 \equiv 0 \pmod{4}$. This mod 4 equivalence holds if and only if the parities of m and n are equal, completing the proof. \square

Even more is true regarding $\mathbb{Z}[\omega]$:

Problem 5.6 (4 Points). Prove that the subset of elements of $\mathbb{Q}(\omega)$ integral over $\mathbb{Z}[\omega]$ is again $\mathbb{Z}[\omega]$.

Solution. By Problem 5.5, it suffice to prove that an element of $\mathbb{Q}(\omega)$ is integral over $\mathbb{Z}[\omega]$ if and only if it is integral over \mathbb{Z} .



Assume $z \in \mathbb{Q}(\omega)$ is integral over $\mathbb{Z}[\omega]$, i.e. z is a root of a monic polynomial $f(x) = x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_1x + \alpha_0$ for $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{Z}[\omega]$. Consider the monic polynomial $f(x)g(x)$, where

$$g(x) := x^n + \overline{\alpha_{n-1}}x^{n-1} + \dots + \overline{\alpha_1}x + \overline{\alpha_0}$$

is the polynomial obtained by complex conjugating the coefficients of f . Since $\overline{\alpha_0}, \overline{\alpha_1}, \dots, \overline{\alpha_{n-1}} \in \mathbb{Z}[\omega]$, we have $f(x)g(x) \in \mathbb{Z}[\omega][x]$. Moreover, the coefficient of x^m for $0 \leq m \leq 2n$ of $f(x)g(x)$, is $\sum_{j=0}^m \overline{\alpha_j} \alpha_{m-j}$, where $\alpha_n = \overline{\alpha_n} = 1$, $\alpha_j = \overline{\alpha_j} = 0, n+1 \leq j \leq 2n$ implicitly. However, the complex conjugate of $\sum_{j=0}^m \overline{\alpha_j} \alpha_{m-j}$ is itself, meaning that $f(x)g(x)$ has real coefficients. An element of $\mathbb{Z}[\omega]$ is in \mathbb{Z} if and only if it is real, so $f(x)g(x) \in \mathbb{Z}[x]$. Hence, z is integral over \mathbb{Z} . The converse is obvious because $\mathbb{Z} \subset \mathbb{Z}[\omega]$. \square

We say that $\mathbb{Z}[\omega]$ is *integrally closed* in $\mathbb{Q}(\omega)$. Problem 5.6 illustrates a special case of a general fact about integral dependence in commutative algebra:

Let $A \subseteq B \subseteq C$ be commutative rings with 1, such that B is integral over A and C is integral over B . Then, C is integral over A .