CHMMC
Caltech Harvey Mudd Math Competition

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

Please read: Section 1 presents the basics of the Eisenstein integers, and is crucial for the remainder of this round. Sections 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 $a_0, a_1, \ldots, a_n$. We may also refer to $\mathbb{Z}[\omega]$ as the *Eisenstein numbers* or the *Eisenstein number system*.

Note that two choices of coefficients $a_0, a_1, \ldots, a_n$ and $b_0, b_1, \ldots, b_m$, 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 $\omega^2 + \omega + 1 = 0$].

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]:

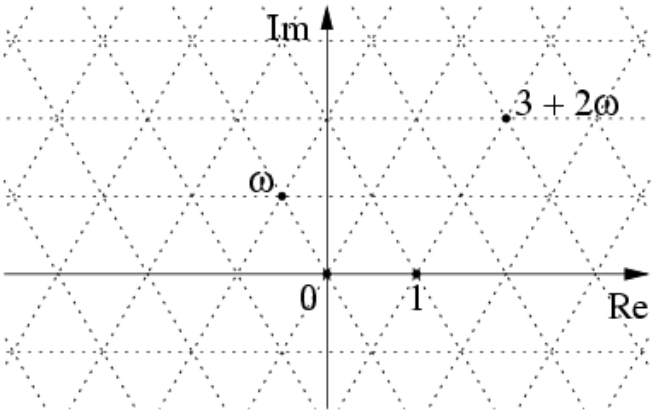

Figure 1: Eisenstein Lattice in $\mathbb{C}$

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, $\omega^2 + \omega + 1 = 0$].

[1] Source: `https://en.wikipedia.org/wiki/Eisenstein_integer`

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

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) $N(a+b\omega) = (a+b\omega)(a+b\omega^2)$.

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 $N(z_1 z_2) = N(z_1)N(z_2)$.

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

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 $N(\alpha) = 1$.

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].

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

$$a = qb + r \qquad \text{and} \qquad 0 \leq |r| < |b|. \tag{3}$$

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

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

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).

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.

Now let's try some examples.

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

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

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

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

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.

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 $\pi'_1, \dots, \pi'_s$ such that the Eisenstein primes π_j, π'_j are associates for all $1 \le j \le r$.

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].

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.

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).

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 $p = a^2 - ab + b^2$.

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 $\mathbb{Z}[\omega]$.

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 $2 \pmod 3$
- Eisenstein integers of norm 3
- Eisenstein integers of prime norm congruent to $1 \pmod 3$

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) $z = 15\omega^2 - 25$.

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 $a^2-ab+b^2=7$].

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 $1 \pmod 3$ and $q_1,\dots,q_s$ are distinct primes congruent to $2 \pmod 3$. 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].

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

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

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 $1 \pmod 3$.
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

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

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

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_n\omega^n \tag{9}$$

for rational numbers $a_0, a_1, \ldots, a_n$.

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 $\alpha, \beta \in \mathbb{Z}[\omega]$.

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.

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.

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 $\mathbb{Z}[x]$.

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!"

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 $\mathbb{Z}[\omega]$.

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.