A tour of the Eisenstein integers

Rasmus Frigaard Lemvig

January 2024

Contents

1 Introduction

The aim of this paper is to give a thourough introduction to the Eisenstein integers. We will discuss how basic arithmetic works for these integers and we shall see that they share many of the properties of ordinary integers such as the existence of a Euclidean algorithm and unique factorization into prime elements. Towards the end, we will briefly touch upon some more advanced topics. We use $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ to denote the integers, $\mathbb{N} = \{1, 2, ...\}$ to denote the positive integers (without zero) and $\mathbb{N}_0 = \{0, 1, 2, ...\}$ to denote the non-negative integers. The focus of the text is almost purely mathematical, but some of the procedures in the proofs are also implemented as algorithms. If the reader is interested in the computational aspects, they are encouraged to implement these algorithms in their favorite programming language. Code for these algorithms in C++ are available here: `https://github.com/RasmusFL/EisensteinIntegers`.

The prerequisites for reading the paper is a basic understanding of the integers. This includes some experience with modular arithmetic, primes and the Euclidean algorithm. For the more advanced topics, references are included.

1.1 Basic arithmetic

Let us first and foremost define the main object of interest.

Definition 1.1. Let $\omega = e^{\frac{2\pi i}{3}}$. The set $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ is called the set of *Eisenstein integers*.

We note that $\mathbb{Z}[\omega]$ is a subset of the complex numbers $\mathbb{C}$. We can thus do arithmetic as we usually do with the complex numbers. Explicitly, let $\alpha = a + b\omega$ and $\beta = c + d\omega$ denote two Eisenstein integers. Then

$$\begin{aligned} \alpha + \beta &= a + b\omega + c + d\omega = (a + c) + (b + d)\omega \\ \alpha \cdot \beta &= (a + b\omega)(c + d\omega) = ac + ad\omega + bc\omega + bd\omega^2 \\ &= (ac - bd) + (ad + bc - bd)\omega \end{aligned}$$

where we have used that ω is a root of the polynomial $x^2 + x + 1$. The above identities show that $\mathbb{Z}[\omega]$ is closed under addition and multiplication.

1.2 The norm and the conjugate

Definition 1.2. We define the *norm* N on $\mathbb{Z}[\omega]$ as the map $N : \mathbb{Z}[\omega] \to \mathbb{N}_0$ given by $N(a + b\omega) = a^2 - ab + b^2$.

For example, $N(1-\omega) = 1^2 - 1 \cdot (-1) + (-1)^2 = 3$ and $N(3+2\omega) = 3^2 - 3 \cdot 2 + 2^2 = 9 - 6 + 4 = 7$. We use this norm instead of the ordinary complex norm $|\cdot|$ since N only attains integer values. This will be very useful later on. Let us start by convincing ourselves that the norm always gives non-negative values.

Proposition 1.3. *For any $\alpha \in \mathbb{Z}[\omega]$, we have $N(\alpha) \geq 0$. Furthermore, $N(\alpha) = 0$ if and only if $\alpha = 0$.*

Proof. Let $\alpha = a + b\omega$. Then

$$N(\alpha) = a^2 - ab + b^2 = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

so the norm is a quadratic form. The matrix

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix}$$

has the eigenvalues 3/2 and 1/2 and hence it is positive definite. The claim follows. ■

There are two essential properties of the norm. The first is that the norm only takes non-negative integer values. The other is the property of multiplicativity.

Proposition 1.4. *The norm N is multiplicative i.e. for $\alpha, \beta \in \mathbb{Z}[\omega]$ we have $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Proof. Write $\alpha = a + b\omega$ and $\beta = c + d\omega$. We compute

$$\begin{aligned} N(\alpha\beta) &= N((ac - bd) + (ad + bc - bd)\omega) \\ &= (ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ad + bc - bd)^2 \\ &= a^2c^2 + b^2d^2 - 2abcd - (a^2cd + abc^2 - abcd - abd^2 - b^2cd + b^2d^2) \\ &+ (a^2d^2 + 2abcd - 2abd^2 + b^2c^2 - 2b^2cd + b^2d^2) \\ &= a^2c^2 - a^2cd + a^2d^2 - abc^2 + abcd - abd^2 + b^2c^2 - b^2cd + b^2d^2 \end{aligned}$$

and

$$\begin{aligned} N(\alpha)N(\beta) &= (a^2 - ab + b^2)(c^2 - cd + d^2) \\ &= a^2c^2 - a^2cd + a^2d^2 - abc^2 + abcd - abd^2 + b^2c^2 - b^2cd + b^2d^2. \end{aligned}$$

We see that the two expressions coincide. ■

In the integers $\mathbb{Z}$, only two elements are invertible with respect to multiplication, namely 1 and -1. We call such elements *units*.

Definition 1.5. An element $\alpha \in \mathbb{Z}[\omega]$ is a *unit* if there exists some other element $\beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = 1$. We call β the *multiplicative inverse* or simply the *inverse* of α, and we write α^{-1} for β.

It is meaningful to say "the" inverse since an inverse is unique. See the exercises for details. To determine the units for the Eisenstein integers, we will apply the following useful result.

Lemma 1.6. *$\alpha \in \mathbb{Z}[\omega]$ is a unit if and only if $N(\alpha) = 1$.*

Proof. Assume that α is a unit and let β denote the inverse of α. Using Proposition 1.4, we obtain $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$. We know that the norm only takes non-negative integer values and hence we have $N(\alpha) = N(\beta) = 1$. Conversely, assume α is an element of norm 1. Write $\alpha = a + b\omega$. Let $\beta = a - b - b\omega$. We then have

$$\begin{aligned} \alpha\beta = (a + b\omega)(a - b - b\omega) &= a^2 - ab - ab\omega + ab\omega - b^2\omega - b^2\omega^2 \\ &= a^2 - ab - b^2\omega - b^2(-\omega - 1) = a^2 - ab + b^2 - b^2\omega + b^2\omega = 1 \end{aligned}$$

as desired. ■

The choice of β in the proof above may seem arbitrary, but it turns out to be a natural guess for an inverse (when it exists). Recall that for a complex number $a + bi$ ($a, b \in \mathbb{R}$), the conjugate is given by

$$\overline{a + bi} = a - bi.$$

The following result captures the connection between the norm and the conjugate.

Proposition 1.7. *Let $\alpha = a + b\omega \in \mathbb{Z}[\omega]$.*

(1) We have $\overline{\alpha} = (a - b) - b\omega$.

(2) $N(\alpha) = \alpha\overline{\alpha}$.

(3) If α is invertible, then the inverse is given by $\overline{\alpha}$.

Proof. See the exercises. ■

Let us return to the task of determining all units in $\mathbb{Z}[\omega]$.

Proposition 1.8. *$\mathbb{Z}[\omega]$ has six units, namely $\pm 1, \pm\omega$ and $\pm(1 + \omega)$.*

Proof. Using the lemma from before, we have to solve the equation $a^2 - ab + b^2 = 1$ when a and b are integers. We do so using the following clever tricks:

$$a^2 - ab + b^2 = 1 \quad \Leftrightarrow \quad 4a^2 - 4ab + 4b^2 = 4 \quad \Leftrightarrow \quad (2a - b)^2 + 3b^2 = 4.$$

We now see that $b \in \{\pm 1\}$. In any case, we must have $2a - b \in \{\pm 1\}$ as well. It follows that all solutions are exactly as stated in the proposition. ■

Before moving on to divisibility, we introduce a concept which will become important later.

Definition 1.9. Two elements α and β in $\mathbb{Z}[\omega]$ are called *associates* if they only differ by a unit i.e. there is a unit u in $\mathbb{Z}[\omega]$ such that $\alpha = u\beta$.

It is clear that associated elements have the same norm.

1.3 Divisibility in $\mathbb{Z}[\omega]$

Divisibility in $\mathbb{Z}[\omega]$ is completely analogous to division in $\mathbb{Z}$.

Definition 1.10. Let $\alpha, \beta \in \mathbb{Z}[\omega]$. We say that β *divides* α (or that β is a *factor* of α) if there exists some $\gamma \in \mathbb{Z}[\omega]$ such that $\alpha = \beta\gamma$. In this case, we write $\beta \mid \alpha$.

Example 1.11. Let $\alpha = -2 + 6\omega$ and $\beta = 3 + 4\omega$. We investigate whether β divides α. To do so, we use the usual strategy of division in the complex numbers.

$$\begin{aligned}\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{(-2 + 6\omega)(3 - 4 - 4\omega)}{3^2 - 3 \cdot 4 + 4^2} &= \frac{(-2 + 6\omega)(-1 - 4\omega)}{13} \\ &= \frac{(-2)(-1) - (6(-4)) + ((-2)(-4) + 6(-1) - 6(-4))}{13} \\ &= \frac{26 + 26\omega}{13} = 2 + 2\omega \in \mathbb{Z}[\omega].\end{aligned}$$

We conclude that β does indeed divide α.

Using the multiplicativity of the norm, it is often easier to decide whether an element divides another in $\mathbb{Z}[\omega]$.

Proposition 1.12. *Assume $\beta \mid \alpha$ in $\mathbb{Z}[\omega]$. Then $N(\beta) \mid N(\alpha)$.*

Proof. By definition, $\alpha = \beta\gamma$ for some $\gamma \in \mathbb{Z}[\omega]$. Proposition 1.4 then yields $N(\alpha) = N(\beta)N(\gamma)$, proving the claim. ■

Example 1.13. Does $\beta = 1 + 3\omega$ divide $\alpha = -2 + 6\omega$. We compute $N(\beta) = 7$ and $N(\alpha) = 52$. Since 7 does not divide 52, β does not divide α.

As we shall see later, the element $1-\omega$ plays a special role. It has norm 3 and it turns out that every element with norm divisible by 3 has $1-\omega$ as a factor.

Proposition 1.14. *Let $\alpha \in \mathbb{Z}[\omega]$. Then α has $1-\omega$ as a factor if and only if $N(\alpha)$ is divisible by 3.*

Proof. If $1-\omega$ is a factor of α, then $N(1-\omega) = 3$ divides $N(\alpha)$ by the above proposition. Conversely, suppose 3 divides $N(\alpha)$. If $\alpha = a + b\omega$, the goal is to determine c and d in $\mathbb{Z}$ such that

$$a + b\omega = (1-\omega)(c + d\omega).$$

The right hand side can be expanded as

$$(1-\omega)(c + d\omega) = (c + d) + (2d - c)\omega$$

and thus we need to solve the system of linear equations

$$\begin{aligned} a &= c + d \\ b &= 2d - c. \end{aligned}$$

Solving this system yields the real solution

$$c = \frac{2a-b}{3}, \quad d = a - \frac{2a-b}{3}.$$

Hence we are done once we prove that 3 divides $2a - b$. We have $N(\alpha) = a^2 - ab + b^2$ and hence

$$4N(\alpha) = (2a)^2 - 2 \cdot 2ab + b^2 + 3b^3 = (2a-b)^2 + 3b^2.$$

By assumption, 3 divides the left hand side. It follows that 3 divides $(2a-b)^2$. As 3 is prime, 3 also divides $2a - b$ as desired. ■

1.4 Exercises

Exercise 1.4.1:
Let $\alpha = 3 - 5\omega$ and $\beta = -7 + 2\omega$. Compute $\alpha + \beta, \alpha - \beta, \alpha\beta$, $N(\alpha)$ and $N(\beta)$.

Exercise 1.4.2:
Show that ω is a root of the polynomial $x^2 + x + 1$ and use this to verify the identity

$$(a + b\omega)(c + d\omega) = (ac - bd) + (ad + bc - bd)\omega.$$

Exercise 1.4.3:
Let $\alpha \in \mathbb{Z}[\omega]$ be a unit. Prove directly from the definition of a unit that the inverse of α is unique.

Exercise 1.4.4:
Prove Proposition 1.7.

Exercise 1.4.5:
Provide an alternative proof of Proposition 1.4 using Proposition 1.7.

Exercise 1.4.6:
Prove that the relation on $\mathbb{Z}[\omega]$ given by $\alpha \sim \beta$ if and only if α and β are associates is an equivalence relation. Describe the equivalence classes $[2 + 3\omega], [4\omega]$ and $[1-\omega]$.

Exercise 1.4.7:
Let $\alpha = 2 + 5\omega$. Determine whether α divides the following elements:

1)$17 + 14\omega$.

2)$4 + 7\omega$.

3)$9 + 5\omega$.

4)$1 - 7\omega$.

2 The Euclidean algorithm and Bezout's theorem

2.1 Euclidean division in $\mathbb{Z}[\omega]$

Let us briefly recall Euclidean division in $\mathbb{Z}$.

Proposition 2.1. ***Euclidean division in*** $\mathbb{Z}$ *Let a and b be integers with $b \neq 0$. There exists unique integers q and r satisfying $a = bq + r$ such that $0 \leq r < |b|$. We call q the* quotient *and r the* remainder*.*

Example 2.2. Let $a = 46$ and $b = 13$. 13 divides 46 3 times with a remainder of 7. Thus, $46 = 13 \cdot 3 + 7$. The above proposition says that there is no other choice if we want the remainder to be non-negative. However, there is nothing stopping us from instead writing $46 = 13 \cdot 4 - 6$, and we note that $|-6| < |7|$. In a sense, choosing -6 instead of 7 as the remainder is a more optimal choice. The price is the loss of uniqueness of the remainder.

The idea in the above example will be used to do Euclidean division in $\mathbb{Z}[\omega]$. We will use a modified Euclidean algorithm in the following. The algorithm is described in the following result.

Proposition 2.3 (**Modified Euclidean division in** $\mathbb{Z}$)**.** *Let a and b be integers with $b \neq 0$. There exists integers q and r satisfying $a = bq + r$ and such that $|r| \leq (1/2)|b|$.*

Proof. Partition the real number line into half-open intervals of the form $[bq, b(q+1))$ for $q \in \mathbb{Z}$. a is in exactly one of these intervals, say $[bq', b(q'+1))$. Now choose either q' or $q'+1$ according to which one of bq' or $b(q'+1)$ is closest to a. This provides us with a q such that $|a - bq| \leq (1/2)|b|$. Let $r = a - bq$ for this q. ■

We are now ready to study Euclidean division in $\mathbb{Z}[\omega]$. Let us first, however, do an example.

Example 2.4. We wish to do division with remainder with $\alpha = 13 - 4\omega$ and $\beta = -1 + 4\omega$. The quotient is

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{(13 - 4\omega)(-5 - 4\omega)}{21} = -\frac{81}{21} - \frac{48}{21}\omega.$$

$-81/21 \approx -3.857$ and $-48/21 \approx -2.286$. If we just carelessly choose the quotient $\gamma = -3 - 3\omega$, we get a remainder ρ of

$$\rho = \alpha - \beta\gamma = 13 - 4\omega - (-1 + 4\omega)(-3 - 3\omega) = -2 - 7\omega$$

which has norm $39 > 21 = N(\beta)$. However, if we choose $\gamma = -4 - 2\omega$ instead (the integers closest to the above fractions using the modified Euclidean algorithm), we obtain the remainder

$$\rho = \alpha - \beta\gamma = 13 - 4\omega - (-1 + 4\omega)(-4 - 2\omega) = 1 + 2\omega$$

which has norm 3. A much better choice.

The above example tells us how to do Euclidean division in $\mathbb{Z}[\omega]$.

Theorem 2.5 (**Euclidean division in $\mathbb{Z}[\omega]$**)**.** *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ with $\beta \neq 0$. There exist $\gamma, \rho \in \mathbb{Z}[\omega]$ with $\alpha = \beta\gamma + \rho$ such that $N(\rho) < N(\beta)$. γ is referred to as the* quotient *and ρ as the* remainder*.*

Proof. Write $\alpha\overline{\beta} = a + b\omega$. Then

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{a}{N(\beta)} + \frac{b}{N(\beta)}\omega.$$

Apply the modified Euclidean algorithm on the pairs $(a,\ N(\beta))$ and $(b,\ N(\beta))$. This will provide us with q_1, q_2, r_1, r_2 such that $a = N(\beta)q_1 + r_1$, $b = N(\beta)q_2 + r_2$ and $|r_1|, |r_2| \leq (1/2)N(\beta)$.

$$\frac{\alpha}{\beta} = \frac{N(\beta)q_1 + r_1 + (N(\beta)q_2 + r_1)\omega}{N(\beta)} = q_1 + q_2\omega + \frac{r_1 + r_2\omega}{N(\beta)}.$$

Define $\gamma = q_1 + q_2\omega$. The equation above becomes

$$\frac{\alpha}{\beta} = \gamma + \frac{r_1 + r_2\omega}{N(\beta)}$$

which can be rewritten as

$$\alpha - \beta\gamma = \frac{r_1 + r_2\omega}{\overline{\beta}}.$$

With $\rho = \alpha - \beta\gamma$, we claim that $N(\rho) < N(\beta)$. In the following, we use the fact that the norm N can also be applied on $a + b\omega$ for any $a, b \in \mathbb{R}$ with all properties preserved (except that it no longer needs to take on integer values). Consider the computation:

$$\begin{aligned}
N(\rho) = N\left(\frac{r_1 + r_2\omega}{\overline{\beta}}\right) &= N\left(\frac{r_1}{N(\beta)} + \frac{r_2}{N(\beta)}\omega\right) N(\beta) \\
&= \left(\frac{r_1^2}{N(\beta)^2} - \frac{r_1 r_2}{N(\beta)^2} + \frac{r_2^2}{N(\beta)^2}\right) N(\beta) \\
&\leq \left(\frac{(N(\beta)/2)^2}{N(\beta)^2} + \frac{|r_1||r_2|}{N(\beta)^2} + \frac{(N(\beta)/2)^2}{N(\beta)^2}\right) N(\beta) \\
&\leq \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) N(\beta) = \frac{3}{4}N(\beta) < N(\beta).
\end{aligned}$$

This bound completes the proof. ■

Remark 2.6. Note that we actually proved something slightly stronger, namely that the remainder ρ can be choosen such that $N(\rho) \leq (3/4)N(\beta)$.

Example 2.7. Let $\alpha = -11 + 4\omega$ and $\beta = 5 + 7\omega$. We have $N(\beta) = 39$ and thus

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{(-11 + 4\omega)(-2 - 7\omega)}{39} = \frac{50}{39} + \frac{97}{39}\omega.$$

$50/39 \approx 1.282$ which we round down to 1. $97/39 \approx 2.487$ which we round down to 2. Hence our choice for the quotient is $\gamma = 1 + 2\omega$. For the remainder, we get

$$\rho = \alpha - \beta\gamma = -2 + \omega.$$

$N(\rho) = 7 < 39 = N(\beta)$ as desired.

2.2 Greatest common divisors and the Euclidean algorithm

Greatest common divisors work very much in the same way in $\mathbb{Z}[\omega]$ as in the ordinary integers.

Definition 2.8. Let $\alpha, \beta \in \mathbb{Z}[\omega]$ with at least one of α and β not equal to zero. A greatest common divisor of α and β is an element of $\mathbb{Z}[\omega]$ which divides both α and β and has maximal norm. We will sometimes write $\gcd(\alpha, \beta)$ for a greatest common divisor of α and β.

Remark 2.9. If δ is a greatest common divisor of α and β, so are any of the associates of δ. Hence a greatest common divisor is never unique.

We now introduce the Euclidean algorithm for the Eisenstein integers. It works in exactly the same way as for the integers.

Theorem 2.10 (Euclidean algorithm for Eisenstein integers). *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be non-zero. Applying Euclidean division in the following fashion*

$$\begin{aligned} \alpha &= \beta\gamma_1 + \rho_1, \quad N(\rho_1) < N(\beta) \\ \beta &= \rho_1\gamma_2 + \rho_2, \quad N(\rho_2) < N(\rho_1) \\ \rho_1 &= \rho_2\gamma_3 + \rho_3, \quad N(\rho_3) < N(\rho_2) \\ &\vdots \end{aligned}$$

will after finitely many steps result in a division with a remainder of zero. The last non-zero remainder is a greatest common divisor of α and β.

Proof. To see that the algorithm terminates, note that all norms are non-negative and attain integer values. As the sequence of norms $(N(\rho_i))$ is strictly decreasing, the algorithm has to terminate after finitely many steps. Now consider the first equation $\alpha = \beta\gamma_1 + \rho_1$. By rewriting as $\rho = \alpha - \beta\gamma_1$, we see that a common divisor of α and β is also a common divisor of β and ρ_1. Repeating the argument, this element is also a common divisor of ρ_1 and ρ_2 and so far down until the final equation where we see that this element is also a divisor of the last non-zero remainder. It follows that a greatest common divisor is a factor of the last non-zero remainder. Traversing the algorithm in reverse also shows that the last non-zero remainder is a common divisor of α and β. To summarise, the last non-zero remainder has all other common divisors as a factor and in particular, it must have maximal norm among all common divisors. This concludes the proof. ∎

Corollary 2.11. *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be non-zero and let δ denote a greatest common divisor produced by the Euclidean algorithm. Any other greatest common divisor of α and β is an associate of δ.*

Proof. From the proof of correctness of the Euclidean algorithm, we see that any greatest common divisor must divide δ. Hence if δ' denotes another greatest common divisor, we have $\delta = \delta'\gamma$ for some $\gamma \in \mathbb{Z}[\omega]$. Using that δ' and δ both have maximal norm, we obtain

$$N(\delta') \geq N(\delta) = N(\delta')N(\gamma) \geq N(\delta').$$

This shows that we must have equality throughout and hence $N(\gamma) = 1$ implying that γ is a unit, completing the proof. ∎

Example 2.12. Let us compute the greatest common divisor of $\alpha = 34 - 21\omega$ and $\beta = 17 + 8\omega$. Applying Euclidean division iteratively gives

$$\begin{aligned}
34 - 21\omega &= (17 + 8\omega)(1 - 3\omega) + (-7 - 2\omega) \\
17 + 8\omega &= (-7 - 2\omega)(-3 - \omega) + (-2 - 3\omega) \\
-7 - 2\omega &= (-2 - 3\omega)(-2\omega) - 1 \\
-2 - 3\omega &= (-1)(2 + 3\omega)
\end{aligned}$$

and we conclude that -1 is a greatest common divisor.

The situation in the previous example is so important that it gets its own name.

Definition 2.13. If a greatest common divisor of α and β is a unit, α and β are called *coprime* or *relatively prime*.

Let us consider one more example with two elements that are not coprime.

Example 2.14. Let $\alpha = 24 + 57\omega$ and $\beta = -42 - 12\omega$. Applying the Euclidean algorithm gives

$$\begin{aligned}
24 + 57\omega &= (-42 - 12\omega)(-1 - 2\omega) + 6 - 15\omega \\
-42 - 12\omega &= (6 - 15\omega)(-2 - 2\omega)
\end{aligned}$$

and so $6 - 15\omega$ is a greatest common divisor.

Implementing the Euclidean algorithm is as simple as for the integers. We denote the algorithm by EUCLID(α, β) and state it below.

Algorithm 1: EUCLID(α, β)

```
Input: $\alpha, \beta \in \mathbb{Z}[\omega]$
Output: $\gcd(\alpha, \beta)$
if $\alpha \equiv 0 \pmod{\beta}$ then
    return $\beta$
return EUCLID($\beta, \alpha \bmod \beta$)
```

2.3 Bezout's theorem

Recall Bezout's theorem for ordinary integers. If $\gcd(a, b)$ denotes the greatest common divisor of two integers a and b, Bezout's theorem says that we may find integers x and y such that $ax + by = \gcd(a, b)$. This is done by working through the Euclidean algorithm backwards. Let us demonstrate this procedure with an example.

Example 2.15. Let $a = 258$ and $b = 78$. Applying the Euclidean algorithm yields

$$\begin{aligned}
258 &= 78 \cdot 3 + 24 \\
78 &= 24 \cdot 3 + 6 \\
24 &= 6 \cdot 4
\end{aligned}$$

so $\gcd(258, 78) = 6$. Using the second equation, we obtain

$$6 = 78 - 24 \cdot 3,$$

and using the first equation, we get

$$6 = 78 - (258 - 78 \cdot 3) \cdot 3 = -3 \cdot 258 + 10 \cdot 78.$$

So in this case, we may choose $x = -3$ and $y = 10$.

As it turns out, Bezout's theorem works in exactly the same way in $\mathbb{Z}[\omega]$.

Theorem 2.16 (Bezout's theorem). *Let δ denote a greatest common divisor of α and β in $\mathbb{Z}[\omega]$. There exist $x, y \in \mathbb{Z}[\omega]$ such that $\alpha x + \beta y = \delta$.*

Proof. Due to Corollary 2.11, we can assume that the greatest common divisor given is the one produced by the Euclidean algorithm by multiplying through with a unit if necessary. Consider all the equations from the Euclidean algorithm. Isolate the greatest common divisor (the last non-zero remainder) in the second-to-last equation and substitute iteratively backwards until we are left with a linear combination of α and β. ■

Corollary 2.17. *α and β are coprime if and only if there exist $x, y \in \mathbb{Z}[\omega]$ such that*

$$1 = \alpha x + \beta y.$$

Proof. Assume that α and β are coprime. Then the greatest common divisor is a unit u, and by Bezout's theorem, we may write $u = \alpha x' + \beta y'$ for some $x', y' \in \mathbb{Z}[\omega]$. Let $x = u^{-1}x'$ and $y = u^{-1}y'$, then $1 = \alpha x + \beta y$ as desired. Conversely, suppose that $1 = \alpha x + \beta y$ for some $x, y \in \mathbb{Z}[\omega]$. Then any common divisor of α and β divides 1 and thus a greatest common divisor is a unit. ■

Example 2.18. Let us again consider $\alpha = 34 - 21\omega$ and $\beta = 17 + 8\omega$. The computations from the Euclidean division from before were

$$\begin{aligned}
34 - 21\omega &= (17 + 8\omega)(1 - 3\omega) + (-7 - 2\omega)\\
17 + 8\omega &= (-7 - 2\omega)(-3 - \omega) + (-2 - 3\omega)\\
-7 - 2\omega &= (-2 - 3\omega)(-2\omega) - 1\\
-2 - 3\omega &= (-1)(2 + 3\omega).
\end{aligned}$$

We can now work backwards to obtain a solution (x, y) to $-1 = \alpha x + \beta y$. We have

$$\begin{aligned}
-1 &= -7 - 2\omega - (-2 - 3\omega)(-2\omega)\\
&= -7 - 2\omega - (17 + 8\omega - (-7 - 2\omega)(-3 - \omega))(-2\omega)\\
&= -(17 + 8\omega)(-2\omega) + (-7 - 2\omega)(1 + (-3 - \omega)(-2\omega))\\
&= -(17 + 8\omega)(-2\omega) + (34 - 21\omega - (17 + 8\omega)(1 - 3\omega))(1 + (-3 - \omega)(-2\omega))\\
&= (1 + (-3 - \omega)(-2\omega))(34 - 21\omega) + (17 + 8\omega)(2\omega - (1 - 3\omega)(1 + (-3 - \omega)(-2\omega)))\\
&= (-1 + 4\omega)\alpha + (-11 - 17\omega)\beta
\end{aligned}$$

so the solution is $x = -1 + 4\omega$ and $y = -11 - 17\omega$.

Example 2.19. Let us consider $\alpha = 3 + 4\omega$ and $\beta = \overline{\alpha} = -1 - 4\omega$. We use Euclidean division and obtain

$$\begin{aligned}
3 + 4\omega &= (-1 - 4\omega)(-1 + \omega) + (-2 - 3\omega)\\
-1 - 4\omega &= (-2 - 3\omega)(2 + \omega) + \omega\\
-2 - 3\omega &= \omega(-1 + 2\omega)
\end{aligned}$$

so a greatest common divisor of α and β is ω. In particular, α is coprime to its conjugate. We now solve the equation $\alpha x + \beta y = \omega$ as follows:

$$\begin{aligned}
\omega &= -1 - 4\omega - (-2 - 3\omega)(2 + \omega)\\
&= -1 - 4\omega - (3 + 4\omega - (-1 - 4\omega)(-1 + \omega))(2 + \omega)\\
&= (3 + 4\omega)(-2 - \omega) + (-1 - 4\omega)(-2)
\end{aligned}$$

so $x = -2 - \omega$ and $y = -2$ is a solution.

When we dive into modular arithmetic in the next section, it will be useful to have an algorithm to solve for x and y in the equation $\alpha x + \beta y = \delta$ where $\delta = \gcd(\alpha, \beta)$. For the integers this algorithm is typically called the extended Euclidean algorithm, and we will also refer to this procedure as the extended Euclidean algorithm in $\mathbb{Z}[\omega]$. As we did for the (ordinary) Euclidean algorithm, we will implement it as a recursive procedure. The algorithm, which we denote by EUCLIDEXT, is below.

Algorithm 2: EUCLIDEXT(α, β)

```
Input: $\alpha, \beta \in \mathbb{Z}[\omega]$
Output: $[\gcd(\alpha, \beta), x, y]$ such that $\alpha x + \beta y = \gcd(\alpha, \beta)$
if $\beta == 0$ then
    return $[\alpha, 1, 0]$
else
    temp = EUCLIDEXT($\beta, \alpha \bmod \beta$)
    return $[\text{temp}[1], \text{temp}[3], \text{temp}[2] - \alpha/\beta \cdot \text{temp}[3]]$
```

In the algorithm α/β denotes the quotient when we do Euclidean division with α and β. We end this section with some important results that will be useful when we get to unique factorization.

Proposition 2.20. *Let α and β in $\mathbb{Z}[\omega]$ be coprime and $\gamma \in \mathbb{Z}[\omega]$.*

(1) If $\alpha \mid \beta\gamma$ then $\alpha \mid \gamma$.

(2) If $\alpha \mid \gamma$ and $\beta \mid \gamma$ then $\alpha\beta \mid \gamma$.

Proof. Both proofs rely on Bezout's theorem in the form of Corollary 2.17.

(1) As α and β are coprime, we may choose $x, y \in \mathbb{Z}[\omega]$ such that

$$\alpha x + \beta y = 1.$$

Multiply this equation by γ, then

$$\alpha\gamma x + \beta\gamma y = \gamma.$$

As α divides both terms on the left hand side, α must divide γ as desired.

(2) Exercise for the reader.

■

2.4 Exercises

Exercise 2.4.1:
Let $\alpha = 1 - 2\omega$ and $\beta = -4$. Find a greatest common divisor δ and determine $x, y \in \mathbb{Z}[\omega]$ such that $\alpha x + \beta y = \delta$.

Exercise 2.4.2:
Let $\alpha = 3 + \omega$ and $\beta = 1 - \omega$. Find a greatest common divisor δ and determine $x, y \in \mathbb{Z}[\omega]$ such that $\alpha x + \beta y = \delta$.

Exercise 2.4.3:
Prove Proposition 2.20 (2).

Exercise 2.4.4:
Let $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ be non-zero. Prove that α and β are coprime to γ if and only if $\alpha\beta$ and γ are coprime.

3 Modular arithmetic

Modular arithmetic is defined for $\mathbb{Z}[\omega]$ exactly as for ordinary integers.

Definition 3.1. Let $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ with $\gamma \neq 0$. We say that α is congruent to β modulo γ if $\gamma \mid \alpha - \beta$. In that case we write $\alpha \equiv \beta \pmod{\gamma}$.

Just like for ordinary integers, $\equiv$ is an equivalence relation that behaves nicely with addition and multiplication. The proofs are also identical. We will return to this in section 6. We also note that if we apply Euclidean division on α and β and obtain $\alpha = \beta\gamma + \rho$, then $\alpha \equiv \rho \pmod{\gamma}$. We will often apply Euclidean division in order to get a representative of the equivalence class with smallest possible norm.

3.1 Modular exponentiation

For some applications, it is essential to be able to compute high (integer) powers of Eisenstein integers modulo some other Eisenstein integer. Let $\alpha, \gamma \in \mathbb{Z}[\omega]$ and $n \in \mathbb{N}$. A naive approach is to compute $\alpha \cdot \alpha \cdots \alpha$ a total of n times and then reduce modulo γ. This can be very costly computationally however. Luckily, there is a simple algorithm that does the trick extremely effectively. The algorithm is the same as in $\mathbb{Z}$ and can be described as follows: Write

$$n = b_{l-1}2^{l-1} + \cdots + b_1 \cdot 2 + b_0$$

for $b_i \in \{0, 1\}$. We let $(b_{l-1}, ..., b_1, b_0)$ denote the binary representation of n. We call l the bitlength of n. Note that we may write

$$\alpha^n = (\alpha^{b_{l-1}})^{2^{l-1}} \cdots (\alpha^{b_1})^2 \cdot \alpha^{b_0}.$$

Hence we can let i iterate from $l-1$ to 0 and if $b_i = 1$, we multiply by α and reduce modulo γ. Each step we also have to square the result we have so far. The algorithm, which we denote by MODEXP, is stated below.

Algorithm 3: MODEXP(α, γ, n)

```
Input: $\alpha, \gamma \in \mathbb{Z}[\omega], n \in \mathbb{N}$
Output: $\alpha^n \pmod{\gamma}$
$r \leftarrow 1$
let $(b_{l-1}, ..., b_1, b_0)$ be the binary representation of $n$
for $i = l - 1$ down to 0 do
    $r \leftarrow r^2 \pmod{\gamma}$
    if $b_i = 1$ then
        $r \leftarrow r \cdot \alpha \pmod{\gamma}$
return $r$
```

Example 3.2. Let us compute $(2 + 5\omega)^{10} \pmod{6 + 7\omega}$. The binary representation of $n = 10$ is $(b_3, b_2, b_1, b_0) = (1, 0, 1, 0)$. We let $r = 1$ and $i = 3$.

$i = 3$: $r \leftarrow 1^2 \equiv 1 \pmod{6 + 7\omega}$. $b_3 = 1$, so $r \leftarrow 1 \cdot (2 + 5\omega) \equiv -4 - 2\omega \pmod{6 + 7\omega}$.

$i = 2$: $r \leftarrow (-4 - 2\omega)^2 \equiv -2\omega \pmod{6 + 7\omega}$. $b_2 = 0$ so we stop.

$i = 1$: $r \leftarrow (-2\omega)^2 \equiv 2 + 3\omega \pmod{6 + 7\omega}$. $b_1 = 1$ so $r \leftarrow (2 + 3\omega) \cdot (2 + 5\omega) \equiv 3 + 3\omega \pmod{6 + 7\omega}$.

$i = 0$: $r \leftarrow (3 + 3\omega)^2 \equiv 1 + 3\omega \pmod{6 + 7\omega}$. $b_0 = 0$ so we are done.

Hence $(2 + 5\omega)^{10} \equiv 1 + 3\omega \pmod{6 + 7\omega}$.

3.2 Linear congruences and the Chinese Remainder Theorem

In the integers, it is a well known fact that the equation

$$ax \equiv b \pmod{n}$$

has a solution if and only if $\gcd(a, n) \mid b$. This result carries over directly to the Eisenstein integers. The proof is also the same.

Proposition 3.3. *For $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$, the equation*

$$\alpha\rho \equiv \beta \; (mod\ \gamma)$$

has a solution if and only if $\gcd(\alpha, \gamma) \mid \beta$*.*

Proof. Let δ denote a greatest common divisor of α and γ. Assume ρ is a solution to the equation. Then $\alpha\rho - \beta = \gamma\tau$ for some $\tau \in \mathbb{Z}[\omega]$. As δ divides $\alpha\rho$ and $\gamma\tau$, δ also divides β. Conversely, suppose δ divides β. From Bezout's theorem, we can write

$$\alpha x + \gamma y = \delta$$

for some $x, y \in \mathbb{Z}[\omega]$. In particular,

$$\frac{\alpha}{\delta}x + \frac{\gamma}{\delta}y = 1$$

and multiplying by β and rearranging yields

$$\alpha x\frac{\beta}{\delta} = \beta - \frac{\beta}{\delta}y\gamma$$

hence $x\beta/\delta$ is a solution to the equation. Note that this solution indeed is an element of $\mathbb{Z}[\omega]$ by assumption. ■

The proof of the above proposition is constructive. Indeed, if we have access to an extended Euclidean algorithm that provides a solution x, y to $\alpha x + \gamma y = \delta$ and $\delta \mid \beta$, a solution is $x\beta/\delta$. Denoting our algorithm to solve this problem by MODLINEARSOLVE, we can explicitly state the algorithm as follows.

Algorithm 4: MODLINEARSOLVE(α, β, γ)

```
Input: $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$
Output: $\rho \in \mathbb{Z}[\omega]$ such that $\alpha\rho \equiv \beta \pmod{\gamma}$ if such a $\rho$ exists, otherwise an
  error message
$S \leftarrow$ EUCLIDEXT($\alpha$, $\gamma$)
if $\beta$ mod $S[1] == 0$ then
    return $S[2] \cdot \beta/S[1] \pmod{\gamma}$
print("Error, gcd($\alpha, \gamma$) does not divide $\beta$")
```

Example 3.4. Let $\alpha = 5 + 3\omega$, $\beta = 3 - 4\omega$ and $\gamma = 3 + 7\omega$ and consider the equation

$$\alpha\rho \equiv \beta \pmod{\gamma}.$$

Using the Euclidean algorithm, we compute $\gcd(\alpha, \gamma) = 1$ and so there is a solution to the above equation. From the Extended Euclidean algorithm, we get

$$\alpha(3 + 4\omega) + \gamma(-3 - \omega) = 1$$

and so a solution ρ is given by

$$\rho = (3+4\omega)\frac{\beta}{1} = 25+16\omega.$$

Reducing modulo γ, we obtain the nicer solution

$$\rho = 4+4\omega.$$

The last thing we consider in this section is the Chinese Remainder Theorem. We will use it later in section 6.

Theorem 3.5 (Chinese Remainder Theorem). *Let $\alpha_1, ..., \alpha_n \in \mathbb{Z}[\omega]$ and assume $\gamma_1, ..., \gamma_n \in \mathbb{Z}[\omega]$ are pairwise coprime. Then the system of n equations*

$$\alpha_i \equiv \rho \pmod{\gamma_i}, \quad i = 1, ..., n$$

has a solution ρ which is unique modulo $\gamma_1 \cdots \gamma_n$.

Proof. We prove the theorem via induction. The claim is trivial for $n = 1$ as we may choose $\rho = \alpha_1$. Now assume $n = 2$. Consider the equation

$$\alpha_1 + \gamma_1\rho' \equiv \alpha_2 \pmod{\gamma_2}$$

which we can rewrite as

$$\gamma_1\rho' \equiv \alpha_2 - \alpha_1 \pmod{\gamma_2}.$$

$\gcd(\gamma_1, \gamma_2) = 1$ so there is a solution ρ' to this equation by Proposition 3.3. Then it is easy to see that $\rho = \alpha_1 + \gamma_1\rho'$ is a solution to both equations. Now assume $n > 2$ and that the claim is proved for $n-1$. Let ρ' denote a solution to

$$\alpha_i \equiv \rho' \pmod{\gamma_i}, \quad i = 1, ..., n-1.$$

Consider the equation

$$\rho' + \rho''\gamma_1 \cdots \gamma_{n-1} \equiv \alpha_n \pmod{\gamma_n}.$$

Using that $\gamma_1 \cdots \gamma_{n-1}$ and γ_n are coprime, we have a solution ρ'' by Proposition 3.3 just like in the case $n = 2$. Letting

$$\rho = \rho' + \rho''\gamma_1 \cdots \gamma_{n-1},$$

we have found a solution ρ to the system with n equations. To prove uniqueness, let ρ_1 and ρ_2 denote two solutions to the system of equations. Then $\rho_1 - \rho_2 \equiv 0 \pmod{\gamma_i}$ for $i = 1, ..., n$. Using that the γ_i are coprime, $\gamma_1 \cdots \gamma_n \mid \rho_1 - \rho_2$ which proves uniqueness modulo $\gamma_1 \cdots \gamma_n$. ■

Even though the theorem was proved using induction, the proof is constructive. The reader is very welcome to rewrite the proof as an algorithm.

4 Primes in $\mathbb{Z}[\omega]$

4.1 Primes and irreducibility

Primes in $\mathbb{Z}[\omega]$ are defined in the same way as in $\mathbb{Z}$.

Definition 4.1. A nonunit $\alpha \in \mathbb{Z}[\omega]$ is a *prime* if the only factors of α are units and associates of α. If α is not prime, we call α *composite.*

In other words, α is prime if and only if whenever we write $\alpha = \beta\gamma$, then either β or γ is a unit.

Example 4.2. 7 is a prime in $\mathbb{Z}$ but not in $\mathbb{Z}[\omega]$. Indeed, $7 = (3 + 2\omega)(1 - 2\omega)$ and $N(3 + 2\omega) = N(1 - 2\omega) = 7$ so neither $3 + 2\omega$ or $1 - 2\omega$ are units.

In this section, we will use the norm extensively. The following lemma characterizes those divisors of an Eisenstein integer α which have norm $N(\alpha)$.

Lemma 4.3. *Let $\alpha \in \mathbb{Z}[\omega]$ be non-zero. Let β be a divisor of α with $N(\beta) = N(\alpha)$. Then β is an associate of α.*

Proof. Write $\alpha = \beta\gamma$ for some $\gamma \in \mathbb{Z}[\omega]$. Taking norms yields $N(\alpha) = N(\beta)N(\gamma) = N(\alpha)N(\gamma)$. As $N(\alpha) \neq 0$, we have $N(\gamma) = 1$ so γ is a unit and β is an associate of α. ■

Note that the lemma only concerns divisors of α. It does not say that any two Eisenstein integers with the same norm are associates. For example, $\alpha = 2 + 3\omega$ and $\beta = -1 - 3\omega$ are not associates but they both have norm 7. The following theorem is a simple but powerful tool to find Eisenstein primes.

Theorem 4.4. *Let $\alpha \in \mathbb{Z}[\omega]$. If $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is a prime in $\mathbb{Z}[\omega]$.*

Proof. Consider a factorization $\alpha = \beta\gamma$. We then have $N(\alpha) = N(\beta)N(\gamma)$. If $N(\alpha)$ is prime, then either $N(\beta) = 1$ or $N(\gamma) = 1$. In any case, either β or γ is a unit and hence the factorization is trivial. This proves that α is prime. ■

Example 4.5. Consider $2 + 3\omega$. Since $N(2 + 3\omega) = 7$, $2 + 3\omega$ is an Eisenstein prime.

Example 4.6. The statement of Theorem 4.4 is not an equivalence. For example, $N(2) = 4$ which is composite, but 2 turns out to be an Eisenstein prime.

We have one goal for the rest of this section, namely to classify the primes in $\mathbb{Z}[\omega]$. This can be done in an elegant fashion by introducing *ideals*. This is the content of the next subsection.

4.2 Ideals in $\mathbb{Z}$ and $\mathbb{Z}[\omega]$

An ideal is a particularly nice subset of $\mathbb{Z}[\omega]$. They are generally defined for algebraic objects known as *rings* of which $\mathbb{Z}$ and $\mathbb{Z}[\omega]$ are examples. We will not dive into the general theory but instead refer to chapter 7 to 9 of [2].

Definition 4.7. An ideal I of $\mathbb{Z}[\omega]$ is a non-zero subset of $\mathbb{Z}[\omega]$ that is closed under addition and under multiplication by **all** elements of $\mathbb{Z}[\omega]$. That is, an ideal satisfies

(1) For each $\alpha, \beta \in I$, we have $\alpha + \beta \in I$.

(2) For each $\alpha \in I$ and $\beta \in \mathbb{Z}[\omega]$, we have $\alpha\beta \in I$.

An ideal is called *proper* if it is strictly contained in $\mathbb{Z}[\omega]$ i.e. if $I \neq \mathbb{Z}[\omega]$. An ideal in $\mathbb{Z}$ is defined in exactly the same way (just replace $\mathbb{Z}[\omega]$ by $\mathbb{Z}$ above).

Lemma 4.8. *Let I and J be ideals.*

(1) $I + J = \{\alpha + \beta \mid \alpha \in I, \beta \in J\}$ is an ideal.

(2) $IJ = \{\alpha\beta \mid \alpha \in I, \beta \in J\}$ is an ideal.

(3) $I \cap J$ is an ideal.

(4) $IJ \subseteq I \cap J \subseteq I + J$.

Proof. (1) - (3) are immediate from the definition of an ideal. (4) is an exercise for the reader. ■

A particularly nice type of ideal is generated by a single element.

Definition 4.9. For $\alpha \in \mathbb{Z}[\omega]$, we define the ideal generated by α to be

$$(\alpha) = \{\beta\alpha \mid \beta \in \mathbb{Z}[\omega]\}.$$

Similarly, for $a \in \mathbb{Z}$, define the ideal generated by a to be

$$(a) = \{ba \mid b \in \mathbb{Z}\}.$$

An ideal generated by a single element is called a *principal ideal.*

Clearly, (α) defines an ideal. It turns out that this is the only type of ideal in $\mathbb{Z}[\omega]$ and it is a direct consequence of the existence of the Euclidean algorithm.

Lemma 4.10. *The following hold:*

(1) The only ideals in $\mathbb{Z}[\omega]$ *are ideals of the form* (α) *for some* $\alpha \in \mathbb{Z}[\omega]$.

(2) The only ideals in $\mathbb{Z}$ *are ideals of the form* (a) *for some* $a \in \mathbb{Z}$.

Proof. We prove (1). The proof of (2) is identical. The zero ideal is clearly of the desired form, so assume we have a non-zero ideal I in $\mathbb{Z}[\omega]$. Consider the set $\mathcal{N} = \{N(\alpha) \mid \alpha \in I \setminus \{0\}\}$. $\mathcal{N} \subseteq \mathbb{N}$ and by the well-ordering of $\mathbb{N}$ there exists a minimal element m in $\mathcal{N}$. Choose an $\alpha \in I$ such that $m = N(\alpha)$. Trivially, $(\alpha) \subseteq I$. We claim that the other inclusion holds. Let $\beta \in I$ be arbitrary. Apply Euclidean division to obtain $\beta = \alpha\gamma + \rho$ with $N(\rho) < N(\alpha)$. As $\alpha \in I$, $\alpha\gamma \in I$ also since I is an ideal. $\beta \in I$ so $\rho = \beta - \alpha\gamma \in I$. α has minimal norm among the non-zero elements of I, so $N(\rho) < N(\alpha)$ implies that $N(\rho) = 0$ and thus $\rho = 0$. Hence $\beta = \alpha\gamma \in (\alpha)$ and we have proved $I \subseteq (\alpha)$. ■

Remark 4.11. In ring theory, a ring in which every ideal is principal is called a *principal ideal domain.*

We will need the important notion of a prime ideal.

Definition 4.12. A proper ideal I in $\mathbb{Z}[\omega]$ (or in $\mathbb{Z}$) is called a *prime ideal* if whenever $\alpha\beta \in I$ then $\alpha \in I$ or $\beta \in I$.

It turns out that an ideal (α) is prime if and only if α is prime (see the exercises). We will return to ideals when we study the quotient $\mathbb{Z}[\omega]/(\alpha)$ in a later section.

4.3 The classification of primes in $\mathbb{Z}[\omega]$

We can now return to the main task of this section, namely classifying the primes in $\mathbb{Z}[\omega]$. The following lemma tells us that the primes of $\mathbb{Z}[\omega]$ are closely linked to those in $\mathbb{Z}$.

Lemma 4.13. *Let* $\pi \in \mathbb{Z}[\omega]$ *be an Eisenstein prime. Then* π *divides some integer prime* p.

Proof. According to the exercises, $(\pi) \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$. Hence $(\pi) \cap \mathbb{Z} = (a)$ for some $a \in \mathbb{Z}$. If $bc \in (\pi) \cap \mathbb{Z}$ for $b, c \in \mathbb{Z}$, $bc = \pi \cdot \beta$ for some $\beta \in \mathbb{Z}[\omega]$. In particular, π must divide at least one of b or c. It follows that $(\pi) \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Hence $(\pi) \cap \mathbb{Z} = (p)$ for some prime integer p. In particular, $p = \pi \cdot \alpha$ for some $\alpha \in \mathbb{Z}[\omega]$ and the claim follows. ■

Corollary 4.14. *For a prime $\pi \in \mathbb{Z}[\omega]$, either $\pi\overline{\pi} = p$ for some prime $p \in \mathbb{Z}[\omega]$ or π is associated to a prime in $\mathbb{Z}$.*

Proof. We know from the previous lemma that π divides some prime p in $\mathbb{Z}$. Write $p = \pi \cdot \alpha$ for some $\alpha \in \mathbb{Z}[\omega]$. Taking norms, we get $p^2 = N(\pi)N(\alpha)$. This leaves the two possibilities $N(\pi) = p$ or $N(\pi) = p^2$. If $N(\pi) = p$, we have $\pi\overline{\pi} = p$. If $N(\pi) = p^2$, $N(\alpha) = 1$ and so π is associated to p. ■

We now know two essential facts. If a prime p in $\mathbb{Z}$ is not a prime in $\mathbb{Z}[\omega]$ it can only happen because p factors as exactly $p = \pi\overline{\pi}$ for an Eisenstein prime π. Therefore, we need to study the equation $a^2 - ab + b^2 = p$. If integer solutions for a and b exist, then $\pi = a + b\omega$ satisfies $\pi\overline{\pi} = p$. If solutions do not exist, p must remain prime. We are on the verge of solving this problem once and for all, but in order to do so, we need a small technical lemma.

Lemma 4.15. *Let $p \equiv 1$ (mod 3) be a prime. There exists a k satisfying $0 \leq k < p$ such that p divides $k^2 + 3$.*

Proof. It is known from elementary number theory that the group of units $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$. We refer to chapter 4 in [3] for details. Let g be a generator of this group. Then the element $c = g^{(p-1)/3}$ is well-defined by our assumption on p and has order 3. Consider the element $(2c + 1)^2$. Multiplying $(2c + 1)^2 + 3$ by $c - 1$ yields

$$\begin{aligned}(c-1)((2c+1)^2+3) &= (c-1)(4c^2+1+4c+3) = 4(c-1)(c^2+c+1)\\ &= 4(c^3-1) \equiv 0 \pmod{p}.\end{aligned}$$

Hence either $c - 1 \equiv 0 \pmod{p}$ or $(2c + 1)^2 + 3 \equiv 0 \pmod{p}$. Since c has order 3, the first case is impossible and it follows that $(2c + 1)^2 \equiv -3 \pmod{p}$. Hence we have constructed a solution k to $k^2 \equiv -3 \pmod{p}$. By reducing modulo p, we can also assume that $0 \leq k < p$. This concludes the proof. ■

The first part of the proof of the previous lemma can be carried out using quadratic reciprocity. The reader is encouraged to carry out this step, should the reader be familiar with said theorem.

Lemma 4.16. *An associate of an integral prime p is an Eisenstein prime if and only if $p \equiv 2$ (mod 3).*

Proof. We start by noting that associates of $p = 3$ are not prime in $\mathbb{Z}[\omega]$ since we have the non-trivial factorization $3 = (1 - \omega)(2 + \omega)$. We thus only need to consider the case $p > 3$.

Assume $p \equiv 1 \pmod{3}$. Assume p is a prime in $\mathbb{Z}[\omega]$. By the previous corollary, $mp = k^2 + 3$ for some m and $0 \leq k < p$. Defining $\beta = 1 + k + 2\omega$, a quick computation shows that $k^2 + 3 = \beta\overline{\beta}$. Then p must divide either β or $\overline{\beta}$. Then $p^2 \mid N(\beta) = N(\overline{\beta})$ and it follows that

$$m^2p^2 = N(\beta)^2 \geq p^4$$

and in particular $m \geq p$. However, we have that

$$mp = k^2 + 3 \leq (p-1)^2 + 3 = p^2 - 2p + 4 < p(p-1)$$

since $p \equiv 1 \pmod 3$ implies that $p > 4$. Dividing by p, we obtain $m < p - 1$, so $m \geq p$ is a contradiction. We conclude that p cannot be a prime in $\mathbb{Z}[\omega]$ as claimed.

Conversely, suppose p is not a prime. By the previous corollary, p must factor as $p = \pi\overline{\pi}$. Write $\pi = a + b\omega$. Then we have $p = a^2 - ab + b^2$. Hence $4p = (2a - b)^2 + 3b^2$. Reducing modulo 3, we get $p \equiv (2a - b)^2$ and since a square is always 0 or 1 modulo 3, we have $p \equiv 1 \pmod 3$ as desired. ■

We now have the results needed to state the main theorem of this section.

Theorem 4.17 (Classification of primes in $\mathbb{Z}[\omega]$). *Up to associates, the primes in $\mathbb{Z}[\omega]$ are:*

(1) $1 - \omega$.

(2) Integral primes $p \equiv 2$ *(mod 3).*

(3) π *with* $N(\pi) = p$ *a prime with* $p \equiv 1$ *(mod 3).*

Proof. Combine the results of this section in a suitable manner. ■

Example 4.18. $-2 - 2\omega$ is an Eisenstein prime since it is associated to the prime 2.

4.4 Exercises

Exercise 4.4.1:
Verify that $3 + 7\omega$, $1 + 4\omega$ and $1 - \omega$ are Eisenstein primes.

Exercise 4.4.2:
Prove (4) of Lemma 4.8.

Exercise 4.4.3:
Let I be an ideal in $\mathbb{Z}[\omega]$. Show that $I \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Exercise 4.4.4:
Show that for an ideal I in $\mathbb{Z}[\omega]$, $I = \mathbb{Z}[\omega]$ if and only if I contains a unit.

Exercise 4.4.5:
Let $\alpha, \beta \in \mathbb{Z}[\omega]$. Prove that $(\alpha) + (\beta) = (\delta)$ with δ a greatest common divisor of α and β.

Exercise 4.4.6:
Prove that (α) is a prime ideal if and only if α is prime.

Exercise 4.4.7:
Show that $(\alpha) = (\beta)$ if and only if α and β are associates.

Exercise 4.4.8:
A proper ideal M is called a *maximal ideal* if it is maximal with respect to inclusion amongst all proper ideals i.e. if I is another proper ideal with $M \subseteq I$, then $M = I$. Prove that in $\mathbb{Z}[\omega]$ or $\mathbb{Z}$, a maximal ideal is prime.

This also holds for general rings. The converse, that a prime ideal is maximal, does not hold in general. It does hold for $\mathbb{Z}$ and $\mathbb{Z}[\omega]$, however (except for the zero ideal).

Exercise 4.4.9:
Use quadratic reciprocity to show that $k^2 \equiv -3 \pmod{p}$ has a solution for $p \equiv 1 \pmod{3}$.

Exercise 4.4.10:
Determine whether the following are Eisenstein primes:
1)$3 - 7\omega$.
2)$3 + 5\omega$.
3)$1 - 4\omega$.
4)$-3 + 5\omega$.
5)$8 - 2\omega$.
6)7ω.
7)$-5 - 5\omega$.
8)$1 + 36\omega$.

5 Unique factorization

5.1 The fundamental theorem of arithmetic for $\mathbb{Z}[\omega]$

The fundamental theorem of arithmetic in $\mathbb{Z}$ says that any integer not equal to 1, -1 or 0 has an essentially unique factorization into primes. It is important to understand what is meant by ”essentially unique”. A usual formulation is that an integer can be written as a unique product of either 1 or -1 and a list of *positive* primes up to permutation. For example,

$$18 = 2 \cdot 3^2, \quad -30 = -1 \cdot 2 \cdot 3 \cdot 5.$$

Up to permutation means that we don’t distinguish between the order of the prime factors. As an example, the three factorizations

$$18 = 2 \cdot 3^2, \quad 18 = 3 \cdot 2 \cdot 3, \quad 18 = 3^2 \cdot 2$$

are considered to be the same. But this does not fully capture the uniqueness we will work with in this paper. There is nothing stopping us from writing

$$18 = 2 \cdot (-3)^2 \quad \text{or} \quad 18 = (-1)(-2) \cdot 3^2$$

for example. However, we still don’t consider these factorizations to be different from the ones above since all the primes are still the same up to permutation and up to associates. In other words, every prime in one factorization is associated to some prime in the other factorization and there are the same number of primes involved. This is the uniqueness we will be working with. The difference is that instead of two units, we have six units in $\mathbb{Z}[\omega]$. To prove the fundamental theorem of arithmetic for $\mathbb{Z}[\omega]$, we will break it down into a sequence of lemmata.

Lemma 5.1. *Every $\alpha \in \mathbb{Z}[\omega]$ with $N(\alpha) > 1$ is a product of primes.*

Proof. We use induction on the norm. No elements of norm two exist, so the base case is $N(\alpha) = 3$. But then α is a prime by Theorem 4.4. Now consider some $n > 3$. If there are no Eisenstein integers of norm n we are done, so assume that there exists at least one Eisenstein integer α with $N(\alpha) = n$. If α is prime, we are done, so assume

α is composite and let $\alpha = \beta\gamma$ be a non-trivial factorization. As $N(\beta), N(\gamma) < N(\alpha)$, the induction hypothesis implies that β and γ are products of primes. But then α is a product of primes and the induction step is complete. ■

Now we know that any Eisenstein integer has a prime factorization. But still two problems remain. The first is that we need to show uniqueness which we get to now. The other problem is the question of actually computing the factorization. We will get to that in the following subsection.

Lemma 5.2 (**Euclid's lemma**). *If π is an Eisenstein prime and $\pi \mid \alpha\beta$ then either $\pi \mid \alpha$ or $\pi \mid \beta$. More generally, if π divides $\alpha_1 \cdots \alpha_k$, then π divides at least one α_i.*

Proof. If π divides α we are done so assume not. As π is prime, this implies that π and α are coprime. By Bezout's theorem, there exist $x, y \in \mathbb{Z}[\omega]$ such that $\alpha x + \pi y = 1$. Multiply by β and we have $\alpha\beta x + \pi\beta y = \beta$. As π divides the left hand side, π divides β and we are done. The rest of the argument is left to the reader. ■

Theorem 5.3 (**The fundamental theorem of arithmetic**). *Any Eisenstein integer α with $N(\alpha) > 1$ has a unique factorization into primes in the following sense: There exists a list of primes $\pi_1, ..., \pi_k$ such that $\alpha = \pi_1 \cdots \pi_k$ and if $\alpha = \pi_1' \cdots \pi_m'$ is a different factorization then $k = m$ and each π_i is associated to some π_j'.*

Proof. We use induction on the norm to prove the theorem. The base case is again $N(\alpha) = 3$ and we know that α is a prime so the theorem holds. Now assume $N(\alpha) > 3$ and that every Eisenstein integer of norm strictly less than $N(\alpha)$ has a unique prime factorization as given in the theorem. We can again assume that there exist Eisenstein integers of norm $N(\alpha)$ as otherwise there is nothing to prove. By the previous lemma, there exists some prime factorization $\alpha = \pi_1 \cdots \pi_k$. Let $\alpha = \pi_1' \cdots \pi_m'$ be another factorization.

π_1 divides $\pi_1' \cdots \pi_m'$ so using Lemma 5.2, π divides at least one of $\pi_1', ..., \pi_m'$. By relabeling if necessary, we can assume that π_1 divides π_1'. This is only possible if these primes are associates i.e. $\pi_1 = u\pi_1'$ for some unit u. We hence have

$$\pi_1 \cdots \pi_k = u\pi_1\pi_2' \cdots \pi_m'$$

implying

$$\pi_2 \cdots \pi_k = u\pi_2' \cdots \pi_m'.$$

$\beta = \pi_2 \cdots \pi_k$ has norm strictly less than $N(\alpha)$, so the induction hypothesis implies that β has a unique prime factorization as stated in the theorem. This implies that $k - 1 = m - 1$ and so $k = m$. Furthermore, each of the primes on the left hand side is associated to one of the primes on the right hand side. This concludes the induction step and hence the proof. ■

We have now proved existence and uniqueness of prime factorizations in $\mathbb{Z}[\omega]$. However, the proofs have been unconstructive. In the following subsection we will provide an explicit algorithm for computing prime factorizations.

5.2 A factorization algorithm

We are already familiar with some simple prime factorization algorithms in $\mathbb{Z}$. In this paper we will sweep factorization methods in $\mathbb{Z}$ under the rug and the reader is free to use any method that they please. The following algorithm relies on the classification of primes given in Theorem 4.17. The strategy for computing the prime factorization of α is as follows:

(1) Compute $N(\alpha)$ and factor $N(\alpha) = p_1 \cdots p_k$ into a product of primes in $\mathbb{Z}$. Let $P = (p_1, ..., p_k)$ be a tuple denoting the prime factors of $N(\alpha)$, and let $F = ()$ denote the tuple of factors of α.

(2) For each p_i, do the following:

- If $p_i = 3$, remove p_i from P and add $1 - \omega$ to F.
- If $p_i \equiv 2 \pmod 3$, remove **2 copies** of p_i from P. Add p_i to F.
- If $p_i \equiv 1 \pmod 3$, remove p_i from P and determine an integer k such that $k^2 \equiv -3 \pmod{p_i}$. Let $\delta = \gcd(1 + k + 2\omega, p_i)$ denote a greatest common divisor of $1 + k + 2\omega$ and p_i. If this greatest common divisor divides α, add it to F. If not, add $\overline{\delta}$ instead.

(3) $F = (\pi_1, ..., \pi_k)$ is now a list of prime factors of α. To obtain the final factorization, compute the product of the elements in F and divide α by this product. This yields a unit u such that $\alpha = u\pi_1 \cdots \pi_k$.

We now explain the steps in the algorithm. The first step is self-explanatory. Concerning step (2), we know that $3 = (1 + \omega)(1 - \omega)^2$ and that $N(1 - \omega) = 3$. Hence $1 - \omega$ is a factor of α if 3 shows up in the factorization of the norm. From the proof of a previous result, if a prime $p \equiv 2 \pmod 3$ is a factor of the norm, it can only come from a prime associated to p in $\mathbb{Z}[\omega]$. This prime has norm p^2 and thus two factors should be removed from the norm. If $p \equiv 1 \pmod 3$ shows up, we know that $p = \pi\overline{\pi}$ for some Eisenstein prime π. We also know that $mp = k^2 + 1$ for some $0 \leq k < p$ and $1 \leq m < p - 1$. Let $\beta = 1 + k + 2\omega$, then $mp = \beta\overline{\beta}$. In particular, $\pi \mid \beta$ or $\pi \mid \overline{\beta}$. As $N(p) = p^2 > mp = N(\beta)$, p cannot divide β. It follows that if $\pi \mid \beta$, then $\gcd(p, \beta) = \pi$ (up to associates). If $\pi \mid \overline{\beta}$, then $\pi = \gcd(p, \overline{\beta})$ and thus $\gcd(p, \beta) = \overline{\pi}$ (see the exercises). We do not know which of π and $\overline{\pi}$ is the correct factor, so we simply check by dividing.

The algorithm can be written in a formal manner as follows:

Algorithm 5: Prime factorization in $\mathbb{Z}[\omega]$

```
Input: $\alpha \in \mathbb{Z}[\omega]$
Output: A list of a single unit $u$ and primes $\pi_1, ..., \pi_m$ such that $\alpha = u\pi_1 \cdots \pi_m$.
Compute the prime factors $p_1, ..., p_k$ of $N(\alpha)$
$F \leftarrow []$
$i \leftarrow 1$
while $i \leq k$ do
    if $p_i = 3$ then
        Push $1 - \omega$ to $F$
        $\alpha \leftarrow \alpha/(1 - \omega)$
    if $p_i \equiv 2 \pmod 3$ then
        Push $p_i$ to $F$
        $\alpha \leftarrow \alpha/p_i$
        $i \leftarrow i + 1$
    if $p_i \equiv 1 \pmod 3$ then
        Determine $k$ such that $k^2 \equiv -3 \pmod{p_i}$
        $\pi \leftarrow \gcd(p_i, 1 + k + 2\omega)$
        if $\pi \nmid \alpha$ then
            $\pi \leftarrow \overline{\pi}$
        Push $\pi$ to $F$
        $\alpha \leftarrow \alpha/\pi$
    $i \leftarrow i + 1$
Push $\alpha$ to $F$
return $F$
```

Example 5.4. Let us factor $\alpha = 10 + 2\omega$. The norm is

$$N(\alpha) = 10^2 - 10 \cdot 2 + 2^2 = 84 = 2^2 \cdot 3 \cdot 7.$$

2 is a factor of the norm, so 2 is a factor of α and we have 3 and 7 left to consider. We see that $1-\omega$ is a factor of α and we only have to consider 7. We need to find a k such that $k^2 + 3$ is divisible by 7. $k = 2$ is an obvious choice. In fact, $1 + k + 2\omega = 3 + 2\omega$ has norm 7. Hence we can skip the part with the greatest common divisor. We check whether $3 + 2\omega$ divides α:

$$\frac{10 + 2\omega}{3 + 2\omega} = \frac{(10 + 2\omega)(1 - 2\omega)}{7} = \frac{14 - 14\omega}{7} = 2 - 2\omega$$

which is in $\mathbb{Z}[\omega]$. We conclude that the prime factors of $10+2\omega$ are $2, 1-\omega$ and $3+2\omega$. The product of these is $10 + 2\omega$, so the factorization is $10 + 2\omega = 2(1 - \omega)(3 + 2\omega)$.

Example 5.5. Let us factor $\alpha = 5 + 16\omega$. We compute

$$N(\alpha) = 201 = 3 \cdot 67.$$

Hence $1 - \omega$ is a factor. Also, $8^2 + 3 = 67$, so we have either $\pi = 1 + 8 + 2\omega = 9 + 2\omega$ or $\overline{\pi}$ as a factor. It is checked that π divides α and thus the prime factors are $1 - \omega$ and $9 + 2\omega$. The product of these is $11 - 5\omega$. Dividing α by $11 - 5\omega$ gives ω. Hence $\alpha = \omega(1 - \omega)(9 + 2\omega)$ is the factorization of α.

5.3 Factorization and greatest common divisors

In $\mathbb{Z}$ there is an alternative way of computing greatest common divisors based on the prime factorization of the two numbers involved. As an example, consider 126 and 78. We factor

$$126 = 2 \cdot 3^2 \cdot 7, \quad 78 = 2 \cdot 3 \cdot 13.$$

The trick is to take the lower power of each prime which shows up in either of the two factorizations. In this case, these primes are 2, 3, 7 and 13. Rewriting a bit, we have

$$126 = 2^1 \cdot 3^2 \cdot 7^1 \cdot 13^0, \quad 78 = 2^1 \cdot 3^1 \cdot 7^0 \cdot 13^1.$$

Taking the smaller power of each prime, we arrive at the greatest common divisor $2^1 \cdot 3^1 \cdot 7^0 \cdot 13^0 = 6$. The same formula works for Eisenstein integers.

Proposition 5.6. *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ have norms $N(\alpha), N(\beta) > 1$. Let $\pi_1, ..., \pi_k$ denote the primes involved in the prime factorizations of α and β and write*

$$\alpha = \pi_1^{e_1} \cdots \pi_k^{e_k}, \quad \beta = \pi_1^{f_1} \cdots \pi_k^{f_k}.$$

Then a greatest common divisor of α and β is given by

$$\pi_1^{\min(e_1, f_1)} \cdots \pi_k^{\min(e_k, f_k)}.$$

Proof. Let δ be a common divisor. Any prime in the factorization of δ must be among $\pi_1, ..., \pi_k$ as otherwise δ could not be a divisor in the first place. Hence δ is of the form

$$\delta = \pi_1^{m_1} \cdots \pi_k^{m_k}.$$

Consider a prime factor of δ, say π_i. Then π_i also divides both α and β at least m_i times due to uniqueness of prime factorizations. Hence $m_i \leq e_i, f_i$ and thus $m_i \leq \min(e_i, f_i)$. It follows that for each prime factor π_i of δ, $\pi_i^{m_i}$ divides $\pi_1^{\min(e_1,f_1)} \cdots \pi_k^{\min(e_k,f_k)}$. Using Proposition 2.20 inductively, it follows that δ divides $\pi_1^{\min(e_1,f_1)} \cdots \pi_k^{\min(e_k,f_k)}$. Hence the latter has maximal norm among all common divisors and is thus a greatest common divisor. ■

Example 5.7. Consider $\alpha = 6 - 8\omega$ and $\beta = -4 + 2\omega$. Factoring gives

$$\alpha = -1 \cdot 2(-3 + 4\omega), \quad \beta = \omega \cdot 2(3 + 2\omega)$$

and it is readily checked that 2 is the only common divisor up to associates in the factorizations. Hence 2 is a greatest common divisor of α and β.

The above proposition is not recommended if one is interested in computing greatest common divisors. First of all, computing prime factorizations is difficult, especially by hand if primes congruent to 1 modulo 3 show up. Second, it is not always easy to see whether two prime factors are associates. If two associated (but not identical) primes show up, one has to rewrite one as a unit multiple of the other in order to apply the proposition. This is not a concern when applying the Euclidean algorithm. The result is not useful for computations but it is useful since it provides a nice relation between greatest common divisors and least common multiples, the latter being the subject of the next subsection.

5.4 Least common multiples

For two integers a and b, the least common multiple is the smallest integer m such that both a and b divide m. The corresponding definition in $\mathbb{Z}[\omega]$ is below.

Definition 5.8. Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be non-zero. A *least common multiple* of α and β is an Eisenstein integer γ of minimal norm such that $\alpha, \beta \mid \gamma$. We will at times denote a least common multiple by $\mathrm{lcm}(\alpha, \beta)$.

Just like greatest common divisors are not unique, least common multiples are not unique. Indeed, one can multiply a least common multiple by a unit and still have a least common multiple.

Proposition 5.9. *If α and β are non-zero and coprime, a least common multiple is $\alpha\beta$.*

Proof. Let $\gamma \in \mathbb{Z}[\omega]$ such that $\alpha, \beta \mid \gamma$. By Proposition 2.20 (2), $\alpha\beta \mid \gamma$. Hence $N(\alpha\beta) \leq N(\gamma)$ proving that $\alpha\beta$ is a common multiple of α and β with minimal norm. ■

Just like with greatest common divisors, we can compute least common multiples using the prime factorizations of the integers involved.

Proposition 5.10. *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ have norms $N(\alpha), N(\beta) > 1$. Let $\pi_1, ..., \pi_k$ denote the primes involved in the prime factorizations of α and β and write*

$$\alpha = \pi_1^{e_1} \cdots \pi_k^{e_k}, \quad \beta = \pi_1^{f_1} \cdots \pi_k^{f_k}.$$

Then a least common multiple of α and β is given by

$$\pi_1^{\max(e_1,f_1)} \cdots \pi_k^{\max(e_k,f_k)}.$$

Proof. Let γ denote a common multiple of α and β i.e. an element of $\mathbb{Z}[\omega]$ such that $\alpha \mid \gamma$ and $\beta \mid \gamma$. Consider one of the primes $\pi_1, ..., \pi_k$, say π_i. π_i divides either α or β, so π_i also divides γ. Furthermore, both $\pi_i^{e_i}$ and $\pi_i^{f_i}$ must divide γ due to uniqueness of prime factorizations. Using Proposition 2.20 inductively, we have that

$$\pi_1^{\max(e_1,f_1)} \cdots \pi_k^{\max(e_k,f_k)}.$$

must divide δ and $N(\pi_1^{\max(e_1,f_1)} \cdots \pi_k^{\max(e_k,f_k)}) \leq N(\delta)$. As $\pi_1^{\max(e_1,f_1)} \cdots \pi_k^{\max(e_k,f_k)}$ is a common multiple of α and β and δ was an arbitrary common multiple, the proposition follows. ■

Example 5.11. Consider $\alpha = 14 + 80\omega$ and $\beta = -8 + 4\omega$. Factoring these elements yield

$$\alpha = -1 \cdot 2(-3 + 4\omega)^2, \quad \beta = \omega \cdot 2^2(3 + 2\omega).$$

$-3 + 4\omega$ and $3 + 2\omega$ are not associates so using the above theorem, a least common multiple is given by

$$\mathrm{lcm}(\alpha, \beta) = 2^2(-3 + 4\omega)^2(3 + 2\omega) = 236 - 216\omega.$$

Computing a least common multiple using the prime factorization of both elements is a slow method in general. Thankfully, we do not have to use this method. We have a fast method for computing the greatest common divisor, namely the Euclidean algorithm, and we can use this method indirectly to compute the least common multiple. The following result formalizes this.

Proposition 5.12. *Let $\alpha, \beta \in \mathbb{Z}[\omega]$, and let δ denote a greatest common divisor and γ a least common multiple of α and β. Then $\alpha\beta$ is associated to $\delta\gamma$. In other words, for a suitable unit u, we have*

$$\alpha\beta = u \operatorname{gcd}(\alpha, \beta)\operatorname{lcm}(\alpha, \beta).$$

Proof. Using the setup of propositions 5.6 and 5.10, simply note that $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$. The result now follows immediately from the mentioned propositions. ■

5.5 Exercises

Exercise 5.5.1:
Prove the second part of Lemma 5.2.

Exercise 5.5.2:
Prove that $1 - \omega$ is associated to its conjugate.

Exercise 5.5.3:
Let $\alpha, \beta \in \mathbb{Z}[\omega]$. Prove that if δ is a greatest common divisor of α and β then $\overline{\delta}$ is a greatest common divisor of $\overline{\alpha}$ and $\overline{\beta}$.

Exercise 5.5.4:
Factor $-9 + 4\omega$ into a product of primes in $\mathbb{Z}[\omega]$.

Exercise 5.5.5:
Factor $12 - 8\omega$ into a product of primes in $\mathbb{Z}[\omega]$.

Exercise 5.5.6:
Factor $-16 + \omega$ into a product of primes in $\mathbb{Z}[\omega]$.

Exercise 5.5.7:
Compute the least common multiple of $\alpha = 3 + 6\omega$ and $\beta = 5 + \omega$.

Exercise 5.5.8:
Compute the least common multiple of $\alpha = 3 - 9\omega$ and $\beta = 3 + 7\omega$.

6 The ring $\mathbb{Z}[\omega]/(\gamma)$

6.1 The structure of $\mathbb{Z}[\omega]/(\gamma)$

Recall that for a fixed element $\gamma \in \mathbb{Z}[\omega] \setminus \{0\}$, we say that $\alpha \equiv \beta \pmod{\gamma}$ if $\gamma \mid \alpha - \beta$. As mentioned previously, $\equiv$ is an equivalence relation on $\mathbb{Z}[\omega]$ (which of course depends on the chosen γ). Hence we get a partition of $\mathbb{Z}[\omega]$ into equivalence classes. This is formalized in the following definition.

Definition 6.1. We use $[\cdot]_\gamma$ to denote the equivalence class of elements such that $\alpha \equiv \beta \pmod{\gamma}$. Explicitly,

$$[\alpha]_\gamma = \{\beta \in \mathbb{Z}[\omega] \mid \alpha \equiv \beta \pmod{\gamma}\}.$$

When γ is clear from the context, we will usually just write $[\cdot]_\gamma = [\cdot]$. We let $\mathbb{Z}[\omega]/(\gamma)$ denote the set of these equivalence classes i.e.

$$\mathbb{Z}[\omega]/(\gamma) = \{[\alpha]_\gamma : \alpha \in \mathbb{Z}[\omega]\}.$$

If $\beta \in [\alpha]_\gamma$, we call β a *representative* for this class.

The goal of this section is to describe $\mathbb{Z}[\omega]/(\gamma)$ in detail. We start by describing the simplest possible example.

Example 6.2. Let γ be a unit. Then γ divides every element of $\mathbb{Z}[\omega]$ i.e. $\gamma \mid \alpha - 0$ for every $\alpha \in \mathbb{Z}[\omega]$. Hence $[\alpha]_\gamma = [0]_\gamma$ for every $\alpha \in \mathbb{Z}[\omega]$ and thus

$$\mathbb{Z}[\omega]/(\gamma) = \{[0]_\gamma\}$$

is a set with one element. Note that $1 = N(\gamma)$.

In the next subsection we will determine the number of elements in $\mathbb{Z}[\omega]/(\gamma)$. Before doing so, we investigate the structure of $\mathbb{Z}[\omega]$ more thoroughly. We want to define addition and multiplication on $\mathbb{Z}[\omega]/(\gamma)$ in a natural way, namely by

$$[\alpha]_\gamma + [\beta]_\gamma = [\alpha + \beta]_\gamma$$
$$[\alpha]_\gamma \cdot [\beta]_\gamma = [\alpha\beta]_\gamma.$$

The following lemma shows that these operations are indeed well-defined.

Lemma 6.3. *$+$ and $\cdot$ on $\mathbb{Z}[\omega]/(\gamma)$ defined as above are well-defined arithmetic operations.*

Proof. We need to show that

$$[\alpha]_\gamma + [\beta]_\gamma = [\alpha + \beta]_\gamma$$

regardless of the chosen representatives of the equivalence classes. Assume $\alpha', \beta' \in \mathbb{Z}[\omega]$ satisfy $[\alpha]_\gamma = [\alpha']_\gamma$ and $[\beta]_\gamma = [\beta']_\gamma$. We have $\gamma \mid \alpha - \alpha'$ and $\gamma \mid \beta - \beta'$ so

$$\gamma \mid (\alpha - \alpha') + (\beta - \beta') = (\alpha + \beta) - (\alpha' + \beta')$$

showing that $[\alpha + \beta]_\gamma = [\alpha' + \beta']_\gamma$. Hence $+$ is well-defined. We let the reader verify that $\cdot$ is also well-defined. ■

It is not difficult to see that addition and multiplication on $\mathbb{Z}[\omega]/(\gamma)$ also behave well with respect to each other i.e. that the usual distributive laws hold,

$$[\alpha]_\gamma([\beta]_\gamma + [\rho]_\gamma) = [\alpha]_\gamma[\beta]_\gamma + [\alpha]_\gamma[\rho]_\gamma.$$

This makes computations in $\mathbb{Z}[\omega]/(\gamma)$ straightforward. One simply works like one would do in $\mathbb{Z}[\omega]$ and reduce modulo γ.

Example 6.4. Consider $\mathbb{Z}[\omega]/(\gamma)$ for $\gamma = 3 + 2\omega$. Let $\alpha = 8 + 9\omega$. We have

$$8 + 9\omega = (4 + 2\omega)(3 + 2\omega) - \omega$$

and so

$$[8 + 9\omega]_\gamma = [-\omega]_\gamma.$$

A natural question to ask is when an element of $\mathbb{Z}[\omega]/(\gamma)$ is invertible i.e. when an inverse exists. Before doing so, we need to specify what an invertible element is. Clearly, every element of $\mathbb{Z}[\omega]/(\gamma)$ has an additive inverse since

$$[\alpha]_\gamma + [-\alpha]_\gamma = [\alpha - \alpha]_\gamma = [0]_\gamma$$

for any $\alpha \in \mathbb{Z}[\omega]$. Hence it is only interesting to study the problem for multiplicative inverses.

Definition 6.5. An element $[\alpha]_\gamma$ of $\mathbb{Z}[\omega]/(\gamma)$ is called *invertible* if there exists some $[\beta]_\gamma \in \mathbb{Z}[\omega]/(\gamma)$ such that

$$[\alpha]_\gamma[\beta]_\gamma = [1]_\gamma.$$

If u is a unit in $\mathbb{Z}[\omega]$, $[u]_\gamma$ is clearly invertible with inverse $[u^{-1}]_\gamma$. But this is not the only possible case. The following theorem characterizes the invertible elements in $\mathbb{Z}[\omega]/(\gamma)$.

Theorem 6.6. *An element $[\alpha]_\gamma \in \mathbb{Z}[\omega]/(\gamma)$ is invertible if and only if α and γ are coprime.*

Proof. Assume $[\alpha]_\gamma$ is invertible and let $[\beta]_\gamma$ be an inverse. This is equivalent to

$$\begin{aligned} 1 = [\alpha]_\gamma[\beta]_\gamma = [\alpha\beta]_\gamma \quad &\Leftrightarrow \quad \alpha\beta \equiv 1 \pmod{\gamma} \\ &\Leftrightarrow \quad \alpha\beta = 1 + \rho\gamma \text{ for some } \rho \in \mathbb{Z}[\omega] \\ &\Leftrightarrow \quad \alpha\beta - \rho\gamma = 1 \text{ for some } \rho \in \mathbb{Z}[\omega] \\ &\Leftrightarrow \quad \alpha \text{ and } \gamma \text{ are coprime.} \end{aligned}$$

The last equivalence follows from Bezout's theorem. ■

The case where γ is a prime is so nice that it deserves its own corollary.

Corollary 6.7. *If γ is a prime, every element of $\mathbb{Z}[\omega]/(\gamma)$ except $[0]_\gamma$ is invertible.*

Recall *Fermat's little theorem* for the integers. If p is a prime that does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

We end this subsection by proving a similar result for $\mathbb{Z}[\omega]$.

Theorem 6.8 (Fermat's little theorem). *If π is a prime that does not divide α, then*

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}.$$

Proof. As π does not divide α, π and α are coprime. By the above corollary, the invertible elements of $\mathbb{Z}[\omega]/(\pi)$ are $(\mathbb{Z}[\omega]/(\pi)) \setminus \{[0]_\pi\}$ so $N(\pi) - 1$ invertible elements in total. $[\alpha]_\pi$ is invertible so the map $\varphi : \mathbb{Z}[\omega]/(\pi) \to \mathbb{Z}[\omega]/(\pi)$ given by

$$\varphi([\beta]_\pi) = [\alpha]_\pi[\beta]_\pi$$

is a bijection (exercise). Hence

$$\prod_{[\beta]_\pi \neq [0]_\pi} [\beta]_\pi = \prod_{[\beta]_\pi \neq [0]_\pi} [\alpha]_\pi[\beta]_\pi = [\alpha]_\pi^{N(\pi)-1} \prod_{[\beta]_\pi \neq [0]_\pi} [\beta]_\pi$$

and since the product is itself invertible, $[\alpha]_\pi^{N(\pi)-1} = [1]_\pi$ as desired. ■

6.2 The number of elements in $\mathbb{Z}[\omega]/(\gamma)$

It remains to determine the number of elements in $\mathbb{Z}[\omega]/(\gamma)$. This takes a bit of work, so we do it in steps.

Lemma 6.9. *Let $\gamma = 1 - \omega$. Then $\mathbb{Z}[\omega]/(\gamma)$ contains three elements. Explicitly,*

$$\mathbb{Z}[\omega]/(\gamma) = \{[0]_\gamma, [1]_\gamma, [-1]_\gamma\}.$$

Proof. Let $\alpha \in \mathbb{Z}[\omega]$ and apply Euclidean division to obtain $\alpha = \beta\gamma + \rho$ where $N(\rho) < N(\gamma) = 3$. We thus have $N(\rho) \in \{0, 1, 2\}$. 2 is not of the form $a^2 - ab + b^2$ for integers a, b so 2 is not a norm of any Eisenstein integer. Hence $N(\rho) \in \{0, 1\}$. If $N(\rho) = 0$, $\rho = 0$ and γ divides α. Hence the case $N(\rho) = 0$ corresponds to $[\alpha]_\gamma = [0]_\gamma$. Assume $N(\rho) = 1$. This implies that ρ is a unit. We have six cases:

- $\rho = 1$: $[\alpha]_\gamma = [1]_\gamma$.
- $\rho = -1$: $[\alpha]_\gamma = [-1]_\gamma$.
- $\rho = \omega$: $\omega \equiv \omega + (1 - \omega) \equiv 1 \pmod{\gamma}$ so $[\alpha]_\gamma = [1]_\gamma$.
- $\rho = -\omega$: $-\omega \equiv -\omega - (1 - \omega) \equiv -1 \pmod{\gamma}$ so $[\alpha]_\gamma = [-1]_\gamma$.
- $\rho = 1 + \omega$: $1 + \omega \equiv 1 + \omega - (1 - \omega) \equiv 2\omega \pmod{\gamma}$. 3 is divisible by γ so $2 \equiv -1 \pmod{\gamma}$ and hence $1 + \omega \equiv -\omega \equiv -1 \pmod{\gamma}$.
- $\rho = -1 - \omega$: $-1 - \omega \equiv 1 \pmod{\gamma}$.

■

Lemma 6.10. *Assume $\gamma_1, \gamma_2 \in \mathbb{Z}[\omega]$ are non-zero associates. Then*

$$\mathbb{Z}[\omega]/(\gamma_1) = \mathbb{Z}[\omega]/(\gamma_2).$$

Proof. Write $\gamma_2 = u\gamma_1$ for a unit u in $\mathbb{Z}[\omega]$. For $\alpha, \beta \in \mathbb{Z}[\omega]$, $\alpha \equiv \beta \pmod{\gamma_1}$ means that $\gamma_1 \mid \beta - \alpha$ i.e $\beta - \alpha = \rho\gamma_1$ for some $\rho \in \mathbb{Z}[\omega]$. We can write the right hand side as $\rho\gamma_1 u u^{-1} = \rho\gamma_2 u^{-1}$ and so γ_2 also divides $\beta - \alpha$. It follows that the equivalence classes modulo γ_1 and γ_2 are the same. ■

The next step in determining the number of elements in $\mathbb{Z}[\omega]/(\gamma)$ concerns the case where γ is a prime. We need a definition before considering this case.

Definition 6.11. Let γ be non-zero. A *set of representatives* for $\mathbb{Z}[\omega]/(\gamma)$ is a subset of elements of $\mathbb{Z}[\omega]$ such that each equivalence class of $\mathbb{Z}[\omega]/(\gamma)$ has exactly one representative in the list.

Example 6.12. For $\gamma = 1 - \omega$, a set of representatives is given by $\{0, 1, -1\}$.

Theorem 6.13. *Let γ be a prime in $\mathbb{Z}[\omega]$. Then $\mathbb{Z}[\omega]/(\gamma)$ contains $N(\gamma)$ elements.*

Proof. By the classification of primes, Theorem 4.17, and the lemma just proved, there are three cases to check:

(1) $\gamma = 1 - \omega$. This is Lemma 6.9 above.

(2) $\gamma = p$ where p is an integral prime $p \equiv 2 \pmod{3}$. We claim that the set

$$\mathcal{R} = \{a + b\omega \mid 0 \leq a, b < p\}$$

is a set of representatives for $\mathbb{Z}[\omega]/(\gamma)$. Let $\alpha = c + d\omega \in \mathbb{Z}[\omega]$ be arbitrary and apply Euclidean division (in the integers) to obtain

$$c = q_1 p + r_1, \quad d = q_2 p + r_2$$

with $0 \leq r_1, r_2 < p$. Then $r_1 + r_2\omega$ is a representative of $[\alpha]_\gamma$ contained in the aforementioned set. Hence every element of $\mathbb{Z}[\omega]/(\gamma)$ has a representative in

$\mathcal{R}$. Now assume that $a + b\omega$ and $c + d\omega$ represent the same class $[\alpha]_\gamma$. Then $a + b\omega \equiv c + d\omega \pmod{p}$ and thus

$$p \mid (a + b\omega) - (c + d\omega) = (a - c) + (b - d)\omega$$

implying that $p \mid a - c$ and $p \mid b - d$. But $0 \leq a, b, c, d < p$ so we must have $a - c = 0$ and $b - d = 0$ i.e. $a = c$ and $b = d$. We conclude that $\mathcal{R}$ is indeed a set of representatives. $\mathcal{R}$ contains $p^2 = N(\gamma)$ elements and we are done with this case.

(3) $\gamma = \pi$ where $N(\pi) = p$ a prime with $p \equiv 1 \pmod{3}$. We claim that

$$\mathcal{R} = \{0, 1, ..., p - 1\}$$

is a set of representatives for $\mathbb{Z}[\omega]/(\gamma)$. Write $\pi = a + b\omega$. $p = a^2 - ab + b^2$ and so p cannot divide b. Because p is a prime, $\gcd(b, p) = 1$. If $\alpha = c + d\omega$ denotes any element of $\mathbb{Z}[\omega]$ we can find an integer n such that $nb \equiv d \pmod{p}$. Then

$$\alpha - n\pi \equiv c - na + (d - nb)\omega \equiv c - na \pmod{p}$$

and since $\pi \mid p$, this implies that $\alpha - n\pi \equiv c - na \pmod{\pi}$. We have shown that every $[\alpha]_\gamma \in \mathbb{Z}[\omega]/(\gamma)$ has a representative which is an integer. By reducing modulo p, we can choose this representative to be in $\mathcal{R}$. Assume $k \equiv k' \pmod{\pi}$ with $k, k' \in \mathcal{R}$. Then $\pi \mid k - k'$ and in particular, the norm of π, i.e. p, divides the norm of $k - k'$ which is $(k - k')^2$. Hence $p \mid k - k'$ and since $0 \leq k, k' < p$, this implies $k = k'$. We conclude that $\mathcal{R}$ is a set of representatives. $\mathcal{R}$ contains $p = N(\gamma)$ elements and we are done.

■

We have shown that for γ a prime, $\mathbb{Z}[\omega]/(\gamma)$ has $N(\gamma)$ elements. This property also holds for any $\gamma \neq 0$ as the next theorem shows.

Theorem 6.14. *If $\gamma \neq 0$, $\mathbb{Z}[\omega]/(\gamma)$ has $N(\gamma)$ elements.*

Proof. Factor γ into a product of primes as $\gamma = \pi_1^{e_1} \cdots \pi_n^{e_n}$ where the primes π_i are distinct. Then the $\pi_i^{e_i}$ are pairwise coprime. Consider the product

$$\mathbb{Z}[\omega]/(\pi_1^{e_1}) \times \cdots \times \mathbb{Z}[\omega]/(\pi_n^{e_n}).$$

From the previous theorem we know that the number of elements of the right hand side is $N(\pi_1^{e_1}) \cdots N(\pi_n^{e_n}) = N(\gamma)$. Hence we are done if we can establish a bijection

$$\varphi : \mathbb{Z}[\omega]/(\gamma) \to \mathbb{Z}[\omega]/(\pi_1^{e_1}) \times \cdots \times \mathbb{Z}[\omega]/(\pi_n^{e_n}).$$

Let $[\alpha]_\gamma \in \mathbb{Z}[\omega]$. Define φ by

$$\varphi([\alpha]_\gamma) = ([\alpha]_{\pi_1^{e_1}}, ..., [\alpha]_{\pi_n^{e_n}}).$$

We leave it as an exercise for the reader to verify that this map is well-defined. We now show that it is surjective and injective. For surjectivity, let $([\alpha_1]_{\pi_1^{e_1}}, \ldots, [\alpha_n]_{\pi_n^{e_n}})$ be an element of the product. Unwinding the definitions, we need to determine an element $\alpha \in \mathbb{Z}[\omega]$ such that

$$\alpha \equiv \alpha_i \pmod{\pi_i^{e_i}}, \quad i = 1, ..., n.$$

But such an α exists by the Chinese Remainder Theorem, Theorem 3.5. The same theorem says that α is unique modulo $\pi_1^{e_1} \cdots \pi_n^{e_n} = \gamma$ which tells us that the map is injective as well. This completes the proof. ■

6.3 Exercises

Exercise 6.3.1:
Prove that $\cdot$ on $\mathbb{Z}[\omega]/(\gamma)$ defined by

$$[\alpha]_\gamma \cdot [\beta]_\gamma = [\alpha\beta]_\gamma$$

is well-defined.

Exercise 6.3.2:
Prove that the map φ defined in the proof of Fermat's little theorem is indeed a bijection.

Exercise 6.3.3:
Find a set of representatives for $\mathbb{Z}[\omega]/(\gamma)$ when $\gamma = 17$.

Exercise 6.3.4:
Find a set of representatives for $\mathbb{Z}[\omega]/(\gamma)$ when $\gamma = 3 + 7\omega$.

Exercise 6.3.5:
Verify that the map φ given in Theorem 6.14 is well-defined.

7 Cubic reciprocity

7.1 The cubic residue symbol

We now dive into a more advanced topic, namely cubic reciprocity. If p is an odd integral prime, we define the *quadratic residue symbol/Legendre symbol* to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1, & x^2 \equiv a \pmod{p} \text{ has no solution} \\ 0, & p \mid a \end{cases}.$$

An elegant and useful result is that if p and q are different odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

This result is called the *law of quadratic reciprocity.* In words, the result states that when $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, the equation $x^2 \equiv p \pmod q$ has a solution if and only if $x^2 \equiv q \pmod p$ has a solution. If either p or q is congruent to 3 modulo 4, $x^2 \equiv p \pmod q$ has a solution if and only if $x^2 \equiv q \pmod p$ does not have a solution.

A similar result exists for $\mathbb{Z}[\omega]$ and it is in some ways a lot nicer than the one in $\mathbb{Z}$. The result does not concern quadratic residues but *cubic residues.*

Definition 7.1. Let $\gamma \neq 0$. $\alpha \in \mathbb{Z}[\omega]$ is a *cubic residue* modulo γ if the equation

$$x^3 \equiv \alpha \pmod{\gamma}$$

has a solution x in $\mathbb{Z}[\omega]$.

The goal of this section is to present effective methods for determining when an Eisenstein integer is a cubic residue modulo γ. We start by considering the case where γ is a prime. Let π be an Eisenstein prime with $1-\omega \nmid \pi$. Recall from the first section that this is equivalent to $N(\pi)$ not being divisible by 3. We note that $1, \omega$ and ω^2 $(= -1-\omega)$ cannot be congruent to each other modulo π (exercise). Earlier we saw that the norm of any Eisenstein integer cannot be congruent to 2 modulo 3 and thus $N(\pi) \equiv 1 \pmod 3$. If $\pi \nmid \alpha$, we can make the factorization

$$\alpha^{N(\pi)-1} - 1 = \left(e^{\frac{N(\pi)-1}{3}} - 1\right)\left(e^{\frac{N(\pi)-1}{3}} - \omega\right)\left(e^{\frac{N(\pi)-1}{3}} - \omega^2\right).$$

By Fermat's little theorem, π divides the left hand side. As π is prime, it must divide at least one of the three factors on the right hand side. By the previous discussion, π can only divide one of them. This makes the following definition valid.

Definition 7.2. For a prime $\pi \in \mathbb{Z}[\omega]$ with $N(\pi) \neq 3$ and $\alpha \in \mathbb{Z}[\omega]$, define the *cubic residue symbol* of α modulo π to be

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0, & \pi \mid \alpha \\ \omega^m, & \alpha^{(N(\pi)-1)/3} \equiv \omega^m \pmod{\pi} \end{cases}$$

Note the similarity between this definition and the result from elementary number theory that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

which is known as *Euler's criterion*. See the beginning of chapter five in [3]. We are interested in determining when an element is a cubic residue. The following proposition shows that we are indeed on the right track.

Proposition 7.3. *Let π be a prime, $N(\pi) \neq 3$. Then*

$$\left(\frac{\alpha}{\pi}\right)_3 = 1$$

if and only if α is a cubic residue modulo π.

Proof. We will use the fact that the invertible elements of $\mathbb{Z}[\omega]/(\pi)$ form a cyclic group (see Theorem 1 in chapter seven of [3]). In other words, there exists some γ such that every Eisenstein integer modulo π is a power of γ. The equation

$$x^3 \equiv \alpha \pmod \pi$$

can thus be rewritten to $\gamma^{3a} \equiv \gamma^b \pmod \pi$ for some integers a, b. The equation has a solution if and only if $3a \equiv b \pmod{N(\pi)-1}$ and we know that $\gcd(3, N(\pi)-1) = 3$. Hence the equation is solvable if and only if $3 \mid b$. But this is equivalent to $(\alpha/\pi)_3 = 1$. ■

Example 7.4. $1+6\omega$ is a prime since $N(1+6\omega) = 31$ is an integer prime. Consider $8-11\omega$. We wish to determine whether $x^3 \equiv 8-11\omega \pmod{1+6\omega}$ has a solution. We need to compute

$$\left(\frac{8-11\omega}{1+6\omega}\right)_3 \equiv (8-11\omega)^{\frac{31-1}{3}} \equiv (8-11\omega)^{10} \pmod{1+6\omega}.$$

This computation is easily done using modular exponentiation and gives $(8-11\omega/1+6\omega)_3 = 1$. We conclude that $x^3 \equiv 8-11\omega \pmod{1+6\omega}$ is solvable.

The following lemma is trivial but still important enough to state.

Lemma 7.5. *Let π be a prime with $N(\pi) \neq 3$.*

(i) $(\cdot/\pi)_3$ is multiplicative in the top argument i.e. for $\alpha, \beta \in \mathbb{Z}[\omega]$,

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 .$$

(ii) If $\alpha \equiv \beta$ (mod π), then

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3 .$$

Proof. Exercise. ■

Translating the problem of solving an equation into a function like $(\cdot/\pi)_3$ has many advantages from a computational perspective. We actually have all the tools we need to determine whether an equation

$$x^3 \equiv \alpha \pmod{\gamma}$$

has a solution. Indeed, factor γ into a product of primes and compute the cubic residue symbol of α (using modular exponentiation) for all these primes. If all of these are one, the equation has a solution, otherwise not. But our study does not end here. We want to generalize the cubic residue symbol to the case where γ can be an element which is not prime. This will allow us to compute the symbol effectively using cubic reciprocity.

Definition 7.6. Let $\alpha \in \mathbb{Z}[\omega]$ be a non-unit and assume $3 \nmid N(\alpha)$. Let $\beta \in \mathbb{Z}[\omega]$ and factor $\alpha = \pi_1 \cdots \pi_n$ into prime elements. Define the *(generalized) cubic residue symbol* as

$$\left(\frac{\beta}{\alpha}\right)_3 = \prod_{i=1}^{n} \left(\frac{\beta}{\pi_i}\right)_3 .$$

The generalized cubic residue symbol enjoys many nice properties. Some of these are stated in the proposition below.

Proposition 7.7. *Let $\alpha, \beta, \lambda, \rho \in \mathbb{Z}[\omega]$ with $3 \nmid N(\lambda), N(\rho)$. The following hold:*

(i)

$$\left(\frac{\alpha}{\lambda}\right)_3 \neq 0$$

if and only if α and λ are coprime.

(ii)

$$\left(\frac{\alpha\beta}{\lambda}\right)_3 = \left(\frac{\alpha}{\lambda}\right)_3 \left(\frac{\beta}{\lambda}\right)_3 .$$

(iii) If $\alpha \equiv \beta$ (mod λ), then

$$\left(\frac{\alpha}{\lambda}\right)_3 = \left(\frac{\beta}{\lambda}\right)_3 .$$

(iv)

$$\left(\frac{\alpha}{\lambda\rho}\right)_3 = \left(\frac{\alpha}{\lambda}\right)_3 \left(\frac{\alpha}{\rho}\right)_3$$

(v)

$$\left(\frac{-1}{\lambda}\right)_3 = 1.$$

Proof. See the exercises. ■

Note that the proposition says nothing about the solvability of $x^3 \equiv \alpha \pmod{\lambda}$. The reason is simple. The connection between the cubic residue symbol and the solvability of this equation breaks down in general when λ is not a prime. Later we will see an example that illustrates this.

7.2 The law of cubic reciprocity

In this subsection we will state the law of cubic reciprocity, but we need a bit more work before we can do so.

Definition 7.8. $\alpha \in \mathbb{Z}[\omega]$ is called *primary* if $\alpha \equiv 2 \pmod 3$.

$\alpha = a + b\omega \in \mathbb{Z}[\omega]$ with $N\alpha \neq 3$ is primary if and only if $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$. Recall that we have six associates of every element in $\mathbb{Z}[\omega]$. Hence the notion of being primary is a way of avoiding the ambiguity caused by these associates. In $\mathbb{Z}$, we only have the two units, namely 1 and -1. In this case the ambiguity is easily removed by simply requiring that the lower argument of the Legendre symbol is non-negative. The notion of being primary is only useful if exactly one of the six associates of α is primary. This turns out to be the case when $3 \nmid N(\alpha)$:

Proposition 7.9. *Let $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ and assume $3 \nmid N(\alpha)$. Exactly one of the associates of α is primary.*

Proof. Let us write down all the associates explicitly:

$$a + b\omega, \quad -b + (a-b)\omega, \quad (b-a) - a\omega, \quad -a - b\omega, \quad b + (b-a)\omega, \quad (a-b) + a\omega$$

We first show uniqueness. If $a + b\omega$ is primary, $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$, from which it easily follows by considering congruence classes that none of the associates are primary. The proof of existence is a straightforward check. If $a \equiv 0 \pmod 3$ and $b \equiv 1 \pmod 3$, the primary associate is $(a-b) + a\omega$. For $a \equiv 0 \pmod 3$ and $b \equiv 2 \pmod 3$, the primary associate is $(b-a) - a\omega$. We let the reader check the remaining four possible cases. Note that we cannot have the three cases with $a + b \equiv 0 \pmod 3$, since the norm is divisible by 3 in those cases. ■

The following technical lemma will be useful later.

Lemma 7.10. *Any primary element λ in $\mathbb{Z}[\omega]$ can be written as a product $\lambda = \pm\lambda_1 \cdots \lambda_t$ with each λ_i a primary prime.*

Proof. By unique factorization, factor $\lambda = u\pi_1 \cdots \pi_m q_1 \cdots q_n$ with $u \in \mathbb{Z}[\omega]^\times$ and $N(\pi_i) \equiv 1 \pmod 3$, $q_i \equiv 2 \pmod 3$. For each i, let $\pi_i' = u_i\pi_i$ be the unique primary associate of π_i and $v = u \cdot \prod_i u_i$. Then $\lambda = v\pi_1' \cdots \pi_m' q_1 \cdots q_n$ is a factorization into primary primes. Reducing modulo 3, we obtain $2 \equiv v2^{m+n} \pmod 3$ implying $v = \pm 1$ since a power of 2 is either 1 or -1 modulo 3. ■

We are now ready to state the main theorem of this section.

Theorem 7.11 (Law of cubic reciprocity)**.** *Let λ and ρ be relatively prime primary elements in $\mathbb{Z}[\omega]$ with $N(\lambda), N(\rho) \neq 3$ and $N(\lambda) \neq N(\rho)$. Then*

$$\left(\frac{\lambda}{\rho}\right)_3 = \left(\frac{\rho}{\lambda}\right)_3. \tag{1}$$

For λ of the form $\lambda = 3m - 1 + 3n\omega$ for integers m and n, we have the supplementary law:

$$\left(\frac{1-\omega}{\lambda}\right)_3 = \omega^{2m} \tag{2}$$

And for the units, we have:

$$\left(\frac{\omega}{\lambda}\right)_3 = \omega^{\frac{N(\lambda)-1}{3}} = \begin{cases} 1, & N(\lambda) \equiv 1 \pmod 9 \\ \omega, & N(\lambda) \equiv 4 \pmod 9 \\ \omega^2, & N(\lambda) \equiv 7 \pmod 9 \end{cases} \tag{3}$$

Proof. An elementary proof of this relies on a lot of machinery in the form of Gauss and Jacobi sums. A full proof with all the necessary preliminaries can be found in [5]. ■

The following example illustrates how one (or more likely, a computer) would use cubic reciprocity to compute the cubic residue symbol.

Example 7.12. Let $\alpha = -1165 + 2880\omega$ and $\beta = 134 - 429\omega$. One can check that $1 - \omega$ does not divide β so that the cubic residue symbol $(\alpha/\beta)_3$ is well-defined. Let us use cubic reciprocity to compute the symbol:

$$\begin{aligned}
\left(\frac{-1165+2880\omega}{134-429\omega}\right)_3 &= \left(\frac{-227-123\omega}{134-429\omega}\right)_3 = \left(\frac{227+123\omega}{134-429\omega}\right)_3 = \left(\frac{134-429\omega}{227+123\omega}\right)_3 \\
&= \left(\frac{-8+6\omega}{227+123\omega}\right)_3 = \left(\frac{8-6\omega}{227+123\omega}\right)_3 = \left(\frac{227+123\omega}{8-6\omega}\right)_3 \\
&= \left(\frac{3-5\omega}{8-6\omega}\right)_3 = \left(\frac{-\omega}{8-6\omega}\right)_3 \left(\frac{8+3\omega}{8-6\omega}\right)_3 \quad (N(8-6\omega) = 148 \equiv 4 \pmod 9) \\
&= \omega \left(\frac{9\omega}{8-6\omega}\right)_3 = \omega \left(\frac{\omega}{8-6\omega}\right)_3^2 \left(\frac{(1-\omega)^4}{8-6\omega}\right)_3 \\
&= \omega\omega^2 \left(\frac{1-\omega}{8-6\omega}\right)_3 = \omega^{2\frac{8+1}{3}} = \omega^6 = 1.
\end{aligned}$$

The example illustrates an important point. The above symbol was equal to 1, but α is not a cubic residue modulo β. This can only happen when β is not a prime, and in the above case, the factorization of β is given by $\beta = \omega(1-2\omega)(5+2\omega)(-51-26\omega)$. If α was a cubic residue modulo β, α would also be a cubic residue modulo each prime factor of β. In this case however, as the reader may verify,

$$\left(\frac{\alpha}{1-2\omega}\right)_3 = \left(\frac{\alpha}{5+2\omega}\right)_3 = \left(\frac{\alpha}{-51-26\omega}\right)_3 = \omega.$$

7.3 Computing the cubic residue symbol

The fully generalized theorem of cubic reciprocity allows us to write an efficient algorithm for computing the cubic residue character. In the following, for $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, let $\alpha.a$ denote the value for a in a given iteration and likewise with $\alpha.b$. primary(α) denotes the unique primary associate of α.

Algorithm 6: Cubic residue symbol

```
Input: $\alpha, \beta \in \mathbb{Z}[\omega]$ with $1 - \omega \nmid \beta$
Output: $\left(\frac{\alpha}{\beta}\right)_3$
$r \leftarrow 1$
while (true) do
    $\beta \leftarrow$ primary($\beta$)
    $\alpha \leftarrow \alpha \bmod \beta$

    if $\alpha = 0$ then
        if $N(\beta) \neq 1$ then
            return 0                                  // $\alpha$ and $\beta$ have a common factor
        else
            return $r$

    while $1 - \omega \mid \alpha$ do
        $\alpha \leftarrow \alpha/(1-\omega)$
        $r \leftarrow r \cdot \omega^{(2(\beta.a+1))/3}$                 // supplementary law for $1-\omega$

    $u \leftarrow \alpha$/primary($\alpha$)
    $\alpha \leftarrow$ primary($\alpha$)                       // supplementary law for the units
    if $u = \pm\omega$ then
        if $N(\beta) \equiv 4 \bmod 9$ then
            $r \leftarrow r \cdot \omega$
        if $N(\beta) \equiv 7 \bmod 9$ then
            $r \leftarrow r \cdot \omega^2$
    if $u = \pm\omega^2$ then
        if $N(\beta) \equiv 4 \bmod 9$ then
            $r \leftarrow r \cdot \omega^2$
        if $N(\beta) \equiv 7 \bmod 9$ then
            $r \leftarrow r \cdot \omega$
    $(\alpha, \beta) \leftarrow (\beta, \alpha)$                               // cubic reciprocity
```

7.4 Exercises

Exercise 7.4.1:
Show that none of $1, \omega, \omega^2$ can be congruent to each other modulo π when $N(\pi) \neq 3$.

Exercise 7.4.2:
Prove Lemma 7.5.

Exercise 7.4.3:
For $\alpha, \pi \in \mathbb{Z}[\omega]$ with π a prime and $N(\pi) \neq 3$, prove the following:

(i)

$$\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha}{\pi}\right)_3^2.$$

(ii)

$$\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3.$$

Exercise 7.4.4:
Prove Proposition 7.7 (most of the proofs consist of convincing one-self that they are obvious).

Exercise 7.4.5:
Generalize Exercise 7.4.3 to a primary element λ with $3 \nmid N(\lambda)$.

8 Applications

8.1 Cubic residues in the integers

We will use the theory developed in the previous section to determine when the equation

$$x^3 \equiv a \pmod{p}$$

has a solution for a prime p. Not surprisingly, we call a a *cubic residue* modulo p if there is a solution and a *cubic nonresidue* otherwise. The reader can verify that any a is a cubic residue modulo 3, so assume $p > 3$. Then we have two cases, namely $p \equiv 1 \pmod{3}$ and $p \equiv 2 \pmod{3}$. We consider these two cases separately. In the following, we assume that the reader is familiar with elementary abstract algebra.

Lemma 8.1. *If p is a prime $p \equiv 2 \pmod{3}$, then $x^3 \equiv a \pmod{p}$ is always solvable.*

Proof. If $3 \mid a$, simply choose $x = 0$. Hence we may assume that $3 \nmid a$. The order of the group $\mathbb{Z}/p\mathbb{Z}^\times$ of non-zero units under multiplication is cyclic of order $p - 1$. As $p \equiv 2 \pmod{3}$, 3 does not divide the order of $\mathbb{Z}/p\mathbb{Z}^\times$ so a^3 is a generator of $\mathbb{Z}/p\mathbb{Z}^\times$. As a is clearly a generator, the map $a \mapsto a^3$ is an automorphism and this clearly implies that $x^3 \equiv a \pmod{p}$ has a solution x. ∎

So far we have not applied any results from the previous sections. They will come into play when we consider the case $p \equiv 1 \pmod{3}$.

Lemma 8.2. *If p is a prime $p \equiv 1 \pmod{3}$, then $x^3 \equiv a \pmod{p}$ is solvable if and only if*

$$\left(\frac{a}{\pi}\right)_3 = 1$$

where $p = \pi\overline{\pi}$ is the factorization of p into primes in $\mathbb{Z}[\omega]$.

Proof. Recall from theorem 6.14 that $\mathbb{Z}[\omega]/(\pi)$ has p elements. Hence $\mathbb{Z}[\omega]/(\pi)$ is a field with p elements. It follows that $\mathbb{Z}[\omega]/(\pi)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and the claim follows. ∎

Let us summarise our findings.

Theorem 8.3. *For a prime $p > 1$, consider the equation $x^3 \equiv a \pmod{p}$. If $p = 3$ or $p \equiv 2 \pmod{3}$, the equation always has a solution. If $p \equiv 1 \pmod{3}$, the equation is solvable if and only if*

$$\left(\frac{a}{\pi}\right)_3 = 1.$$

8.2 Primes of the form $x^2 + 27y^2$

A classical problem in number theory that has sparked many innovations in the field is the question of when a prime p is of the form $x^2 + ny^2$ for integers x, y and n. We can use cubic reciprocity to solve the problem for the case of $n = 27$.

Theorem 8.4. *Let p be a prime. p is of the form $x^2 + 27y^2$ if and only if $p \equiv 1$ (mod 3) and 2 is a cubic residue modulo p.*

Proof. Assume $p = x^2 + 27y^2$. Reducing modulo 3 gives $p \equiv x^2 \pmod 3$ and since any square is congruent to 1 modulo 3, $p \equiv 1 \pmod 3$ as desired. We now show that 2 is a cubic residue modulo p using the theorem in the previous subsection. Let $\pi = x + 3\sqrt{-3}y$, then $p = \pi\overline{\pi}$ is the factorization of p in $\mathbb{Z}[\omega]$. We have to show that $(2/\pi)_3 = 1$. π and 2 are both primary primes (exercise) so by cubic reciprocity,

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3$$

and by definition of the cubic residue symbol,

$$\left(\frac{\pi}{2}\right)_3 \equiv \pi^{(N(2)-1)/3} \equiv \pi \pmod 2.$$

As $\sqrt{-3} = 1 + 2\omega$, $\pi = x + 3y + 6y\omega$ so $\pi \equiv x + 3y \equiv x + y \pmod 2$. But as x and y must have opposite parity, $x + y \equiv 1 \pmod 2$, and the above symbol equals 1 as desired. Conversely, suppose $p \equiv 1 \pmod 3$ and that 2 is a cubic residue modulo p. We can write p on the form $p = \pi\overline{\pi}$ where π is a primary prime (see Lemma 7.10). Hence $\pi = a + 3b\omega$ for some integers a and b. We have

$$4p = 4\pi\overline{\pi} = 4(a^2 - 3ab + 9b^2) = (2a - b)^2 + 27b^2.$$

If b is even, we may divide both sides by 4 and obtain that p is of the desired form. We have assumed $(2/\pi) = 1$ and by cubic reciprocity, $(\pi/2) = 1$. As before, $\pi \equiv 1 \pmod 2$ so that $a + 3b\omega \equiv 1 \pmod 2$. This implies that a is odd and b is even. This completes the proof.

■

A whole book is dedicated to the study of primes of the form $x^2 + ny^2$, namely [1]. The above proof is also from that book (see Theorem 4.15).

Example 8.5. Consider $p = 19$. Is p of the form $x^2 + 27y^2$? We see that $p \equiv 1$ (mod 3). We also have $p = \pi\overline{\pi}$ with $\pi = 5 + 2\omega$. One can show that

$$\left(\frac{2}{5 + 2\omega}\right)_3 = \omega \neq 1$$

and since $5 + 2\omega$ is prime, 2 is not a cubic residue modulo 19. The above theorem says that p is not of the desired form.

8.3 References and further reading

Some information on the Eisenstein integers can be found in [3]. For more information on ring theory, consult [2]. As for cubic reciprocity, [3] is a good source. See also the book [4] for a very thorough monologue on the subject that also includes other reciprocity laws.

8.4 Exercises

Exercise 8.4.1:
Prove that any integer a is a cubic residue modulo 3.

Exercise 8.4.2:
Is 31 of the form $x^2 + 27y^2$ for some integers x and y?

Exercise 8.4.3:
Is 79 of the form $x^2 + 27y^2$ for some integers x and y?

References

[1] David A. Cox. *Primes of the form $x^2 + ny^2$.* John Wiley & Sons, Inc., 1989. ISBN 0-471-50654-0.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra.* Wiley, 3 edition, 2003. ISBN 978-0-471-43334-7.

[3] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer, 2 edition, 1990. ISBN 0-387-97329-X.

[4] Franz Lemmermeyer. *Reciprocity Laws - From Euler to Eisenstein.* Springer, 2000. ISBN 3-540-66957-4.

[5] Rasmus Frigaard Lemvig. *Cubic and quartic reciprocity - Bachelor's thesis.* 2021.

A - Hints for the exercises

Exercise 2.4.4

Use Bezout's theorem on both (α, γ) and (β, γ). Then substitute one of the equations into the other and apply the corollary to Bezout's theorem.

Exercise 4.4.5

Use Bezout's theorem.

Exercise 4.4.7

$(\alpha) = (\beta)$ if and only if α divides β and β divides α.

Exercise 4.4.8

If M is a maximal ideal, $M = (\alpha)$ for some α (this holds for any ideal as was shown earlier). If $\beta\gamma \in M$ and $\beta \notin M$, then $(\alpha) + (\beta)$ is an ideal strictly larger than M. Use that M is a maximal ideal and Bezout's theorem.

Exercise 4.4.9

You will need both quadratic reciprocity and the supplement for -1.

Exercise 5.5.1

Use induction.

Exercise 6.3.1

If $[\alpha]_\gamma = [\alpha']_\gamma$ and $[\beta]_\gamma = [\beta']_\gamma$, use that

$$\gamma \mid \beta(\alpha - \alpha') \quad \text{and} \quad \gamma \mid \alpha'(\beta - \beta').$$

Exercise 6.3.2

Use the proof of Theorem 6.12.

Exercise 6.3.3

Use the proof of Theorem 6.12.

Exercise 7.4.3

Show/use that $\overline{\omega} = \omega^2$.

B - Solutions for the exercises

Exercise 1.4.1

$\alpha+\beta=-4-3\omega$, $\alpha-\beta=10-7\omega$, $\alpha\beta=-11+51\omega$. $N(\alpha)=49$ and $N(\beta)=67$.

Exercise 1.4.2

We have $\omega^3=1$ and so

$$\omega(\omega^2+\omega+1)=1+\omega^2+\omega$$

and since $\omega\neq 1$, we must have $\omega^2+\omega+1=0$. We can now verify the identity:

$$\begin{aligned}(a+b\omega)(c+d\omega)&=ac+ad\omega+bc\omega+bd\omega^2=ac+(ad+bc)\omega+bd(-1-\omega)\\&=ac-bd+(ad+bc-bd)\omega.\end{aligned}$$

Exercise 1.4.3

Let $\beta,\gamma\in\mathbb{Z}[\omega]$ satisfy $\alpha\beta=1=\alpha\gamma$. Then

$$\beta=(\alpha\gamma)\beta=\gamma(\alpha\beta)=\gamma.$$

This shows that the inverse is unique.

Exercise 1.4.4

Note that

$$\omega=e^{\frac{2\pi i}{3}}=\frac{-1+i\sqrt{3}}{2}$$

and so

$$\overline{\omega}=\frac{-1-i\sqrt{3}}{2}=-1-\omega.$$

Hence

$$\overline{\alpha}=a+b\overline{\omega}=a+b(-1-\omega)=(a-b)-b\omega$$

which proves (1). We now verify (2):

$$\begin{aligned}\alpha\overline{\alpha}&=(a+b\omega)(a-b-b\omega)=a(a-b)-ab\omega+b(a-b)\omega-b^2\omega^2\\&=a^2-ab-ab\omega+ab\omega-b^2\omega-b^2(-1-\omega)=a^2-ab-b^2=N(\alpha).\end{aligned}$$

(3) follows immediately from (2).

Exercise 1.4.5

Using Proposition 1.7 (2), we have

$$N(\alpha\beta)=\alpha\beta\overline{\alpha\beta}=\alpha\overline{\alpha}\beta\overline{\beta}=N(\alpha)N(\beta).$$

Exercise 1.4.6

$\alpha = 1 \cdot \alpha$ so $\alpha \sim \alpha$. This shows reflexivity. If $\alpha \sim \beta$, then $\alpha = u\beta$ for a unit $u \in \mathbb{Z}[\omega]$. Then $\beta = u^{-1}\alpha$ so $\beta \sim \alpha$. This proves symmetry. Now assume $\alpha \sim \beta$ and $\beta \sim \gamma$. Then $\alpha = u\beta$ and $\beta = v\gamma$ for units u and v. Then $\alpha = uv\gamma$, so $\alpha \sim \gamma$, showing transitivity. We have

$$[2+3\omega] = \{2+3\omega, -2-3\omega, -3-\omega, 3+\omega, -1+2\omega, 1-2\omega\},$$
$$[4\omega] = \{4\omega, -4\omega, -4-4\omega, 4+4\omega, -4, 4\}$$

and

$$[1-\omega] = \{1-\omega, -1+\omega, 1+2\omega, -1-2\omega, 2+\omega, -2-\omega\}.$$

Exercise 1.4.7

1)

$$\frac{17+14\omega}{2+5\omega} = \frac{(17+14\omega)(-3-5\omega)}{19} = \frac{19-57\omega}{19} = 1-3\omega$$

so α divides $17+14\omega$.

2)

As $N(4+7\omega) = 37$ and $N(2+5\omega) = 19$ does not divide 37, α cannot divide $4+7\omega$.

3)

As $N(9+5\omega) = 61$ and $N(2+5\omega) = 19$ does not divide 61, α cannot divide $9+5\omega$.

4)

$$\frac{1-7\omega}{2+5\omega} = \frac{(1-7\omega)(8+7\omega)}{19} = \frac{57}{19} = 3$$

so α divides $1-7\omega$.

Exercise 2.4.1

We apply the Euclidean algorithm. Note that $N(\alpha) = 7$ and $N(\beta) = 16$. So we apply Euclidean division with β and α:

$$\begin{aligned} -4 &= (-2-\omega)(1-2\omega) - \omega \\ 1-2\omega &= (3+\omega)(-\omega) \end{aligned}$$

so a greatest common divisor is $\delta = -\omega$. We now substitute back to find x, y,

$$-\omega = -4 + (2+\omega)(1-2\omega).$$

Hence $x = 2+\omega$ and $y = 1$.

Exercise 2.4.2

Using a method identical to the previous exercise, one can find the least common divisor ω and $x = 1, y = -2-\omega$.

Exercise 2.4.3

As α and β are coprime, there exist $x, y \in \mathbb{Z}[\omega]$ such that $\alpha x + \beta y = 1$. Multiply by γ, then $\alpha\gamma x + \beta\gamma y = \gamma$. As α and β divide γ, we can write $\gamma = \alpha\rho_1 = \beta\rho_2$. Hence

$$\alpha\beta\rho_2 x + \alpha\beta\rho_1 y = \gamma$$

and since $\alpha\beta$ divides the left hand side, $\alpha\beta$ divides γ as desired.

Exercise 2.4.4

Assume that α and β are coprime to γ. Then

$$\alpha x + \gamma y = 1 \quad \text{and} \quad \beta x' + \gamma y' = 1$$

for some $x, x', y, y' \in \mathbb{Z}[\omega]$. Multiply the first equation by β on both sides and plug this expression into the next equation to obtain

$$(\alpha\beta x + \gamma\beta y)x' + \gamma y' = 1$$

and expanding and rearranging the left hand side yields

$$\alpha\beta x x' + \gamma(y' + \beta y x') = 1$$

so by the corollary to Bezout's theorem, $\alpha\beta$ and γ are coprime. We prove the converse by contraposition. Assume without loss of generality that α and γ share a divisor with norm greater than one. Then $\alpha\beta$ and γ share the same divisor, so α and β are not coprime. This completes the exercise.

Exercise 4.4.1

$N(3 + 7\omega) = 37, N(1 + 4\omega) = 13$ and $N(1 - \omega) = 3$ are all integer primes. The claim follows.

Exercise 4.4.2

An element of IJ is of the form $\alpha\beta$ with $\alpha \in I$ and $\beta \in J$. As $\alpha\beta \in I$ and $\alpha\beta \in J$, the first inclusion holds. If $\alpha \in I \cap J$, then $\alpha = \alpha + 0 \in I + J$, proving the second inclusion.

Exercise 4.4.3

Let $a, b \in I \cap \mathbb{Z}$. Then $a + b \in I$ and $a + b \in \mathbb{Z}$ so $a + b \in I \cap \mathbb{Z}$. Now let $a \in \mathbb{Z}$ and $b \in I \cap \mathbb{Z}$. As $a \in \mathbb{Z}[\omega]$ in particular, $ab \in I$ and since $ab \in \mathbb{Z}$ trivially, $ab \in I \cap \mathbb{Z}$. This shows that $I \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Exercise 4.4.4

If $I = \mathbb{Z}[\omega]$, I contains all units. Conversely, suppose I contains the unit u. Let $\alpha \in \mathbb{Z}[\omega]$. Then $\alpha = (\alpha u^{-1})u \in I$. As α was arbitrary, we must have $I = \mathbb{Z}[\omega]$.

Exercise 4.4.5

Let $\gamma \in (\alpha) + (\beta)$. Then γ can be written as $\gamma = \alpha x + \beta y$. As δ divides α and β, δ divides γ so that $\gamma = \delta\rho$ for some $\rho \in \mathbb{Z}[\omega]$. This is equivalent to $\gamma \in (\delta)$. Conversely, if $\gamma \in (\delta)$ then δ divides γ i.e. $\gamma = \delta\rho$. Using Bezout's theorem, write $\alpha x + \beta y = \delta$ and multiply by ρ to obtain

$$\alpha x\rho + \beta y\rho = \delta\rho = \gamma$$

which shows that $\gamma \in (\alpha) + (\beta)$. We have proved inclusion both ways and hence the proof is complete.

Exercise 4.4.6

(α) is a prime ideal if and only if whenever $\beta\gamma \in (\alpha)$ then $\beta \in (\alpha)$ or $\gamma \in (\alpha)$. The latter is equivalent to $\beta = \alpha\rho_1$ or $\gamma = \alpha\rho_2$ for some $\rho_1, \rho_2 \in \mathbb{Z}[\omega]$ i.e. that α divides either β or γ. But this is exactly the definition of a prime element.

Exercise 4.4.7

$(\alpha) = (\beta)$ if and only if α divides β and β divides α i.e. $\beta = \alpha\gamma$ and $\alpha = \beta\rho$ for some $\gamma, \rho \in \mathbb{Z}[\omega]$. Combining these yield $\alpha = \alpha\gamma\rho$. If $\alpha = 0$ the claim is clear so assume not. Then $\gamma\rho = 1$ i.e. they are both units and α and β are associates.

Exercise 4.4.8

We only prove the exercise for $\mathbb{Z}[\omega]$. The proof for $\mathbb{Z}$ is identical.

Let M be a maximal ideal. We need to show that M is a prime ideal. We know that $M = (\alpha)$ for some α. Let $\beta\gamma \in (\alpha)$. Assume that β is not in (α). We need to show that $\gamma \in (\alpha)$. The ideal $(\beta) + (\alpha)$ is strictly larger than (α). But (α) is maximal, so we must have $(\beta) + (\alpha) = \mathbb{Z}[\omega]$. Hence there exist $x, y \in \mathbb{Z}[\omega]$ such that $1 = \alpha x + \beta y$ i.e. α and β are coprime. Multiplying by γ gives

$$\gamma = \alpha\gamma x + \beta\gamma y \in (\alpha)$$

which proves that (α) must be prime.

Exercise 4.4.9

Let $p \equiv 1 \pmod 3$. Using quadratic reciprocity, we have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = 1$$

which proves the claim.

Exercise 4.4.10

1)
$N(3 - 7\omega) = 79$ which is prime, so $3 - 7\omega$ is a prime.

2)
$N(3 + 5\omega) = 19$ which is prime, so $3 + 5\omega$ is a prime.

3)
$1 - 4\omega$ is not a prime. Indeed, $N(1 - 4\omega) = 21$ so $1 - \omega$ is a non-trivial factor.

4)
$-3+5\omega$ is not a prime. Indeed, $N(-3+5\omega) = 49$ which is not a prime, and $-3+5\omega$ is not conjugate to an integral prime.

5)
$8 - 2\omega$ is not a prime since 2 is clearly a non-trivial factor.

6)
7ω is not a prime. Indeed, 7ω is associated to 7 and $7 \equiv 1 \pmod 3$.

7)
$-5 - 5\omega$ is prime since $-5 - 5\omega = (-1 - \omega)5$ so $-5 - 5\omega$ is associated to $5 \equiv 2 \pmod 3$.

8)
$1 + 36\omega$ is not a prime. Indeed, $N(1 + 36) = 1261 = 13 \cdot 97$ and $1 + 36\omega$ is not associated to an integral prime.

Exercise 5.5.1

We prove the remaining part by induction. The case $k = 1$ is trivial. Let $k > 1$ and assume that the statement is true for $k - 1$. Define $\alpha' = \alpha_1 \cdots \alpha_{k-1}$. As $\pi \mid \alpha_1 \cdots \alpha_k$, by the case $n = 2$ proved in the lemma, we have $\pi \mid \alpha'$ or $\pi \mid \alpha_k$. In the latter case we are done. If $\pi \mid \alpha'$, π divides at least one α_i $(i = 1, ..., k - 1)$ by the induction hypothesis. This completes the proof.

Exercise 5.5.2

We have $\overline{1 - \omega} = 1 - (-1) + \omega = 2 + \omega$. The associates of $1 - \omega$ besides $1 - \omega$ are

- $-1(1 - \omega) = -1 + \omega$,
- $\omega(1 - \omega) = \omega - \omega^2 = \omega - (-1 - \omega) = 1 + 2\omega$,
- $-\omega(1 - \omega) = -1 - 2\omega$,
- $\omega^2(1 - \omega) = \omega^2 - 1 = -1 - \omega - 1 = -2 - \omega$,
- $-\omega^2(1 - \omega) = 2 + \omega$,

and so $-\omega^2(1 - \omega) = \overline{1 - \omega}$.

Exercise 5.5.3

As δ is a divisor of α and β, we have $\alpha = \delta\rho$ and $\beta = \delta\gamma$ for some $\rho, \gamma \in \mathbb{Z}[\omega]$. Hence $\overline{\alpha} = \overline{\delta}\overline{\rho}$ and $\overline{\beta} = \overline{\delta}\overline{\gamma}$. This shows that $\overline{\delta}$ is a divisor of $\overline{\alpha}$ and $\overline{\beta}$. As $N(\delta) = N(\overline{\delta})$, $\overline{\delta}$ is a divisor of maximal norm. Indeed, if this was not the case, δ could not have maximal norm either.

Exercise 5.5.4

$N(-9 + 4\omega) = 133 = 7 \cdot 19$. Both of these primes are congruent to 1 modulo 3, so we need to come up with an Eisenstein integer π such that $N(\pi) = 7$. Testing a few values yields $\pi = 1 - 2\omega$. We know that either π or its conjugate is the correct choice. We check

$$\frac{-9 + 4\omega}{1 - 2\omega} = \frac{(-9 + 4\omega)(3 + 2\omega)}{7} = \frac{-35 - 14\omega}{7} = -5 - 2\omega,$$

and so $1 - 2\omega$ is indeed a prime factor. The remaining prime factor must be $-5 - 2\omega$ (which indeed has norm 19). We conclude that

$$-9 + 4\omega = (1 - 2\omega)(-5 - 2\omega)$$

is the prime factorization.

Exercise 5.5.5

We immediately see that $12 - 8\omega = 2^2(3 - 2\omega)$ and $3 - 2\omega$ has norm 19, so this is the prime factorization.

Exercise 5.5.6

Using techniques similar to the ones in Exercise 5.5.4, the result is seen to be $-16+\omega = (1 + \omega)(1 - \omega)(3 + 2\omega)(1 + 4\omega)$.

Exercise 5.5.7

Factoring yields $\alpha = -1(1-\omega)^3$ and $\beta = (1-\omega)(3+2\omega)$. Hence a least common multiple is $(1-\omega)^3(3+2\omega) = 3-12\omega$.

Exercise 5.5.8

Factoring yields $\alpha = (1-\omega)^2(4+\omega)$ and β is a prime different from the primes in the factorization of α. Hence a least common multiple is $\alpha\beta$.

Exercise 6.3.1

Let $\alpha', \beta' \in \mathbb{Z}[\omega]$ satisfy $[\alpha]_\gamma = [\alpha']_\gamma$ and $[\beta]_\gamma = [\beta']_\gamma$. We have $\gamma \mid \alpha - \alpha'$ and $\gamma \mid \beta - \beta'$. Hence

$$\gamma \mid \beta(\alpha - \alpha') = \alpha\beta - \alpha'\beta$$

and

$$\gamma \mid \alpha'(\beta - \beta') = \alpha'\beta - \alpha'\beta'$$

so in particular

$$\gamma \mid \alpha\beta - \alpha'\beta'$$

and thus $[\alpha\beta]_\gamma = [\alpha'\beta']_\gamma$. This shows that multiplication is independent of the choice of representative and hence well-defined.

Exercise 6.3.2

φ is a bijection since it has a two sided inverse, namely $\varphi^{-1}([\beta]_\pi) = [\alpha]_\beta^{-1}[\beta]_\pi$. $[\alpha]_\pi^{-1}$ exists since α and π are coprime.

Exercise 6.3.3

Note that $17 \equiv 2 \pmod 3$, so γ is a prime. From the proof of Theorem 6.12, a set of representatives is given by

$$\mathcal{R} = \{a + b\omega \mid 0 \leq a, b < 17\}.$$

Exercise 6.3.4

Note that $N(\gamma) = 37$ is a prime. From the proof of Theorem 6.12, a set of representatives is given by

$$\mathcal{R} = \{0, 1, ..., 36\}.$$

Exercise 6.3.5

As $\pi_1^{e_1}, ..., \pi_n^{e_n}$ are all factors of γ, $\alpha \equiv \alpha' \pmod \gamma$ implies that $\alpha \equiv \alpha' \pmod{\pi_i^{e_i}}$ for all i. Hence the map is well-defined.

Exercise 7.4.1

If $1 \equiv \omega \pmod \pi$, then $\pi \mid 1 - \omega$ and in particular, $N(\pi) \mid 3$, impossible. If $1 \equiv \omega^2 \equiv -1 - \omega \pmod \pi$ then $\pi \mid 2 + \omega$ and $N(2+\omega) = 3$ so again $N(\pi) \mid 3$ which is not possible. The remaining cases are just as easy to check.

Exercise 7.4.2

(i) By definition,

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{(N(\pi)-1)/3} \equiv \alpha^{(N(\pi)-1)/3}\beta^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3\left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}.$$

(ii) By definition,

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N(\pi)-1)/3} \equiv \beta^{(N(\pi)-1)/3} \equiv \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}.$$

Exercise 7.4.3

(i) We see that $\overline{\omega} = \omega^2$, so the claim follows since $(\alpha/\pi)_3$ can only attain the values $1, \omega$ and ω^2.

(ii) By definition,

$$\overline{\left(\frac{\alpha}{\pi}\right)_3} \equiv \overline{\alpha^{N(\pi)-1)/3}} \equiv \overline{\alpha}^{(N(\pi)-1)/3} \equiv \overline{\alpha}^{(N(\overline{\pi})-1)/3} \equiv \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3 \pmod{\pi},$$

where we used that $N(\pi) = N(\overline{\pi})$.

Exercise 7.4.4

(i) follows since $(\alpha/\lambda)_3 = 0$ if and only if a prime factor of λ divides α. (ii) and (iii) follow immediately from the fact that they hold for primes. (iv) is immediate from the definition. (v) follows from $(-1)^3 = -1$.

Exercise 7.4.5

Replace π with λ, a primary element with $3 \nmid N(\lambda)$, then the claim still holds. Indeed, it follows directly from the multiplicativity of the cubic residue symbol and the definition of the generalized cubic residue symbol.

Exercise 8.3.1

By Fermat's little theorem (in the integers), $a^3 \equiv a \pmod 3$ so $x = a$ is a solution to the equation $x^3 \equiv a \pmod 3$.

Exercise 8.3.2

Yes, choose $x = 2$ and $y = 1$. Clearly, $y = \pm 1$ is the only choice that could possibly work, and choosing x is obvious after choosing y.

We can also see this using Theorem 8.4. We have $31 \equiv 1 \pmod 3$. $31 = \pi\overline{\pi}$ for $\pi = 1 + 6\omega$, and

$$\left(\frac{2}{1+6\omega}\right)_3 = 1.$$

Exercise 8.3.3

We check the conditions of Theorem 8.4. $79 \equiv 1 \pmod 3$. We have $79 = \pi\overline{\pi}$ for $\pi = 3 - 7\omega$, and

$$\left(\frac{2}{3-7\omega}\right)_3 = \omega \neq 1,$$

so 2 is not a cubic residue modulo 79 and hence 79 is not of the desired form.