PERFECT NUMBERS IN THE RING OF EISENSTEIN INTEGERS

ZACHARY PARKER, JEFF RUSHALL, AND JORDAN HUNT

Abstract. One of the many number theoretic topics investigated by the ancient Greeks was perfect numbers, which are positive integers equal to the sum of their proper positive integral divisors. Mathematicians from Euclid to Euler investigated these mysterious numbers. We present results on perfect numbers in the ring of Eisenstein integers.

1. Introduction

The Pythagoreans, whose motto was All is Number, believed that integers possessed mystical and magical properties, which led them to thoroughly investigate the properties of our counting numbers [1]. For instance, they recognized that 6, 28, 496, and 8128 were the only positive integers less than 10,000 with the property that each was equal to the sum of its proper divisors. This can easily be verified by hand; the proper divisors of 496 are 1, 2, 4, 8, 16, 31, 62, 124, and 248, and of course

\[ 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496. \]

Greek mathematicians referred to these special integers as ideal numbers, complete numbers or perfect numbers. Over time, mathematicians chose to use the last of these labels.

Definition 1.1. A positive integer \( n \) is perfect if \( n \) is equal to the sum of its proper and positive divisors.

In Introduction to Arithmeticae (circa 100 C.E.), Nicomachus listed the first four perfect numbers, the only ones known to the ancient Greeks. Despite the fact that only a few had been discovered, Euclid, in Book IX, Proposition 36 of his classic text The Elements (c. 300 B.C.E.) gives sufficient conditions for the existence of even perfect numbers [1]. More specifically:

Theorem 1.2. Given any integer \( k > 1 \), if \( 2^k - 1 \) is prime, then \( n = 2^{k-1}(2^k - 1) \) is an even perfect number.

Leonhard Euler (C.E. 1707–1783) later proved that all even perfect numbers are of Euclid’s specified form. It is worth noting that 33,550,336, the fifth smallest perfect number, remained undiscovered until the 15th century, where it was revealed in an anonymous manuscript. To date, only 49 even perfect numbers have been found.

Integers of the form \( 2^k - 1 \), where \( k \) is a positive integer, are known as Mersenne numbers, their name derived from Marin Mersenne (C.E. 1588–1648), a monk who had achieved some renown as a number theorist. His investigation of these types of integers was partially inspired by the search for large prime numbers.

Definition 1.3. Primes of the form \( 2^k - 1 \), where \( k \) is a prime number, are known as Mersenne primes.

It is important to note that the primality of the exponent in \( 2^k - 1 \) is a necessary but not sufficient condition to guarantee the primality of the corresponding Mersenne number. For instance, the Mersenne number \( 2^{11} - 1 = 2047 \) has a prime exponent, but \( 2047 = 23 \cdot 89 \) is not prime.

As seen in the theorem above and in Euler’s subsequent result, Mersenne primes are central to the study of even perfect numbers; both objects will be generalized later in this paper.

In addition to the contributions Euler made concerning even perfect numbers, he proved the following result, which describes the possible structure of an odd perfect number.

Theorem 1.4. If \( n \) is an odd perfect number, then \( n = p^k \cdot q^2 \), where \( p \equiv 1 \) (mod 4) is an odd prime, \( k \equiv 1 \) (mod 4), and the greatest common divisor of \( p \) and \( q \) is 1.
It is unknown if any odd perfect numbers exist; exhaustive computer searches have determined that any odd perfect numbers must exceed $10^{300}$.

The rest of this paper is structured as follows: In Section 2 we give the appropriate background information from algebraic number theory needed to define the ring of Eisenstein integers, which will serve as the context in which we generalize perfect numbers and Mersenne primes. In Section 3 we will motivate the existence of Mersenne primes from a slightly different perspective, which will then allow us to rigorously define Eisenstein Mersenne primes. In Section 4, we will define an Eisenstein perfect number and present conditions for the existence of even perfect numbers in this generalized setting. Finally, in Section 5, we offer concluding remarks and suggest some open questions that require further investigation.

2. Background

As part of his Ph.D. thesis, the great Karl Friedrich Gauss (C.E. 1777–1855) proved a version of what is now referred to as the Fundamental Theorem of Algebra. As a consequence of this result, given any positive integer $n$, a polynomial of the form $x^n - 1$ has exactly $n$ solutions in the complex plane. These solutions are known as complex $n$th roots of unity, and it is well-known that they are of the form $e^{2\pi ik/n}$ for each integer value of $k$, $1 \leq k \leq n$. We may then write

$$x^n - 1 = \prod_{k=1}^{n} (x - e^{2\pi ik/n}).$$

When we restrict this sum to those values of $k$ that are relatively prime to $n$ (i.e., $k$ and $n$ share no common factors), we obtain what is known as the $n$th cyclotomic polynomial, denoted $\Phi_n(x)$. More precisely,

$$\Phi_n(x) = \prod_{(k,n)=1} (x - e^{2\pi ik/n}).$$

Cyclotomic polynomials arise in the study of various problems in field theory and algebraic number theory. We are interested exclusively in the third cyclotomic polynomial, namely $\Phi_3(x) = 1 + x + x^2$. The specific root of $\Phi_3(x)$ that will serve as a focus of this paper is this cubic complex root of unity, henceforth denoted $\omega$:

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

This leads to the following proposition.

**Proposition 2.1.** The set $\mathbb{Z}[\omega] = \{a + b \omega : a, b \in \mathbb{Z}\}$, under the usual operations of addition and multiplication of complex numbers, forms an integral domain, known as the ring of **Eisenstein integers**.

It is relatively easy to show that the Eisenstein integers form an integral domain (i.e., a commutative ring with unity having no zero divisors; a proof can be found in many abstract algebra textbooks, such as [2] and [3]). For the remainder of this paper, the term **ring** will always refer to an integral domain. To distinguish between elements of $\mathbb{Z}$ and $\mathbb{Z}[\omega]$, we will often refer to elements (or primes) in $\mathbb{Z}$ as **rational integers** (or **rational primes**).

It will be useful for us to verify the closure axiom under multiplication in $\mathbb{Z}[\omega]$, since doing so will help the reader begin to understand arithmetic in this context. Remember that our complex root of unity $\omega$ satisfies $1 + \omega + \omega^2 = 0$, and hence $\omega^2 = -1 - \omega$.

**Proposition 2.2.** The ring of Eisenstein integers is closed under multiplication.

**Proof.** Given any $a + b \omega, c + d \omega \in \mathbb{Z}[\omega]$, their product is:

$$(a + b \omega) \cdot (c + d \omega) = ac + (ad + bc) \cdot \omega + (bd) \cdot \omega^2
= ac + (ad + bc) \cdot \omega + bd \cdot (-1 - \omega)
= ac + (ad + bc) \cdot \omega - bd - (bd) \cdot \omega
= (ac - bd) + (ad + bc - bd) \cdot \omega.$$
Since \( \mathbb{Z} \) is closed under both addition and multiplication, it then follows that \( \mathbb{Z}[\omega] \) is closed under multiplication.  

We will now present several ring-based definitions that are necessary stepping stones toward understanding objects in our particular ring, \( \mathbb{Z}[\omega] \). Each are familiar versions of objects and processes in \( \mathbb{Z} \).

**Definition 2.3.** Let \( \alpha \) and \( \beta \) be elements in a ring \( R \). We say that \( \alpha \) divides \( \beta \), written \( \alpha \mid \beta \), if there exists some \( \gamma \in R \) such that \( \alpha \cdot \gamma = \beta \).

**Definition 2.4.** An element \( \alpha \) in a ring \( R \) is a unit if it has a multiplicative inverse – that is, if there exists some \( \beta \in R \) such that \( \alpha \cdot \beta = 1 \).

**Definition 2.5.** An element \( \alpha \) of a ring \( R \) is prime if, whenever \( \alpha \mid \beta \gamma \) for some \( \beta, \gamma \in R \), then either \( \alpha \mid \beta \) or \( \alpha \mid \gamma \).

A visual depiction of \( \mathbb{Z}[\omega] \) appears in Figure 1, which shows a selection of Eisenstein integers: The units are pink, the origin dark blue, and random integers light blue.

![Figure 1](image_url)

An important tool used to study \( \mathbb{Z}[\omega] \) is the norm function. Informally, one may think of the norm function as a kind of “measuring the distance from the origin” device, not unlike the role the absolute value function plays over \( \mathbb{R} \).

**Definition 2.6.** Given any \( \alpha = a + b\omega \) in \( \mathbb{Z}[\omega] \), the norm function \( N : \mathbb{Z}[\omega] \to \mathbb{Z} \) is defined as

\[
N(\alpha) = a^2 - ab + b^2.
\]

The norm function possesses some useful qualities. First, the function always provides a nonnegative integer output, and in fact takes on nonzero values at all nonzero Eisenstein integers. We leave it to the curious reader to verify this fact. Second, the norm function is completely multiplicative, as shown in the following lemma.
Lemma 2.7. If \( \alpha, \beta \in \mathbb{Z}[\omega] \), then \( N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) \).

Proof. Let \( \alpha = a + b\omega \) and \( \beta = c + d\omega \). Then:

\[
N(\alpha \cdot \beta) = N((a + b\omega) \cdot (c + d\omega)) \\
= N((ac - bd) + (ad + bc - bd)\cdot \omega) \\
= [ac - bd]^2 - [ac - bd][ad + bc - bd] + [ad + bc - bd]^2 \\
= a^2c^2 - 2abcd + b^2d^2 - [a^2cd + abc^2 - abcd - bad^2 - b^2cd + b^2d^2] \\
+ [a^2d^2 + abcd - abd^2 + abcd + b^2c^2 - b^2cd - abd^2 - b^2cd + b^2d^2] \\
= a^2c^2 - a^2cd + a^2d^2 - abc^2 + abcd - abd^2 + b^2c^2 - b^2cd + b^2d^2 \\
= a^2(c^2 - cd + d^2) - ab(c^2 - cd + d^2) + b^2(c^2 - cd + d^2) \\
= (a^2 - ab + b^2)(c^2 - cd + d^2) \\
= N(\alpha)N(\beta). 
\]

Using the norm function, it can be shown that \( \mathbb{Z}[\omega] \) is a Euclidean ring. A key step in this proof is verifying that the norm function imposes enough structure on \( \mathbb{Z}[\omega] \) to allow for something akin to the division algorithm to exist. Specifically, one needs the following result, whose proof can be found in many sources, such as [2].

Proposition 2.8. If \( \alpha, \beta \in \mathbb{Z}[\omega], \beta \neq 0 \), there exist \( \gamma, \delta \in \mathbb{Z}[\omega] \) that satisfy \( \alpha = \gamma \beta + \delta \), and such that \( N(\delta) < N(\beta) \).

Since \( \mathbb{Z}[\omega] \) is a Euclidean ring, it is also a principal ideal domain and hence a unique factorization domain, a chain of implications that is discussed in most abstract algebra textbooks (see, for instance, [4]). Naturally, we must now determine those elements of \( \mathbb{Z}[\omega] \) that are units; we leave verification of the next result to the curious reader.

Proposition 2.9. An element \( \alpha \) of \( \mathbb{Z}[\omega] \) is a unit if and only if \( N(\alpha) = 1 \).

It then follows that the only units of \( \mathbb{Z}[\omega] \) are \( \{\pm 1, \pm \omega, \pm \omega^2\} \). In any given ring, elements that differ only via multiplication by a unit are known as associates. Thus, every element in \( \mathbb{Z}[\omega] \) has six different associates. Later in this section, we will show how to select the appropriate associate to allow our generalizations in \( \mathbb{Z}[\omega] \) of perfect numbers to be well-defined. This complete classification of units in \( \mathbb{Z}[\omega] \) can be used to help determine when a given element in the ring of Eisenstein integers is prime.

Proposition 2.10. Let \( \alpha \in \mathbb{Z}[\omega] \). If \( N(\alpha) \) is a rational prime in the integers, then \( \alpha \) is prime in the Eisenstein integers.

Proof. Let \( \alpha \in \mathbb{Z}[\omega] \). Assume \( N(\alpha) \) is prime and suppose \( \alpha = \beta \cdot \gamma \) for some \( \beta, \gamma \in \mathbb{Z}[\omega] \). Then:

\[
N(\alpha) = N(\beta \cdot \gamma) \\
= N(\beta) \cdot N(\gamma). 
\]

Because \( N(\alpha) \) is by assumption an integer prime, we may assume without loss of generality that \( N(\beta) = 1 \). Thus, \( \beta \) is a unit, which implies that \( \alpha \) and \( \gamma \) are associates, and the result follows. \( \square \)

It follows directly from the definitions and prior results that if \( \alpha \) and \( \gamma \) are associates in \( \mathbb{Z}[\omega] \), then \( N(\alpha) = N(\gamma) \). This is another property of the norm function that mimics the absolute value function over \( \mathbb{R} \), and will be important in later sections.
Example 2.11. The Eisenstein integer $1 - \omega$ is a prime in $\mathbb{Z}[\omega]$. This follows by simply applying our previous proposition:

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

which is prime in $\mathbb{Z}$. We leave it to the curious reader to verify that, up to multiplication by a unit, $1 - \omega$ is the prime of minimal norm value in $\mathbb{Z}[\omega]$.

The following lemma completely determines which integer primes remain prime in $\mathbb{Z}[\omega]$; a formal proof may be found in [2].

**Proposition 2.12.** Let $p$ be prime in $\mathbb{Z}$.

- If $p = 3$, then $p$ is not prime in $\mathbb{Z}[\omega]$.
- If $p \equiv 1$ (mod 3), there exists a prime $\pi \in \mathbb{Z}[\omega]$ such that $p = \pi \overline{\pi}$, where $\overline{\pi}$ denotes the complex conjugate of $\pi$.
- If $p \equiv 2$ (mod 3), then $p$ remains prime in $\mathbb{Z}[\omega]$.

This proposition highlights some of the fundamental computational differences between $\mathbb{Z}$ and $\mathbb{Z}[\omega]$. For instance, observe that $3 = -\omega^2 \cdot (1 - \omega)^2$ (the reader may easily verify this statement). Consequently, the rational prime 3, having a nontrivial factorization in the ring of Eisenstein integers, is no longer prime in $\mathbb{Z}[\omega]$. Similarly, note that $7 \equiv 1$ (mod 3), and that $7 = -\omega^2 \cdot (2 - \omega)^2$. Thus, the rational prime 7 is not a prime in $\mathbb{Z}[\omega]$.

Another useful and necessary generalization from $\mathbb{Z}$ to $\mathbb{Z}[\omega]$ is that of evenness. As with the rational integers, we classify evenness in the Eisenstein integers via divisibility by a prime, specifically $1 - \omega$.

**Definition 2.13.** An element $a + b\omega \in \mathbb{Z}[\omega]$ is even if it is divisible by $1 - \omega$ - that is, if there exists some $c + d\omega \in \mathbb{Z}[\omega]$ such that $a + b\omega = (1 - \omega)(c + d\omega)$. Any element of $\mathbb{Z}[\omega]$ that is not divisible by $1 - \omega$ is said to be odd.

The reason for the reliance on $1 - \omega$ for determining evenness in $\mathbb{Z}[\omega]$ will be made clear in the next section. The following contains an easy computational test for verifying evenness in the Eisenstein sense.

**Theorem 2.14.** An Eisenstein integer $a + b\omega$ is even if and only if $a + b \equiv 0$ (mod 3).

**Proof.** Suppose $a + b\omega$ is even. We may then write $a + b\omega = (1 - \omega)(c + d\omega)$ for some $c + d\omega \in \mathbb{Z}[\omega]$. Simplifying yields

$$(a + b\omega) = (1 - \omega) \cdot (c + d\omega) = c + d\omega - c\omega - d\omega^2 = c + d\omega - c\omega + d + d\omega = (c + d) + (2d - c)\omega.$$

We must now consider the nine possible pairs of congruence classes modulo 3 to which $c$ and $d$ belong:

- If $c \equiv d \equiv 0$ (mod 3), it then easily follows that $a \equiv b \equiv 0$ (mod 3), and hence $a + b \equiv 0$ (mod 3).
- If $c \equiv 0$ (mod 3) and $d \equiv 1$ (mod 3), it again follows that $a \equiv 1$ (mod 3) and $b \equiv 2$ (mod 3), and hence $a + b \equiv 0$ (mod 3).
- If $c \equiv 0$ (mod 3) and $d \equiv 2$ (mod 3), it again follows that $a \equiv 2$ (mod 3) and $b \equiv 1$ (mod 3), and hence $a + b \equiv 0$ (mod 3).

The remaining cases are similar and left to the reader. Thus, if $a + b\omega$ is even, then $a + b \equiv 0$ (mod 3). For the reverse direction, suppose that $a + b \equiv 0$ (mod 3). As above, we consider the nine possible pairs of congruence classes modulo 3 to which $a$ and $b$ belong.
Lemma 2.15. An Eisenstein integer $a + b\omega$ is even if and only if $N(a + b\omega) \equiv 0 \pmod{3}$.

Proof. Assume $a + b\omega$ is even, say, $a + b\omega = (1 - \omega)(c + d\omega)$ for some $c + d\omega$. Then by our previous work, we have that

$$N(a + b\omega) = N((1 - \omega)(c + d\omega)) = N(1 - \omega)N(c + d\omega) = (1^2 - 1)(-1 + (-1)^2)(N(c + d\omega)) = 3\cdot N(c + d\omega) \equiv 0 \pmod{3}.$$ 

On the other hand, if $N(a + b\omega) \equiv 0 \pmod{3}$, then a simple case-by-case check, as seen in the proof of Theorem 2.14, shows that all such elements $a + b\omega$ are divisible by $1 - \omega$, and the result follows. \qed

This result, together with the fact that the norm function $N$ only achieves integer values that are congruent to 0 or 1 modulo 3, leads directly to the following corollary.

Corollary 2.16. An Eisenstein integer $a + b\omega$ is not even if and only if $N(a + b\omega) \equiv 1 \pmod{3}$.

3. The $\sigma$ Function and Mersenne Primes in $\mathbb{Z}[\omega]$

An important number theoretic tool that can be extended from $\mathbb{Z}$ to $\mathbb{Z}[\omega]$ and will be useful for our purposes is the classic sum of divisors function.

Definition 3.1. Given any $n \in \mathbb{Z}$, the sum of divisors function $\sigma(n)$ denotes the sum of positive factors of $n$. That is,

$$\sigma(n) = \sum_{d|n} d.$$ 

It should be noted that perfect numbers are positive integer solutions to the equation $\sigma(n) = 2n$. The sum of divisors function has several useful and well-known properties, including those in the next proposition, whose proof is left to the reader.

Proposition 3.2. Let $p$ be a prime and $n$ be any integer. Then:

- $\sigma(p) = p + 1$
- $\sigma(p^n) = \frac{p^{n+1} - 1}{p - 1}$
- If $m$ and $n$ are relatively prime, then $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$.

In particular, note that $\sigma(n)$ is multiplicative. A direct consequence of these properties is that we can compute the value of $\sigma(n)$ at every positive integer $n$. That is, writing $n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ where $p_1, \ldots, p_s$ are distinct primes and $\alpha_1, \ldots, \alpha_s$ are positive integers, then
\[
\sigma(n) = \sigma(p_1^{a_1}) \cdot \sigma(p_2^{a_2}) \cdot \ldots \cdot \sigma(p_s^{a_s}) \\
= \frac{p_1^{a_1 + 1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2 + 1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_s^{a_s + 1} - 1}{p_s - 1} \\
= \prod_{j=1}^{s} \frac{p_j^{a_j + 1} - 1}{p_j - 1}.
\]

To extend \(\sigma\) to a well-defined function \(\sigma^*\) on \(\mathbb{Z}[\omega]\), we take advantage of the fact that the ring of Eisenstein integers features unique factorization, together with the geometric properties inherent in the multiplication of complex numbers. More precisely, recall that every Eisenstein integer \(\alpha\) has six associates, since there are six units in \(\mathbb{Z}[\omega]\). Initially, one has the freedom to select any of these six associates to serve as the representative when computing something akin to a sum of divisors in \(\mathbb{Z}[\omega]\). However, the \(\sigma\)-function features the property that \(\sigma(n) \geq n\) for every \(n \in \mathbb{N}\). Thus, it would be advantageous to pick a particular associate \(\alpha'\) of \(\alpha\) that satisfies

\[N(\sigma^*(\alpha')) \geq N(\alpha').\]

The associates that satisfy this inequality are precisely those located in our shaded region of the complex plane, as indicated in Figure 2. We may assume without loss of generality that the shaded region in Figure 2 contains the Eisenstein integers located on the lower boundary (and not the upper boundary). Note that this shaded region contains the Eisenstein integer \(a + b\omega\) if and only if \(a > b \geq 0\).

![Figure 2](image_url)

Using these particular associates in \(\mathbb{Z}[\omega]\) allows us to generalize \(\sigma(n)\) in a well-defined manner. Moreover, selecting these particular prime associates in \(\mathbb{Z}[\omega]\) allows, among other things, for \(\mathbb{Z}[\omega]\) to contain all primes in \(\mathbb{Z}\) that remain prime in \(\mathbb{Z}[\omega]\). Consequently, we may think of \(\sigma^*\) as being an extension of \(\sigma\) from \(\mathbb{Z}\) to \(\mathbb{Z}[\omega]\).
Let $\nu \in \mathbb{Z}[\omega]$ be arbitrary. Via unique factorization in $\mathbb{Z}[\omega]$ and without loss of generality, $\nu$ can be written as

$$\nu = \epsilon \prod_{q=1}^{s} \pi_{q}^{k_{q}},$$

where $\epsilon$ is a unit, each $\pi_{q}$ is a prime in the shaded section of Figure 2 and each $k_{q}$ is a positive integer. For the rest of this paper, we will assume that all prime factorizations of elements in $\mathbb{Z}[\omega]$ are of this form. We can now define the complex sum of divisors function $\sigma^{*}(\nu)$ in the following manner.

**Definition 3.3.** Given any $\nu = \epsilon \prod_{q=1}^{s} \pi_{q}^{k_{q}}$ in $\mathbb{Z}[\omega]$, the expression $\sigma^{*}(\nu)$, the complex sum of divisors function evaluated at $\nu$, is defined as

$$\sigma^{*}(\nu) = \prod_{q=1}^{s} \frac{\pi_{q}^{k_{q}+1} - 1}{\pi_{q} - 1}.$$

Note that if $\nu \in \mathbb{Z}[\omega]$ has no imaginary part, then $\nu \in \mathbb{Z}$, in which case the definition of $\sigma^{*}$ is equivalent to that of $\sigma$ in $\mathbb{Z}$. Moreover, $\sigma^{*}$ is multiplicative over $\mathbb{Z}[\omega]$, a property that will play a key role when attempting to define perfect numbers in $\mathbb{Z}[\omega]$.

We will now generalize the concepts of Mersenne numbers and Mersenne primes from the rational integers to $\mathbb{Z}[\omega]$. To begin, we first give a somewhat different motivation for the structure of Mersenne primes.

Consider the expression $b^{n} - 1$, where $n$ is any positive integer and, for the moment, assume that $b \in \mathbb{Z}$. Because $b^{n} - 1 = (b - 1)(b^{n-1} + b^{n-2} + \cdots + b + 1)$, in order for $b^{n} - 1$ to be prime in $\mathbb{Z}$, exactly one of $b - 1$ and $b^{n-1} + b^{n-2} + \cdots + b + 1$ must be a unit in $\mathbb{Z}$. As Pershell and Huff demonstrate in [6], this is only possible when $b - 1$ is a unit – that is, when $b - 1 = \pm 1$, in which case $b = 0$ or $b = 2$. Clearly, $b = 0$ yields no prime, and so only the $b = 2$ case is worth pursuing.

Now consider the expression $b^{n} - 1$, but assume that $b \in \mathbb{Z}[\omega]$. Once again, in order for $b^{n} - 1$ to be prime in $\mathbb{Z}[\omega]$, exactly one of $b - 1$ and $b^{n-1} + b^{n-2} + \cdots + b + 1$ must be one of the six units in $\mathbb{Z}[\omega]$. There are four possibilities:

- If $b - 1 = \pm 1$, we again find that $b = 2$ or $b = 0$. The former yields rational Mersenne primes, while the latter yields no primes.
- If $b - 1 = \omega$, then $b = 1 + \omega = -\omega^{2}$, which is a unit, and the corresponding expression $b^{n} - 1$ yields only the primes $\omega - 1$ and $\omega^{2} - 1$.
- If $b - 1 = \omega^{2}$, then $b = 1 + \omega^{2} = -\omega$, which is a unit, and again the corresponding expression $b^{n} - 1$ yields only two primes, which are complex conjugates of the last case.
- Finally, if $b - 1 = -\omega$, then $b = 1 - \omega$ (the case where $b - 1 = -\omega^{2}$ differs only by multiplication by a unit, and yields no new information). This particular case requires further investigation.

As demonstrated in [6], when considering the possibility of $b^{n-1} + b^{n-2} + \cdots + b + 1$ being a unit, no new information is gleaned. Thus, the expression $b^{n} - 1$ can only be prime in $\mathbb{Z}[\omega]$ when $b = 1 - \omega$. The curious reader can refer to the aforementioned work by Pershell and Huff for more information.

It is for these reasons that the prime 2 plays a key role when defining a Mersenne prime in $\mathbb{Z}$, and why $1 - \omega$ should play the same role when attempting to generalize Mersenne primes to $\mathbb{Z}[\omega]$. Moreover, since the prime of smallest norm in $\mathbb{Z}[\omega]$ is $1 - \omega$, it seems reasonable to use $1 - \omega$ in this context. Consequently, the following definitions should come as no surprise.

**Definition 3.4.** Given any positive rational integer $k$, an **Eisenstein Mersenne number**, denoted $M_{k}$, is an element of $\mathbb{Z}[\omega]$ of the form $(1 - \omega)^{k} - 1$, and an **Eisenstein Mersenne prime** is a prime in $\mathbb{Z}[\omega]$ of the form $(1 - \omega)^{p} - 1$ where $p$ is a prime in $\mathbb{Z}$.

Below we provide examples of both prime and non-prime Eisenstein Mersenne numbers. Note the role that the norm function plays in these verifications.
Example 3.5. Let $k = 2$ (which of course is prime in $\mathbb{Z}$) in the definition of an Eisenstein Mersenne number. The resulting expression simplifies to

$$M_2 = (1 - \omega)^2 - 1$$
$$= (1 - 2\omega + \omega^2) - 1$$
$$= -2\omega + \omega^2$$
$$= -2\omega - 1 - \omega$$
$$= -1 - 3\omega.$$

We now compute the norm of this simplified Eisenstein integer:

$$N(-1 - 3\omega) = (-1)^2 - (-1)(-3) + (-3)^2$$
$$= 1 - 3 + 9$$
$$= 7.$$

Because 7 is prime in $\mathbb{Z}$, we know via Lemma 2.7 that $M_2 = (1 - \omega)^2 - 1$ is prime in $\mathbb{Z}[\omega]$ and hence is an Eisenstein Mersenne prime.

Example 3.6. Let $k = 3$ in the definition of an Eisenstein Mersenne number. Then

$$M_3 = (1 - \omega)^3 - 1$$
$$= (1 - 3\omega + 3\omega^2 - \omega^3) - 1$$
$$= -3\omega + 3\omega^2 - \omega^3$$
$$= -3\omega - 3 - 3\omega - 1$$
$$= -4 - 6\omega.$$

Since both coefficients are even rational integers, it is clear that this Eisenstein integer can be factored in a nontrivial way in $\mathbb{Z}[\omega]$. But the norm function also verifies this:

$$N(-4 - 6\omega) = (-4)^2 - (-4)(-6) + (-6)^2$$
$$= 16 - 24 + 36$$
$$= 28.$$

As a result, the Eisenstein Mersenne number $M_3 = (1 - \omega)^3 - 1$ is not prime in $\mathbb{Z}[\omega]$.

Eisenstein Mersenne primes are in some sense even rarer than Mersenne primes in $\mathbb{Z}$. For instance, there are 12 rational primes of the form $2^n - 1$ with $n \leq 160$, but only 7 Eisenstein Mersenne primes exist in the same exponent range, namely $n = 2, 5, 7, 11, 17, 19$ and 79. The curious reader may consult [6] for more information.

Observe that the exponent in the expression $(1 - \omega)^k - 1$ is necessarily prime in $\mathbb{Z}$; if it were not, $(1 - \omega)^k - 1$ would have, as is the case with Mersenne numbers in $\mathbb{Z}$, at least one nontrivial factor. It is also important to reiterate that having a prime exponent in the expression $(1 - \omega)^k - 1$ is a necessary but not sufficient condition to guarantee the primality of the corresponding Eisenstein Mersenne number.
4. Perfect Numbers in $\mathbb{Z}[\omega]$

Recall that a perfect number is a positive integer $n$ such that $\sigma(n) = 2n$. The use of our complex sum-of-divisors function $\sigma^*$ allows us to generalize perfect numbers in a seemingly natural way from $\mathbb{Z}$ to $\mathbb{Z}[\omega]$.

**Definition 4.1.** An Eisenstein integer $\alpha$ is said to be perfect if $\sigma^*(\alpha) = (1 - \omega) \cdot \alpha$.

This characterization of perfectness in the Eisenstein integers seems both logical and appropriate. But as others, such as Spira in [7] and McDaniel in [5] have noted, this particular generalization of perfect numbers, while natural to consider, is somewhat limited. Using a norm function, both Spira and McDaniel gave an alternative definition of perfect numbers in $\mathbb{Z}[i]$, the ring of Gaussian integers. We follow suit, noting that $1 - \omega$ is the prime of minimal norm in $\mathbb{Z}[\omega]$, and in fact $N(1 - \omega) = 3$.

**Definition 4.2.** An Eisenstein integer $\alpha$ is said to be norm–perfect if $N(\sigma^*(\alpha)) = 3 \cdot N[\alpha]$.

A moment’s thought reveals that every perfect Eisenstein integer is in fact a norm–perfect Eisenstein integer. Regardless of which definition we choose to investigate, one key point must be addressed. Namely, in Euclid’s proof of the structure of even perfect numbers in $\mathbb{Z}$, we find the following:

$$\sigma(2^k - 1) = 2^k - 1 + 1 = 2^k$$

This statement is valid, of course, because the expression $2^k - 1$ is a Mersenne prime. However, in our generalized context, the complex sum of divisors function $\sigma^*$ requires inputs that are specific associates, namely, those that live in our region as depicted in Figure 2. More precisely, we hope that the following computation is correct:

$$\sigma^*((1 - \omega)^p - 1) = (1 - \omega)^p - 1 + 1 = (1 - \omega)^p$$

This computation is only valid, however, if the Eisenstein Mersenne prime in question is the correct associate. In order to verify if this is the case, we must analyze expressions of the form $(1 - \omega)^p$ to determine the values of $p$ that result in $M_p$ belonging to our region of usable associates. In what follows, we rewrite $(1 - \omega)^p$ as $a + b\omega$, where $a$ and $b$ are rational integers, and $h = \lfloor \frac{p}{12} \rfloor$. Due to the periodic behavior of $a$ and $b$ as $p$ increases, we need only consider the values of $p$ modulo 12, which are given in the top row of the table.

**Table 1. Values of $a$ and $b$ such that $(1 - \omega)^p = a + b\omega$**

| $p$ | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 |
|-----|----|----|----|----|----|----|----|----|----|----|----|----|
| $a$ | 3$^h$ | 0  | $-3^h$ | $-3^h$ | $-2 \cdot 3^h$ | $-3^h$ | $-3^h$ | 0  | $3^h$ | $3^h$ | $2 \cdot 3^h$ | $3^h$ |
| $b$ | $-3^h$ | $-3^h$ | $-2 \cdot 3^h$ | $-3^h$ | $-3^h$ | 0  | $3^h$ | $3^h$ | $2 \cdot 3^h$ | $3^h$ | $3^h$ | 0  |

It is clear that the only values of $p$ which result in the corresponding Eisenstein Mersenne prime being the appropriate associate are $p \equiv 11 \pmod{12}$.

Classifying perfect numbers in $\mathbb{Z}[\omega]$ using the norm–perfect approach suits our purposes well. Note that the structure of the even norm–perfect Eisenstein integer $\alpha$ in the next result parallels the characterization of even perfect numbers that first appeared in the works of Euclid.

**Theorem 4.3.** Given any rational integer $k > 1$, if $(1 - \omega)^k - 1$ is an Eisenstein Mersenne prime and if $k \equiv 11 \pmod{12}$, then $\alpha = (1 - \omega)^k - 1 [(1 - \omega)^k - 1]$ is an even norm–perfect Eisenstein integer.

**Proof.** To begin, we will simplify the expression $N[\sigma^*(\alpha)]$ by using the multiplicative property of $\sigma^*$:

$$N[\sigma^*(\alpha)] = N[\sigma^* (((1 - \omega)^k - 1) \cdot (1 - \omega)^{k-1})]$$

$$= N[\sigma^* ((1 - \omega)^{k-1}) \cdot \sigma^* ((1 - \omega)^k - 1)]$$
Next, we exploit the fact that the inputs to $\sigma^*$ are a prime power and an Eisenstein Mersenne prime, respectively, together with the multiplicativity of the norm function.

$$N \left[ \sigma^* \left( (1 - \omega)^{k-1} \right) \cdot \sigma^* \left( (1 - \omega)^{k} - 1 \right) \right] = N \left[ \frac{(1 - \omega)^k - 1}{1 - \omega - 1} \cdot \left( (1 - \omega)^k - 1 + 1 \right) \right]$$

$$= N \left[ \frac{(1 - \omega)^k - 1}{1 - \omega - 1} \right] \cdot N \left[ (1 - \omega)^k - 1 + 1 \right]$$

$$= N \left[ \frac{-1}{\omega} \cdot \left( (1 - \omega)^k - 1 \right) \right] \cdot N \left[ (1 - \omega)^k \right]$$

$$= N \left[ \frac{-1}{\omega} \right] \cdot N \left[ (1 - \omega)^k - 1 \right] \cdot N \left[ (1 - \omega)^k \right]$$

Our desired result now easily follows from the fact that $-\omega^2$ is a unit, together with properties of the norm function:

$$N \left[ \frac{-1}{\omega} \right] \cdot N \left[ (1 - \omega)^k - 1 \right] \cdot N \left[ (1 - \omega)^k \right] = N \left[ -\omega^2 \right] \cdot N \left[ \left( (1 - \omega)^k - 1 \right) \cdot (1 - \omega)^k \right]$$

$$= N \left[ \left( (1 - \omega)^k - 1 \right) \cdot (1 - \omega)^{k-1} (1 - \omega) \right]$$

$$= N \left[ (1 - \omega) \right] \cdot N \left[ \left( (1 - \omega)^k - 1 \right) \cdot (1 - \omega)^{k-1} \right]$$

$$= N \left[ 1 - \omega \right] \cdot N \left[ \alpha \right]$$

$$= 3 \cdot N \left[ \alpha \right].$$

\[ \square \]

5. Future work

We have been unable to show that every even norm-perfect Eisenstein integer is of the form given in Theorem 4.3, but we suspect that this is indeed the case, in part because an extensive computer search using Mathematica has to date failed to find any other types of even norm-perfect Eisenstein integers.

Similarly, we have failed to find even a single odd norm-perfect Eisenstein integer. But if such an object exists, we believe it satisfies the following.

Conjecture 5.1. Any odd norm–perfect Eisenstein integer $\alpha$ must be of the form $\alpha = \pi^k \gamma^3$, where $\pi$ and $\gamma$ are both odd Eisenstein integers, $\pi$ is an odd prime, $k \equiv 2 \pmod{3}$, and $\pi$ and $\gamma$ share no common non-unit factors.

References

[1] David M. Burton, The History of Mathematics: An Introduction, third ed., Wm. C. Brown Publishers, Dubuque, 1995.
[2] David Cox, Primes of the Form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, Wiley, New York, 2013.
[3] David S. Dummit and Richard M. Foote, Abstract Algebra, third ed., Wiley, New York, 2004.
[4] Serge Lang, Algebra, third ed., Springer, New York, 2002.
[5] Wayne L. McDaniel, Perfect Gaussian Integers, ACTA Arithmerica XXV (1974), 137–144.
[6] K Pershell and L Huff, Mersenne Primes in Imaginary Quadratic Number Fields, (2002).
[7] Robert Spira, The Complex Sum of Divisors, The American Mathematical Monthly 68 (1961), no. 2, 120–124.