Primality Proving Based on Eisenstein Integers

By
Miaoqing Jia

****

Submitted in partial fulfillment
of the requirements for
Honors in the Department of Mathematics

UNION COLLEGE
June 2016

Abstract

JIA, MIAOQING Primality Proving Based on Eisenstein Integers.

Department of Mathematics, June 2016

ADVISOR: Kathryn Lesh

According to the Berrizbeitia theorem, a highly efficient method for certifying the primality of an integer $N \equiv 1 \pmod 3$ can be created based on pseudocubes in the ordinary integers $\mathbb{Z}$. In 2010, Williams and Wooding moved this method into the Eisenstein integers $\mathbb{Z}[\omega]$ and defined a new term, Eisenstein pseudocubes. By using a precomputed table of Eisenstein pseudocubes, they created a new algorithm in this context to prove primality of integers $N \equiv 1 \pmod 3$ in a shorter period of time. We will look at the Eisenstein pseudocubes and analyze how this new algorithm works with the Berrizbeitia theorem.

Contents

1 Introduction **1**

2 Unique Factorization **3**

3 The Eisenstein Integers **7**

4 Cubic Reciprocity **12**

5 Congruence Criteria for Eisenstein Pseudocubes **21**

6 Eisenstein Pseudocubes and Primality Testing **30**

1 Introduction

This paper introduces an improved primality test with Eisenstein Pseudocubes created by Wooding and Williams [10]. A primality test is an algorithm that is used to determine whether or not an integer N is prime. In this paper, we focus on integers N that are congruent to 1 mod 3.

The subject of primality testing is important because public key cryptosystems, in particular the RSA cryptosystem, depend heavily on the use of prime numbers in their keys. The RSA cryptosystem, designed by Ron Rivest, Adi Shamir, and Leonard Adleman [6], is one of the first practical public-key cryptosystems and is still widely used for secure data transmission. The RSA algorithm involves a public key and a private key for encrypting and decrypting messages. As indicated in the meaning of the words, the public key is known by everyone and is used for encrypting messages. An encrypted message can only be decrypted in a reasonable amount of time using the private key.

In the RSA cryptosystem, the public key consists of the modulus n, which is the product of two distinct secret primes p and q, and the public exponent e. The private key consists of the same modulus n and the private exponent d, which is determined using the secret values of p and q. Suppose there are two people, Alice and Bob. Bob would like to send a message to Alice by using the public key provided by Alice, n and e. If p and q are easily-guessed primes, then someone else will be able to figure out the values of p and q and thus decrypt the message. Therefore, in order to ensure the security of the RSA cryptosystem, it is necessary for Alice to use large, randomly-chosen prime numbers p and q.

Instead of choosing a prime number from a list of all prime numbers, cryptographers generate a random integer N and apply primality testing to determine whether or not N is prime. Thus, primality testing plays a significant role in the creation of the encryption and decryption keys.

The most common used primality tests are probabilistic tests, which can determine that a random integer is definitely not prime, or estimate the probability that it is. The Miller-Rabin [5] and the Solovay-Strassen [7] tests are two typical probabilistic primality tests. The algorithm for the Miller-Rabin primality test proceeds as follows. Suppose $N = 2^r s + 1$ is an odd integer where r and s are both positive integers and s is odd. Pick a random integer a where $1 \leqslant a \leqslant n-1$. If $a^s \equiv 1 \pmod{N}$, then N could be prime. If $a^s \not\equiv 1 \pmod{N}$ but $a^{2^r i} \equiv -1 \pmod{N}$ holds for some $i < s$, then N could be prime. Otherwise, N is composite. The running time of the Miller-Rabin primality test is $O(k(\log N)^3)$ where k is the number of different values of a we test. Furthermore, the probability an integer N is prime in this primality test is $1 - \frac{1}{4^k}$.

The Solovay-Strassen primality test, developed by Robert M. Solovay and Volker Strassen, determines whether an integer n is composite or probably prime. The algorithm for Solovay-Strassen primality test depends on the Jacobi symbol and Euler's Criterion. Specifically, it proceeds as follows: given an odd number N, if $a^{(N-1)/2} \not\equiv \left(\frac{a}{N}\right) \pmod{N}$ holds for some a, then N is composite. If for a randomly chosen value of a we have $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{N}$, then there is 50% chance that N is prime. The running time of the Solovay-Strassen primality test is still $O(k(\log N)^3)$, where k is the number of different values of a we test. However, the probability an integer N is prime in this primality test is $1 - \frac{1}{2^k}$, smaller than that of the Miller-Rabin primality test.

Instead of proving that N is a prime number, the probabilistic primality test only determines a probability that an integer N is prime. Thus, some cryptographers use deterministic

primality proving algorithms to actually prove whether an integer N is prime. The AKS primality test [1], known as the Agrawal-Kayal-Saxena primality test, is an example of deterministic primality proving. Based on the theorem that an integer $N \geqslant 2$ is prime if and only if the polynomial congruence relation $(x+a)^N \equiv (x^N + a) \pmod{N}$ holds for some a coprime to N, the running time for this algorithm is $O((\log N)^6)$.

Although deterministic primality proving proves the primality of an integer N directly, its algorithms spend relatively longer times than those of probabilistic primality testing. Instead of computing the primality of an integer N directly, some cryptographers came up with strategies that involve some precomputations in order to save more time. For example, in 1996, Lukes [4] created a primality test that used a precomputed table of pseudosquares. In particular, based on the precomputed table, the running time of this primality proving is $O((\log N)^{3+o(1)})$, far less than $O((\log N)^6)$.

Several years later, Berrizbeitia [2] introduced a more efficient primality test that relied on a precomputed table of pseudocubes. However, because this the size of this precomputed table is relatively large, this method cannot be used practically. Thus, Wooding and Williams [10] proposed an alternate definition of pseudocube, the Eisenstein pseudocube, based on Eisenstein integers. According to their conjecture, they believed that the size of the precomputed table of Eisenstein pseudocubes is relatively smaller than that of the precomputed table of ordinary pseudocubes. Therefore, the primality test based on this precomputed table has an even shorter running time than the one proposed by Berrizbeitia. Thus, this paper focuses on deterministic primality proving based on Eisenstein psedocubes and explains how this primality test works with the Berrizbeitia theorem. Before introducing the algorithm of this primality test, we will first introduce the Berrizbeitia theorem.

Berrizbeitia Theorem. [2] Let $\nu = a + b\omega$ be a primary element of $\mathbb{Z}[\omega]$, where $\gcd(a,b) = 1$, ν is not a unit, prime, or perfect power in $\mathbb{Z}[\omega]$, and $\mathbf{N}(\nu) < \mathbf{N}(\mu_p)$. Suppose integer $N \equiv 1 \pmod{3}$. Then there must exist a rational prime $q \leqslant p$ such that $\left(\frac{q}{\nu}\right)_3 \not\equiv q^{\frac{N-1}{3}} \pmod{\nu}$.

With a precomputed table of Eisenstein pseudocubes, this algorithm operates in the following way to test the primality of an integer N congruent to 1 mod 3:

1. Test that N is not a perfect power.
2. Find a primary $\nu \in \mathbb{Z}[\omega]$, such that $\mathbf{N}(\nu) = N$. If this step fails, then N is composite.
3. From a precomputed table of Eisenstein pseudocubes, choose $\mu_p \in \mathbb{Z}[\omega]$ of minimal norm such that $N < \mathbf{N}(\mu_p)$.
4. For each prime $q \leqslant p$, if $\left(\frac{q}{\nu}\right)_3 \equiv q^{\frac{N-1}{3}} \pmod{\nu}$ for all q, then N is prime.

As indicated in (4), we know that if N is prime, then for all $q < p$, we have $\left(\frac{q}{\nu}\right)_3 \equiv q^{\frac{N-1}{3}} \pmod{\nu}$. This contradicts the Berrizbeitia theorem. Therefore, ν is either a unit, prime, or prefect power. In particular, since N is neither a perfect power nor a unit as reflected in the algorithm, it has to be prime. Consequently, if ν is prime, then N is prime.

This paper first recalls background information on ring theory, particularly, Euclidean domains and unique factorization domains in Section 2. Then we introduce and study the

ring of Eisenstein integers and its properties in Section 3. Section 4 describes quadratic and cubic residues, and quadratic and cubic reciprocity. In Section 5, we discuss the congruence sieving method to compute the table for Eisenstein pseudocubes. Finally, in Section 6, we describe and analyze the algorithm proposed by Williams and Wooding of primality proving for an integer $N \equiv 1 \pmod 3$ based on a precomputed table of Eisenstein pseudocubes.

2 Unique Factorization

This section recalls definitions and properties about integral domains, Euclidean domains, and the Euclidean algorithm. Our goal is to show that every Euclidean domain is a unique factorization domain (UFD). In order to achieve this, we first prove that every Euclidean domain is a principal ideal domain (PID). Then, we give a separate proof that every PID is a UFD.

We begin by defining basic ring theoretic terminology.

Definition 2.1.

1. Let $\mathbf{R}$ be a commutative ring that has a multiplicative identity. A *unit* of $\mathbf{R}$ is an element u such that $uv = 1$ for some $v \in \mathbf{R}$. In particular, the set U of all units is called the *group of units* of $\mathbf{R}$.

2. Given $a, b \in \mathbf{R}$, we say a and b are *associates* and write $a \sim b$ if $a = ub$ for some $u \in U$.

3. An *ideal* $\boldsymbol{I}$ of $\mathbf{R}$ is a non-empty subset such that:

   (a) if $a, b \in \boldsymbol{I}$, then $a - b \in \boldsymbol{I}$;

   (b) if $a \in \boldsymbol{I}$ and $r \in \mathbf{R}$, then $ra \in \boldsymbol{I}$.

   A *proper ideal* is an ideal such that $\boldsymbol{I} \neq \{0\}$ and $\boldsymbol{I} \neq \mathbf{R}$.

4. An *integral domain* is a ring that has a multiplicative identity and has no zero divisors.

5. Let $\mathbf{D}$ be an integral domain and suppose $a, b \in \mathbf{D}$ with $a \neq 0$. If there exists $z \in \mathbf{D}$ such that $az = b$, then we say a *divides* b, written $a \mid b$.

6. A *principal ideal domain* (PID) is an integral domain in which every proper ideal can be generated by a single element.

Definition 2.2. An integral domain $\mathbf{D}$ is said to be a Euclidean domain if there is a function:

$$\delta : \mathbf{D} \backslash \{0\} \to \mathbb{N}$$

such that for all $a \in \mathbf{D}$ and all nonzero $b \in \mathbf{D}$, there exist $q, r \in \mathbf{D}$ such that:

$$a = qb + r \text{ with } r = 0 \text{ or } \delta(r) < \delta(b).$$

In this case, we also say that $\mathbf{D}$ *has a division algorithm*.

Example 2.3. Integers, $\mathbb{Z}$, with the function $\delta(x) = |x|$, is a Euclidean domain.

The function δ allows us to mimic the proof that the integers are a PID in order to prove that every Euclidean domain is a PID.

Theorem 2.4. Every Euclidean domain is a principal ideal domain.

Proof. Let $\boldsymbol{I}$ be an ideal of a Euclidean domain. If $\boldsymbol{I} = 0$, then $\boldsymbol{I} = \langle 0 \rangle$ is a principal ideal. If $\boldsymbol{I} \neq 0$, then we consider

$$S = \{\delta(a) \mid a \in \boldsymbol{I} \backslash \{0\}\} \subseteq \mathbb{N}.$$

Since $\boldsymbol{I} \neq 0$, there exists $a \in \boldsymbol{I}$, such that $a \neq 0$. Thus, $a \in \boldsymbol{I} \backslash \{0\}$ and $\delta(a) \in S$. As a result, $S \neq \varnothing$. Therefore, we can assume S has a least element $\delta(b)$ where $b \in \boldsymbol{I} \backslash \{0\}$. Since $b \in \boldsymbol{I}$, then $\langle b \rangle \subseteq \boldsymbol{I}$.

To conclude that $\langle b \rangle = \boldsymbol{I}$, we must also show $\boldsymbol{I} \subseteq \langle b \rangle$. We suppose $a \in \boldsymbol{I}$. Because we have a Euclidean domain, we can write $a = qb + r$ where $0 \leqslant \delta(r) < \delta(b)$. Because $\delta(r) < \delta(b)$ and $\delta(b)$ is the least element in S, we know that $\delta(r) \notin S$. Hence, we know that $r \notin \boldsymbol{I} \backslash \{0\}$. Since $\boldsymbol{I}$ is an ideal, $r = a - qb \in \boldsymbol{I}$. Thus, r has to be 0 in order to fulfill the requirement that $r \notin \boldsymbol{I} \backslash \{0\}$. As a result, we have $a = qb + r = qb + 0 = qb$, and $a \in \langle b \rangle$. Therefore, we have shown that $\boldsymbol{I} \subseteq \langle b \rangle$. We conclude that $\boldsymbol{I} = \langle b \rangle$, so $\boldsymbol{I}$ is a principal ideal, as required. ■

Since integers have an ordering, we can define the greatest common divisor (GCD) in integers by understanding both of the following terms: "greates" and "common divisor". First, "greatest" means that the GCD is the greatest number in the sequence. Second, "common divisor" means that the GCD divides both given integers. In general, the GCD in integers is the greatest number that can be divided by both given integers. On the other hand, a Euclidean domain is (in general) not ordered. Thus, we can only define GCD in Euclidean domain terms by testing whether or not it satisfies the following properties.

Definition 2.5. Let $\mathbf{D}$ be an integral domain. For any $a, b, d \in \mathbf{D}$, we argue d is a greatest common divisor of a and b if the following conditions hold:

GCD1 $d \mid a$ and $d \mid b$.

GCD2 if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Proposition 2.6. Suppose $\mathbf{D}$ is a PID. Then, for any non-zero $a, b \in \mathbf{D}$, there exists $\gcd(a, b)$ and $\langle a, b \rangle = \langle d \rangle$.

Proof. Consider the ideal $\langle a, b \rangle = \{sa + tb \mid s, t \in \mathbf{D}\}$. Because $\mathbf{D}$ is a PID, there exists $d \in \mathbf{D}$, such that $\langle a, b \rangle = \langle d \rangle$. Since $d \in \langle a, b \rangle$, there exist $s, t \in \mathbf{D}$ such that $d = sa + tb$. We need to verify that d satisfies GCD1 and GCD2.

For GCD1, since $a \in \langle d \rangle$, we know there exists $k \in \mathbf{D}$, such that $a = dk$. Therefore, we have $d \mid a$. Similarly, we have $d \mid b$.

For GCD2, we assume $d' \mid a$ and $d' \mid b$. Then there exist $m, n \in \mathbf{D}$ such that $a = d'm$ and $b = d'n$. Therefore, we have $d = sa + tb = s(d'm) + t(d'n) = d'(ms + tn)$. Since m, s, t, n are all in $\mathbf{D}$, then $ms + tn \in \mathbf{D}$ as well. We then have $d' \mid d$.

Therefore, we have $\gcd(a, b) = d$ and $\langle a, b \rangle = \langle d \rangle$. ■

Two elements a and b are said to be relatively prime if the only common divisors are units.

Corollary 2.7. if $\mathbf{D}$ is a PID and $a, b \in \mathbf{D}$ are relatively prime, then $\langle a, b \rangle = \mathbf{D}$.

Proof. Suppose 1 is the unit in $\mathbf{D}$. According to Proposition 2.6, we have shown that $\langle a, b \rangle = \langle 1 \rangle$. Since 1 is a unit, for any $\alpha \in \mathbf{D}$, we have $\alpha = \alpha \cdot 1$. Thus, $\alpha \in \mathbf{D}$. Therefore, $\langle 1 \rangle = \mathbf{D}$, as desired. ■

We now introduce the Euclidean Algorithm, which computes the GCD in the Euclidean domain.

Definition 2.8. Suppose $a, b \neq 0$ in a Euclidean domain $\mathbf{D}$. Then we can define elements $r_1, r_2, ...$ in $\mathbf{D}$ by the recursive formula that contains the function δ:

$$r_{k-2} = q_k r_{k-1} + r_k \text{ with } r_k = 0 \text{ or } \delta(r_k) < \delta(r_{k-1}).$$

Thus, we have:

$$\begin{aligned}
&a = q_1 b + r_1, && \delta(r_1) < \delta(b) \\
&b = q_2 r_1 + r_2, && \delta(r_2) < \delta(r_1) \\
&r_1 = q_3 r_2 + r_3, && \delta(r_3) < \delta(r_2) \\
&..... &&
\end{aligned}$$

The process must end because $\delta(b) > \delta(r_1) > \delta(r_2)...$ and δ takes nonnegative values. We suppose the last two steps are:

$$\begin{aligned}
&r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}, && \delta(r_{k-1}) < \delta(r_{k-2}) \\
&r_{k-2} = q_k r_{k-1}. &&
\end{aligned}$$

Lemma 2.9. $\gcd(a, b) = r_{k-1}$.

Proof. We sketch the verification that r_{k-1} fulfills GCD1 and GCD2.

GCD1: (work up) If $r_{k-1} \mid r_{k-2}$ and $r_{k-2} \mid r_{k-3}$, then $r_{k-1} \mid r_{k-3}$ due to $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$. By upward induction, we get $r_{k-1} \mid a$ and $r_{k-1} \mid b$.

GCD2: (work down) We suppose $d' \mid a$ and $d' \mid b$. Since $r_1 = a - q_1 b$, we have $d' \mid r_1$. By downward induction, we get $d' \mid r_{k-1}$. ■

Example 2.10. Determine the greatest common divisor of 615 and 345, and verify whether or not it fulfills both GCD1 and GCD2.

Proof.

$$\begin{aligned}
615 &= 1 \times 345 + 270 \\
345 &= 1 \times 270 + 75 \\
270 &= 1 \times 45 + 30 \\
45 &= 1 \times 30 + 15 \\
30 &= 2 \times 15 + 0.
\end{aligned}$$

As indicated in these equations, the greatest common divisor of 615 and 345 is 15, the last non-zero remainder.

We now test whether or not 15 fulfills both GCD1 and GCD2.

For GCD1: We have $615 = 15 \times 41$ and $345 = 15 \times 23$.

For GCD2: We suppose there exists d' such that $d' \mid 615$ and $d' \mid 345$. Thus, we have

$$\begin{aligned}
&d' \mid (615 - 345) = 270 \\
&d' \mid (345 - 270) = 75 \\
&d' \mid (270 - 75 \times 3) = 45 \\
&d' \mid (75 - 45) = 30 \\
&d' \mid (45 - 30) = 15.
\end{aligned}$$

Therefore, any integer d' that divides both 615 and 345 must divide 15.

Thus, we have shown that 15 fulfills both GCD1 and GCD2. Hence, 15 is the greatest common divisor of 615 and 345. ■

The remainder of this section is devoted to proving that every PID is a UFD. Assume $\mathbf{D}$ is a PID. We first show that every non-unit a in $\mathbf{D}$ can be written as a product of irreducibles. Then we prove that every factorization of a into irreducibles is unique.

Definition 2.11. Suppose $\mathbf{D}$ is an integral domain.

1. Suppose $p \neq 0$ in $\mathbf{D}$. Then p is *irreducible* if p is a non-unit and if $p = ab$, then either a is a unit, or b is a unit.

2. We say that d has a *factorization into irreducibles* if there exist irreducibles $p_1, p_2 ... p_k$ in $\mathbf{D}$ such that $d = p_1 p_2 ... p_k$.

3. The factorization for d is *essentially unique*. That is, if given factorizations $d = p_1 p_2 ... p_k$ and $d = q_1 q_2 ... q_l$ into irreducibles, it follows that $k = l$ and there exists a permutation τ of $\{1, 2, .., k\}$ such that $p_l \sim q_{\tau(l)}$.

4. We say $\mathbf{D}$ is a *unique factorization domain* (UFD) when every non-unit $a \neq 0$ has an essentially unique factorization.

5. A non-unit $p \neq 0$ in $\mathbf{D}$ is said to be *prime* if for any $a, b \in \mathbf{D}$, we have $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

6. In $\mathbf{D}$, every prime element is irreducible. In general, the converse is not true; it is only true when $\mathbf{D}$ is a UFD.

Lemma 2.12. If $\mathbf{D}$ is a PID, then $\mathbf{D}$ has no infinite ascending chains of ideals.

Proof. Suppose $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle ...$ is an infinite chain of ideals. Let $\boldsymbol{I} = U_{i=1}^{\infty} \langle a_i \rangle$, the union of ideals. First, we assert that $\boldsymbol{I}$ is an ideal. To prove this, suppose m is an arbitrary element in $\boldsymbol{I}$, and r is an arbitrary element in $\mathbf{D}$, not in $\boldsymbol{I}$. There exists $i \in \mathbb{N}$ such that $m \in \langle a_i \rangle$. Becasue $\langle a_i \rangle$ is an ideal in $\mathbf{D}$, we have $mr \in \langle a_i \rangle$ and $rm \in \langle a_i \rangle$. Therefore, we have both mr and $rm \in \boldsymbol{I}$. $\boldsymbol{I}$ is an ideal in $\mathbf{D}$.

Because $\mathbf{D}$ is a PID, there exists $a \in \mathbf{D}$ such that $I = \langle a \rangle$. Then there exists $k \in \mathbb{N}$ such that $a \in \langle a_k \rangle$. Because $\langle a \rangle = \boldsymbol{I}$, so $a \in \boldsymbol{I}$. As a result, we have $\langle a \rangle \subseteq \langle a_k \rangle \subseteq \langle a_{k+1} \rangle \subseteq ... \subseteq I = \langle a \rangle$. Therefore, all $\langle a_i \rangle$ for $i \in \mathbb{N}$ are equal and the chain is finite. ■

Corollary 2.13. Let $\mathbf{D}$ be a PID and $a \neq 0$, a non-unit in $\mathbf{D}$. Then there exists $z \in \mathbf{D}$ such that z is irreducible and $z \mid a$.

Proof. If a is irreducible, we are finished. If not, a must have a proper (non-unit, non-zero) divisor a_1, such that $a_1 \mid a$. Similarly, either a_1 is irreducible or there exists a proper divisor a_2, such that $a_2 \mid a_1$. Continuing this process, we have a sequence $a_1, a_2, a_3 ... a_k$ where a_i is a proper divisor of a_{i-1} for $1 \leqslant i \leqslant k$. Therefore, we have $\langle a_{i-1} \rangle \subsetneq \langle a_i \rangle$. By Lemma 2.12, the sequence terminates at a_k, which must be irreducible. ■

Lemma 2.14. Let $\mathbf{D}$ be a PID. If $p \in \mathbf{D}$ is irreducible, then p is prime.

Proof. Let $a, b \in \mathbf{D}$ with $p \mid ab$. Based on the definition of prime in Definition 2.11, we want to show that either $p \mid a$ or $p \mid b$. Since $p \mid ab$, there exists $m \in \mathbf{D}$, such that $pm = ab$. If $p \mid a$, we are finished. If $p \nmid a$, because p is prime, we have $\gcd(p, a) = 1$. By *Bezout's identity*, there exist $t, s \in \mathbf{D}$ such that $tp + sa = 1$. Thus, we have $btp + bsa = btp + (ba)s = btp + pms = p(bt + ms) = b$. Hence, $p \mid b$ and p is prime. ■

Theorem 2.15. Every PID is a UFD.

Proof. Assume $\mathbf{D}$ to be a PID, and let $a \neq 0$ be a non-unit in $\mathbf{D}$. Based on the Corollary 2.13, there exists an irreducible $p_1 \in \mathbf{D}$ such that $p_1 \mid a$. Say $a = p_1 b_1$ for some $b_i \in \mathbf{D}$, where $i \in \mathbb{N}$. If b_1 is irreducible, then a is a product of irreducibles. Otherwise, $b_1 = p_2 b_2$ where p_2 is irreducible. Continuing this process, we notice that $\langle b_1 \rangle \subseteq \langle b_2 \rangle \subseteq ... \subseteq \langle b_k \rangle$ must terminate by Lemma 2.12. We assume it will terminate at b_k where $b_k = p_k$ is irreducible. Then we have $a = p_1 p_2 p_3 ... p_k$.

To show uniqueness, we suppose $a = p_1 p_2 p_3 ... p_k$ and $a = q_1 q_2 q_3 ... q_l$ where $q_1 ... q_l$ are irreducible. Without the loss of generality, we assume $k \leqslant l$. Since p_1 is irreducible, we have $p_1 \mid q_1 q_2 ... q_l$. Based on the Lemma 2.14, we know that p_1 is prime. By Definition 2.11, there exists $i \in \mathbb{N}$ such that $p_1 \mid q_i$. That is, there exists a unit u_i in $\mathbf{D}$ such that $q_i = u_i p_1$. After reordering, we have $q_1 = u_1 p_1$. As a result, we get $p_1 p_2 ... p_k = p_1 u_1 q_2 q_3 ... q_l$. Both sides divide $p_1 p_2 ... p_k$ and we will get $1 = u_1 u_2 ... u_k q_{k+1} ... q_l$. This contradicts the claim that q_l is not a unit. Therefore, $k = l$ and $p_1 \sim q_i$ for $i = 1, 2....k$. Hence, $\mathbf{D}$ is a UFD. ■

3 The Eisenstein Integers

This section introduces the Eisenstein integers, $\mathbb{Z}[\omega]$, a subset of $\mathbb{C}$ obtained by adjoining a primitive cube root of unity, $\omega = 1/2(-1 + i\sqrt{3}) = e^{2\pi i/3}$, to the rational integers. Elements of $\mathbb{Z}[\omega]$ are complex numbers of the form $z = a + b\omega$, where a and b are rational integers. We discuss the norm function on $\mathbb{Z}[\omega]$, and we use the norm of $\mathbb{Z}[\omega]$ as the function δ to prove that $\mathbb{Z}[\omega]$ is a Euclidean domain, and therefore is a UFD. We also use the norm function to classify the different types of primes in $\mathbb{Z}[\omega]$. Finally, we compute the units in $\mathbb{Z}[\omega]$ and discuss the choice of a preferred ("primary") associate of an Eisenstein integer.

Consider the set $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$. It is clear that $\mathbb{Z}[\omega]$ is closed under addition and subtraction. In addition, since $\omega^2 = -1 - \omega$, we have that $\mathbb{Z}[\omega]$ is closed under multiplication and is a ring. Since $\mathbb{Z}[\omega]$ is a subset of the complex numbers, we can see that $\mathbb{Z}[\omega]$ is an integral domain. We also assert that $\mathbb{Z}[\omega]$ is closed under complex conjugation.

Let $i = \sqrt{-1}$. Since $\overline{\sqrt{-3}} = \overline{\sqrt{3}i} = -\sqrt{3}i = -\sqrt{-3}$, we see that $\overline{\omega} = \omega^2$. Thus, for any $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, the complex conjugate $\overline{\alpha} = a + b\overline{\omega} = a + b\omega^2 = (a - b) - b\omega$ is also in $\mathbb{Z}[\omega]$.

We define a norm function on $\mathbb{Z}[\omega]$ by $\mathbf{N}(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha}$ denotes the complex conjugate of α. Since $\alpha\overline{\alpha} = a^2 - ab + b^2 = (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2$, it is clear that $\mathbf{N}(\alpha) \in \mathbb{Z}^+$ for all

$\alpha \in \mathbb{Z}[\omega]$. In particular, if $\mathbf{N}(\alpha) = 0$, then $\alpha = 0$. The norm function is multiplicative: for any $\alpha, \beta \in \mathbb{Z}[\omega]$, we have

$$\begin{aligned}\mathbf{N}(\alpha)\mathbf{N}(\beta) &= (a^2 - ab + b^2)(c^2 - cd + d^2) \\ &= (ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ac + bc - bd)^2 \\ &= \mathbf{N}(\alpha\beta).\end{aligned}$$

In addition, we have $\mathbf{N}(1) = 1 \cdot 1 = 1$.

Lemma 3.1. Let $\alpha \in \mathbb{Z}[\omega]$, then we have α is a unit if and only if $\mathbf{N}(\alpha) = 1$.

Proof. Let α be a unit in $\mathbb{Z}[\omega]$. Then we have $\alpha\beta = 1$ for some β in $\mathbb{Z}[\omega]$. Thus, $\mathbf{N}(1) = \mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta) = 1$. Since both $\mathbf{N}(\alpha)$ and $\mathbf{N}(\beta)$ are rational integers, they must both equal 1. Hence, $\mathbf{N}(\alpha) = \mathbf{N}(\beta) = 1$. Therefore, for any $\alpha \in \mathbb{Z}[\omega]$, it is a unit if and only if $\mathbf{N}(\alpha) = 1$. ■

Corollary 3.2. For any non unit $\alpha \in \mathbb{Z}[\omega]$, we have $\mathbf{N}(\alpha) > 1$.

Proof. From the norm function, we notice that for any non-zero $\alpha \in \mathbb{Z}[\omega]$, its norm is larger than or equal to 1. In addition, we conclude that α is a unit if and only if $\mathbf{N}(\alpha) = 1$ according to Lemma 3.1. Thus, if α is not a unit, its norm should lager than 1.

■

We now find units in $\mathbb{Z}[\omega]$.

Lemma 3.3. The units in $\mathbb{Z}[\omega] = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.

Proof. Now we suppose $\alpha = a + b\omega \in \mathbb{Z}[\omega]$. According to Lemma 3.1, we have concluded that if α is a unit in $\mathbb{Z}[\omega]$, then $\mathbf{N}(\alpha) = a^2 - ab + b^2 = 1$. Furthermore, we have $1 = a^2 - ab + b^2 = (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2$. Since a and b are integers and $\frac{3}{4}b^2 \leqslant 1$, we conclude that b can only be 0 or ± 1. Now consider the following cases:

1. When $b = 0$, we have $1 = a^2$, indicating that $a = \pm 1$.
2. When $b = 1$, we have $(a - \frac{1}{2})^2 = \frac{1}{4}$, indicating that $(a - \frac{1}{2}) = \pm\frac{1}{2}$. Therefore, $a = 1$ or $a = 0$ correspondingly.
3. When $b = -1$, we have $(a + \frac{1}{2})^2 = \frac{1}{4}$, indicating that $(a + \frac{1}{2}) = \pm\frac{1}{2}$. Therefore, $a = 0$ or $a = -1$ correspondingly.

Thus, the units in $\mathbb{Z}[\omega]$ are $1, -1, \omega, -\omega, 1 + \omega, -1 - \omega$. Since $\omega^2 + \omega + 1 = 0$, the last two units can be written as ω^2 and $-\omega^2$. ■

Since $\mathbb{Z}[\omega]$ is an integral domain, we now use the norm function on $\mathbb{Z}[\omega]$ to serve as the function δ in Definition 2.2 to show that $\mathbf{D}$ is a Euclidean domain.

Proposition 3.4. $\mathbb{Z}[\omega]$ is a Euclidean domain.

Proof. For any $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, we define $\delta(\alpha) = \mathbf{N}(\alpha) = \alpha\overline{\alpha} = a^2 - ab + b^2$. Now we assume $\alpha, \beta \in \mathbb{Z}[\omega]$ and suppose that $\beta \neq 0$. We must show that we can find $\rho, z \in \mathbb{Z}[\omega]$ such that $\alpha = z\beta + \rho$, where either $\rho = 0$ or $\mathbf{N}(\rho) < \mathbf{N}(\beta)$.

In order to achieve this, we extend our attention to $\mathbf{Q}[\omega]$, which helps us to produce z. Consider $\alpha/\beta = \alpha\overline{\beta}/\beta\overline{\beta} = \alpha\overline{\beta}/\mathbf{N}(\beta)$. Since $\mathbf{N}(\beta) \in \mathbb{N}$ and $\alpha, \overline{\beta} \in \mathbb{Z}[\omega]$, we have

$\alpha\overline{\beta}/\mathbf{N}(\beta) = \alpha/\beta \in \mathbf{Q}[\omega]$, say $\alpha/\beta = c + d\omega$ where $c, d \in \mathbf{Q}$. Now we seek an approximation to α/β in $\mathbb{Z}[\omega]$. There exist $c, d \in \mathbf{Q}$ such that $\alpha/\beta = c + d\omega$. We can find $r, s \in \mathbb{Z}$, such that $|c - r| \leqslant \frac{1}{2}$ and $|d - s| \leqslant \frac{1}{2}$, and we set $z = r + s\omega$.

We now calculate how "close" z is to α/β and z by using the norm function. We assert the norm of $\alpha/\beta - z$ is smaller than 1. To show this, we have

$$\begin{aligned}\mathbf{N}(\alpha/\beta - z) &= \mathbf{N}(c + d\omega - (r + s\omega)) \\ &= \mathbf{N}(c - r + (d - s)\omega) \\ &= (c - r)^2 - (c - r)(d - s) + (d - s)^2 \\ &\leqslant \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1.\end{aligned}$$

Since z is a close integer approximate to α/β, we expect that the remainder $\rho = \alpha - \beta z \in \mathbb{Z}[\omega]$ to be small. Then we use the norm function to serve as the δ in Definition 2.11 to compare $\mathbf{N}(\beta)$ and $\mathbf{N}(\rho)$. Observe that:

$$\mathbf{N}(\rho) = \mathbf{N}(\alpha - \beta z) = \mathbf{N}(\beta(\alpha/\beta - z)) = \mathbf{N}(\beta)\mathbf{N}(\alpha/\beta - z) < \mathbf{N}(\beta) \cdot 1 = \mathbf{N}(\beta).$$

Thus, given $\alpha, \beta \in \mathbb{Z}[\omega]$, we have found $\rho, z \in \mathbf{D}$ such that $\alpha = z\beta + \rho$, where $\mathbf{N}(\rho) < \mathbf{N}(\beta)$. Hence, $\mathbb{Z}[\omega]$ is a Euclidean domain, as desired. ■

Corollary 3.5. $\mathbb{Z}[\omega]$ is a PID and a UFD.

Proof. From Proposition 3.4, we know that $\mathbb{Z}[\omega]$ is a Euclidean domain. But in Theorem 2.4, we proved that every Euclidean domain is a PID. It follows that $\mathbb{Z}[\omega]$ is a UFD by Theorem 2.15, as desired. ■

We now use this norm function to classify primes in $\mathbb{Z}[\omega]$.

Proposition 3.6. If π is prime in $\mathbb{Z}[\omega]$, then there is a rational prime p such that $\mathbf{N}(\pi) = p$ or p^2. In the former case, π is not associate to a rational prime; in the latter case, π is associate to p.

Proof. We assume π is prime in $\mathbb{Z}[\omega]$ and that we have $\mathbf{N}(\pi) = \pi\overline{\pi} = n \in \mathbb{Z}$. Since n is a product of rational primes, there exists a rational prime p such that $\pi \mid p$. Thus, there exists $\gamma \in \mathbb{Z}[\omega]$, such that $p = \pi\gamma$. Because the norm is multiplicative, we have $\mathbf{N}(p) = \mathbf{N}(\pi\gamma) = \mathbf{N}(\pi)\mathbf{N}(\gamma)$. Since p is a rational prime, then we have $\mathbf{N}(p) = p\overline{p} = p^2$. Thus, $\mathbf{N}(\pi)\mathbf{N}(\gamma) = \mathbf{N}(p) = p^2$. Since p is a rational prime and $\mathbf{N}(\pi)$ is an integer, then either $\mathbf{N}(\pi) = p$ or $\mathbf{N}(\pi) = p^2$.

If $\mathbf{N}(\pi) = p$,we proceed by contrapositive. Assume that π is associate to a rational prime, say $\pi = \mu q$ where μ is a unit and q is a rational prime. Then we have $p = \mathbf{N}(\pi) = \mathbf{N}(\mu)\mathbf{N}(q) = q^2$, which contradicts that p is a rational prime. Thus, π is not associate to a rational prime. On the other hand, if $\mathbf{N}(\pi) = p^2 = \mathbf{N}(\pi)\mathbf{N}(\gamma)$, then $\mathbf{N}(\gamma) = 1$. Therefore, γ is a unit by Lemma 3.1 and π is associate to p. ■

Besides detecting the associates of a prime number in $\mathbb{Z}[\omega]$, the norm function can also help to detect primes in $\mathbb{Z}[\omega]$.

Proposition 3.7. If $\pi \in \mathbb{Z}[\omega]$ is such that $\mathbf{N}(\pi)$ is a rational prime, then π is prime in $\mathbb{Z}[\omega]$.

Proof. We prove this by contrapositive. Assume that π is not prime in $\mathbb{Z}[\omega]$ and write $\pi = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\omega]$. We want to show that $\mathbf{N}(\pi)$ is not a rational prime. Since $\pi = \alpha\beta$, we have $\mathbf{N}(\pi) = \mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta)$. Because both α and β are not units, we have $\mathbf{N}(\alpha), \mathbf{N}(\beta) \in \mathbb{Z}^+$ by Corollary 3.2. Thus, $\mathbf{N}(\pi) = \mathbf{N}(\alpha)\mathbf{N}(\beta)$ is not a rational prime. Therefore, π is prime in $\mathbb{Z}[\omega]$, as desired. ■

Based on this sections's discussion of primes in $\mathbb{Z}[\omega]$, we are now able to classify primes in $\mathbb{Z}[\omega]$ into three different types. In fact, based on Proposition 3.7, we can infer that some rational primes remain prime in $\mathbb{Z}[\omega]$, while others do not. Hence, the congruence class of a rational prime mod 3 tells us precisely whether or not it remains prime in $\mathbb{Z}[\omega]$.

Proposition 3.8. Suppose that p is a rational prime. If $p \equiv 2 \pmod 3$, then p is prime in $\mathbb{Z}[\omega]$. If $p \equiv 1 \pmod 3$, then $p = \pi\overline{\pi}$ where π is prime in $\mathbb{Z}[\omega]$ with $\mathbf{N}(\pi) = \mathbf{N}(\overline{\pi})$. Finally, if $p = 3$, we have $p = -\omega^2(1-\omega)^2$, and $1-\omega$ is prime in $\mathbb{Z}[\omega]$.

Proof. First, we want to show that if $p \equiv 2 \pmod 3$, then p is prime in $\mathbb{Z}[\omega]$. Suppose p is not prime. There exist non-units $\alpha, \beta \in \mathbb{Z}[\omega]$ such that $p = \alpha\beta$ with $\mathbf{N}(\alpha) > 1$ and $\mathbf{N}(\beta) > 1$. Because p is a rational prime and $\mathbf{N}(p) = \mathbf{N}(\alpha)\mathbf{N}(\beta) = p^2$ where $\mathbf{N}(\alpha), \mathbf{N}(\beta) > 1$, we have $\mathbf{N}(\alpha) = p$. Since $\alpha \in \mathbb{Z}[\omega]$, there exist $m, n \in \mathbb{Z}$ such that $\alpha = m + n\omega$. By the definition of norm, we have $\mathbf{N}(\alpha) = m^2 - mn + n^2 = p$. Now we consider different pairs of m and n.

$m \pmod 3$	$n \pmod 3$	$m^2 - mn + n^2$
0	0	0
0	1	1
0	2	1
1	0	1
1	1	1
1	2	0
2	0	1
2	1	0
2	2	0

Based on above table, it is clear that in any case, if $p = \mathbf{N}(\alpha)$, p cannot congruent to 2 modulo 3. Therefore, if $p \equiv 2 \pmod 3$, we have $p \neq \mathbf{N}(\alpha)$ and this contradicts that $p = \mathbf{N}(\alpha)$. Hence, if $p \equiv 2 \pmod 3$, p is prime in $\mathbb{Z}[\omega]$.

Secondly, suppose that $p \equiv 1 \pmod 3$, in which case we want to show that $p = \pi\overline{\pi}$ where π is prime in $\mathbb{Z}[\omega]$. By Euler's Critertion and quadratic reciprocity we have:

$$\begin{aligned}
\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\
&= (-1)^{(\frac{p-1}{2})}\left(\frac{3}{p}\right) \\
&= (-1)^{(\frac{p-1}{2})}\left(\frac{p}{3}\right)(-1)^{(\frac{p-1}{2})(\frac{3-1}{2})} \\
&= (-1)^{((\frac{p-1}{2})+(\frac{p-1}{2}))}\left(\frac{p}{3}\right) \\
&= (-1)^{(p-1)}\left(\frac{p}{3}\right)
\end{aligned}$$

Since p is a rational prime and $p \neq 2$, we have $(-1)^{(p-1)} = 1$. Thus, we have:

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

Hence, there exists $a \in \mathbb{Z}$ such that $a^2 \equiv -3 \pmod{p}$ and $p \mid (a^2+3)$. Since $(a^2+3) = (a+\sqrt{-3})(a-\sqrt{-3})$, if p is prime in $\mathbb{Z}[\omega]$, then $p \mid (a^2+3)$ implies that p divides one of the factors of a^2+3. In fact, since the conjugate of $(a+\sqrt{-3})$ is $(a-\sqrt{-3})$, it has to divide both of them if it divides one of them. To prove this, suppose $(a+\sqrt{-3}) = z$ and $p \mid z$. Then there exits $\gamma \in \mathbb{Z}[\omega]$ such that $z = p\gamma$. Therefore, $\overline{z} = \overline{p\gamma} = p\overline{\gamma}$. Hence, we have $p \mid \overline{z}$. Therefore, p has to divide both of them and the sum of them. That is $p \mid (a+\sqrt{-3}) + (a-\sqrt{-3}) = 2a$. The fact that $p \nmid 2$ indicates $p \mid a$. Certainly, $p \mid a$ indicates that $p \mid a^2$ and $a^2 \equiv 0 \pmod{p}$, contradicting that $a^2 \equiv -3 \pmod{p}$. Therefore, p is not prime in $\mathbb{Z}[\omega]$ and there must exist a prime number $\pi \in \mathbb{Z}[\omega]$ such that $p = \pi\gamma$ with γ a non-unit. Since $\mathbf{N}(p) = \mathbf{N}(\pi)\mathbf{N}(\gamma) = p^2$ and γ is a non-unit, we have $\mathbf{N}(\pi) = p = \pi\overline{\pi}$ where π is prime.

Lastly, we show that $p = 3$ is an associate of $(1-\omega)$ and that $1-\omega$ is a prime number in $\mathbb{Z}[\omega]$. Since $\mathbf{N}(1-\omega) = 3$ is a rational prime number, then we have $(1-\omega)$ is prime in $\mathbb{Z}[\omega]$ according to Proposition 3.7. ■

After analyzing whether a rational prime remains prime in $\mathbb{Z}[\omega]$ with the help of the congruence class of the rational prime mod 3, we are now ready to classify primes in the Eisenstein integers. There are three types:

Proposition 3.9 (Primes in Eisenstein Integers)**.**

Type 1 The rational primes $p \equiv 2 \pmod{3}$, which have norm p^2.

Type 2 Non-rational Eisenstein integers π such that $\mathbf{N}(\pi)$ is a rational prime p satisfying $p \equiv 1 \pmod{3}$.

Type 3 $p = 3$ is an associate of $1-\omega$ where $1-\omega$ is prime.

According to Lemma 3.3, there are six units in $\mathbb{Z}[\omega]$. We are now use these units to help us find associate for each Eisenstein integer and define the term primary to choose the preferred associate.

Definition 3.10. A primary element α in $\mathbb{Z}[\omega]$ is an element congruent to 2 modulo 3. In other words, the element $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ is primary if and only if $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$.

Theorem 3.11. Suppose that $\mathbf{N}(\pi) = p$ a prime number in $\mathbb{Z}$, and $p \equiv 1 \pmod{3}$. Then among the associates of π, exactly one is primary.

Proof. Since $\pi = a + b\omega$, then we have $\mathbf{N}(\pi) = a^2 - ab + b^2 = p \equiv 1 \pmod{3}$. The six

associates of π can be found by multiplying π by each of the six units in $\mathbb{Z}[\omega]$:

$$\begin{aligned}
(\pi)\cdot(1) &= \pi = a + b\omega \\
(\pi)\cdot(-1) &= -\pi = -a - b\omega \\
(\pi)\cdot(\omega) &= \omega\pi = a\omega + b\omega^2 = -b + (a-b)\omega \\
(\pi)\cdot(-\omega) &= -\omega\pi = -a\omega - b\omega^2 = b + (b-a)\omega \\
(\pi)\cdot(\omega^2) &= \omega^2\pi = a\omega^2 + b = (b-a) - a\omega \\
(\pi)\cdot(-\omega^2) &= -\omega^2\pi = -a\omega^2 - b = (a-b) + a\omega.
\end{aligned}$$

We may now restrict the congruence possibilities for a and b in to six cases:

$a \pmod 3$	$b \pmod 3$	primary
0	1	$-\omega^2\pi$
0	2	$\omega^2\pi$
1	0	$-\pi$
1	1	$\omega\pi$
2	0	π
2	2	$-\omega\pi$

■

4 Cubic Reciprocity

Throughout this section, we use $\mathbf{D}$ to represent the Eisenstein integers, $\mathbb{Z}[\omega]$. We will establish a parallel between square roots in rational integers modulo an ordinary prime number and cube roots in Eisenstein integers modulo an Eisenstein prime number.

In rational integers, given a prime number $p \in \mathbb{Z}$, then $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements. The multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$ is a cyclic group with $p-1$ elements. Similarly, we prove that in the Eisenstein integers, given a prime number $\pi \in \mathbf{D}$, then $\mathbf{D}/\pi\mathbf{D}$ is a finite field. In particular, this means that the multiplicative group $\mathbf{D}/\pi\mathbf{D}^*$ is a cyclic group, and we show that $\mathbf{D}/\pi\mathbf{D}^*$ has $\mathbf{N}(\pi)-1$ elements.

If $\alpha, \beta, \delta \in \mathbf{D}$ and $\delta \neq 0$ is a non-unit, we say that $\alpha \equiv \beta \pmod{\delta}$ if δ divides $\alpha - \beta$. The congruence classes of $\mathbf{D}$ modulo δ may be made into the residue class ring modulo δ, denoted $\mathbf{D}/\delta\mathbf{D}$.

Proposition 4.1. Suppose δ is a non zero element of $\mathbf{D}$. Then $\mathbf{D}/\delta\mathbf{D}$ is finite.

Proof. We must show that a finite number of elements of $\mathbf{D}$ suffice to represent the cosets of $\mathbf{D}/\delta\mathbf{D}$. Consider an arbitrary $\alpha \in \mathbf{D}$. Since $\mathbf{D}$ is a Euclidean domain and $\delta \neq 0$, there exist $\beta, \gamma \in \mathbf{D}$ such that $\alpha = \delta\beta + \gamma$ and $\mathbf{N}(\gamma) < \mathbf{N}(\delta)$. Hence, every coset in $\mathbf{D}/\delta\mathbf{D}$ can be represented by an element whose norm is strictly less than $\mathbf{N}(\delta)$.

However, we claim that for any $m \in \mathbb{Z}^+$, only finitely many values of $\gamma \in \mathbf{D}$ satisfy $\mathbf{N}(\gamma) < m$. For if $\gamma = a + b\omega$ with $a, b \in \mathbb{Z}$, then we conclude that $\mathbf{N}(\gamma) = a^2 - ab + b^2 = (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2 < m$. Because this requires $\frac{3}{4}b^2 < m$, there are only finitely many choices for b. For a given b, there are only finitely many integers a satisfying $(a - \frac{1}{2}b)^2 < m - \frac{3}{4}b^2$. Therefore, there are finitely many $\gamma \in \mathbf{D}$ with $\mathbf{N}(\gamma) < \mathbf{N}(\delta)$. All cosets in $\mathbf{D}/\delta\mathbf{D}$ can be represented by such a γ, so $\mathbf{D}/\delta\mathbf{D}$ is finite, as desired.

■

Now we consider the quotient of $\mathbf{D}$ by a prime number π. To show $\mathbf{D}/\pi\mathbf{D}$ is a finite field, we need to show that it has no zero divisors and every nonzero element is invertible. For arbitrary $\alpha \in \mathbf{D}$, we use $\underline{\alpha}$ to denote $\alpha + \pi\mathbf{D}$ in $\mathbf{D}/\pi\mathbf{D}$.

Proposition 4.2. Let $\pi \in \mathbf{D}$ be prime. Then $\mathbf{D}/\pi\mathbf{D}$ is a field.

Proof. To show $\mathbf{D}/\pi\mathbf{D}$ has no zero divisors, we suppose $\underline{\alpha} \in \mathbf{D}/\pi\mathbf{D}$ and $\underline{\beta} \in \mathbf{D}/\pi\mathbf{D}$ multiply to 0 in $\mathbf{D}/\pi\mathbf{D}$. Therefore, we have $\pi \mid \alpha\beta$. By Definition 2.11, since π is a prime and $\pi \mid \alpha\beta$, then we have $\pi \mid \alpha$ or $\pi \mid \beta$, indicating that either $\underline{\alpha}$ or $\underline{\beta}$ is zero in $\mathbf{D}/\pi\mathbf{D}$.

To show elements of $\mathbf{D}/\pi\mathbf{D}$ are invertible, suppose a non-zero $\underline{\alpha} \in \mathbf{D}/\pi\mathbf{D}$. Since $\mathbf{D}/\pi\mathbf{D}$ is finite, there must be some repetition in the list $\underline{\alpha}^0, \underline{\alpha}^1, \underline{\alpha}^2$..... Hence there exist exponents $i < j$ with $\underline{\alpha}^i = \underline{\alpha}^j$, so $\underline{\alpha}^i(\underline{\alpha}^{j-i} - 1) = 0$. Since $\mathbf{D}/\pi\mathbf{D}$ has no zero divisors, we get $\underline{\alpha}^{j-i} - 1 = 0$ and $\underline{\alpha} \cdot \underline{\alpha}^{j-i-1} = 1$. Since $i < j$, we have $j - i - 1 \geqslant 0$, indicating that $\underline{\alpha}^{j-i-1} \in \mathbf{D}$ and $\underline{\alpha}$ is invertible. Therefore, $\mathbf{D}/\pi\mathbf{D}$ is a field. ■

Now we establish the cardinality of $\mathbf{D}/\pi\mathbf{D}$.

Proposition 4.3. Let $\pi \in \mathbf{D}$ be prime. Then $\mathbf{D}/\pi\mathbf{D}$ is a finite field with $\mathbf{N}(\pi)$ elements.

Proof. By Proposition 4.1 and Proposition 4.2, $\mathbf{D}/\pi\mathbf{D}$ is a finite field. To show that it has $\mathbf{N}(\pi)$ elements, we consider the following two cases, according to whether or not π is a rational prime (Proposition 3.9).

First Case We first consider rational primes in $\mathbf{D}$. Suppose $\pi = p$ where $p \equiv 2 \pmod 3$ is a rational prime. From Proposition 3.6, we know $\mathbf{N}(\pi) = \mathbf{N}(p) = p^2$, so we want to show that $\mathbf{D}/\pi\mathbf{D}$ has p^2 elements. We claim that a complete set of coset representatives for $\mathbf{D}/\pi\mathbf{D}$ is given by the set $S = \{i + j\omega \mid 0 \leqslant i < p \text{ and } 0 \leqslant j < p\}$. Let $\mu = m + n\omega$ be an arbitrary element in $\mathbf{D}$. Apply the Division Algorithm for dividing p into m and n, respectively, to obtain $s, t, i, j \in \mathbb{Z}$ such that $m = ps + i$ and $n = pt + j$ where $0 \leqslant i, j < p$. Thus, $i + j\omega \in S$, and we then conclude that $\mu = m + n\omega = p(s + t\omega) + (i + j\omega) \equiv i + j\omega \pmod p$.

We have proved $\mathbf{D}/\pi\mathbf{D}$ has at most p^2 elements, but we still need to show that the p^2 elements of S represent distinct cosets. Suppose that $a + b\omega$ and $a' + b'\omega$ are in S, and $a + b\omega \equiv a' + b'\omega \pmod p$. Then $p \mid [(a - a') + (b - b')\omega]$, so we have $((a - a')/p) + ((b - b')/p)\omega \in \mathbf{D}$. Since both $(a - a')/p$ and $(b - b')/p$ must be in $\mathbb{Z}$ and since $0 \leqslant a, b, a', b' < p$, we conclude that $a = a'$ and $b = b'$. Thus, elements in S represent distinct elements of $\mathbf{D}/\pi\mathbf{D}$, and $\mathbf{D}/\pi\mathbf{D}$ has p^2 elements, as desired.

Second Case Now we consider non-rational primes in $\mathbf{D}$. Suppose that $\pi \in \mathbf{D}$ where $\mathbf{N}(\pi)$ is a rational prime p satisfying $p \equiv 1 \pmod 3$. We claim that a complete set of coset representatives for $\mathbf{D}/\pi\mathbf{D}$ is given by the set $T = \{0, 1, ..., p - 1\}$. We want to show that an arbitrary $\alpha = m + n\omega \in \mathbf{D}$ is congruent modulo π to an element in T. Suppose $\pi = a + b\omega$ where $a, b \in \mathbb{Z}$. We know that there exists an integer c such that $cb \equiv n \pmod p$. Therefore, $m + n\omega \equiv m + cb\omega \pmod p$. Since $\mathbf{N}(\pi) = \pi\overline{\pi} = p$, then $m + n\omega \equiv m + cb\omega \pmod \pi$. We rewrite α through a sequence of congruences mod π:

$$\begin{aligned}\alpha &= m + n\omega \\ &\equiv m + cb\omega \\ &\equiv m + cb\omega + ca - ca \\ &\equiv c(a + b\omega) + m - ca \\ &\equiv c\pi + m - ca \\ &\equiv m - ca \pmod{\pi}.\end{aligned}$$

This indicates that every element of $\mathbf{D}$ is congruent to a rational integer mod π. But every rational integer is congruent to an integer in T modulo p, and hence also modulo π.

We have proved that $\mathbf{D}/\pi\mathbf{D}$ has at most p elements, but we still need to show that different elements in T represent distinct cosets. Suppose $t \equiv t' \pmod{\pi}$ with $t, t' \in \mathbb{Z}$ and $0 \leqslant t, t' < p$. Then there exists $\gamma \in \mathbf{D}$ such that $t - t' = \pi\gamma$. Taking the norm of both sides, we have:

$$(t - t')^2 = \mathbf{N}(t - t') = \mathbf{N}(\pi)\mathbf{N}(\gamma) = p\mathbf{N}(\gamma).$$

Thus $p \mid (t - t')$, and since $0 \leqslant t, t' < p$, we then have $t = t'$. Thus, if $t, t' \in T$ represent the same element of $\mathbf{D}/\pi\mathbf{D}$, then $t = t'$, as desired.

■

Now we introduce Fermat's Little Theorem and square roots in $\mathbb{Z}/p\mathbb{Z}^*$ and then state the corresponding results in $\mathbf{D}/\pi\mathbf{D}^*$.

Theorem 4.4 (Fermat's Little Theorem)**.** Suppose $p \in \mathbb{Z}$ is an odd prime. Then for any $a \in \mathbb{Z}$ where $p \nmid a$, we have $a^{p-1} \equiv 1 \pmod{p}$.

When p is an odd prime, $\frac{p-1}{2} \in \mathbb{Z}$ and $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$ by Theorem 4.4. Hence, $a^{\frac{p-1}{2}}$ is a square root of 1. Now we want to determine all possible values of $a^{\frac{p-1}{2}}$.

Lemma 4.5. Suppose p is an odd prime and $a \in \mathbb{Z}$. If $p \nmid a$, then $x^2 \equiv a \pmod{p}$ either has no solutions or two solutions.

Proof. If $x^2 \equiv a \pmod{p}$ has any solutions, it has at least two solutions: if $x^2 \equiv a \pmod{p}$, then $(-x)^2 \equiv a \pmod{p}$ also, and x and $-x$ are distinct in $\mathbb{Z}/p\mathbb{Z}$ when $p > 2$. We want to show that $x^2 \equiv a \pmod{p}$ has no more than two solutions. Suppose $b^2 \equiv x^2 \equiv a \pmod{p}$ where $b \in \mathbb{Z}$. Then $b^2 - x^2 \equiv (b - x)(b + x) \equiv 0 \pmod{p}$, indicating $p \mid (b - x)(b + x)$. By Definition 2.11, $p \mid (b - x)$ or $p \mid (b + x)$. Consequently, we have $b \equiv x$ or $b \equiv -x \pmod{p}$. Thus, if $x^2 \equiv a \pmod{p}$ has any solutions, it must have exactly two solutions. ■

In Eisenstein integers, we have an analog of Fermat's Little Theorem.

Proposition 4.6. Suppose $\pi \nmid \alpha$ where $\alpha \in \mathbf{D}$ and π is prime in $\mathbf{D}$. Then:

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

Proof. By Proposition 4.3, $\mathbf{D}/\pi\mathbf{D}$ is a finite field with $\mathbf{N}(\pi)$ elements. It follows that the multiplicative group $\mathbf{D}/\pi\mathbf{D}^*$ has $\mathbf{N}(\pi)-1$ elements. By Lagrange's Theorem, any element $\underline{\alpha} \in \mathbf{D}/\pi\mathbf{D}^*$ satisfies $\underline{\alpha}^{\mathbf{N}(\pi)-1} \equiv 1 \pmod{\pi}$, as desired. ■

Just as a rational prime p in $\mathbb{Z}$ is assumed to be odd, we determine several analogous "pre-requirements" about π in Eisenstein integers in order to introduce Euler's Criterion for Eisenstein integers.

In particular, the reason that we let prime p in $\mathbb{Z}$ to be odd is that we want to ensure that the square roots of 1 (1 and -1) are distinct mod p in $\mathbb{Z}$. Similarly, we construct "pre-requirements" on π in Eisenstein integers in order to ensure that the cube roots of 1 (1, ω, and ω^2) are distinct mod π in $\mathbf{D}$.

Proposition 4.7. Suppose π is prime in $\mathbf{D}$ such that $\mathbf{N}(\pi) \neq 3$. The residue classes of 1, ω and ω^2 are distinct in $\mathbf{D}/\pi\mathbf{D}$.

Proof. Suppose 1 and ω are not distinct in $\mathbf{D}/\pi\mathbf{D}$. Then $\omega \equiv 1 \pmod{\pi}$, indicating that $\pi \mid (1-\omega)$. Because $1-\omega$ is prime, π and $1-\omega$ must be associate to each other. Thus, $\mathbf{N}(\pi) = \mathbf{N}(1-\omega) = 3$, a contradiction. We can show that $\omega \not\equiv \omega^2 \pmod{\pi}$ and $1 \not\equiv \omega^2 \pmod{\pi}$ by the same method. ■

By Proposition 4.7, when $\mathbf{N}(\pi) \neq 3$, the residue classes of 1, ω and ω^2 are distinct mod π in $\mathbf{D}$. Thus, the "pre-requirement" for prime π in $\mathbf{D}$ is that $\mathbf{N}(\pi) \neq 3$. In the remainder of this section, we suppose π is prime in $\mathbf{D}$ such that $\mathbf{N}(\pi) \neq 3$.

Lemma 4.8. Suppose $\beta \in \mathbf{D}$ and suppose π is prime in $\mathbf{D}$ such that $\mathbf{N}(\pi) \neq 3$ and $\pi \nmid \beta$. If $\beta^3 \equiv 1 \pmod{\pi}$, then $\beta \equiv 1$, ω, or $\omega^2 \pmod{\pi}$.

Proof. Since $\beta^3 \equiv 1 \equiv 1^3 \pmod{\pi}$, indicating that $\beta^3 - 1^3 \equiv 0 \pmod{\pi}$. Thus, we have $\beta^3 - 1^3 \equiv (\beta-1)(\beta^2+\beta+1) \equiv (\beta-1)(\beta-\omega)(\beta-\omega^2) \equiv 0 \pmod{\pi}$. Since π is prime in $\mathbf{D}$, it must divide one of the factors of $(\beta-1)(\beta-\omega)(\beta-\omega^2)$. Therefore, we have $\beta \equiv 1$, ω, $\omega^2 \pmod{\pi}$. ■

Corollary 4.9. Suppose π is prime in $\mathbf{D}$ such that $\mathbf{N}(\pi) \neq 3$. Then we have $3 \mid \mathbf{N}(\pi)-1$.

Proof. Since 1, ω, and ω^2 are distinct in $\mathbf{D}/\pi\mathbf{D}$ when $\mathbf{N}(\pi) \neq 3$ by Proposition 4.7, we have $\{1, \omega, \omega^2\}$ is a cyclic group of order 3. By Lagrange Theorem, we have 3 divides the order of $\mathbf{D}/\pi\mathbf{D}^*$, indicating $3 \mid \mathbf{N}(\pi)-1$. ■

Since $a^{\mathbf{N}(\pi)-1} \equiv 1 \pmod{p}$ by Proposition 4.6, we assert that $a^{\frac{\mathbf{N}(\pi)-1}{3}}$ is a cube root of 1. Now we want to determine the possible values that $a^{\frac{\mathbf{N}(\pi)-1}{3}}$ can be.

Lemma 4.10. Suppose π is prime in $\mathbf{D}$ such that $\mathbf{N}(\pi) \neq 3$, and suppose $\pi \nmid \alpha$. Then the congruence $x^3 \equiv \alpha \pmod{\pi}$ has either no solutions or exactly three solutions.

Proof. If $x^3 \equiv \alpha \pmod{\pi}$ has any solutions, we want to show that $x^3 \equiv \alpha \pmod{\pi}$ has exactly three solutions. Suppose $\beta^3 \equiv x^3 \pmod{\pi}$ where $\beta \in \mathbf{D}$. Then we have the following:

$$\beta^3 - x^3 \equiv (\beta - x)(\beta^2 + \beta x + x^2) \equiv (\beta - x)(\beta - x\omega)(\beta - x\omega^2) \equiv 0 \pmod{\pi}.$$

Since π is prime in $\mathbf{D}$, it must divide one of the factors of $(\beta-x)(\beta-x\omega)(\beta-x\omega^2)$. Therefore, we have $\beta \equiv x$, $x\omega$ or $x\omega^2 \pmod{\pi}$. From Proposition 4.7, we have shown that 1, ω, ω^2 are distinct in $\mathbf{D}/\pi\mathbf{D}$. It follows that x, $x\omega$, and $x\omega^2$ are distinct as well. Therefore, if $x^3 \equiv \alpha \pmod{\pi}$ has any solutions, it must have exactly three solutions. ■

Corollary 4.11. Suppose $\alpha \in \mathbf{D}$ and suppose π is prime in $\mathbf{D}$ such that $\mathbf{N}(\pi) \neq 3$ and $\pi \nmid \alpha$. Then we have $\alpha^{(\mathbf{N}(\pi)-1)/3} \equiv 1$, ω or $\omega^2 \pmod{\pi}$.

Proof. By Lemma 4.8, we have shown that $1, \omega, \omega^2$ are the only cube roots of 1. Also, by Proposition 4.6, we have shown that $\alpha^{\mathbf{N}(\pi)-1} \equiv 1 \pmod{\pi}$. Since $3 \mid \mathbf{N}(\pi) - 1$, we get $(\mathbf{N}(\pi) - 1)/3$ is an integer. Therefore, $\alpha^{(\mathbf{N}(\pi)-1)/3}$ is a cube root of 1 mod π and can only be congruent to 1, ω, or ω^2 mod π, as desired. ■

We introduce *Euler's Criterion* in rational integers by applying Fermat's Little Theorem in rational integers. With Euler's Criterion, we are able to determine whether or not an arbitrary integer a can be written as the form of a perfect square of another integer x mod p. In particular, we introduce the term *quadratic residue* to classify whether or not $a \equiv x^2 \pmod{p}$ has solutions.

Definition 4.12. Let $p \in \mathbb{Z}$ be an odd prime and let $a \in \mathbb{Z}$ be relatively prime to p. Then a is called a quadratic residue modulo p if there exists $x \in \mathbb{Z}$ such that $a \equiv x^2 \pmod{p}$. Otherwise, a is called a quadratic nonresidue modulo p.

Proposition 4.13 (Euler's Criterion for $\mathbb{Z}$)**.** Let $p \in \mathbb{Z}$ be an odd prime and let $a \in \mathbb{Z}$ be relatively prime to p. Then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ if and only if a is a quadratic residue.

Proof. We need to prove both directions. Suppose a is a quadratic residue. Then there exists x such that $a \equiv x^2 \pmod{p}$. Therefore, we have

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \; x^{p-1} \equiv \; 1 \pmod{p}$$

by Theorem 4.4, as desired.

To prove the other direction, suppose $a^{\frac{p-1}{2}} = 1 \pmod{p}$. We want to show that there exists $x \in \mathbb{Z}/p\mathbb{Z}^*$ such that $a \equiv x^2 \pmod{p}$. Let b be a generator of the cyclic group $\mathbb{Z}/p\mathbb{Z}^*$, so $\operatorname{ord}(b) = (p-1)$. There exists $i \in \mathbb{Z}$ such that $a \equiv b^i \pmod{p}$. We now have $a^{\frac{p-1}{2}} \equiv (b^i)^{\frac{p-1}{2}} \equiv b^{\frac{i(p-1)}{2}} \equiv 1 \pmod{p}$. Thus, $\operatorname{ord}(b) \mid \frac{i(p-1)}{2}$, that is, there exists $k \in \mathbb{Z}$ such that $\frac{i(p-1)}{2} = k \operatorname{ord}(b)$. But $\operatorname{ord}(b) = (p-1)$, so $\frac{i(p-1)}{2} = k(p-1)$, indicating that $i = 2k$. Hence, we have $b^i = b^{2k} = (b^k)^2$ and a is a quadratic residue. ■

By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. By Proposition 4.13, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ if and only if a is a quadratic residue. Thus, we are able to conclude the following:

Proposition 4.14. Let p be an odd prime and a is relatively prime to p. Then

$$a^{\frac{p-1}{2}} \equiv \begin{cases} +1 \pmod{p} \text{ if } a \text{ is a quadratic residue} \\ -1 \pmod{p} \text{ if } a \text{ is a quadratic nonresidue.} \end{cases}$$

We can follow the discussion above to develop a parallel theory for cube roots in Eisenstein integers. We first introduce the term *cubic residue*.

Definition 4.15. Let $\alpha \in \mathbf{D}$, and let π be prime in $\mathbf{D}$. Then α is called a cubic residue modulo π if there exists $\beta \in \mathbf{D}$ such that $\alpha \equiv \beta^3 \pmod{\pi}$. Otherwise, α is called a cubic nonresidue modulo π.

Proposition 4.16 (Euler's Criterion for $\mathbf{D}$)**.** Let $\alpha \in \mathbf{D}$, and let π be prime in $\mathbf{D}$. Then $\alpha^{\frac{\mathbf{N}(\pi)-1}{3}} \equiv 1 \pmod{\pi}$ if and only if α is a cubic residue mod π.

Proof. We need to prove both directions. Suppose α is a cubic residue. There exists x such that $\alpha \equiv x^3 \pmod{\pi}$. Thus, $\alpha^{\frac{\mathbf{N}(\pi)-1}{3}} \equiv (x^3)^{\frac{\mathbf{N}(\pi)-1}{3}} \equiv x^{\mathbf{N}(\pi)-1} \equiv 1 \pmod{\pi}$, where the last congruence follows from Proposition 4.6.

To prove the other direction, suppose $\alpha^{\frac{\mathbf{N}(\pi)-1}{3}} \equiv 1 \pmod{\pi}$. We want to show that there exists $x \in \mathbf{D}/\pi\mathbf{D}^*$ such that $\alpha \equiv x^3 \pmod{\pi}$. Since $\mathbf{D}/\pi\mathbf{D}$ is a finite field, the multiplicative group $\mathbf{D}/\pi\mathbf{D}^*$ is a cyclic group. Let ζ be a generator of $\mathbf{D}/\pi\mathbf{D}^*$, so $\operatorname{ord}(\zeta) = \mathbf{N}(\pi) - 1$ by Proposition 4.2. There exists $i \in \mathbb{Z}$ such that $\alpha \equiv \zeta^i \pmod{\pi}$. We now have $\alpha^{\frac{\mathbf{N}(\pi)-1}{3}} \equiv (\zeta^i)^{\frac{\mathbf{N}(\pi)-1}{3}} \equiv \zeta^{\frac{i(\mathbf{N}(\pi)-1)}{3}} \pmod{\pi}$. Thus, $\operatorname{ord}(\zeta) \mid \frac{i(\mathbf{N}(\pi)-1)}{3}$, that is, there exists $k \in \mathbb{Z}$ such that $\frac{i(\mathbf{N}(\pi))-1}{3} = k \operatorname{ord}(\zeta)$. But $\operatorname{ord}(\zeta) = \mathbf{N}(\pi) - 1$, indicating that $i = 3k$. Hence, we have $\zeta^i = \zeta^{3k} = (\zeta^k)^3$ and α is a cubic residue mod π. ■

By Corollary 4.11, we have $\alpha^{\frac{\mathbf{N}(\pi)-1}{3}} \equiv 1$, ω or ω^2. By Proposition 4.16, we know that $\alpha^{\frac{\mathbf{N}(\pi)-1}{3}} \equiv 1 \pmod{\pi}$ if and only if α is a cubic residue. Thus, we are able to conclude the following.

Proposition 4.17. Let $\alpha \in \mathbf{D}$ and π be prime in $\mathbf{D}$. Then

$$\alpha^{\mathbf{N}(\pi)-1/3} = \begin{cases} 1 \pmod{\pi} \text{ if } \alpha \text{ is a cubic residue} \\ \omega \text{ or } \omega^2 \pmod{\pi} \text{ if } \alpha \text{ is a cubic nonresidue} \end{cases}$$

In the remainder of this section, we focus on how to calculate whether an integer a is a quadratic residue or quadratic nonresidue mod p. Similarly, we also focus on how to calculate whether an Eisenstein integer α is a cubic residue or cubic nonresidue mod π.

We introduce the multiplicative function *Legendre symbol* in rational integers. In particular, the value of Legendre symbol, $\left(\frac{a}{p}\right)$, can be defined by whether or not a is a quadratic residue mod p.

Definition 4.18. Let p be an odd prime number and a be an integer larger than 0. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 \text{ if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p} \\ 0 \text{ if } a \equiv 0 \pmod{p} \\ -1 \text{ if } a \text{ is a quadratic nonresidue } p \end{cases}$$

The Legendre symbol can be generalized to the *Jacobi symbol* in rational integers. The Jacobi symbol obeys the same rule as the Legendre symbol. The difference between the Legendre symbol and Jacobi symbol is that the "denominator" in the Legendre symbol must be a prime integer while the "denominator" in Jacobi symbol can be any odd integer.

Definition 4.19. Let n be any positive odd integer and $a \geqslant 0$ any integer. The Jacobi symbol $\left(\frac{a}{n}\right)$ is defined as $\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$ where $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$.

With the definition of Legendre symbol and Jacobi symbol in rational integers, we are able to deduce properties of Jacobi symbol, including the law of quadratic reciprocity and its corresponding supplements, in order to make it even easier to calculate.

Proposition 4.20 (Properties of Jacobi symbol)**.** Suppose m, n are odd integers and $a, b \in \mathbb{Z}$. We have:

1. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
2. $\left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$
3. If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

Theorem 4.21 (Quadratic Reciprocity)**.** Let m, n be odd positive coprime integers. Then

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right).$$

Proposition 4.22 (Supplements of Quadratic Reciprocity)**.** Let n be an odd integer.

1. $$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 \text{ if } n \equiv 1 \pmod{4} \\ -1 \text{ if } n \equiv 3 \pmod{4} \end{cases}$$
2. $$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 \text{ if } n \equiv 1 \text{ or } 7 \pmod{8} \\ -1 \text{ if } n \equiv 3 \text{ or } 5 \pmod{8} \end{cases}$$

Example 4.23. Suppose $a = 1001$ and $p = 9907$. We calculate the value of $\left(\frac{1001}{9907}\right)$. We first apply the quadratic reciprocity:

$$\left(\frac{1001}{9907}\right) = \left(\frac{9907}{1001}\right).$$

Since 9907 is larger than 1001, we use the Euclidean Algorithm as defined in Definition 2.8 to simplify $\left(\frac{9907}{1001}\right)$. Since $9907 = 1001 \cdot 9 + 898$, we have

$$\left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right).$$

By applying the properties of thr Jacobi symbol, we then get

$$\left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right).$$

Continuing this simplifying process, we have

$$\left(\frac{1001}{9907}\right) = \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right) = \left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right)$$
$$\left(\frac{1001}{449}\right) = \left(\frac{103}{449}\right) = \left(\frac{449}{103}\right) = \left(\frac{37}{103}\right) = \left(\frac{103}{37}\right)$$
$$\left(\frac{103}{37}\right) = \left(\frac{29}{37}\right) = \left(\frac{37}{29}\right) = \left(\frac{8}{29}\right) = \left(\frac{2}{29}\right)^3 = -1$$

We now introduce the analog of Legendre symbol in the Eisenstein integers, *cubic residue character*, which is denoted $\left(\frac{\alpha}{\pi}\right)_3$. Its value is determined by whether or not α is a cubic residue mod π.

Definition 4.24. Let $\alpha \in \mathbf{D}$ and π be prime in $\mathbf{D}$. If $\mathbf{N}(\pi) \neq 3$, the cubic residue character $\left(\frac{\alpha}{\pi}\right)_3$ is defined as:

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 \text{ if } \alpha \equiv 0 \pmod{\pi} \\ \alpha^{\mathbf{N}(\pi)-1/3} \pmod{\pi} \text{ otherwise.} \end{cases}$$

By applying Proposition 4.16, we can observe that:

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 1 \text{ if } \alpha \text{ is a cubic residue modulo } \pi \text{ and } \alpha \not\equiv 0 \pmod{\pi} \\ 0 \text{ if } \alpha \equiv 0 \pmod{\pi} \\ \omega \text{ or } \omega^2 \text{ if } \alpha \text{ is a cubic nonresidue modulo } \pi \end{cases}$$

The cubic residue character plays the same role in the theory of cubic residues as the Legendre symbol plays in the theory of quadratic residues. However, there is only one option for the answer of a when it is a quadratic nonresidue mod p while there are two options for the answer of α when it is a cubic nonresidue mod π. Thus, the definition of Legendre symbol for integers $\left(\frac{a}{p}\right)$ is different from that of cubic residue character for Eisenstein integers $\left(\frac{\alpha}{\pi}\right)_3$.

We also generalize the cubic residue character to a cubic Jacobi symbol in the Eisenstein integers. By using the cubic Jacobi symbol, determining whether or not an element in $\mathbf{D}/\pi\mathbf{D}^*$ is a cubic residue can be done computationally. In particular, the cubic Jacobi symbol obeys the same rule as the cubic character residue.

Definition 4.25. If $\alpha, \beta \in \mathbf{D}$ with $3 \nmid \mathbf{N}(\beta)$, we define

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

where $\beta = \pi_1^{e_1}\pi_2^{e_2}\pi_3^{e_3}...\pi_k^{e_k}$. In particular, $\left(\frac{\alpha}{\pi}\right)_3$ represents the cubic residue character.

With the definition of cubic residue character and cubic Jacobi symbol in Eisenstein integers, we are able to state properties of cubic Jacobi symbol, including the cubic reciprocity and the supplements of cubic reciprocity.

Proposition 4.26 (Properties of Cubic Jacobi Symbol)**.**

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

2. $\left(\frac{\pi}{\alpha\beta}\right)_3 = \left(\frac{\pi}{\alpha}\right)_3 \left(\frac{\pi}{\beta}\right)_3$
   (1) and (2) are also called *the Bimultiplicity of the Cubic Jacobi Symbol*.

3. If $\alpha \equiv \beta \pmod{\pi}$, then $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

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

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

Theorem 4.27 (Cubic Reciprocity)**.** Let π_1, π_2 be primary in $\mathbf{D}$. Suppose that $\mathbf{N}(\pi_1), \mathbf{N}(\pi_2) \neq 3$ and $\mathbf{N}(\pi_1) \neq \mathbf{N}(\pi_2)$. Then $\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3$

Moreover, when π is primary in $\mathbf{D}/\pi\mathbf{D}$, we are able to state the supplements of cubic reciprocity.

Proposition 4.28 (Supplements of Cubic Reciprocity)**.** Suppose that $\mathbf{N}(\pi) \neq 3$. Suppose π is a primary prime in $\mathbf{D}$, say $\pi = a + b\omega$ where $a = 3m - 1$. Then we have:

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

and

$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{m+b}.$$

Proof. This can be proved by applying the fact that $(1-\omega)^2 = -3\omega$ and using the properties of the cubic residue character and cubic reciprocity. ■

Example 4.29. Suppose $\alpha = 10$ and $\pi = 5 + 6\omega$. We calculate the value of $\left(\frac{10}{5+6\omega}\right)_3$ by applying properties of the cubic character residue, cubic reciprocity, and the corresponding supplements.

Since $\mathbf{N}(10)$ is larger than $\mathbf{N}(5+6\omega)$, we first simplify $\left(\frac{10}{5+6\omega}\right)_3$ by reducing 10 modulo $5 + 6\omega$. In order to achieve this, we use the Euclidean algorithm, as described in Proposition 3.4, to compute $10 \div (5 + 6\omega)$.

We begin by rationalizing the denominator by multiplying by the complex conjugate of $5 + 6\omega$, which is $-1 - 6\omega$:

$$\frac{10}{(5+6\omega)} \cdot \frac{(-1-6\omega)}{(-1-6\omega)} = -\frac{10}{31} - \frac{60}{31}\omega.$$

The closet rational integer to $-\frac{10}{31}$ and $-\frac{60}{31}$ are 0 and -2 respectively. Hence, as in Proposition 3.4, we take $0-2\omega$ as the integer quotient of $\frac{10}{(5+6\omega)}$, and observe we can write $10=(-2\omega)(5+6\omega)+(-2-2\omega)$. (Note that $\mathbf{N}(-2-\omega)<\mathbf{N}(10)$.)

$$\left(\frac{10}{5+6\omega}\right)_3=\left(\frac{-2-2\omega}{5+6\omega}\right)_3=\left(\frac{(2)(-1-\omega)}{5+6\omega}\right)_3.$$

By properties of cubic Jacobi symbol, we have:

$$\left(\frac{(2)(-1-\omega)}{5+6\omega}\right)_3=\left(\frac{2}{5+6\omega}\right)_3\left(\frac{-1-\omega}{5+6\omega}\right)_3.$$

By cubic reciprocity, we have:

$$\left(\frac{2}{5+6\omega}\right)_3=\left(\frac{5+6\omega}{2}\right)_3=(5+6\omega)^{(\mathbf{N}(2)-1)/3}\equiv 1 \pmod{5+6\omega}.$$

Since $1+\omega+\omega^2=0$, we have $-1-\omega=\omega^2$, indicating that:

$$\left(\frac{-1-\omega}{5+6\omega}\right)_3=\left(\frac{\omega^2}{5+6\omega}\right)_3=(\omega^2)^{(\mathbf{N}(5+6\omega)-1)/3}=\omega^{20}=\omega^2 \pmod{5+6\omega}.$$

Thus, we have:

$$\left(\frac{10}{5+6\omega}\right)_3=1\cdot\omega^2=\omega^2 \pmod{5+6\omega}.$$

Since $\left(\frac{10}{5+6\omega}\right)_3\neq 1$, we conclude that 10 is a cubic nonresidue modulo $5+6\omega$.

5 Congruence Criteria for Eisenstein Pseudocubes

In this section, we use the technique of congruential sieving to compute a table of Eisenstein pseudocubes. First, we introduce the definition of an Eisenstein pseudocube. Then, we describe the congruential sieving method that we will use to create the Eisenstein pseudocubes table. Finally, we will construct the Eisenstein pseudocubes table based on the three types of primes in Eisenstein integers.

Before introducing the definition of an Eisenstein pseoducbe, we first briefly explain the main idea behind the prefix "pseudo." An element can be called "pseudo" if it seems to have some characteristics but it actually does not have such characteristics. Specifically, an "Eisenstein pseudocube" is an element in $\mathbb{Z}[\omega]$ seems to fulfill the requirement of being a cube but in fact is not a cube.

Definition 5.1. Let p be a fixed rational prime. We say $\mu_p=a+b\omega\in\mathbb{Z}[\omega]$ is an Eisenstein pseudocube for p if the following conditions hold:

1. μ_p is primary;
2. $\gcd(a,b)=1$;
3. $\left(\frac{q}{\mu_p}\right)_3=1$ for all rational primes $q\in\mathbb{Z}$ that $q\leqslant p$;

4. μ_p not a cube in $\mathbb{Z}[\omega]$.

In particular, we will call μ_p a minimal Eisenstein pseudocube for the prime p if the norm of μ_p is the smallest among all the norms of Eisenstein pseudocube for p.

We explain this sense in which μ_p resembles a cube in $\mathbb{Z}[\omega]$, suppose μ_p is actually a cube in $\mathbb{Z}[\omega]$. We then can write $\mu_p = \alpha^3$ for some $\alpha \in \mathbb{Z}[\omega]$, indicating that $\left(\frac{q}{\mu_p}\right)_3 = \left(\frac{q}{\alpha^3}\right)_3$. After applying the bimultiplicity of the cubic character as shown in Proposition 4.26, we have $\left(\frac{q}{\mu_p}\right)_3 = \left(\frac{q}{\alpha^3}\right)_3 = \left(\frac{q}{\alpha}\right)_3\left(\frac{q}{\alpha}\right)_3\left(\frac{q}{\alpha}\right)_3$. Based on Lemma 4.10, we know that $\left(\frac{q}{\alpha}\right)_3$ equals to 1, ω, ω^2, so we always have $\left(\frac{q}{\alpha}\right)_3\left(\frac{q}{\alpha}\right)_3\left(\frac{q}{\alpha}\right)_3 = 1$ whether or not q is a cubic residue mod μ_p.

Suppose $\mu_p = x_p + y_p$, we then use a method called congruential sieving [9] to compute a table of Eisenstein pseudocubes μ_p. The main idea behind the congruential sieving is to delete all "impossible" pseudocubes μ_p for possible prime p by using the criterion $\left(\frac{q}{\mu_p}\right)_3 \neq 1$ in Eisenstein integers for some $q < p$, then those are left are pseudocubes. We need only test starting from the smallest remaining value to find the first one that is not an actual cube. As described by Williams and Wooding [10], we need to first find all possible values of μ_p by establishing a set of acceptable residue conditions S_q on μ_p for all primes $q \leqslant p$ before applying congruential sieving. Based on three types of primes in Eisenstein integers, we consider three cases of Eisenstein pseudocubes.

Case 1: $q \equiv -1 \pmod 3$

In this case, $q = q + 0\omega$ is primary based on the Definition 3.10. Since μ_p is also primary, we can invoke cubic reciprocity from Theorem 4.27:

$$1 = \left(\frac{q}{\mu_p}\right)_3 = \left(\frac{\mu_p}{q}\right)_3.$$

Since $\left(\frac{\mu_p}{q}\right)_3 = 1$, we conclude μ_p is a cubic residue mod q. We compute the total number of cubic residues mod q to see how many possible values remain for μ_p mod q. As shown in Proposition 4.3, $\mathbf{D}/\pi\mathbf{D}^*$ is a finite field with $\mathbf{N}(\pi) - 1$ elements where $\mathbf{D}$ represents $\mathbb{Z}[\omega]$. In this case, since $q \equiv 2 \pmod 3$, we have q is prime in $\mathbf{D}$ and the number of elements in $\mathbf{D}/q\mathbf{D}^*$ is $q^2 - 1$ based on Proposition 3.9. there is a homomorphism, denoted $f(\overline{\alpha}) = \overline{\alpha}^3$, from $\mathbf{D}/\pi\mathbf{D}^*$ to $\mathbf{D}/\pi\mathbf{D}^*$. Since 1 is the identity element in $\mathbf{D}/\pi\mathbf{D}^*$ and there are 3 elements cubing to 1 based on Lemma 4.10, we conclude that the kernel of f consists of those three elements: $\{1, \omega, \omega^2\}$. Therefore, by the first Homomorphism Theorem, the image of f has cardinality $\frac{q^2-1}{3}$. That is, there are $\frac{q^2-1}{3}$ residue classes μ_p in $\mathbf{D}/\pi\mathbf{D}$ satisfying $\left(\frac{\mu_p}{q}\right) = 1$.

Now we focus on specific solutions of μ_p by computing $\mu_p \equiv (a + b\omega)^3 \pmod q$ for all $0 \leqslant a, b < q$. Since $(a + b\omega)^3 = a^3 + (b\omega)^3 + 3a^2(b\omega) + 3a(b\omega)^2$, we then have $(a + b\omega)^3 = (a^3 + b^3 - 3ab^2) + (3a^2b - 3ab^2)\omega = x_p + y_p\omega$ after replacing $\omega^3 = 1$

and $\omega^2 = -1 - \omega$. Thus, we conclude:

$$x_p \equiv a^3 - 3ab^2 + b^3 \pmod q$$
$$y_p \equiv 3ab(a-b) \pmod q.$$

Since $0 \leqslant a, b < q$, there are a total of $q^2 - 1$ different pairs (a, b). Since μ_p is a primary, then $x_p \equiv 2 \pmod 3$ and $y_p \equiv 0 \pmod 3$. Since q and 3 are relatively prime, we then conclude that $x_p \equiv 2 \equiv a^3 - 3ab^2 + b^3 \pmod q$ and $y_p \equiv 0 \equiv 3ab(a-b) \pmod q$. We now consider three different cases about the pair (a, b).

Case 1 $a \equiv 0 \pmod 3$. Since $a^3 - 3ab^2 + b^3 \equiv 2 \pmod q$, we then have $b \equiv 2 \pmod 3$. Based on the fact that $0 \leqslant a, b < q$ and $q \equiv -1 \pmod 3$, there are $\frac{q+1}{3}$ different possible values for a and $\frac{q-2}{3}$ different possible values for b. Thus, there are in total $\left(\frac{q+1}{3}\right)\left(\frac{q-2}{3}\right) = \frac{q^2-q-2}{9}$ possibilities for the pair (a, b).

Case 2 $a \equiv 1 \pmod 3$. Since $a^3 - 3ab^2 + b^3 \equiv 2 \pmod q$, we then have $b \equiv 1 \pmod 3$. Based on the fact that $0 \leqslant a, b < q$ and $q \equiv -1 \pmod 3$, there are $\frac{q+1}{3}$ different possible values for a and $\frac{q+1}{3}$ different possible values for b. Thus, there are in total $\left(\frac{q+1}{3}\right)\left(\frac{q+1}{3}\right) = \frac{q^2+2q+1}{9}$ possibilities for the pair (a, b).

Case 3 $a \equiv 2 \pmod 3$. Since $a^3 - 3ab^2 + b^3 \equiv 2 \pmod q$, we then have $b \equiv 0 \pmod 3$. Based on the fact that $0 \leqslant a, b < q$ and $q \equiv -1 \pmod 3$, there are $\frac{q-2}{3}$ different possible values for a and $\frac{q+1}{3}$ different possible values for b. Thus, there are in total $\left(\frac{q-2}{3}\right)\left(\frac{q+1}{3}\right) = \frac{q^2-q-2}{9}$ possibilities for the pair (a, b).

However, there are some repetitions in Case 1 and Case 3. Specifically, in Case 1, the pair $(a, b) = (0, x)$ will produce exactly the same x_p and y_p as the pair $(a, b) = (x, 0)$ in Case 3 where $0 \leqslant x < q$. Therefore, we need to subtract the number of repetitions, which equals to $\frac{q-2}{3}$.

On the other hand, we notice that when $y_p = 0$, x_p can be any number smaller than q. Thus, we focus on how to calculate the "remaining" solutions. When one of the a, b equals 0 and the other one congruent to 0 mod 3, the pair (a, b) will produce a new x_p and y_p. Since there are $\frac{q-2}{3}$ different numbers strictly smaller than and congruent to 0 mod 3, indicating that there are $\frac{q-2}{3}$ different new μ_p. After combining all these cases, there are

$$\frac{q^2-q-2}{9} + \frac{q^2+2q+1}{9} + \frac{q^2-q-2}{9} - \frac{q-2}{3} + \frac{q-2}{3} = \frac{q^2-1}{3}$$

such solutions modulo q.

Example 5.2. The set of acceptable residues for Eisenstein pseudocubes modulo 11 is given by

$$\begin{aligned} S_{11} = \{&(1+0\omega),(2+0\omega),(3+0\omega),(4+0\omega),(5+0\omega),(6+0\omega),(7+0\omega),(8+0\omega),\\ &(9+0\omega),(10+0\omega),(3+1\omega),(6+1\omega),(9+1\omega),(1+2\omega),(6+2\omega),(7+2\omega),\\ &(5+3\omega),(7+3\omega),(9+3\omega),(1+4\omega),(2+4\omega),(3+4\omega),(1+5\omega),(4+5\omega),\\ &(8+5\omega),(3+6\omega),(7+6\omega),(10+6\omega),(8+7\omega),(9+7\omega),(10+7\omega),(2+8\omega),\\ &(4+8\omega),(6+8\omega),(4+9\omega),(5+9\omega),(10+9\omega),(2+10\omega),(5+10\omega),(8+10\omega)\}. \end{aligned}$$

Case 2: $q = 3$ In this case, we first observe that $-3\omega = (1-\omega)^2$. Then we have:

$$\left(\frac{-3\omega}{\mu_p}\right)_3 = \left(\frac{(1-\omega)^2}{\mu_p}\right)_3.$$

Multiplying both sides by $\left(\frac{\omega^2}{\mu_p}\right)_3$, we have:

$$\left(\frac{\omega^2}{\mu_p}\right)_3\left(\frac{-3\omega}{\mu_p}\right)_3 = \left(\frac{\omega^2}{\mu_p}\right)_3\left(\frac{(1-\omega)^2}{\mu_p}\right)_3.$$

By the properties of the cubic Jacobi symbol from Proposition 4.26, we get:

$$\left(\frac{-3\omega\cdot\omega^2}{\mu_p}\right)_3 = \left(\frac{(1-\omega)^2\cdot\omega^2}{\mu_p}\right)_3.$$

Then we multiply both sides by $\left(\frac{-1}{\mu_p}\right)_3$, which equals to 1 no matter what value μ_p is. Thus, we have:

$$\left(\frac{-3}{\mu_p}\right)_3\left(\frac{-1}{\mu_p}\right)_3 = \left(\frac{\omega(1-\omega)}{\mu_p}\right)_3^2\cdot 1.$$

$$\left(\frac{3}{\mu_p}\right)_3 = \left(\frac{\omega(1-\omega)}{\mu_p}\right)_3^2$$

Since μ_p is primary, we can write $\mu_p = x_p + y_p\omega = (-1)^{k-1}\prod_{i-1}^{k}\alpha_i$ where $\alpha_i = r_i + s_i\omega$ are primary primes. From the supplement of the cubic reciprocity as shown in Proposition 4.28, we know that:

$$\left(\frac{1-\omega}{\alpha_i}\right)_3 = \omega^{\frac{2(r_i+1)}{3}}$$

and

$$\left(\frac{\omega}{\alpha_i}\right)_3 = \omega^{\frac{r_i+1+s_i}{3}}.$$

Then we have:

$$\left(\frac{1-\omega}{\mu_p}\right)_3 = \prod_{i=1}^{k}\omega^{\frac{2(r_i+1)}{3}} = \omega^{2\sum_{i=1}^{k}(r_i+1)/3}$$

and

$$\left(\frac{\omega}{\mu_p}\right)_3 = \prod_{i=1}^{k} \omega^{\frac{r_i+1+s_i}{3}} = \omega^{\sum_{i=1}^{k}(r_i+1)/3+\sum_{i=1}^{k} s_i/3}.$$

After multiplying these two terms, we get:

$$\begin{aligned}\left(\frac{\omega(1-\omega)}{\mu_p}\right)_3 &= \omega^{2\sum_{i=1}^{k}(r_i+1)/3} \cdot \omega^{\sum_{i=1}^{k}(r_i+1)/3+\sum_{i=1}^{k} s_i/3} \\ &= \omega^{2\sum_{i=1}^{k}(r_i+1)/3+\sum_{i=1}^{k}(r_i+1)/3+\sum_{i=1}^{k} s_i/3} \\ &= \omega^{\sum_{i=1}^{k} 2(r_i+1)/3+(r_i+1)/3+\sum_{i=1}^{k} s_i/3} \\ &= \omega^{\sum_{i=1}^{k}(r_i+1)+\sum_{i=1}^{k} s_i/3}\end{aligned}$$

Since α_i is a primary, it needs to fulfill that $r_i \equiv 2 \pmod 3$ and $s_i \equiv 0 \pmod 3$. After considering $\omega^3 = 1$, we get:

$$\left(\frac{\omega(1-\omega)}{\mu_p}\right)_3 = \omega^{\sum_{i=1}^{k}(r_i+1)+\sum_{i=1}^{k} s_i/3} = \omega^{\sum_{i=1}^{k} s_i/3}.$$

As a result, we have:

$$\begin{aligned}\left(\frac{3}{\mu_p}\right)_3 &= \left(\frac{\omega(1-\omega)}{\mu_p}\right)_3^2 \\ &= (\omega^{\sum_{i=1}^{k} s_i/3})^2 \\ &= \omega^{\frac{2}{3}\sum_{i=1}^{k} s_i}.\end{aligned}$$

In conclusion, we have $\left(\frac{\omega(1-\omega)}{\mu_p}\right)_3 = \omega^{\sum_{i=1}^{k} s_i/3}$ and $\left(\frac{3}{\mu_p}\right)_3 = \omega^{\frac{2}{3}\sum_{i=1}^{k} s_i}$.

Lemma 5.3. Let $\mu_p = x_p + y_p\omega = (-1)^{n-1}\prod_{i=1}^{n}\alpha_i$ where $\alpha_i = r_i + s_i\omega$ are primary primes. Then $x_p \equiv (-1)^{n-1}\prod_{i=1}^{n} r_i \pmod 9$ and $y_p \equiv \sum_{i=1}^{n} s_i \pmod 9$.

Proof. We prove by induction. If $n = 1$, we have $\mu_p = x_p + y_p\omega = \alpha_1 = r_1 + s_1\omega$. This proves that $x_p \equiv r_1 \pmod 9$ and $y_p \equiv s_1 \pmod 9$. Now we let $a_j = r_j + s_j\omega$ and $a_k = r_k + s_k\omega$ be primary. According to the definitions of primary, we can write $s_i = 3S_i$ and $r_i = -1 + 3R_i$ for some $S_i, R_i \in \mathbb{Z}$. Then we have:

$$\begin{aligned}-(r_k + s_k\omega)(r_j + s_j\omega) &= -(r_k + 3S_k\omega)(r_j + 3S_j\omega) \\ &= -r_kr_j - 3(S_jr_k + S_kr_j)\omega \\ &= -r_kr_j - 3(S_j(-1+3R_k) + S_k(-1+3R_j))\omega \\ &= -r_kr_j - 3(-S_k + 3R_jS_k - S_j + 3R_kS_j)\omega \\ &= -r_kr_j + (s_k + s_j)\omega \pmod 9\end{aligned}$$

which is still primary.

Therefore, we conclude that:

$$(-1)^{n-1}\prod_{i=1}^{n}(r_i+s_i\omega)\equiv(-1)^{n-1}\prod_{i=1}^{n}r_i+\sum_{i=1}^{n}s_i\omega \pmod 9.$$

Based on the assumption that $\mu_p = x_p + y_p\omega = (-1)^{n-1}\prod_{i=1}^{n} r_i + s_i\omega$, we get:

$$x_p \equiv (-1)^{n-1}\prod_{i=1}^{n} r_i \pmod 9$$

and

$$y_p \equiv \sum_{i=1}^{n} s_i \pmod 9.$$

■

From Lemma 5.3, we have $y_p = \sum_{i=1}^{k} s_i \pmod 9$, indicating that $y_p/3 \equiv \sum_{i=1}^{k} s_i/3 \pmod 3$. Therefore, we obtain $\left(\frac{3}{\mu_p}\right)_3 = \omega^{\frac{2}{3}\sum_{i=1}^{k} s_i} = \omega^{\frac{2}{3}y_p}$. Thus, if $\left(\frac{3}{\mu_p}\right)_3 = \omega^{\frac{2}{3}y_p} = 1$, then $3 \mid \frac{y_p}{3}$ based on the fact $\omega^3 = 1$, which is equivalent to $9 \mid y_p$. After considering the requirement that μ_p is primary, we conclude that if $\left(\frac{3}{\mu_p}\right)_3 = 1$, then $9 \mid y_p$ and $x_p \equiv -1 \pmod 3$.

Example 5.4. The set of acceptable residues for Eisenstein pseudocube modulo 9 is given by

$$S_9 = \{(2+0\omega), (5+0\omega), (8+0\omega)\}.$$

Case 3: $q \equiv 1 \pmod 3$

In this case, since $q \equiv 1 \pmod 3$, we can write $q = \pi_q\overline{\pi_q}$ where $\pi_q = a + b\omega$ is primary based on Proposition 3.9. The conjugate of π_q, denoted $\overline{\pi_q}$, equals $(a-b) - b\omega$ and is also primary.

Lemma 5.5. Let q be a rational prime, $q = \pi_q\overline{\pi_q}$ with $\pi_q \in \mathbb{Z}[\omega]$ prime and primary. Then we have $\left(\frac{q}{\mu_p}\right)_3 = 1$ if and only if $\left(\frac{\mu_p}{\pi_q}\right)_3 = \left(\frac{\overline{\mu_p}}{\pi_q}\right)_3$

Proof. Since $q, \mu_p, \pi_q, \overline{\pi_q}$ are all primary, we can invoke the cubic reciprocity and the properties of cubic Jacobi symbol to get:

$$\begin{aligned}\left(\frac{q}{\mu_p}\right)_3 &= \left(\frac{\pi_q\overline{\pi_q}}{\mu_p}\right)_3 = \left(\frac{\pi_q}{\mu_p}\right)_3\left(\frac{\overline{\pi_q}}{\mu_p}\right)_3 \\ &= \left(\frac{\mu_p}{\pi_q}\right)_3\left(\frac{\mu_p}{\overline{\pi_q}}\right)_3 = \left(\frac{\mu_p}{\pi_q}\right)_3\overline{\left(\frac{\overline{\mu_p}}{\pi_q}\right)_3} \\ &= \left(\frac{\mu_p}{\pi_q}\right)_3\left(\frac{\overline{\mu_p}}{\pi_q}\right)_3^{-1}\end{aligned}$$

Therefore, we conclude that $\left(\frac{q}{\mu_p}\right)_3 = 1$ if and only if $\left(\frac{\mu_p}{\pi_q}\right)_3 = \left(\frac{\overline{\mu_p}}{\pi_q}\right)_3$. ■

If $\left(\frac{q}{\mu_p}\right)_3 = 1$, then we have $\left(\frac{\mu_p}{\pi_q}\right)_3 = \left(\frac{\overline{\mu_p}}{\pi_q}\right)_3$ from Lemma 5.5. Based on the Definition 4.24, we have $\left(\frac{\mu_p}{\pi_q}\right)_3 \equiv \mu_p^{\frac{q-1}{3}} \pmod{\pi_q}$ and $\left(\frac{\overline{\mu_p}}{\pi_q}\right)_3 \equiv \overline{\mu}_p^{\frac{q-1}{3}} \pmod{\pi_q}$. Thus, we conclude that $\mu_p^{\frac{q-1}{3}} \equiv \overline{\mu}_p^{\frac{q-1}{3}} \pmod{\pi_q}$. After taking complex conjugate of both $\left(\frac{\mu_p}{\pi_q}\right)_3$ and $\left(\frac{\overline{\mu_p}}{\pi_q}\right)_3$, we get $\left(\frac{\overline{\mu_p}}{\overline{\pi_q}}\right)_3 = \left(\frac{\mu_p}{\overline{\pi_q}}\right)_3$. Based on the Definition 4.24, we have $\left(\frac{\overline{\mu_p}}{\overline{\pi_q}}\right)_3 \equiv \overline{\mu_p}^{\frac{q-1}{3}} \pmod{\overline{\pi_q}}$ and $\left(\frac{\mu_p}{\overline{\pi_q}}\right)_3 \equiv \overline{\mu}_p^{\frac{q-1}{3}} \pmod{\overline{\pi_q}}$. This indicates that $\overline{\mu_p}^{\frac{q-1}{3}} \equiv \mu_p^{\frac{q-1}{3}} \pmod{\overline{\pi_q}}$.

After combining $\mu_p^{\frac{q-1}{3}} \equiv \overline{\mu}_p^{\frac{q-1}{3}} \pmod{\pi_q}$ and $\overline{\mu_p}^{\frac{q-1}{3}} \equiv \mu_p^{\frac{q-1}{3}} \pmod{\overline{\pi_q}}$, we conclude that:

$$\left(\frac{q}{\mu_p}\right)_3 = 1 \text{ if and only if } \mu_p^{\frac{q-1}{3}} \equiv \overline{\mu_p}^{\frac{q-1}{3}} \pmod{\pi_q\overline{\pi_q}}.$$

Since $\pi_q\overline{\pi_q} = q$, we have:

$$\left(\frac{q}{\mu_p}\right)_3 = 1 \text{ if and only if } \mu_p^{\frac{q-1}{3}} \equiv \overline{\mu_p}^{\frac{q-1}{3}} \pmod{q}. \tag{5.1}$$

As suggested by Williams and Wooding [10], Lucas sequence is able to help us to determine a set of congruence conditions on μ_p based on Equation 5.1. Now suppose $\mu_p = x_p + y_p\omega$. We then can rewrite $\mu_p^{\frac{q-1}{3}} \equiv \overline{\mu_p}^{\frac{q-1}{3}} \pmod{q}$ to be:

$$(x_p + y_p)\omega^{\frac{q-1}{3}} \equiv \overline{(x_p + y_p\omega)}^{\frac{q-1}{3}} \equiv (x_p - y_p) - y_p\omega \pmod{q}. \tag{5.2}$$

When $q \mid y_p$, Equation 5.2 becomes $x_p \equiv x_p \pmod{q}$ where $1 \leqslant x_p \leqslant q-1$. Thus, $\left(\frac{q}{\mu_p}\right)_3 = 1$ holds whenever $q \mid y_p$ and $1 \leqslant x_p \leqslant q-1$.

Now we consider the remaining case that $q \nmid y_p$. Assume $S_n(x,y), T_n(x,y) \in \mathbb{Z}[x,y]$ are two recurring sequences where:

$$S_1(x,y) = x \tag{5.3}$$
$$T_1(x,y) = y \tag{5.4}$$
$$S_n + T_n\omega = (S_1 + T_1\omega)^n \tag{5.5}$$

with $S_n, T_n \in \mathbb{Z}$. By taking complex conjugate, we have $\overline{S_n + T_n\omega} = S_n + T_n\omega^2$. Thus, we get:

$$S_n + T_n\omega^2 = (S_1 + T_1\omega^2)^n. \tag{5.6}$$

After subtracting Equation 5.6 from Equation 5.5, we get:

$$(\omega - \omega^2)T_n = (S_1 + T_1\omega)^n - (S_1 + T_1\omega^2)^n. \tag{5.7}$$

Now we write $\alpha = \mu_p = x_p + y_p\omega$ and $\beta = \overline{\mu_p} = x_p + y_p\omega^2$. We can represent T_n in a closed form:

$$T_n = \frac{\alpha^n - \beta^n}{\omega - \omega^2}.$$

In particular, we see that $T_0 = \dfrac{\alpha^0 - \beta^0}{\omega - \omega^2} = 0$ and $T_1 = \dfrac{\alpha^1 - \beta^1}{\omega - \omega^2} = y_p$. Now suppose $G = \alpha + \beta$ and $H = \alpha\beta$. Thus, we have $T_n(G, H)$ is given by the second-order recurrence: $T_{n+2} = GT_{n+1} - HT_n$. Therefore, the Equation 5.1 can be rewrite as:

$$\left(\frac{q}{\mu_p}\right)_3 = 1 \text{ if and only if } q \mid \left(\alpha^{\frac{q-1}{3}} - \beta^{\frac{q-1}{3}}\right). \tag{5.8}$$

Hence, we have:

$$\left(\frac{q}{\mu_p}\right)_3 = 1 \text{ if and only if } q \mid T_{\frac{q-1}{3}}(G, H). \tag{5.9}$$

Since $q \nmid y_p$, we now define a new term z_p where $z_p \equiv x_p y_p^{-1} \pmod{q}$. According to Equation 5.8, we have $q \mid (\alpha^{\frac{q-1}{3}} - \beta^{\frac{q-1}{3}})$, indicating that $\alpha^{\frac{q-1}{3}} \equiv \beta^{\frac{q-1}{3}} \pmod{q}$. Since $\alpha = \mu_p = x_p + y_p\omega$ and $\beta = \overline{\mu_p} = x_p + y_p\omega^2$, we then have

$$(x_p + y_p\omega)^{\frac{q-1}{3}} \equiv (x_p + y_p\omega^2)^{\frac{q-1}{3}} \pmod{q}.$$

This indicates that $(z_q + \omega)^{\frac{q-1}{3}} \equiv (z_p + \omega^2)^{\frac{q-1}{3}} \pmod{q}$. Now setting $\alpha' = z_p + \omega$, and $\beta' = z_p + \omega^2$, we obtain:

$$\left(\frac{q}{\mu_p}\right)_3 = 1 \text{ if and only if } q \mid T_{\frac{q-1}{3}}(G', H') \tag{5.10}$$

where

$$\begin{aligned} G' &= \alpha' + \beta' = \alpha' + \beta' - (\omega^2 + \omega + 1) = (\alpha' - \omega) + (\beta' - \omega^2) - 1 = 2z_p - 1 \\ H' &= \alpha'\beta' = (z_p + \omega)(z_p + \omega^2) = z_p^2 + z_p(\omega + \omega^2) + 1 = z_p^2 - z_p + 1. \end{aligned}$$

Furthermore, we define a polynomial $T_n(z)$ that only contains one variable $z \in \mathbb{Z}$ such that:

$$T_0(z) = 0 \tag{5.11}$$

$$T_1(z) = 1 \tag{5.12}$$

$$T_{n+1}(z) = G'T_n(z) - H'T_{n-1}(z) = (2z - 1)T_n(z) - (z^2 - z + 1)T_{n-1}(z). \tag{5.13}$$

Then we observe that $T_n(z) = U_n(G', H')$ where $U_n = \dfrac{\alpha'^n - \beta'^n}{\alpha' - \beta'}$ is the Lucas function such that

$$G' = \alpha' + \beta' = 2z - 1 \tag{5.14}$$

$$H' = \alpha'\beta' = z^2 - z + 1. \tag{5.15}$$

Hence, we conclude that $\alpha' = (z + \omega)$ and $\beta' = (z + \omega^2)$. As described by Wooding and Williams [10], the theory of Lucas sequences can be applied to obtain an efficient algorithm that both computes the acceptable congruence conditions on $x_p, y_p \pmod{q}$ to achieve $\left(\dfrac{q}{\mu_p}\right)_3 = 1$ and calculates number of acceptable residues for q.

Thus, by combining the cases when $q \nmid y_p$ and $q \mid y_p$, we see that there are:

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

acceptable residues for a prime number $q \equiv 1 \pmod 3$.

Example 5.6. Consider the case $q = 13$. We can derive the acceptable residue conditions on μ_p as follows.

If $q \mid y_p$, then $(x + 0\omega)$ is acceptable for $x = 1, ..., (q-1)$.

If $q \nmid y_p$, then we have $\left(\frac{13}{\mu_p}\right)_3 = 1$ if and only if $13 \mid T_{\frac{13-1}{3}}(G', H') = T_4(G', H')$. After considering Equation 5.13, Equation 5.14, and Equation 5.15, we have:

$$\begin{aligned} T_2(G', H') &= G'T_1(G', H') - H'T_0(G', H') \\ &= G' \cdot 1 - H' \cdot 0 \\ &= G' = 2z_p - 1 \end{aligned}$$

$$\begin{aligned} T_3(G', H') &= G'T_2(G', H') - H'T_1(G', H') \\ &= G' \cdot (2z_p - 1) - H' \cdot 1 \\ &= 2z_p - 1^2 - ({z_p}^2 - z_p + 1) \\ &= 3z_p^2 - 3z_p + 2 \end{aligned}$$

$$\begin{aligned} T_4(G', H') &= G'T_3(G', H') - H'T_2(G', H') \\ &= G' \cdot ({G'}^2 - H') - H' \cdot G' \\ &= G'(3z_p^2 - 3z_p + 2) - H'(2z_p - 1) \\ &= (2z_p - 1)(2z_p^2 - 2z_p + 1). \end{aligned}$$

Therefore, we conclude that:

$$\left(\frac{13}{\mu_p}\right)_3 = 1 \text{ if and only if } 13 \mid (2z_p - 1)(2z_p^2 - 2z_p + 1). \tag{5.16}$$

Since 13 is prime, then either $13 \mid (2z_p - 1)$ or $13 \mid (2z_p^2 - 2z_p + 1)$ based on Equation 5.16. Thus, we need to consider both cases.

Case 1: $13 \mid (2z_p - 1)$ In this case, we have $2z_p \equiv 1 \pmod{13}$, indicating that $z_p \equiv 7 \pmod{13}$. This indicates that $x_p \equiv 7y_p \pmod{13}$ based on the fact that $z_p = x_p y_p^{-1}$. Now we obtain solutions by running x_p through all nonzero residue classes mod 13 and computing $y_p \equiv 7^{-1}x_p \equiv 2x_p \pmod{13}$:

x_p	1	2	3	4	5	6	7	8	9	10	11	12
$y_p \equiv 2x_p \pmod{13}$	2	4	6	8	10	12	1	3	5	7	9	11

Case 2: $13 \mid (2z_p^2 - 2z_p + 1)$ In this case, we have $2z_pz_p - 2z_p \equiv 12 \pmod{13}$, indicating that $z_p(z_p-1) \equiv 6 \pmod{13}$. Subtracting 6 on both sides, we then get $(z_p-3)(z_p+2) \equiv 0 \pmod{13}$, and so $(z_p - 3) \equiv 0 \pmod{13}$ or $(z_p + 2) \equiv 0 \pmod{13}$.

If $(z_p-3) \equiv 0 \pmod{13}$, we have $z_p \equiv 3 \pmod{13}$. Based on the fact that $z_p = x_py_p^{-1}$, we get $x_p \equiv 3y_p \pmod{13}$. Now we can obtain solutions by running x_p through all nonzero residue classes mod 13 and computing $y_p \equiv 3^{-1}x_p \equiv 9x_p \pmod{13}$:

x_p	1	2	3	4	5	6	7	8	9	10	11	12
$y_p \equiv 9x_p \pmod{13}$	9	5	1	10	6	2	11	7	3	12	8	4

If $(z_p+2) \equiv 0 \pmod{13}$, we have $z_p \equiv 11 \pmod{13}$. Based on the fact that $z_p = x_py_p^{-1}$, we get $x_p \equiv 11y_p \pmod{13}$. Now we can obtain solutions by running x_p through all nonzero residue classes mod 13 and computing $y_p \equiv 11^{-1}x_p \equiv 6x_p \pmod{13}$:

x_p	1	2	3	4	5	6	7	8	9	10	11	12
$y_p \equiv 6x_p \pmod{13}$	6	12	5	11	4	10	3	9	2	8	1	7

Combining the solutions for both $q \mid y_p$ and $q \nmid y_p$, the set of acceptable residues for Eisenstein pseudocube modulo 13 is given by

$$\begin{aligned} S_{13} = \{&(1+0\omega), (2+0\omega), (3+0\omega), (4+0\omega), (5+0\omega), (6+0\omega), (7+0\omega), (8+0\omega), \\ &(9+0\omega), (10+0\omega), (11+0\omega), (12+0\omega), (2+1\omega), (6+1\omega), (9+1\omega), (4+2\omega), \\ &(5+2\omega), (12+2\omega), (1+3\omega), (5+3\omega), (6+3\omega), (8+4\omega), (10+4\omega), (11+4\omega), \\ &(4+5\omega), (6+5\omega), (10+5\omega), (2+6\omega), (4+6\omega), (12+6\omega), (1+7\omega), (3+7\omega), \\ &(11+7\omega), (3+8\omega), (7+8\omega), (9+8\omega), (2+9\omega), (3+9\omega), (5+9\omega), (6+10\omega), \\ &(7+10\omega), (8+10\omega), (12+11\omega), (8+11\omega), (9+11\omega), (4+12\omega), (7+12\omega), \\ &(11+12\omega)\}. \end{aligned}$$

As described in Williams and Wooding [10], we are able to apply the method of congruential sieving to establish a precomputed table of Eisenstein pseudocubes after considering all three cases. Specifically, Williams and Wooding used the Calgary Scalable Sieve (CASSIE) [9], a software toolkit for congruential sieving, to establish a table for Eisenstein pseudocubes for $p \leqslant 109$.

6 Eisenstein Pseudocubes and Primality Testing

Eisenstein pseudocubes may be used to prove primality for integers N satisfying $N \equiv 1 \pmod 3$ via the Berrizbeitia theorem.

Theorem 6.1. [2] Let $\nu = a+b\omega$ be a primary element of $\mathbb{Z}[\omega]$, where $\gcd(a,b) = 1$, ν is not a unit, prime, or perfect power in $\mathbb{Z}[\omega]$, and $\mathbf{N}(\nu) < \mathbf{N}(\mu_p)$. Suppose integer $N \equiv 1 \pmod 3$. Then there must exist a rational prime $q \leqslant p$ such that $\left(\frac{q}{\nu}\right)_3 \not\equiv q^{\frac{N-1}{3}} \pmod{\nu}$.

Recall that if $N \equiv 1 \pmod 3$ and N is prime in $\mathbb{Z}$, then $N = \nu\overline{\nu}$, where ν is a primary prime in $\mathbb{Z}[\omega]$. Furthermore, if q is any rational prime, then:

$$\left(\frac{q}{\nu}\right)_3 \equiv q^{\frac{N-1}{3}} \pmod{\nu}.$$

Table 1: Eisenstein Pseudocubes

p	$\mathbf{N}(\mu_p)$	μ_p
5	643	$29 + 18\omega$
7	5113	$71 + 72\omega$
11	13507	$23 + 126\omega$
13	39199	$227 + 90\omega$
17	1 07803	$-181 + 198\omega$
19	3 60007	$653 + 126\omega$
23	39 04969	$443 + 2160\omega$
29	61 07191	$-1669 + 1170\omega$
31	103 18249	$3617 + 2520\omega$
37	273 33067	$6023 + 3366\omega$
41	991 79467	$4973 + 11466\omega$
43	5329 97833	$-15451 + 11088\omega$
47	22785 22747	$54017 + 17514\omega$
53	27417 02809	$47477 + 56160\omega$
59	1 85007 66499	$66887 + 156510\omega$
61, 67	4 15475 53813	$235061 + 107172\omega$
71	11 94233 48797	$-139813 + 253764\omega$
73	82 46210 13649	$-267733 + 744120\omega$
79, 83	115 18103 60731	$1227419 + 761670\omega$
89	2507 90827 69801	$5052689 + 4961880\omega$
97	3393 26375 28481	$-2127709 + 4462200\omega$
101	9175 67688 29893	$10322861 + 8601732\omega$
103, 107	21408 90619 32079	$3056387 + 15918570\omega$
109	81221 66151 53761	$-27791551 + 1366560\omega$

If we have a table of Eisenstein pseudocubes available to us, then we will be able to certify primality for an integer $N \equiv 1 \pmod 3$ by the following algorithm.

Step 1 Test that N is not a perfect power.

Step 2 Find a primary $\nu \in \mathbb{Z}[\omega]$, such that $\mathbf{N}(\nu) = N$. If this step fails, then N is composite.

Step 3 In a precomputed table of Eisenstein pseudocubes, find $\mu_p \in \mathbb{Z}[\omega]$ of minimal norm such that $N < \mathbf{N}(\mu_p)$.

Step 4 For each prime $q \leqslant p$, check if $\left(\frac{q}{\nu}\right)_3 \equiv q^{\frac{N-1}{3}} \pmod{\nu}$.

Proposition 6.2. If an integer $N > 1$ passes all four steps in the algorithm, then N is prime.

Proof. As shown in the step 4, we have $\left(\frac{q}{\nu}\right)_3 \equiv q^{\frac{N-1}{3}} \pmod{\nu}$ holds for each prime $q \leqslant p$, which contradicts the conclusion of Theorem 6.1. Therefore, ν is either a unit, prime, or

prefect power. Since $N > 1$, we assert that ν is not a unit. To show this, if ν were a unit, then we would have $N = \mathbf{N}(\nu) = 1$ by Lemma 3.1, contradicting the assumption that $N > 1$. Thus, ν is not a unit.

Since N is not a perfect power from the step 1, we assert that ν is not a perfect power. For $\nu{=}\alpha^k$, where $\alpha \in \mathbf{D}$ and $k \in \mathbb{Z}$. Since $\mathbf{N}(\nu) = N$, we then have $N = \mathbf{N}(\nu) = \mathbf{N}(\alpha^k) = (\mathbf{N}(\alpha))^k$, indicating that N is also a perfect power. Thus, ν is not a perfect power.

So far, we have already shown that ν is neither a perfect power, nor a unit, indicating that ν must be prime. Now we want to show if ν is prime, then N is prime. Assume N is not prime. say $N = mn$. We want to show that either $m = 1$ or $n = 1$. Since $N = \mathbf{N}(\nu) = \nu\overline{\nu}$, we have $mn = \nu\overline{\nu}$. Since ν is prime, either $\nu \mid m$ or $\nu \mid n$. Suppose $\nu \mid m$. Then there exists $\gamma \in \mathbf{D}$ such that $m = \gamma\nu$. Thus, we have $mn = \gamma\nu n = \nu\overline{\nu}$, indicating that $\gamma n = \overline{\nu}$. However, since ν is prime, $\overline{\nu}$ is prime as well. Therefore, since $\overline{\nu} = \gamma n$, we have either γ is a unit or n is a unit. If γ is a unit, we have $\mathbf{N}(m) = m^2 = \mathbf{N}(\gamma\nu) = 1 \cdot \mathbf{N}(\nu) = N$. This indicates that N is a perfect power, contradicting the step 1. On the other hand, if n is a unit, we have $n = \pm 1$ and $m = \pm N$, as desired. Therefore, N has to be prime. ■

Example 6.3. Consider the case $N = 7$. We apply the algorithm and the precomputed table of Eisenstein pseudocubes to show that 7 is prime.

Proof. In the step 1, it is clear that 7 is neither a perfect power nor a unit. In the step 2, we have $7 = \mathbf{N}(2 + 3\omega)$ where $2 + 3\omega$ is a primary in Eisenstein integers. In the step 3, we choose $\mu_p = 29 + 18\omega$ from the precomputed table of Eisenstein pseudocubes where $\mathbf{N}(\mu_p) = 643 > 7$. In particular, we get $p = 5$ from this precomputed table as well. In the step 4, we need to test whether or not $\left(\frac{q}{v}\right)_3 \equiv q^{\frac{N-1}{3}} \pmod{v}$ holds for all $q \leqslant p$. Since $p = 5$, then q can only be 2 or 3. Thus, we only need to make two tests.

1. Check if $\left(\frac{2}{2+3\omega}\right)_3 \equiv 2^{\frac{7-1}{3}} \pmod{2+3\omega}$.

   Since both $2 + 3\omega$ and 2 are primary, we apply cubic reciprocity and get

   $$\left(\frac{2}{2+3\omega}\right)_3 = \left(\frac{2+3\omega}{2}\right)_3 = \left(\frac{\omega}{2}\right)_3 = \omega^{\frac{\mathbf{N}(2)-1}{3}} \equiv \omega \pmod{2+3\omega}.$$

   On the other hand, we apply the Euclidean algorithm and get

   $$2^{\frac{7-1}{3}} = 4 = (-2\omega)(2+3\omega) + (-2-2\omega) \equiv (-2-2\omega) \equiv \omega \pmod{2+3\omega}.$$

   We conclude that $\left(\frac{2}{2+3\omega}\right)_3 \equiv 2^{\frac{7-1}{3}} \pmod{2+3\omega}$.

2. Check if $\left(\frac{3}{2+3\omega}\right)_3 \equiv 3^{\frac{7-1}{3}} \pmod{2+3\omega}$.

   We apply the Euclidean algorithm and get $3 = (-\omega)(2+3\omega) - \omega$. Thus, we have

   $$\left(\frac{3}{2+3\omega}\right)_3 = \left(\frac{-\omega}{2+3\omega}\right)_3 = (-\omega)^{\frac{\mathbf{N}(2+3\omega)-1}{3}} \equiv (-\omega)^2 \equiv \omega^2 \equiv -1-\omega \pmod{2+3\omega}.$$

On the other hand, after applying the Euclidean algorithm, we get

$$3^{\frac{7-1}{3}} = 9 = (-1-4\omega)(2+3\omega) + (-1-\omega) \equiv -1-\omega \pmod{2+3\omega}.$$

Since $-1-\omega \equiv -1-\omega \pmod{2+3\omega}$, we conclude that $\left(\dfrac{3}{2+3\omega}\right)_3 \equiv 3^{\frac{7-1}{3}} \pmod{2+3\omega}$.

Therefore, since both tests hold when $N = 7$, then 7 is a prime number. ■

References

[1] Agrawal, M., Kayal, N. and Saxena, N.: PRIMES is in P. In Annals of mathematics, 781-793. (2004)

[2] Berrizbeitia, P., Müller, S. and Williams, H.C.: Pseudocubes and primality testing. In: Buell, D.A. (ed.) ANTS 2004. LNCS, vol. 3076, pp. 102-116. Springer, Heidelberg. (2004)

[3] Ireland, K. and Rosen, M.: A Classical Introduction to Modern Number Theory, 2nd ed. Graduate Texts in Mathematics, vol. 84. Springer, Heidelberg. (1990)

[4] Lukes, R.F., Patterson, C.D. and Williams, H.: Some results on pseudosquares. Mathematics of Computations 65(213), S25-S27, 361-372. (1996)

[5] Miller, G.L.: Riemann's hypothesis and tests for primality. in Proceedings of seventh annual ACM symposium on Theory of computing, pp 234-239. ACM, (1975)

[6] Rivest, R.L., Shamir, A. and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126. (1978)

[7] Solovay, R. and Strassen, V.: A fast Monte-Carlo test for primality. SIAM journal on Computing 6, 6(1), pp 84-85. (1977)

[8] Wiliams, H.C.: Èdouard Lucas and Primality Testing. Canadian Mathematical Society Series of Monographs and Advanced Tests, vol. 22. Wiley Interscience, Hoboken. (1998)

[9] Wooding, K. and Williams, H.C.: Doubly-focused enumeration of pseudosquares and pseudocubes. In: Hess, F., Pauli, S., Pohst, M. (eds.) ANTS 2006. LNCS, vol. 4076, pp. 208-221. Springer, Heidelberg. (2006)

[10] Wooding, K. and Williams, H.C.: Improved Primality Proving with Eisenstein Pseudocubes. In: Algorithmic number-theory, pp. 331-339. Springer Berline Heidelberg. (2010)