GAUSSIAN INTEGERS

HUNG HO

Abstract. We will investigate the ring of "Gaussian integers" $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. First we will show that this ring shares an important property with the ring of integers: every element can be factored into a product of finitely many "primes". This result is the key to all the remaining concepts in this paper, which includes the ring $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$, analogous statements of famous theorems in $\mathbb{Z}$, and quadratic reciprocity laws.

Contents

1. Principal Ideal Domain and Unique Prime Factorization

Definition 1.1. A ring R is called an *integral domain*, or *domain*, if $1 \neq 0$ and whenever $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$.

Example 1.2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all integral domains.

Example 1.3. The ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is an integral domain.

Example 1.4. The ring $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if n is a prime. This is because if n is not a prime then we can write $n = ab$ where $a, b \in \mathbb{Z} \setminus \{1\}$ and thus $ab = 0$ in $\mathbb{Z}/n\mathbb{Z}$. Conversely, if n is a prime then n divides ab if and only if n divides either a or b, so $a = 0$ or $b = 0$ in $\mathbb{Z}/n\mathbb{Z}$.

Definition 1.5. An ideal I of a commutative ring R is *principal* if it is generated by a single element a of R through multiplication by every element of R. In other words, $I = Ra = \{ra : r \in R\}$.
It is common to denote the ideal generated by a as (a).

Example 1.6. The set of even integers is a principal ideal of $\mathbb{Z}$ generated by 2.

Definition 1.7. A *principal ideal domain* is a domain in which every ideal is principal.

Definition 1.8. Let a, b be elements of the commutative ring R. If there exists $x \in R$ such that $a = bx$ then we say that b *divides* a, or a *is divisible by* b and write $b \mid a$. b is called a *divisor* of a and a is a *multiple* of b.
Elements a and b of an integral domain are *associates* if $a \mid b$ and $b \mid a$. An element u is a *unit* if u divides every element of R, or equivalently, u divides 1.

We can restate the above claims about divisibility and unit in terms of principal ideals. From now on, we always assume R to be a commutative ring and an integral domain.

Proposition 1.9. *Let $a, b \in R$, then b divides a if and only if $(a) \subseteq (b)$.*

Proof. If b divides a, we write $a = bx$ for some $x \in R$. Then for any $y \in (a)$, we have $y = at$ for some $t \in R$, or $y = bxt$ and thus $y \in (b)$. Conversely, if $(a) \subseteq (b)$, then obviously $a \in (b)$ so $a = bx$ for some $x \in R$, so b divides a. □

Corollary 1.10. *An element u is a unit if and only if $(u) = (1) = R$.*

Corollary 1.11. *The following are equivalent:*

(1) a and b are associates.
(2) $a = bu$ for some unit u.
(3) $(a) = (b)$.

Definition 1.12. An element p of the commutative ring R is called *prime* if $p \notin \{0, 1\}$ and whenever p divides ab for $a, b \in R$, then either p divides a or p divides b.

Definition 1.13. A non-zero non-unit element p in an integral domain is *irreducible* if it is not the product of two non-zero units.

In the ring of integers $\mathbb{Z}$, prime and irreducible elements are equivalent and are called interchangeably as prime numbers. In general, however, these two definitions do not coincide. For example, consider the ring $\mathbb{Z}\sqrt{-5} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. It is easy to check that this ring is an integral domain (because it is a subset of the complex numbers). The element 2 is irreducible in $\mathbb{Z}\sqrt{-5}$ because if $2 = (a + b\sqrt{-5})(c+d\sqrt{-5})$, taking absolute value of both sides yields $4 = (a^2+5b^2)(c^2+5d^2)$. This is only possible if $b = d = 0$, hence $|ac| = 2$, where $a, c \in \mathbb{Z}$, so either $|a|$ or $|c|$ must be 1. Therefore either $a+b\sqrt{-5}$ or $c+d\sqrt{-5}$ is a unit in $\mathbb{Z}\sqrt{-5}$. On the other hand, 2 is not a prime in $\mathbb{Z}\sqrt{-5}$ since 2 divides $4 = (-1 + \sqrt{-5})(1 + \sqrt{-5})$ but 2 neither divides $1 + \sqrt{-5}$ nor $-1 + \sqrt{-5}$ (an integer divides a number $a + b\sqrt{-5}$ in $\mathbb{Z}\sqrt{-5}$ if and only if it divides both a and b).
The example above shows that in an integral domain, irreducible elements are not necessarily primes, but what about the reverse statement? The following theorem addresses this issue.

Theorem 1.14. *If p is a prime element in an integral domain R, then p is irreducible.*

Proof. Assume $p \neq 0$ is a prime but not irreducible in R, then there exists $x, y \in R$ that are not units such that $p = xy$. Since p is a prime element, it follows that $p \mid x$ or $p \mid y$. Without loss of generality, suppose $p \mid x$, then $x = pt$ for some $t \in R$. Thus, we can write $p = pty$. Since R is an integral domain and $p \neq 0$, we deduce that $ty = 1$, or y divides 1, so y is a unit, a contradiction. □

If R is a principal ideal domain, then the reverse direction is also true. However, before tackling this property, we need some more notions.

Definition 1.15. Let a, b be two nonzero elements of R. An element $d \in R$ is called a *greatest common divisor* of a and b if d is a divisor of both a and b, and any common divisor of a and b divides d.

Later on we will show that any two greatest common divisors of two elements are associates of each other, hence from now on we will use the notation $\gcd(a, b)$ and the term "the greatest common divisor" to denote any of those associates. However, in a general integral domain, two elements need not have a greatest common divisor. In fact, a domain in which every two elements have a greatest common divisor is called a *GCD domain*. We will show that every principal ideal domain is also a GCD domain.
For elements $a_1, a_2, \ldots, a_n \in R$, we define $(a_1, a_2, \ldots, a_n) = Ra_1 + Ra_2 + \ldots + Ra_n = \{\sum_{i=1}^{n} r_i a_i \mid r_i \in R\}$. It is easy to see that $(a_1, a_2, \ldots, a_n)$ is also an ideal of R .

Theorem 1.16. *Let R be a principal ideal domain and a, b be nonzero elements of R. Then there exists $d = \gcd(a, b)$ and $(a, b) = (d)$.*

Proof. Let $I = (a, b)$ be an ideal of R. Since R is a principal ideal domain, we have $I = (d)$ for some $d \in R$. Because $(a), (b) \subseteq (a, b) = (d)$, we deduce that d divides both a and b. Now let d' be any common divisor of a and b and write $a = d'a', b = d'b'$. Since $d \in (a, b)$, we can also write $d = au + bv$ for some $u, v \in R$. Thus, we have $d = d'(a'u + b'v)$, so $d' \mid d$. Therefore, d is the greatest common divisor of a and b. □

Two elements a and b may have more than one greatest common divisor. If d and d' are both greatest common divisors of a and b, we can deduce from the definition that $d \mid d'$ and $d' \mid d$. Hence, any two greatest common divisors are associates of each other. If $\gcd(a, b) = u$, where u is a unit, then a and b are *relatively prime*. It follows from theorem 1.16 that if a and b are relatively prime, then $(a, b) = R$.

Corollary 1.17. *Let $a, b, c \in R$ and $a \mid bc$. If $(a, b) = R$, then $a \mid c$.*

Proof. Since $(a, b) = R$, there exists $x, y \in R$ such that $ax + by = 1$. We have

$$\begin{aligned} bc &= ak \\ \Rightarrow ybc &= yak \\ \Rightarrow c(1 - ax) &= yak \\ \Rightarrow c &= a(cx + yk). \end{aligned}$$

Thus, a divides c. □

Corollary 1.18. *If p is irreducible in a principal ideal domain R, then p is a prime element.*

Proof. Suppose p divides ab for some $a, b \in R$. Let $p_a = \gcd(p, a)$. If p_a is a unit, then p and a are relatively prime and we conclude from corollary 1.17 that p divdes b. If p_a is not a unit, we write $p = p_a u$ and since p is irreducible, it follows that u is a unit. So p and p_a are associates, hence p divides a. □

From now on, we will not distinguish irreducible and prime elements.

Recall that every positive integer can be uniquely factored into a product of primes (we only consider positive primes). We want to prove a similar result in a

principal ideal domain, that is, every element can be factored into product of prime elements. However, this factorization, provided it exists, may not be unique as we can see via this simple example in $\mathbb{Z}$: $4 = 2 \cdot 2 = (-2) \cdot (-2)$. But this example also shows that in $\mathbb{Z}$, if a number can be factored into different products of primes, then we can find corresponding primes in these products that are associates of each other (2 and -2 in the above example). Therefore, when talking about unique prime factorization in a general principal ideal domain, we understand that it is "unique up to associates".

We will now go on to prove that every element in a principal ideal domain can be factored into irreducible (or prime) elements. The intuition is as followed. Given any element a, if a is irreducible then we are done. If not, then we can write $a = bc$, where b, c are non-units. Now if either b or c is not irreducible, we proceed similarly to factor that element into another two elements. Eventually, if this process terminates after finitely many steps, we have our desired factorization. However, if this process goes on forever, then we have a problem. We will prove that this cannot happen.

Proposition 1.19. *Let a be a non-zero non-unit element of a principal ideal domain R. Then a can be factored into a product of finitely many irreducible elements.*

Proof. First we show that every non-zero non-unit element x has an irreducible divisor. Assume otherwise, then obviously x is not irreducible itself, so we can write $x = x_1y_1$. Since x has no irreducible divisor, we can again factor $x_1 = x_2y_2$, where x_2, y_2 are also not irreducible. Proceed inductively, we have two infinite sequences of (x_n) and (y_n) in R such that all of the terms are not irreducible and $x_{n-1} = x_ny_n$. Thus, $(x_1) \subsetneq (x_2) \subsetneq \dots$ (the strict subset sign is due to the fact that y_n is not irreducible for all n, so a_n is not an associate of a_{n-1}).

Now let $I = \bigcup_{n=1}^{\infty}$. We claim that I is an ideal of R. Indeed, it is obvious that $(I, +)$ is a subgroup of $(R, +)$. For any $t \in I, r \in R$, since t belongs to (x_i) for some i, so does rt, hence $rt \in I$. Thus, I is an ideal and we deduce from the fact that R is a principal ideal domain that $I = (b)$ for some $b \in R$. Since $x_n \in (b) = I$, we have b divides x_n for all n. On the other hand, $b \in (x_k)$ for some k, or x_k divides b. Hence, b and x_k are associates. But then this implies that x_k divides x_{k+1}, which implies $(x_{k+1}) \subseteq (x_k) \subsetneq (x_{k+1})$, a contradiction. So every non-zero non-unit element has an irreducible divisor.

Now consider an arbitrary non-zero non-unit $a \in R$. If a is irreducible, we are done. If not, we can factor $a = a_1b_1$, where a_1 is irreducible. Since a is not irreducible, b_1 is not a unit (otherwise a and a_1 are associates), hence b_1 has an irreducible divisor a_2. We write $b_1 = a_2b_2$, and apply the same argument for b_2. Proceed inductively, if b_n is not a unit, we factor it into $a_{n+1}b_{n+1}$, where a_{n+1} is irreducible. Eventually, if we stop at some N_0 where b_{N_0} is a unit, then b_{N_0-1} is irreducible and $a = a_1a_2 \dots a_{N_0-1}b_{N_0-1}$ is our desired factorization. Otherwise, if we do not stop at some N_0, then we have an infinite sequence of ideals $(b_1), (b_2), \dots$ such that $(b_1) \subsetneq (b_2) \subsetneq \dots$ (a_n is non-unit for all n so b_{n-1} and b_n are not associates). Now repeat the proof as above, we have a contradiction, so we must stop after finitely many steps, and thus a can be factored into a product of irreducible elements. $\square$

Now we know that any non-zero non-unit element can be factored into a product of irreducibles. To prove that his factorization is unique up to associates, we need the following simple lemma.

Lemma 1.20. *Let a, b be two irreducible elements of a principal ideal domain R. Then a and b are relatively prime if and only if they are not associates.*

Proof. The forward direction is obvious because two associates divide each other. For the reverse direction, assume a and b are not relatively prime, let d be their greatest common divisor. Write $a = da'$ and $b = db'$. Since a and b are irreducibles and d is not a unit, it follows that a' and b' are units. Thus, d is an associate of both a and b, so a and b are associates, a contradiction. □

From now on, if a and b are not associates, we say that a and b are *distinct*.

Theorem 1.21. *Let a be a non-zero element of a PID R. Then we can write*

$$a = u \prod_{i=1}^{k} p_i^{\alpha_i},$$

where u is a unit, p_i's are pairwise distinct irreducibles that are unique up to associates, and the exponents α_i's are uniquely determined.

Proof. The existence of such factorization follows from proposition 1.19. Now assume that we have two factorizations $a = u \prod_{i=1}^{k} p_i^{\alpha_i} = v \prod_{i=1}^{l} q_i^{\beta_i}$. For each $i = 1, 2, \ldots, k$, p_i divides $\prod_{i=1}^{l} q_i^{\beta_i}$, so from lemma 1.20 and corollary 1.18, there must exists $j \in \{1, 2, \ldots, l\}$ such that q_j and p_i are associates. Thus, we can map each p_i to its associate q_j, and apparently this is a one-to-one map because two distinct irreducibles have distinct associates. But we can also repeat the argument and deduce that for any q_j, there exists a corresponding associate p_i, hence our map is an isomorphism. Therefore, $k = l$, and Without loss of generality, we can assume that p_i and q_i are associates for $i = 1, 2, \ldots, k$.
It remains to show that $\alpha_i = \beta_i$ for every i. Assume otherwise and without loss of generality, there exists i_0 such that $\alpha_{i_0} > \beta_{i_0}$. Since R is an integral domain, we deduce that $u \prod_{i \neq i_0} p_i^{\alpha_i} p_{i_0}^{\alpha_{i_0} - \beta_{i_0}} = v \prod_{i \neq i_0} q_i^{\beta_i}$, so p_{i_0} divides q_j for some $j \neq i_0$, a contradiction. Therefore, $\alpha_i = \beta_i$ for all i, and thus the theorem is proven. □

Definition 1.22. An *Euclidean domain* R is an integral domain equipped with a function f from $R \setminus \{0\}$ to $\{0, 1, 2, \ldots, \}$ such that if $a, b \in R$ and b is nonzero, then we can write $a = bq + r$ for $q \in R$, and either $r = 0$ or $f(r) < f(b)$.

The main reason to define Euclidean domain is the following proposition.

Proposition 1.23. *Assume R be an Euclidean domain. Then R is a principal ideal domain.*

Proof. Let I be an ideal of R, we shall prove that there exists $a \in R$ such that $I = Ra$. Indeed, let a be a nonzero element of I such that $f(a)$ is minimum (the existence of such element follows from the fact that the function f takes values on the set of non-negative integers). Now, consider any $b \in I$, we can write $b = aq + r$ with $q, r \in R$. Since $f(a)$ is minimum, we cannot have $f(r) < f(a)$, so for all $b \in I$,

$b = aq$ for some $q \in R$ and thus $I \subseteq Ra$. On the other hand, obviously $Ra \subseteq I$ because I is an ideal. Hence, $I = Ra$. □

Proposition 1.23 is important because we may show a ring R is a PID by first proving it is an Euclidean domain. We will conclude the first section with an important result: the Chinese remainder theorem.

Definition 1.24. Two ideals I and J are *coprime* if there exists $i \in I$ and $j \in J$ such that $i + j = 1$.

Remarks 1.25. By theorem 1.16, we know that in a principal ideal domain R, two ideals (a) and (b) are coprime if and only if a and b are relatively prime.

Theorem 1.26. *Let $I_1, I_2, \ldots, I_k$ be ideals of a ring R that are pairwise coprime. Denote $I = \bigcap_{i=1}^{k} I_i$. We have the isomorphism*

$$R/I \to R/I_1 \times \ldots \times R/I_k$$
$$x + I \to (x + I_1, \ldots, x + I_k).$$

Proof. It suffices to prove for $k = 2$, as the general case can be proved similarly using induction. We want to show that for any $x_1, x_2 \in R$ one can find $x \in I$ such that $x \equiv x_1 \mod I_1$ and $x \equiv x_2 \mod I_2$. Since I_1 and I_2 are coprime, there exists $y_1 \in I_1$ and $y_2 \in I_2$ such that $-y_1 + y_2 = x_1 - x_2$. Let $z = y_1 + x_1 = y_2 + x_2$, then apparently $z \in R$ and $z - x_1 \in I_1, z - x_2 \in I_2$. Thus $z \equiv x_1 \mod I_1$ and $z \equiv x_2 \mod I_2$. □

2. The ring $\mathbb{Z}[i]$

Most of this paper is devoted to reproduce many well-known concepts and results from $\mathbb{Z}$ in the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. First and foremost, we will show that $\mathbb{Z}[i]$ is a principal ideal domain and thus inherits the unique prime factorization property.

Proposition 2.1. *$\mathbb{Z}[i]$ is a Euclidean domain.*

Proof. For each $\alpha = a + bi \in \mathbb{Z}[i] \setminus \{0\}$, we define $f(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$. Take an arbitrary $\beta = c + di \in \mathbb{Z}[i]$, we will show that $\beta = \alpha\gamma + \theta$ for $\gamma \in \mathbb{Z}[i]$ and either $\theta = 0$ or $f(\theta) < f(\alpha)$.
Indeed, let $\frac{\beta}{\alpha} = r + si$, where $r, s \in \mathbb{Q}$. Let k be the closest integer to r and l be the closest integer to s, i.e. $|k - r| \leq \frac{1}{2}$ and $|l - s| \leq \frac{1}{2}$. Let $\gamma = k + li, m = r - k, n = s - l$ and $\theta = (a + bi)(m + ni)$, we have:

$$\begin{aligned} c + di &= (a + bi)(r + si) \\ &= (a + bi)(k + li) + (a + bi)(m + ni) \\ \Rightarrow \beta &= \alpha\gamma + \theta. \end{aligned}$$

If $\theta = 0$ then $\beta = \alpha\gamma$, as desired. Otherwise, we have $f(\theta) = \theta\overline{\theta} = (a^2 + b^2)(m^2 + n^2) \leq (a^2 + b^2)(\frac{1}{4} + \frac{1}{4}) < f(\alpha)$.
Thus, $\mathbb{Z}[i]$ is a Euclidean domain with the function f defined as $f(\alpha) = \alpha\overline{\alpha}$. □

Proposition 2.1 is fundamental to the study of the ring $\mathbb{Z}[i]$ as we can relate many results and properties in $\mathbb{Z}[i]$ to their counterparts in $\mathbb{Z}$. However, after we proved that $\mathbb{Z}[i]$ is a unique prime factorization domain, a natural question arises:

"What are primes in $\mathbb{Z}[i]$?. Primes in $\mathbb{Z}[i]$ may have some similarities with primes in $\mathbb{Z}$ but apparently they are not the same, as we can see, for instance, that 5 is a prime in $\mathbb{Z}$ but not a prime in $\mathbb{Z}[i]$ because $5 = (2-i)(2+i)$.

Lemma 2.2. *Let $p = 4k+1$ be a positive prime, then $(\frac{p-1}{2})!^2 + 1$ is divisible by p.*

Proof. Since for any $x \in \{0, 1, \ldots, 2k\}$, $x \equiv (-1)(p-x) \mod p$, it follows that

$$(\frac{p-1}{2})! \equiv (-1)^{2k}(p-1)(p-2)\ldots\frac{(p+1)}{2} \mod p.$$

Hence $(\frac{p-1}{2})!^2 \equiv (p-1)! \equiv -1 \mod p$ (the second congruence is due to Wilson's theorem). □

Lemma 2.3. *Let $p = 4k+3$ be a positive prime and $a, b \in \mathbb{N}$ such that $a^2 + b^2$ is divisible by p. Then both a and b are divisible by p.*

Proof. We have

$$\begin{aligned} a^2 &\equiv -b^2 && \mod p \\ \Rightarrow a^{2(2k+1)} &\equiv (-b^2)^{(2k+1)} && \mod p \\ \Rightarrow a^{p-1} &\equiv -b^{p-1} && \mod p. \end{aligned}$$

Now if a is not divisible by p, so is b because $a^2 + b^2$ is divisible by p. But then by the Fermat's little theorem, $a^{p-1} \equiv b^{p-1} \equiv 1 \mod p$. Thus, by the above congruence equations, it follows that $2a^{p-1}$ is divisible by p, or a is divisible by p, a contradiction. Thus both a and b are divisible by p. □

Corollary 2.4. *Let p be a prime in $\mathbb{Z}$, then there exists $x \in \mathbb{Z}$ such that $x^2 + 1$ is divisible by p if and only if $|p| = 4k+1$.*

Theorem 2.5. *A Gaussian integer $\alpha = a + bi$ is a prime if and only if it falls in one of the following categories:*

(1) $a = 0$ and $|b|$ is a prime number of the form $4k+3$.
(2) $b = 0$ and $|a|$ is a prime number of the form $4k+3$.
(3) $a^2 + b^2$ is a prime number.

Proof. First, we prove that all Gaussian integers described in $(1), (2), (3)$ are prime.

(1) We will prove for the case $b > 0$, the case $b < 0$ is proved similarly. Let $b = 4k+3$ $(k \geq 0)$ be a prime and assume α is not a prime in $\mathbb{Z}[i]$. Then we can write $bi = (u+vi)(x+yi)$, where $u+vi$ and $x+yi$ are not units. We deduce that $b^2 = (u^2+v^2)(x^2+y^2)$. Since b is a prime, either u^2+v^2 or x^2+y^2 is divisible by b. Without loss of generality, assume u^2+v^2 is divisible by b. Now because $b = 4k+3$, it follows from lemma 2.3 that both u and v are divisible by b. But then both u^2 and v^2 are divisible by b^2, and thus $u^2+v^2 \geq b^2$. Now we can conclude from $x^2+y^2 > 1$ that $(u^2+v^2)(x^2+y^2) > b^2$, a contradiction. Hence α is a prime.

(2) The proof is similar to that of (1).

(3) Assume that α is not a prime, then by similar argument we can write $a + bi = (u + vi)(x + yi)$, where $u^2 + v^2$ and $x^2 + y^2$ are both greater than 1. We also have $a^2 + b^2 = (u^2 + v^2)(x^2 + y^2)$, which implies that $(u^2 + v^2)(x^2 + y^2)$ is a prime number. However, this is impossible because the product of two numbers greater than 1 can never be a prime number in $\mathbb{Z}$, thus α must be a prime in $\mathbb{Z}[i]$.

Conversely, we prove that every prime element of $\mathbb{Z}[i]$ belongs to one of the above three categories. Observe that $\alpha = a+bi$ is a prime in $\mathbb{Z}[i]$ if and only if $\overline{\alpha} = a-bi$ is also a prime in $\mathbb{Z}[i]$ (because $a+bi = (u+vi)(x+yi) \Leftrightarrow a-bi = (u-vi)(x-yi)$, where $u^2 + v^2$ and $x^2 + y^2$ are both greater than 1). Also, it is obvious that if both a and b are nonzero, they must be relatively prime in $\mathbb{Z}[i]$. Now we look at $q = a^2 + b^2 = (a + bi)(a - bi)$. Consider the following cases:

(a) q is even.
We have $(a + bi)(a - bi)$ is divisible by $2 = (1 + i)(1 - i)$. Note that both $1 + i$ and $1 - i$ are primes due to our proof for (3) above. So either $a + bi$ or $a - bi$ is divisible by $1 + i$, and because they are all primes in $\mathbb{Z}[i]$, we must have $a + bi = u(1 + i)$, where u is a unit. Thus, $a - bi = \overline{u}(1 - i)$ and finally $a^2 + b^2 = 2$, which is a prime. So α falls in category 3.

(b) q has a prime divisor p with absolute value of the form $4k + 3$.
Then by lemma 2.3, both a and b are divisible by p and thus, a^2+b^2 is divisible by p^2 (in both $\mathbb{Z}$ and $\mathbb{Z}[i]$). Since both $a+bi$ and $a-bi$ are primes in $\mathbb{Z}[i]$, each of them cannot be divisible by p^2, so we deduce that both $a+bi$ and $a-bi$ are divisible by p. However, this implies that their sum $2a$, and their difference $2bi$, are also divisible by p in $\mathbb{Z}[i]$. Since 2 and p are relatively prime in $\mathbb{Z}[i]$ because $p = 4k+3$, it follows that both a and b are divisible by p. This is impossible if a and b are coprime, so one of them must be zero. If $a = 0$, let $b = pk$, then for $\alpha = pki$ to be a prime in $\mathbb{Z}[i]$, $|k|$ must be equal to 1, hence α is in category 1. Similarly, if $b = 0$ then we can also deduce that α is in category 2.

(c) All prime divisors of q have absolute values of the form $4k + 1$.
First we show that if $|p|$ is a prime in $\mathbb{Z}$ of the form $4k + 1$, then p is not a prime in $\mathbb{Z}[i]$. Indeed, assume othrewise, p is also a prime in $\mathbb{Z}[i]$. according to corollary 2.4, there exists $x \in \mathbb{Z}$ such that $p \mid x^2 + 1 = (x + i)(x - i)$. Since p is a prime, it follows that either $x + i$ or $x - i$ is divisible by p in $\mathbb{Z}[i]$. Without loss of generality, assume $x + i = p(r + si)$, then we deduce that $1 = ps$, a contradiction, hence p is not a prime in $\mathbb{Z}[i]$.
Now assume for the sake of contradiction that q is not a prime itself, then there exist primes p_1, p_2 in $\mathbb{Z}$ (p_1 and p_2 are not necessarily distinct) such that q is divisible by p_1p_2. Because both p_1 and p_2 are of the form $4k+1$ and hence are not primes in $\mathbb{Z}[i]$, we know that p_1p_2 is a product of at least four primes in $\mathbb{Z}[i]$. This is impossible because p_1p_2 divides $(a+bi)(a-bi)$, which is a product of two primes. Therefore, $q = a^2 + b^2$ is a prime in $\mathbb{Z}$.

□

3. Some Applications of Unique Prime Factorization in $\mathbb{Z}[i]$

An important corollary of theorem 2.5 is the following theorem that characterize the necessary and sufficient condition to express a prime as a sum of two squares in $\mathbb{N}$.

Theorem 3.1. *A prime $p \in \mathbb{N}$ can be expressed as a sum of two squares if and only if $p = 2$ or $p = 4k + 1$.*

Proof. By lemma 2.3, we know that if $p = 4k + 3$ then p cannot be expressed as a sum of two squares. Now it remains to show that every prime p of the form $4k + 1$ can be written as $p = a^2 + b^2$. Now from theorem 2.5 we know that p is not a prime in $\mathbb{Z}[i]$, so p has a prime divisor $a + bi$ in $\mathbb{Z}[i]$. Write $p = (a + bi)(c + di)$ then we deduce that $ac - bd = p$ and $ad = -bc$. Since $a + bi$ is a Gaussian prime, we must have $\gcd(a, b) = 1$, so from the latter equation we deduce that $a \mid c$ and $b \mid d$. Write $c = ax$ and $d = by$, then because $ad = -bc$ we have $x = -y$, so $c + di = x(a - bi)$. This implies that $p = x(a + bi)(a - bi) = x(a^2 + b^2)$, and thus $x = 1$ because p is a prime. We conclude that there exists a, b such that $p = a^2 + b^2$. □

Proposition 3.2. *Let $\alpha = a + bi$ be a Gaussian integer, where $a, b \in \mathbb{Z} \setminus \{0\}$ are relatively prime in $\mathbb{Z}$. Suppose n is an integer, then n is divisible by α in $\mathbb{Z}[i]$ if and only if n is divisible by $N(\alpha)$ in $\mathbb{Z}$.*

Proof. The reverse direction is obvious because $\alpha \mid N(\alpha)$. For the forward direction, assume $n = (a + bi)(c + di)$, then after expanding we deduce that $ad = -bc$. But since $\gcd(a, b) = 1$, it follows that $a \mid c$ and $b \mid d$. Write $c = ax$ and $d = by$, where $x, y \in \mathbb{Z}$, then from $ad = -bc$ we have $x = -y$. Therefore,

$$n = x(a + bi)(a - bi) = x(a^2 + b^2).$$

From this we conclude that n is divisible by $N(\alpha)$ in $\mathbb{Z}$. □

Example 3.3. Solve the equations $y^3 - 1 = x^2$ in $\mathbb{Z}$.

Solution. First observe that if x is odd then $x^2 \equiv 1 \mod 4$, so $x^2 + 1$ is divisible by 2 but not divisible by 4. However, because then y must be even, $y^3 = x^2 + 1$ is divisible by 8, a contradiction. Therefore, x is even and y is odd.
We have $y^3 = x^2 + 1 = (x + i)(x - i)$. We claim that $x + i$ and $x - i$ are coprime. Indeed, if they have a common prime divisor p in $\mathbb{Z}[i]$, then p divides their difference $2i$, so p is either $1 + i$ or $1 - i$. But then because p divides y, by proposition 3.2 we deduce that y is divisible by 2, a contradiction. Hence, $x+yi$ and $x-yi$ are coprime, so each of them must be a cube of a Gaussian integer times a unit. However, observe that $\mathbb{Z}[i]$ has four units $1, -1, i, -i$ and each of them itself is a cube of another Gaussian integer. To be specific, $1 = 1^3, -1 = (-1)^3, i = (-i)^3, (-i) = i^3$. Hence we can assume that both $x+yi$ and $x-yi$ are cubes of Gaussian integers. We have:

$$\begin{aligned} x + i &= (a + bi)^3 \\ \Rightarrow 3a^2b - b^3 &= 1 \\ \Rightarrow b(3a^2 - b^2) &= 1. \end{aligned}$$

From this we deduce that $|b| = 1 \Rightarrow |3a^2 - 1| = 1 \Rightarrow a = 0 \Rightarrow b = -1$. Thus $x + i = i$, or $x = 0, y = 1$. □

Example 3.4. Let n be a positive integer. Find the numbers of solution $(x, y) \in \mathbb{Z}^2$ of the following equation

$$x^2 + y^2 = n.$$

Solution. For a prime p and positive integers α, n, we write $p^\alpha || n$ if p^α divides n and $p^{\alpha+1}$ does not divide n. Consider two cases:

(a) n is odd.
Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, where p_j are distinct odd primes. By lemma 2.3 we can deduce that if $p^\alpha \mid\mid n$ where p is of the form $4k+3$, then in order for the equation to have solution in $\mathbb{Z}$, we must have $\alpha = 2\beta$ and $p^\beta \mid\mid x, y$. Therefore, we can assume that $p_j \equiv 1 \mod 4$ for all $1 \leq j \leq k$. By theorem 3.1, we can write $p_j = (a_j + b_j i)(a_j - b_j i)$, where $a_j + b_j i$ and $a_j - b_j i$ are Gaussian primes for all j. Now rewrite our equation as

$$(x+yi)(x-yi) = \prod_{j=1}^{k} (a_j + b_j i)^{\alpha_j} (a_j - b_j i)^{\alpha_j}.$$

Because $a_j + b_j i$ and $a_j - b_j i$ are primes in $\mathbb{Z}[i]$, we deduce this representation

$$x + yi = i^s \prod_{j=1}^{k} (a_j + b_j i)^{\beta_j} (a_j - b_j i)^{\gamma_j},$$

where $s \in \{0,1,2,3\}, \beta_j, \gamma_j \in \{0, \dots, \alpha_j\} \; \forall \; j = 1, \dots, k$.
Taking conjugates of both sides, we have

$$(x - yi) = i^{4-s} \prod_{j=1}^{k} (a_j - b_j i)^{\beta_j} (a_j + b_j i)^{\gamma_j},$$

and thus we deduce that $\beta_j + \gamma_j = \alpha_j$ for all j. Since $x - yi$ is uniquely determined if we know $x + yi$, it suffices to find all possible $(k+1)$-tuples of $(s, \beta_1, \dots, \beta_k)$ such that

$$x + yi = i^s \prod_{j=1}^{k} (a_j + b_j i)^{\beta_j} (a_j - b_j i)^{\alpha_j - \beta_j}.$$

However, the only condition required is that $s \in \{0,1,2,3\}$ and $\beta_j \in \{0, \dots, \alpha_j\} \; \forall \; j$. Thus, the total number of the desired $(k+1)$-tuples, which is also the number of solutions to the equation, is $4(\alpha_1 + 1) \dots (\alpha_k + 1)$.

(b) n is even.
Let $n = 2^\alpha p_1^{\alpha_1} \dots p_k^{\alpha_k}$, where p_j are distinct odd primes. By similar argument as in the case n odd, we may assume p_j are all of the form $4k+1$. Denote $v_2(x)$ as the largest number m such that 2^m divides x, and $v_2(y)$ is defined similarly. If $v_2(x) \neq v_2(y)$ then clearly $\alpha = v_2(n) = \min\{2v_2(x), 2v_2(y)\} = 2\beta$. Let $x_0 = \frac{x}{2^\beta}, y_0 = \frac{y}{2^\beta}, n_0 = \frac{n}{2^\alpha}$ and consider the equation $x_0^2 + y_0^2 = n_0$. Since n_0 is odd, we repeat the proof for the first case and conclude that the number of solutions is $4(\alpha_1 + 1) \dots (\alpha_k + 1)$.
If $v_2(x) = v_2(y) = \beta$ then obviously $\alpha \geq 2\beta$. Again let $x_0 = \frac{x}{2^\beta}, y_0 = \frac{y}{2^\beta}, n_0 = \frac{n}{2^{2\beta}}$, our equation becomes

$$x_0^2 + y_0^2 = 2^{\alpha - 2\beta} n_0.$$

Since the sum of two odd squares is even but not divisible by 4, we deduce that $\alpha - 2\beta = 1$. Now proceed similarly as in case 1, write $p_j = (a_j + b_j i)(a_j - b_j i)$ and $2 = (1+i)(1-i)$, we deduce this representation

$$x + yi = i^s (1+i)^t (1-i)^{1-t} \prod_{j=1}^{k} (a_j + b_j i)^{\beta_j} (a_j - b_j i)^{\alpha_j - \beta_j}.$$

where $s \in \{0,1,2,3\}, t \in \{0,1\}$ and $\beta_j \in \{0,1,\ldots,\alpha_j\}\ \forall\ j$. The number of solutions is therefore $8(\alpha_1+1)\ldots(\alpha_k+1)$.

□

4. Congruence Classes in $\mathbb{Z}[i]$

In the ring of integers $\mathbb{Z}$, the *congruence class* modulo m of an integer $n \in \mathbb{Z}$ is the set $[n]_m = \{x \in \mathbb{Z} \mid x \equiv n \mod m\}$. The set of all congruence classes for a modulus m forms the ring $\mathbb{Z}/n\mathbb{Z}$, which is also known as the *ring of integers modulo n*. In this section, we will study the analogue of $\mathbb{Z}/n\mathbb{Z}$ in the ring $\mathbb{Z}[i]$. When $n \neq 0$, $\mathbb{Z}/n\mathbb{Z}$ is usually defined as $\mathbb{Z}/n\mathbb{Z} = \{[0],[1],\ldots,[n-1]\}$. However, it is not so trivial to define the elements of $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ for an arbitrary $\alpha \in \mathbb{Z}[i]$.
From now on, we shall denote $\alpha\mathbb{Z}[i]$ by I_α, the ideal generated by α. Our first observation is that $\mathbb{Z}[i]/I_\alpha$ is a finite ring. That is because from the proof of proposition 2.1, we know that for every $\beta \in \mathbb{Z}[i]$, there exists β^* such that $|\beta^*| < |\alpha|$ and $\beta \equiv \beta^* \mod \alpha$. Thus, $\mathbb{Z}[i]/I_\alpha \subseteq \{x \in \mathbb{Z}[i] \mid |x| < |\alpha|\}$. Since the latter is a finite set, we deduce that $\mathbb{Z}[i]/I_\alpha$ is finite for a given α. We will denote the order (the number of elements) of $\mathbb{Z}[i]/I_\alpha$ by $n(I_\alpha)$.

Lemma 4.1. *Let α, β be non-zero elements of $\mathbb{Z}[i]$, then $n(I_\alpha I_\beta) = n(I_\alpha)n(I_\beta)$.*

Proof. First note that $I_\alpha I_\beta = I_{\alpha\beta}$. That is because for any $n \geq 0$, $\alpha\beta \mid \sum_{i=0}^{n} x_i y_i$ for x_i's $\in I_\alpha$ and y_i's $\in I_\beta$, so $I_\alpha I_\beta \subseteq I_{\alpha\beta}$. Conversely, any $t \in I_{\alpha\beta}$ can be written as $t = \alpha\beta s$, with $\alpha \in I_\alpha$ and $\beta s \in I_\beta$, so $I_{\alpha\beta} \subseteq I_\alpha I_\beta$. Thus $I_\alpha I_\beta = I_{\alpha\beta}$.
Now assume $\mathbb{Z}[i]/I_\alpha = \{[\alpha_1],\ldots,[\alpha_k]\}$ and $\mathbb{Z}[i]/I_\beta = \{[\beta_1],\ldots,[\beta_l]\}$, where $k = n(I_\alpha)$ and $l = n(I_\beta)$. Consider the set S consisting of all elements of the form $\alpha_i\beta + \beta_j$, where $1 \leq i \leq k$ and $1 \leq j \leq l$. We have $|S| = kl$, so it suffices to show that S is a complete residue system modulo $\alpha\beta$. Indeed, for any $x \in \mathbb{Z}[i]$, we can write

$$x = \alpha\beta q + r.$$

where $|r| < |\alpha\beta|$. There exists $j_0 \in \{1,\ldots,l\}$ such that $r \equiv \beta_{j_0} \mod \beta$, so we can write $r = \beta r_0 + \beta_{j_0}$. Hence.

$$x = \alpha\beta q + \beta r_0 + \beta_{j_0} = \beta(\alpha q + r_0) + \beta_{j_0}.$$

Again, there exists $i_0 \in \{1,\ldots,k\}$ such that $r_0 \equiv \alpha_{i_0} \mod \alpha$, thus $r_0 = \alpha r_1 + \alpha_{i_0}$. Finally, we have this expression

$$x = \beta(\alpha q + \alpha r_1 + \alpha_{i_0}) + \beta_{j_0} = \alpha\beta(q + r_1) + \alpha_{i_0}\beta + \beta_{j_0}.$$

From this we deduce that for any $x \in \mathbb{Z}[i]$, there exists $\alpha_{i_0}\beta + \beta_{j_0} \in S$ such that $x \equiv \alpha_{i_0}\beta + \beta_{j_0} \mod \alpha\beta$. It remains to show that for $u, v \in S$, we have $u \equiv v \mod \alpha\beta$ if and only if $u = v$. Assume otherwise, there exists $i_1, i_2 \in \{1,\ldots,k\}$ and $j_1, j_2 \in \{1,\ldots,l\}$ such that

$$\alpha_{i_1}\beta + \beta_{j_1} \equiv \alpha_{i_2}\beta + \beta_{j_2} \mod \alpha\beta$$

This implies that $\beta \mid \beta_{j_1} - \beta_{j_2}$, which yields $j_1 = j_2$. But then, we have $\alpha\beta \mid \beta(\alpha_{i_1} - \alpha_{i_2})$, which is equivalent to $\alpha \mid \alpha_{i_1} - \alpha_{i_2}$, or $i_1 = i_2$. Hence, S is a complete residue system modulo $\alpha\beta$, so $n(I_\alpha I_\beta) = kl = n(I_\alpha)n(I_\beta)$. □

For any ideal I_α, denote $\overline{I}_\alpha = \{a - bi \mid a + bi \in I_\alpha\}$. It is easy to check that $\overline{I}_\alpha$ is also an ideal of $\mathbb{Z}[i]$, and we call it the *conjugate ideal* of I_α. Also, for $\alpha = a + bi \in \mathbb{Z}[i]$, we shall denote $N(\alpha)$ as the "norm" of α, i.e. $N(\alpha) = a^2 + b^2$.

Lemma 4.2. *The product ideal $I = I_\alpha \overline{I_\alpha}$ is the ideal generated by $N(\alpha)$.*

Proof. We already proved $I_\alpha I_\beta = I_{\alpha\beta}$ for non-zero α, β in the proof of lemma 4.1. So it suffices to show that $\overline{I}_\alpha = I_{\overline{\alpha}}$. We have

$$\begin{aligned} & x \in \overline{I}_\alpha \\ \Leftrightarrow\ & \overline{x} \in I_\alpha \\ \Leftrightarrow\ & \overline{x} = \alpha y \\ \Leftrightarrow\ & x = \overline{\alpha y} \\ \Leftrightarrow\ & x \in I_{\overline{\alpha}}. \end{aligned}$$

Thus, $x \in \overline{I}_\alpha$ if and only if $x \in I_{\overline{\alpha}}$, which shows that $\overline{I}_\alpha = I_{\overline{\alpha}}$. Hence, $I_\alpha \overline{I_\alpha} = I_{\alpha\overline{\alpha}} = (N(\alpha))$. □

Lemma 4.3. $n(I_\alpha) = n(\overline{I_\alpha})$.

Proof. Let $\mathbb{Z}[i]/I_\alpha = \{[\alpha_1], \ldots, [\alpha_k]\}$ and consider $S = \{\overline{\alpha}_1, \ldots, \overline{\alpha}_k\}$, we shall prove that $\mathbb{Z}[i]/I_{\overline{\alpha}} = \{[\overline{\alpha_1}], \ldots, [\overline{\alpha_k}]\}$. Indeed, it suffices to show that S is a complete residue system modulo $\overline{\alpha}$. Clearly, for distinct $\overline{\alpha_i}, \overline{\alpha_j} \in S$, we cannot have $\overline{\alpha_i} \equiv \overline{\alpha_j} \mod \overline{\alpha}$, otherwise $\overline{\alpha} \mid \overline{\alpha_i} - \overline{\alpha_j}$, so $\alpha \mid \alpha_i - \alpha_j$, or $\alpha_i \equiv \alpha_j \mod \alpha$, a contradiction. Moreover, for any $x \in \mathbb{Z}[i]$, there exists α_k such that $\overline{x} \equiv \alpha_k \mod \alpha$, hence $x \equiv \overline{\alpha_k} \mod \overline{\alpha}$. Therefore, we conclude that S is a complete residue system modulo $\overline{\alpha}$, so $\mathbb{Z}[i]/I_{\overline{\alpha}} = \{[\overline{\alpha_1}], \ldots, [\overline{\alpha_k}]\}$. Thus, $n(\overline{I_\alpha}) = n(I_{\overline{\alpha}}) = n(I_\alpha)$. □

Proposition 4.4. $n(I_\alpha) = N(\alpha)$.

Before tackling this problem, we need some additional lemmas. However, first observe that from lemma 4.1, 4.2 and 4.3, we deduce that $n(I_\alpha)^2 = n(I_\alpha)n(I_{\overline{\alpha}}) = n(I_{\alpha\overline{\alpha}})$. So it remains to show that $n(I_{\alpha\overline{\alpha}}) = N(\alpha)^2$, i.e.we just have to prove proposition 4.4 for the case $\alpha \in \mathbb{Z}$.

Lemma 4.5. *Let $\alpha \in \mathbb{Z}$ and $\beta = a + bi \in \mathbb{Z}[i]$, then α divides β in $\mathbb{Z}[i]$ if and only if α divides both a and b in $\mathbb{Z}$.*

Proof. The reverse direction is trivial. For the forward direction, assume that $\alpha \mid \beta$, then we can write $\beta = a + bi = \alpha(c + di)$, where $c, d \in \mathbb{Z}$. This is only possible if $a = \alpha c$ and $b = \alpha d$, so α divides both a and b in $\mathbb{Z}$. □

Given $\alpha \in \mathbb{Z}$, we need to show that $n(I_\alpha) = \alpha^2$. This can be accomplished by finding α^2 elements of $\mathbb{Z}[i]$ that form a complete residue system modulo α. Assume we have found our desired set $S_\alpha = \{\alpha_j = a_j + b_j i \mid 1 \leq j \leq \alpha^2\}$. By lemma 4.5, we have $\alpha_k \equiv \alpha_l \mod \alpha$ if and only if $a_k \equiv a_l$ and $b_k \equiv b_l \mod \alpha$. This observation leads to the following result.

Lemma 4.6. *Let $\alpha \in \mathbb{Z}$, then $S_\alpha = \{a + bi \mid 0 \leq a, b \leq \alpha - 1\}$ is a complete residue system modulo α.*

Proof. It follows immediately from lemma 4.5 that for $x \neq y \in S_\alpha$, we cannot have $x \equiv y \mod \alpha$. Now consider any $z = p + qi \in \mathbb{Z}[i]$. Since $\alpha \in \mathbb{Z}$, there exists p_0 and q_0 in $\{0, 1, \ldots, \alpha - 1\}$ such that $p \equiv p_0$ and $q \equiv q_0 \mod \alpha$. Then obviously

$z \equiv p_0 + q_0 i \mod \alpha$, where $p_0 + q_0 i \in S_\alpha$. From this we conclude that S_α is a complete residue system modulo α. □

Corollary 4.7. *Let $\alpha \in \mathbb{Z}$, then $n(I_\alpha) = \alpha^2 = N(\alpha)$.*

Proposition 4.4 follows from lemma 4.1, 4.2, 4.3 and corollary 4.7.

Lemma 4.6 allows us to precisely define $\mathbb{Z}[i]/I_\alpha$ for $\alpha \in \mathbb{Z}$, but what about $\alpha \in \mathbb{Z}[i]$ in general? Assume $\alpha = a + bi$, can we have a complete residue system modulo α consisting entirely of integers, namely $0, 1, \ldots, a^2 + b^2 - 1$? Proposition 3.2 and proposition 4.4 answer this question.

Corollary 4.8. *Let $\alpha = a + bi$ be a Gaussian integer, where $a, b \in \mathbb{Z} \setminus \{0\}$ are relatively prime in $\mathbb{Z}$. Then $\mathbb{Z}[i]/I_\alpha = \{[0], [1], \ldots, [a^2 + b^2 - 1]\}$.*

Now we are ready to describe $\mathbb{Z}[i]/I_\alpha$ for an arbitrary $\alpha \in \mathbb{Z}[i]$.

Proposition 4.9. *Let $\alpha = a + bi \in \mathbb{Z}[i] \setminus \{0\}$. Assume $\gcd(a, b) = d$ in $\mathbb{Z}$ and $a = da_0, b = db_0$, then $S_\alpha = \{x + yi \mid 0 \le x \le d(a_0^2 + b_0^2) - 1, 0 \le y \le d - 1\}$ is a complete residue system modulo α in $\mathbb{Z}[i]$.*

Proof. Note that $|S_\alpha| = a^2 + b^2$, so by proposition 4.4 we just need to check that for $\beta, \gamma \in S_\alpha$, $\beta \equiv \gamma \mod \alpha$ if and only if $\beta = \gamma$. Assume there exists $\beta, \gamma \in S_\alpha$ such that $\beta \equiv \gamma \mod \alpha$. Let $\beta = p + qi$ and $\gamma = r + si$, we have $d \mid \beta - \gamma$, so by lemma 4.5, $d \mid p - r$ and $d \mid q - s$. However, since $0 \le q, s \le d - 1$, it follows that $q = s$.
Now we also have $a_0 + b_0 i \mid \beta - \gamma = p - r$, and since a_0, b_0 are relatively prime, we deduce from proposition 3.2 that $a_0^2 + b_0^2 \mid p - r$. Write $p - r = s(a_0^2 + b_0^2)$, then we have

$$\begin{aligned} \alpha &\mid p - r \\ d(a_0 + b_0 i) &\mid s(a_0^2 + b_0^2) \\ \Rightarrow d &\mid s(a_0 - b_0 i). \end{aligned}$$

Again, by lemma 4.5 we deduce that d divides both sa_0 and sb_0. Suppose that s is not divisible by d in $\mathbb{Z}$. Then there must exists a prime p in $\mathbb{Z}$ and a positive integer m such that $p^m \mid d$ but $p^m \nmid s$. However, since d divides both sa_0 and sb_0, it follows that both a_0 and b_0 is divisible by p, a contradiction because a_0 and b_0 are relatively prime. Therefore, $d \mid s$, so $d(a_0^2 + b_0^2) \mid s(a_0^2 + b_0^2) = p - r$. Now use the fact that $0 \le p, r \le d(a_0^2 + b_0^2) - 1$, we conclude that $p = r$. Thus, $\beta = \gamma$, or S_α is a complete residue system modulo α. □

5. Some important theorems and results

In this section, we shall prove the analogues of some famous theorems and results of $\mathbb{Z}$ for the ring $\mathbb{Z}[i]$. Firstly, recall the Euler's totient function $\varphi(n)$ of a positive integer n is the number of integers in $\{1, 2, \ldots, n-1\}$ that are relatively prime with n. In other words, $\varphi(n)$ is the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$. We will now find the formula for the Euler's totient function of a Gaussian integer α, which denotes the number of elements of $(\mathbb{Z}[i]/I_\alpha)^\times$. Recall from theorem 2.5 that there are three types of prime: the splitting primes $a + bi$ and $a - bi$ where $a^2 + b^2$ is a prime of the form $4k + 1$, the inert primes p where $p = 4k + 3$ and the ramified primes $(1 + i)$ and $(1 - i)$. We will call them type 1,2,3 respectively.

Theorem 5.1. *Let α be a Gaussian integer, then*

$$\varphi(\alpha) = N(\alpha) \prod_{\substack{\eta \mid \alpha \\ \eta \text{ prime}}} \left(1 - \frac{1}{N(\eta)}\right).$$

Proof. Observe that from the Chinese remainder theorem, for $\alpha, \beta \in \mathbb{Z}[i]$ that are relatively prime, we have $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$. Therefore, we only need to find the formula for $\varphi(\alpha^k)$, where α is a Gaussian prime. Also note that two associates have the same Euler's totient function. Consider three cases:

(a) $\alpha = a + bi$ is a prime of type 1.
Let $p = a^2 + b^2$ be a prime in $\mathbb{Z}$ and $\alpha^k = (a + bi)^k = c + di$. We claim that $\gcd(c, d) = 1$. Indeed, assume $q \in \mathbb{Z}$ is a common prime divisor of c and d, then q divides α^k in $\mathbb{Z}[i]$. Let $q* \in \mathbb{Z}[i]$ be a prime divisor of q, then because α is a prime, it follows that $q* \mid \alpha$. This means that $q*$ is an associate of α, so by proposition 3.2, we deduce that p divides both c and d. But then $p \mid \alpha^k$, or $a - bi \mid (a + bi)^k$, a contradiction because $a - bi$ and $a + bi$ are relatively prime. So $\gcd(c, d) = 1$, hence from corollary 4.8, $S_{\alpha^k} = \{0, 1, \ldots, c^2 + d^2 - 1\}$ is a complete residue system modulo α^k. We will need to find all elements in S_{α^k} that are divisible by α. However, again by proposition 3.2, $x \in S_{\alpha^k}$ is divisible by α if and only if x is divisible by p. Hence, we only need to find the number of elements divisible by p in $\{0, 1, \ldots, p^k - 1\}$ (note that $c^2 + d^2 = (a^2 + b^2)^k$). There are p^{k-1} such numbers, so we deduce that $\varphi(\alpha^k) = p^k - p^{k-1} = N(\alpha^k)(1 - \frac{1}{N(\alpha)})$.

(b) α is a prime of type 2.
Without loss of generality, assume $\alpha \in \mathbb{Z}$. By proposition **??**, we know that $S_{\alpha^k} = \{x + yi \mid 0 \leq x, y \leq \alpha^k - 1\}$ is a complete residue system modulo α. We will need to find all elements divisible by α in S_{α^k}, which by lemma 4.5 are elements $x + yi$ such that both x and y are divisible by α. Since $x, y \in \{0, 1, \ldots, \alpha^k - 1\}$, there are $\alpha^{2(k-1)}$ such elements. Thus, $\varphi(\alpha^k) = \alpha^{2k} - \alpha^{2(k-1)} = N(\alpha^k)(1 - \frac{1}{N(\alpha)})$.

(c) $\alpha = 1 + i$
First we show that $\beta = a + bi \in \mathbb{Z}[i]$ is divisible by $1 + i$ if and only if $2 \mid a + b$. Indeed, for the forward direction, let $a + bi = (1 + i)(c + di)$, then we deduce that $a = c - d$ and $b = c + d$ and apparently $a + b = 2c$, an even number. Conversely, suppose $a + b$ is even, then so is $a - b$. Write $\alpha = b(1 + i) + a - b$, then since $1 + i \mid 2 \mid a - b$, it follows immediately that $1 + i \mid \alpha$.
Now a simple induction shows that $(1+i)^{2k} = 2^k i^k$ and $(1+i)^{2k+1} = 2^k i^k (1+i)$. For the first case, we know that all elements $x+yi$ where $0 \leq x, y \leq 2^k - 1$ form a complete residue system modulo $(1+i)^{2k}$. There are $2 \cdot 2^{2k-2} = 2^{2k-1}$ elements among these such that $x+y$ is odd, which are also the elements relatively prime to $(1 + i)$. Hence $\varphi(\alpha^{2k}) = 2^{2k-1}$. For the latter case, the complete residue system modulo $(1 + i)^{2k+1}$ is $S = \{x + yi \mid 0 \leq x \leq 2^{k+1} - 1, 0 \leq y \leq 2^k - 1\}$. There are $2 \cdot 2^k \cdot 2^{k-1} = 2^{2k}$ elements $x + yi$ of S such that $x + y$ is odd, hence $\varphi(\alpha^{2k+1}) = 2^{2k}$. We conclude that $\varphi(\alpha^k) = 2^{k-1} = N(\alpha^k)(1 - \frac{1}{N(\alpha)})$.

From the three cases above, we conclude that for any $\alpha \in \mathbb{Z}[i]$,

$$\varphi(\alpha) = N(\alpha) \prod_{\substack{\eta \mid \alpha \\ \eta \text{ prime}}} \left(1 - \frac{1}{N(\eta)}\right).$$

□

We proved that every element of $\mathbb{Z}[i]$ can be factored into a product of finite irreducible elements and that this factorization is unique up to associates. It is easy to see that every prime $\alpha \in \mathbb{Z}[i]$ has four associates including itself: $\alpha, -\alpha, i\alpha$ and $-i\alpha$. For convenience, we introduce the following definition of *primary prime*.

Definition 5.2. A prime $\alpha \in \mathbb{Z}[i]$ is called *primary* if

$$\alpha \equiv 1 \mod (1+i)^3.$$

Proposition 5.3. *Every prime of type 1 or type 2 is associated to a unique primary prime.*

Proof. Let $\alpha = a + bi$ be a prime of type 1 or type 2. It suffices to show that there exists a unique primary prime in $A_\alpha = \{a+bi, -a-bi, -b+ai, b-ai\}$. First observe that $\beta = (1+i)^3 = -2(1-i)$, hence by theorem 5.1, we know that $|(\mathbb{Z}[i]/I_\beta)^\times| = 4$. Obviously α is relatively prime to β, so $A_\alpha \subseteq (\mathbb{Z}[i]/I_\beta)^\times$. Therefore, if there does not exist $x \in A_\alpha$ such that $x \equiv 1 \mod \beta$, then since $|A_\alpha| = 4$, there must be $y, z \in A_\alpha$ such that $y \equiv z \mod \beta$. However, considering all possible cases, this means that $\beta \mid 2\alpha$, or $(1-i) \mid \alpha$, a contradiction. This proof not only shows that there exists a primary prime in A_α, but this primary prime is unique because we cannot have $y \equiv z \mod \beta$ for $y, z \in A_\alpha$. □

Remarks 5.4. If $\alpha = a + bi$ is a primary prime, we can see that a is odd and b is even. From now on, primes of type 1 or type 2 are assumed to be primary.

Proposition 5.5. *Let p be a prime of type 2, then for any $\beta \in \mathbb{Z}[i]$, we have*

$$\beta^p \equiv \overline{\beta} \mod p.$$

Proof. Assume $\beta = a + bi$, then we have

$$\beta^p = (a+bi)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} i^{p-k}.$$

Since $\binom{p}{k}$ is divisible by p for all $k \geq 1$, we deduce that $\beta^p \equiv a^p + b^p i^p \mod p$. By Fermat's little lheorem for $p \in \mathbb{Z}$, we have $a^p \equiv a \mod p$ and $b^p \equiv b \mod p$. Moreover, since $p = 4k+3$ is a prime of type 2, $i^p = -1$, and thus $\beta^p \equiv a - bi \equiv \overline{\beta} \mod p$. □

Proposition 5.6. *Let $\alpha = a + bi$ be a prime of type 1 and $p = a^2 + b^2$ is a prime. Then for any $\beta \in \mathbb{Z}[i]$ we have*

$$\beta^p \equiv \beta \mod p.$$

Proof. The proof is similar to that of proposition 5.5. □

Note that from proposition 5.5 we can also deduce that for any β relatively prime to p:

$$\begin{aligned} \beta^{p+1} &\equiv \beta\overline{\beta} \mod p \\ \Rightarrow \beta^{p^2-1} &\equiv (\beta\overline{\beta})^{p-1} \mod p \\ \Rightarrow \beta^{N(p)} &\equiv \beta \mod p. \end{aligned}$$

The final equation is a deduction from Fermat's little lheorem because $\beta\overline{\beta} \in \mathbb{Z}$.

Proposition 5.5 and 5.6 imply the analogue statement of Fermat's little theorem in the ring $\mathbb{Z}[i]$.

Corollary 5.7. *Let $\alpha, \beta \in \mathbb{Z}[i]$, where α is a prime. Then we have*

$$\beta^{N(\alpha)} \equiv \beta \mod \alpha.$$

Note that corollary 5.7 can be proved directly without proposition 5.5 and 5.6. Denote $\mathbb{Z}[i]/I_\alpha \setminus \{0\} = T_\alpha$. We know that for $\beta \in T_\alpha$ and every $\eta \in\in T_\alpha$, there exists a unique $x_\eta \in T_\alpha$ such that $\beta\eta \equiv x_\eta \mod \alpha$. From this we deduce that

$$\begin{aligned} \beta^{N(\alpha)-1} \prod_{\eta \in T_\alpha} \eta &\equiv \prod_{\eta \in T_\alpha} x_\eta \mod \alpha \\ \Rightarrow \beta^{N(\alpha)-1} &\equiv 1 \mod \alpha. \end{aligned}$$

We will finish this section with the concept of *primitive root modulo α*.

Definition 5.8. Let α be a non-zero element of $\mathbb{Z}[i]$. An element $z \in \mathbb{Z}[i]$ is called a *primitive root modulo α* if for every u such that u and α are relatively prime, there exists an integer n such that

$$z^n \equiv u \mod \alpha.$$

Definition 5.9. Let $\alpha, \beta \in \mathbb{Z}[i]$ be relatively prime elements. The *order of β modulo α* is the smallest positive integer k such that

$$\beta^k \equiv 1 \mod \alpha.$$

Observe that by corollary 5.7 for every β that is relatively prime to α we always have $\beta^{N(\alpha)-1} \equiv 1 \mod \alpha$, therefore there always exists an order of β modulo α. We denote the order of β modulo α by $\mathrm{ord}_\alpha(\beta)$. It is easy to see that if $\mathrm{ord}_\alpha(\beta) = k$ then $\beta^n \equiv 1 \mod \alpha$ if and only if k divides n (if not, then let $n = kq + r$, where $r < k$ and we deduce that $\beta^r \equiv 1 \mod \alpha$, a contradiction).

Remarks 5.10. β is a primitive root modulo α if and only if $\mathrm{ord}_\alpha(\beta) = N(\alpha)$.

Theorem 5.11. *If α is a prime element of $\mathbb{Z}[i]$, then there always exists a primitive root modulo α.*

Before proving theorem 5.11, we need the following lemmas.

Lemma 5.12. *Let $\alpha \in \mathbb{Z}[i]$, where α is a prime. Then for any polynomial $P(x) \in \mathbb{Z}[x]$ of degree n such that the highest coefficient of P is relatively prime to α, the following congruence equation has at most n solutions in $\mathbb{Z}[i]/I_\alpha$:*

$$P(x) \equiv 0 \mod \alpha.$$

Proof. We will prove by induction on n. The claim is obviously true for $n = 0$, assume it is true for $n = k$, consider $n = k+1$. Assume for the sake of contradiction that there exists $P(x)$, $\deg P = k + 1$ and $x_0, x_1, \ldots, x_{k+1} \in \mathbb{Z}[i]/I_\alpha$ such that $P(x_i) \equiv 0 \mod \alpha \ \forall\ i$. Since $P \in \mathbb{Z}[x]$, we can write $Q(x) = P(x) - P(x_0) = (x - x_0)R(x)$, where $R \in \mathbb{Z}[x]$ is a polynomial of degree k. We know that $Q(x_i) \equiv 0 \mod p$ for all $i = 1, 2, \ldots, k + 1$. However since $x_i \not\equiv x_0 \mod \alpha$, it follows that $R(x_i) \equiv 0 \mod \alpha$ for all $i = 1, 2 \ldots, k+1$. This is a contradiction because $\deg R = k$, so by induction we cannot have $k + 1$ solutions for $R(x) \equiv 0 \mod \alpha$. Hence the claim is also true for $n = k + 1$, and thus true for all n. □

Lemma 5.13. *For any positive integer n, we have*

$$\sum_{d \mid n} \varphi(d) = n.$$

Proof. For any $d \mid n$, let $S_d = \{x \mid x \in \mathbb{N}, x \leq d, \gcd(x,d) = 1\}$ and define the following map:

$$f_d : S_d \to \{1, 2, \ldots, n\}$$
$$x \to \frac{n}{d}x.$$

Denote $f_d(S_d) = T_d$. We wll prove $T_d \cap T_e = \emptyset$ for distinct $d, e \mid n$. Indeed, assume otherwise, there exists $x_0 \in T_d \cap T_e$. Then there exists $y_0 \in S_d$ and $z_0 \in S_e$ such that $x_0 = \frac{n}{d}y_0 = \frac{n}{e}z_0$, or $dz_0 = ey_0$. Since $\gcd(d, y_0) = \gcd(e, z_0) = 1$, it folows that $d \mid e$ and $e \mid d$, so $e = d$, a contradiction. Hence $T_d \cap T_e = \emptyset$ when $d \neq e$. Also note that $T_d \subseteq \{1, 2, \ldots, n\}$ for all d, hence we deduce that

$$\sum_{d \mid n} \varphi(d) = \sum_{d \mid n} |S_d| \leqslant n.$$

Now we will show that for any $m \in \{1, 2, \ldots, n\}$, there exists $m_1 \mid n$ and $n_1 \in S_{m_1}$ such that $m = \frac{n}{n_1}m_1$. Let $q = \gcd(m, n)$ and write $m = qm_1, n = qn_1$, then $\gcd(m_1, n_1) = 1$ and $m = \frac{n}{n_1}m_1$. In other words, for every $m \leq n$, there exists $m_1 \mid n$ and $n_1 \in S_{m_1}$ such that $f_{m_1}(n_1) = m$. From this we deduce that

$$|n| \leq \sum_{d \mid n} |S_d| = \sum_{d \mid n} \varphi(d).$$

Therefore, we can conclude that $\sum\limits_{d \mid n} \varphi(d) = n$. □

Lemma 5.14. *For every $d \mid N(\alpha)-1$, the following equation has exactly d solutions in $\mathbb{Z}[i]/I_\alpha$:*

$$x^d \equiv 1 \mod \alpha.$$

Proof. Let $S_d = \{x^d \mod \alpha \mid x \in (\mathbb{Z}[i]/I_\alpha) \setminus \{0\}\}$, then for any $y \in S_d$, $y^{\frac{N(\alpha)-1}{d}} \equiv 1 \mod \alpha$, so by lemma 5.14,

$$|S_d| \leq \frac{N(\alpha) - 1}{d}.$$

On the other hand, assume $S_d = \{d_1, d_2, \ldots, d_k\}$, for every i we denote

$$[d_i] = \{x \mid x \in \mathbb{Z}[i]/I_\alpha, x^d \equiv d_i \mod \alpha.\}$$

We claim that $|[d_i]| = d$ for all i. Indeed, again by lemma 5.12, we have $|[d_i]| \leq d$ for all i. Now observe that $[d_i] \cap [d_j] = \emptyset$ for $i \neq j$ and

$$\bigcup_{i=1}^{k} [d_i] = (\mathbb{Z}[i]/I_\alpha) \setminus \{0\}.$$

so we deduce that

$$\begin{aligned}\sum_{i=1}^{k} |[d_i]| &= N(\alpha) - 1 \\ \Rightarrow kd &\geq N(\alpha) - 1 \\ \Rightarrow k &\geq \frac{N(\alpha)-1}{d}.\end{aligned}$$

Thus, we must have equalities everywhere, so $|S_d| = \frac{N(\alpha)-1}{d}$ and $|[d_i]| = d \; \forall \; i = 1, 2, \ldots, \frac{N(\alpha)-1}{d}$. Obviously there exists i such that $d_i \equiv 1 \mod \alpha$, so the equation $x^d \equiv 1 \mod \alpha$ has exactly d solutions in $\mathbb{Z}[i]/I_\alpha$. □

Corollary 5.15. *Let $d \mid N(\alpha) - 1$, then the number of $x \in \mathbb{Z}[i]/I_\alpha$ such that $\mathrm{ord}_\alpha(x) = d$ is $\varphi(d)$.*

Proof. For $d \mid N(\alpha) - 1$, let $O_d = \{x \in \mathbb{Z}[i]/I_\alpha \mid \mathrm{ord}_\alpha(x) = d\}$. Now consider the equation $x^d \equiv 1 \mod \alpha$ with $x \in \mathbb{Z}[i]/I_\alpha$. By lemma 5.14, this equation has exactly d solutions, and each solution x belongs to O_e for some $e \mid d$. Therefore,

$$\sum_{e \mid d} |O_e| = d. \quad (1)$$

This holds for every $d \mid N(\alpha) - 1$. Assume there exists d such that $|O_d| \neq \varphi(d)$, choose the smallest d. Apparently $d \neq 1$. But then, because every divisor e of d that is not d itself is strictly smaller than d, we have

$$\sum_{\substack{e \mid d \\ e \neq d}} |O_e| = \sum_{\substack{e \mid d \\ e \neq d}} \varphi(e).$$

By lemma 5.13, the right hand side is $d - \varphi(d)$. Together with the equation at (1), we conclude that $|O_d| = d$, a contradiction. Hence, $|O_d| = d$ for all $d \mid N(\alpha) - 1$. □

Theorem 5.11 follows immediately from corollary 5.15.

6. Quadratic Reciprocity

In this section, we will prove quadratic reciprocity laws for the ring $\mathbb{Z}[i]$. First we will recall important definitions and results about quadratic reciprocity laws for the ring of integers.

Definition 6.1. Let p be a prime and a be any positive integer. We define the Legendre's symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if there exists } n \in \mathbb{Z} \text{ such that } n^2 \equiv a \mod p \\ 0 & \text{if } p \text{ divides } a \\ -1 & \text{otherwise.} \end{cases}$$

The Legendre symbol indicates whether a is a quadratic residue modulo p. It is easy to see that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ and $\left(\frac{a^2}{p}\right) = 1$.

Theorem 6.2. *Let p, q be two odd primes. Then we have*

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

Proposition 6.3 (Supplementary Laws)**.** *Suppose p is an odd prime. Then we have:*

(1) $\left(\dfrac{-1}{p}\right) = 1$ *if and only if* $p = 4k+1$.

(2) $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Theorem 6.2 is called the Gauss reciprocity law and is the most important result regarding quadratic reciprocity over $\mathbb{Z}$. We will apply the above laws to prove the analogous laws in the ring $\mathbb{Z}[i]$.

Definition 6.4. Let α be a Gaussian prime and β be an arbitrary element of $\mathbb{Z}[i]$. We define the following symbol

$$\left[\frac{\beta}{\alpha}\right] = \begin{cases} 1 & \text{if there exists } \eta \in \mathbb{Z}[i] \text{ such that } \eta^2 \equiv \beta \mod \alpha \\ 0 & \text{if } \alpha \text{ divides } \beta \\ -1 & \text{otherwise.} \end{cases}$$

Similar to the Legendre symbol, the above symbol is also multiplicative. Now we introduce the Euler's criterion for the ring $\mathbb{Z}[i]$.

Proposition 6.5. *Let α be a prime of type 1 or 2 in $\mathbb{Z}[i]$ and β be an arbitrary element of $\mathbb{Z}[i]$ not divisible by α. Then we have*

$$\beta^{\frac{N(\alpha)-1}{2}} \equiv \left[\frac{\beta}{\alpha}\right] \mod \alpha.$$

Proof. Let η be the primitive root modulo α. Then for every β there exists a unique $d(\beta)$ such that $\eta^{d(\beta)} \equiv \beta \mod \alpha$. An easy observation is that $\left[\frac{\beta}{\alpha}\right] = 1$ if and only if $d(\beta)$ is even. Moreover,

$$\begin{aligned} \beta^{\frac{N(\alpha)-1}{2}} &\equiv 1 \mod \alpha \\ \Leftrightarrow \eta^{d(\beta)\frac{N(\alpha)-1}{2}} &\equiv 1 \mod \alpha \\ \Leftrightarrow d(\beta) &\equiv 0 \mod 2. \end{aligned}$$

The last equation is due to the fact that η is a primitive root modulo α, hence $\eta^k \equiv 1 \mod \alpha$ if and only if k is divisible by $N(\alpha)-1$.
Now we conclude that $\beta^{\frac{N(\alpha)-1}{2}} \equiv 1 \mod \alpha$ if and only if $\left[\frac{\beta}{\alpha}\right] = 1$, or $\beta^{\frac{N(\alpha)-1}{2}} \equiv \left[\frac{\beta}{\alpha}\right] \mod \alpha$. □

Now observe that if α is a prime of type 2 then $N(\alpha) - 1 = \alpha^2 - 1$, which is divisible by 4, so for any integer $r, r^{\frac{N(\alpha)-1}{2}}$ is a perfect square. Therefore, if α is a prime of type 2, then any integer is a quadratic residue modulo α.

Corollary 6.6. *Suppose α is a prime of type 2. Let $r \in \mathbb{Z}$ be relatively prime to α. We have:*

$$\left[\frac{r}{\alpha}\right] = 1.$$

Proposition 6.7. *Suppose α is a prime of type 1 and let $r \in \mathbb{Z}$ be relatively prime to α. Then we have*

$$\left[\frac{r}{\alpha}\right] = \left(\frac{r}{N(\alpha)}\right).$$

Proof. We will prove that $\left[\frac{r}{\alpha}\right] = 1$ if and only if $\left(\frac{r}{N(\alpha)}\right) = 1$. The reverse direction is obvious since if there exists $x \in \mathbb{Z}$ such that $r \equiv x^2 \mod N(\alpha)$ then we also have $r \equiv x^2 \mod \alpha$ because $\alpha \mid N(\alpha)$. For the forward direction, assume $\exists\ \eta \in \mathbb{Z}[i]$ such that $r \equiv \eta^2 \mod \alpha$. By corollary 4.8, we know that there exists $u \in \mathbb{Z}$ such that $\eta \equiv u \mod \alpha$, hence $r \equiv u^2 \mod \alpha$. This means that $\alpha \mid r - u^2$, so by proposition 3.2, $N(\alpha) \mid r - u^2$. From this we conclude that $\left(\frac{r}{N(\alpha)}\right) = 1$. □

Proposition 6.7 is very useful in terms of relating quadratic reciprocity laws in $\mathbb{Z}[i]$ to those of $\mathbb{Z}$. For instance, from corollary 4.8 we know there exists $u \in \{0, 1, \ldots, N(\alpha) - 1\}$ such that $u \equiv i \mod \alpha$, so for any $r, s \in \mathbb{Z}, r + si \equiv r + su \mod \alpha$. In terms of quadratic reciprocity, we have

$$\left[\frac{r+si}{\alpha}\right] = \left(\frac{r+su}{N(\alpha)}\right).$$

Proposition 6.8. *Suppose $\alpha = a + bi$ is a prime of type 1. Let $p = N(\alpha)$. We have:*

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

Proof. We know that a is odd and $p = a^2 = b^2$. Assume $q_1, q_2, \ldots, q_k$ are all prime divisors of a such that the highest power of q_i that divides a is odd for all i,. In other words, there exists an odd number d_i such that $q_i^{d_i} \mid\mid a$. Apparently, then

$$\left(\frac{a}{p}\right) = \left(\frac{q_1 q_2 \ldots q_k}{p}\right) = \prod_{i=1}^{k} \left(\frac{q_i}{p}\right)$$

By theorem 6.2 and the fact that $p = 4k + 1$, we have

$$\left(\frac{q_i}{p}\right) = \left(\frac{p}{q_i}\right).$$

However, since $p \equiv b^2 \mod q_i$ for all i, we deduce that $\left(\frac{p}{q_i}\right) = 1$, hence $\left(\frac{q_i}{p}\right) = 1$ for all i. From this we conclude that $\left(\frac{a}{p}\right) = 1$. □

Corollary 6.9. *With the above notations, we also have:*

$$\left(\frac{b}{p}\right) = \left(\frac{2}{p}\right).$$

Moreover, using the same technique, if $b = 2^n c$, where c is odd then $\left(\frac{c}{p}\right) = 1$.

Theorem 6.10. *Let α, β be two different primes that are not type 3 in $\mathbb{Z}[i]$. Then we have*

$$\left[\frac{\beta}{\alpha}\right] = \left[\frac{\alpha}{\beta}\right].$$

Proof. Consider the following cases:

(a) α, β are both primes of type 2.

It follows easily from corollary 6.6 that $\left[\frac{\beta}{\alpha}\right] = \left[\frac{\alpha}{\beta}\right] = 1$.

(b) α, β are both primes of type 1.
Let $\alpha = a + bi$ and $\beta = c + di$. Let $u, v \in \mathbb{Z}$ such that $u \equiv i \mod \alpha$ and $v \equiv i \mod \beta$. Note that from $u \equiv i \mod \alpha$ we have

$$\begin{aligned} bu &\equiv bi \mod \alpha \\ \Rightarrow bu &\equiv -a \mod \alpha \\ \Rightarrow bu &\equiv -a \mod a^2 + b^2. \end{aligned}$$

The last equation is due to proposition 3.2. Similarly we have $dv \equiv -c \mod c^2 + d^2$. Now by proposition 6.7 and corollary 6.9, we have:

$$\begin{aligned} \left[\frac{\beta}{\alpha}\right] &= \left(\frac{c+du}{a^2+b^2}\right) \\ \Rightarrow \left[\frac{\beta}{\alpha}\right]\left(\frac{b}{a^2+b^2}\right) &= \left(\frac{bc-ad}{a^2+b^2}\right) \\ \Rightarrow \left[\frac{\beta}{\alpha}\right] &= \left(\frac{2}{a^2+b^2}\right)\left(\frac{bc-ad}{a^2+b^2}\right). \end{aligned}$$

Similarly, we can also prove

$$\left[\frac{\alpha}{\beta}\right] = \left(\frac{2}{c^2+d^2}\right)\left(\frac{bc-ad}{c^2+d^2}\right).$$

So it suffices to show

$$\left(\frac{2}{c^2+d^2}\right)\left(\frac{bc-ad}{c^2+d^2}\right) = \left(\frac{2}{a^2+b^2}\right)\left(\frac{bc-ad}{a^2+b^2}\right)$$

Let $b = 2b_0$ and $d = 2d_0$. It remains to show that

$$\left(\frac{b_0c-ad_0}{c^2+d^2}\right) = \left(\frac{b_0c-ad_0}{a^2+b^2}\right).$$

Let $b_0c - ad_0 = 2^k e$, where e is odd. Because $4(b_0c-ad_0)^2+(ac+4b_0d_0)^2 = (a^2+b^2)(c^2+d^2)$, by repeating the same argument used in the proof of proposition 6.7, we know that $\left(\frac{e}{c^2+d^2}\right) = \left(\frac{e}{a^2+b^2}\right) = 1$. If b_0+d_0 is odd, then b_0c-ad_0 is also odd because a and c are odd, and we are done. Otherwise, if $b_0 + d_0$ is even, then $4(b_0^2 - d_0^2)$ is divisible by 8, and since $a^2 - c^2$ is also divisible by 8 because both a and c are odd, we deduce that $N(\alpha) - N(\beta)$ is divisible by 8. Hence, $N(\alpha)^2 \equiv N(\beta)^2 \mod 16$, which means that $(-1)^{\frac{N(\alpha)^2-1}{8}} = (-1)^{\frac{N(\beta)^2-1}{8}}$. By proposition 6.8, it follows that

$$\left(\frac{2}{a^2+b^2}\right) = \left(\frac{2}{c^2+d^2}\right).$$

Therefore, either case we will eventually have $\left(\frac{b_0c-ad_0}{c^2+d^2}\right) = \left(\frac{b_0c-ad_0}{a^2+b^2}\right)$. This completes our proof.

(c) α is a prime of type 1 and β is a prime of type 2.
e have $\beta \in \mathbb{Z}$, so by proposition 6.7

$$\left[\frac{\beta}{\alpha}\right] = \left(\frac{\beta}{N(\alpha)}\right) = 1.$$

But by theorem 6.2 and the fact that $N(\alpha)$ is a prime of the form $4k+1$ in $\mathbb{Z}$, we have

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

So it suffices to show that $\left(\frac{N(\alpha)}{\beta}\right) = 1$ if and only if $\left[\frac{\alpha}{\beta}\right] = 1$. The reverse direction is trivial, because if we assume there exists $\eta \in \mathbb{Z}[i]$ such that $\eta^2 \equiv \alpha \mod \beta$, then we also have $\overline{\eta}^2 \equiv \overline{\alpha} \mod \beta$, and thus

$$N(\alpha) \equiv N(\eta)^2 \mod \beta.$$

For the forward direction, assume there exists $s \in \mathbb{Z}$ such that $s^2 \equiv N(\alpha) \mod \beta$. By proposition 5.5, we have $\alpha^{\beta+1} \equiv N(\alpha) \mod \beta$. Therefore,

$$\begin{aligned} \alpha^{\beta+1} &\equiv s^2 \mod \beta \\ \Rightarrow \alpha^{\frac{N(\beta)-1}{2}} &\equiv s^{p-1} \mod \beta \\ \Rightarrow \alpha^{\frac{N(\beta)-1}{2}} &\equiv 1 \mod \beta. \end{aligned}$$

The last equation is due to Fermat's little theorem, and now we can conclude from Euler's criterion that $\left[\frac{\alpha}{\beta}\right] = 1$.

□

Acknowledgement

It is a great pleasure to thank my mentor, Tung Nguyen, for helping me throughout the REU program. This paper would not have been completed without his invaluable support and guidance. I'd also want to thank Professor Peter May and the University of Chicago for providing us with such a great learning and researching experience.

References

[1] David Steven Dummit and Richard M. Foote. *Abstract Algebra*. 3rd ed. Hoboken, NJ : Wiley, c2004. 1991.

[2] Kenneth Ireland and Michael Rosen *A Classical Introduction to Modern Number Theory* Springer, 1990.