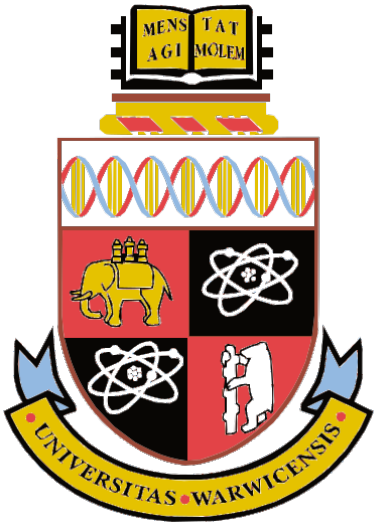

Euclidean Proof of Dirichlet's Theorem on Arithmetic Progressions in Number Fields

by

Au-Yeung Hang Lok Edison

MA4K9 Dissertation

Submitted to The University of Warwick

Mathematics Institute

April, 2023

Contents

1 Introduction

It is well-known that Euclid has proved the existence of infinitely many prime numbers; he proved it by contradiction, a very classical yet simple and beautiful argument. Suppose there are only finitely many of them, then the number constructed by adding 1 to the product of all the primes has to be divisible by a prime not in the finite list. The contradiction therefore forces an infinitude of prime numbers. Many years later, Dirichlet extended this statement and gave the following result.

Theorem 1.1 (Dirichlet's Theorem on primes in progressions, 1837–40)**.** *For any coprime natural numbers q, a, there are infinitely many primes p satisfying $p \equiv a \bmod q$.*

To prove the full result, Dirichlet adopted a lot of analytic methods such as the introduction of the L-function. The proof is relatively complicated, but the tools developed can be used to generalise Dirichlet's Theorem to other algebraic number fields. Without any doubt, the merit and contribution of these analytic methods to the modern study of analytic number theory are significant. Yet, it is also known earlier that for some special choices of a and q, 'elementary tricks' can be used instead. For example, using the properties of the cyclotomic polynomial, it is possible to give a proof for an infinitude of primes $p \equiv 1 \bmod q$ in a very similar manner to Euclid's proof. If Dirichlet's analytic proof for Theorem 1.1 can be generalised to other number fields, can these 'elementary tricks' also be generalised to number fields? This is the primary motivation behind the investigation of this dissertation; we shall say that Dirichlet's Theorem holds for a number field K if for any coprime elements $m, n \in \mathcal{O}_K$, there exists infinitely many $r \in \mathcal{O}_K$ such that $m + nr$ is a prime in $\mathcal{O}_K$ (or equivalently, $m + nr$ is the generator a principal prime ideal in $\mathcal{O}_K$).

Remark 1.2. *The above notion is not the usual way how Dirichlet's Theorem is generalised to other number fields, more terminology will be required for this. Nevertheless, the current description is sufficient to clarify the objective of this dissertation.*

To proceed, we must first give a precise definition for what we mean by 'elementary tricks'. A good starting point would be recalling how we use the cyclotomic polynomial to prove the special case of Dirichlet's Theorem.

Proposition 1.3. *For any natural number n greater than 1, there are infinitely many primes congruent to 1 modulo n.*

Proof. We follow [1, Theorem 47]. Suppose $p_1, ..., p_k$ are all the primes congruent to 1 modulo n. Choose l large enough and let $a = lnp_1...p_k$. Consider the cyclotomic polynomial evaluated at a, write $M = \Phi_n(a)$. Since Φ_n is monic, if l is large enough, then M will be greater than 1 and hence divisible by some prime p.

We claim $p \neq p_i$ for all $1 \leq i \leq k$. It is a fact that Φ_n has constant term 1. By construction, p_i divides all terms of $\Phi_n(a)$ except the constant term. Therefore, p_i must not divide

M for any $1 \leq i \leq k$, implying $p \neq p_i$. By a similar argument, p cannot divide n and l (if so, we would require p to divide 1). Hence, we also have $\gcd(a, p) = 1$.

By definition, $\Phi_n(a) \equiv 0 \bmod p$. Using the fact that $\Phi_n|(x^n - 1)$, we then have $a^n \equiv 1 \bmod p$. Now let $\mathrm{ord}_p(a) = m$, then $m \mid n$. Assume the opposite that we have $m < n$. By the same reason, we must have $a^m \equiv 1 \bmod p$. Since by definition

$$\prod_{d|m} \Phi_d(a) = a^m - 1 \equiv 0 \bmod p,$$

we have $\Phi_d(a) \equiv 0 \bmod p$ for some $d < n$. This shows that $x^n - 1$ has a double root at a modulo p, i.e. $x^n - 1 \equiv (x - a)^2 f(x) \bmod p$ for some polynomial $f(x)$ over the integers. Therefore, the derivative of $x^n - 1$ should also vanish at a modulo p, giving $na^{n-1} \equiv 0 \bmod p$. As argued above, neither n nor a is divisible by p, therefore $m = n$ by contradiction.

We have shown that $\mathrm{ord}_p(a) = n$. Together with Fermat's Little Theorem, this implies $n|(p - 1)$, equivalently $p \equiv 1 \bmod n$. □

In fact, similar proofs also exist for progressions such as $3 \bmod 4$: Suppose $p_1, ..., p_k$ are all the primes congruent to 3 modulo 4, denote their product by P. Consider the polynomial $f(x) = 4x - 1 \in \mathbb{Z}[x]$, clearly $f(P) \equiv 3 \bmod 4$. Since $f(P)$ is a composite number and the product of any two primes congruent to 1 modulo 4 is still congruent to 1 modulo 4, $f(P)$ has to be divisible by one of $p_1, ..., p_k$. However, we also have $f(P) \equiv -1 \bmod p_i$ for all $1 \leq i \leq k$. This is a contradiction.

Observe the proofs above and Euclid's argument are extremely similar: they all use a polynomial, unique to their own cases, namely $f(x) = 4x - 1$ for $3 \bmod 4$ and $g(x) = x + 1$ in Euclid's argument, whose integer values have prime factors in the desired arithmetic progression. Based on this observation, we shall make the following definition:

Definition 1.4 (Euclidean proof)**.** *A Euclidean proof of Dirichlet's Theorem involves the construction of a non constant polynomial $f(x) \in \mathbb{Z}[x]$, which follows Euclid's proof-by-contradiction method to prove the infinitude of primes. In particular, the argument involves primes dividing the polynomial's values at integers.*

It is also worth taking note that the cyclotomic polynomial is an important type of polynomial that is widely used in almost every area in algebra, so one might wonder if it is just pure coincidence that the cyclotomic polynomial is used to prove a particular case of Dirichlet's Theorem. Notice in the proof, we have used the idea of greatest common divisor (hence division), which only makes sense in a unique factorisation domain. Furthermore, notice we have never distinguished between irreducibles and primes in Dirichlet's Theorem, so it seems like only principal ideal domains can obtain an analogous Euclidean proof. With all these criteria, the easiest candidate to come up with is then the Gaussian

integers $\mathbb{Z}[i]$, which is also known for sharing many properties with the integers. Together, they give the objective of this dissertation: generalisation of the cyclotomic polynomial proof for Dirichlet's Theorem on arithmetic progressions in the Gaussian integer, which we formalise as follows:

Guess. There exists a Euclidean proof for the following statement: for any Gaussian integer z, there are infinitely many Gaussian primes satisfying $\pi \equiv 1 \mod z$.

Our first goal is to examine how these polynomials are constructed, outlining the key ingredients behind them. We will then build up on the theories, namely Galois theory and class field theory, with the objective of applying them to the Gaussian integers. Finally, we will state how to find an analogous cyclotomic polynomial proof (abbreviated cyclotomic proof in later sections) for Dirichlet's Theorem in the Gaussian integers.

2 Theory behind the cyclotomic proof

2.1 Infinitude of prime divisors

Our goal here is to dissect the cyclotomic proof in Proposition 1.3 through understanding the construction of polynomials in general cases. Recall when we defined a Euclidean proof, we said it has to involve primes dividing values of a particular polynomial. Yet, in the proofs presented in Section 1, both of them only show that there should be infinitely many such primes. Since it is not obvious that all polynomials should have such a property, we give a proof for it, which is also a type of Euclidean proof without any surprise.

Definition 2.1. *Let $f \in \mathbb{Z}[x]$ be a polynomial over the integers, p be a rational prime. We say p is a prime divisor of f if there exists an integer t such that $p \mid f(t)$. We denote $P(f)$ the set of all prime divisors of the polynomial f.*

Theorem 2.2 (I. Schur)**.** *If $f \in \mathbb{Z}[x]$ is non-constant, then f has infinitely many prime divisors.*

Proof. The proof is due to Murty and Thain [11, Theorem 2]. Let $f \in \mathbb{Z}[x]$ be a non-constant polynomial and suppose $c = f(0) \neq 0$. Otherwise, $p \mid f(p)$ for any rational prime p and the theorem is trivially proved. Note that $P(f)$ is non-empty: $f(x) = \pm 1$ has only finitely many solutions so it can only take on the values ± 1 finitely many times. This means f will take at least one non-unit integer value, therefore having at least 1 prime divisor.

Suppose f only has finitely many prime divisors $p_1, ..., p_k$. Let $Q = p_1 ... p_k$, then $f(Qcx) = cg(x)$ for some $g \in \mathbb{Z}[x]$ of the form $g(x) = 1 + a_1 x + ... + a_k x^k$ with $Q \mid a_i$ for all $1 \leq i \leq k$. Since $P(g)$ is non-empty, by construction, for any prime $p \in P(g), p \in P(f)$, implying $p \mid Q$. However, this cannot be true, otherwise $p \in P(g)$ implies p divides 1. Therefore, f has infinitely many prime divisors by contradiction. □

In this proof, we have only assumed that there are no zero divisors and division makes sense in the integers. Hence, this proof still holds if we replace the integers with any other integral domain, except we need to replace ± 1 with $\pm u$ in the proof, where u is a unit of the domain. This gives us a stronger version of the statements above, in which we have adapted from [3, page 2].

Definition 2.3 (Prime divisor of a polynomial)**.** *Let K be a number field, $f \in \mathcal{O}_K[x]$ be a polynomial over the ring of integers of K, $\mathfrak{p}$ be a prime ideal. We say $\mathfrak{p}$ is a prime divisor of f if $f \bmod \mathfrak{p}$ has a root. We denote $P(f)$ the set of all prime divisors of the polynomial f.*

Theorem 2.4. *Let K be a number field, $\mathcal{O}_K$ the ring of integers of K. If $f \in \mathcal{O}_K[x]$ is non constant, then f has infinitely many prime divisors.*

We are now ready to explore the intuition behind the cyclotomic polynomial in the proof.

2.2 Construction of the polynomial

In this section, the theorems and proofs presented are followed from the article by Murty and Thain [11, Theorem 4], although they originate from an old paper of I. Schur [8].

Let $\zeta_m \in \mathbb{C}$ be a primitive m-th root of unity. From Galois Theory, we know $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$. Let H be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$, and let $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_m)$ be the fixed field of H, where α is guaranteed to exist by the Primitive Element Theorem and $\alpha = h(\zeta_m)$ for some $h \in \mathbb{Z}[x]$.

Lemma 2.5. *With the notations above, let $n = [(\mathbb{Z}/m\mathbb{Z})^\times : H]$ be the index of the subgroup H in $(\mathbb{Z}/m\mathbb{Z})^\times$, let $a_1, ..., a_n$ be the coset representatives of H in $(\mathbb{Z}/m\mathbb{Z})^\times$ and set $\alpha_i = h(\zeta_m^{a_i})$. Define*

$$f(x) \coloneqq \prod_{i=1}^{n} (x - \alpha_i). \tag{2.1}$$

Then the following results hold:

1. *$\alpha_i = h(\zeta_m^{a_i})$ is independent of the choice of coset representatives for all $1 \leq i \leq n$;*
2. *$\alpha_i = h(\zeta_m^{a_i})$ are all distinct conjugates of α for $1 \leq i \leq n$;*
3. *$f(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$.*

Remark 2.6. *The polynomial f constructed above is specific to the subgroup H we choose.*

Proof. Let $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ sending ζ_m to ζ_m^i. Suppose the α_i are not distinct, so there exists some distinct coset representatives x, y of H with $h(\zeta_m^x) = h(\zeta_m^y)$. We can rewrite this as

$$\sigma_x(\alpha) = \sigma_x(h(\zeta_m)) = \sigma_y(h(\zeta_m)) = \sigma_y(\alpha)$$

We can further simplify it to $\sigma_{xy^{-1}}(\alpha) = \alpha$, deducing that $\sigma_{xy^{-1}}$ fixes $\mathbb{Q}(\zeta_m)$ and hence x, y are in the same coset of H, which is a contradiction. Therefore, $\alpha_i = h(\zeta_m^{a_i})$ are distinct conjugates of α for $1 \leq i \leq n$.

Irreducibility of f comes from the fact that the Galois group acts transitively on the set of roots of polynomials over the rationals. Suppose the polynomial f is reducible, so $f = gh$ for some irreducible polynomials $g, h \in \mathbb{Q}[x]$, then any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ will permute the roots of g and h among themselves. Therefore, the Galois group does not act on f transitively, which is a contradiction. Note that for any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, we have $\sigma(f(\alpha_i)) = f(\sigma(\alpha_i)) = 0$, i.e. the automorphisms act on the coefficients of f as the identity, so $f \in \mathbb{Q}[x]$. By definition, $\alpha_i \in \mathbb{Z}[\zeta_m]$ so it is integral over $\mathbb{Q}$. Then by irreducibility of f, the polynomial must have integer coefficients. □

Theorem 2.7. *Let H be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$, and α the generator of the fixed field of H in $\mathbb{Q}(\zeta_m)$. Then there exists an irreducible polynomial $f \in \mathbb{Q}[x]$ such that if $p \in P(f)$, then either p divides m or $[p] \in H$, where $[p]$ denotes the equivalence class of p modulo m.*

Proof. We continue to adopt the notation used in Lemma 2.5. Define

$$f(x) \coloneqq \prod_{i=1}^{n}(x - \alpha_i) \tag{2.2}$$

By Lemma 2.5, $f \in \mathbb{Q}[x]$ is irreducible. We will show that f satisfies the other conditions in the theorem. Denote the discriminant of a polynomial g by $\mathrm{disc}(g)$.

Let $p \in P(f)$ such that $p \nmid \mathrm{disc}(f)$, then there exists $a \in \mathbb{Z}$ such that p divides f. Let $\mathfrak{q}$ be any prime ideal of $\mathbb{Q}(\zeta_m)$ dividing (p), then $\mathfrak{q} \mid (p) \mid f(a)$ for some rational a. Since $\mathfrak{q}$ is a prime ideal in $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$, there exists i such that $\mathfrak{q} \mid (a - \alpha_i) \implies a \equiv \alpha_i \bmod \mathfrak{q}$. We also have $\gcd(a, p) = 1$, so $a \equiv a^p \bmod p$ by Fermat's Little Theorem.
By divisibility, we must have $a \equiv a^p \bmod \mathfrak{q}$ and similarly, $h(x^p) \equiv h(x)^p \bmod \mathfrak{q}$. We therefore have a set of congrueunces:

$$h(\zeta^{a_i}) \equiv \alpha_i \equiv a \equiv a^p \equiv \alpha_i^p \equiv h(\zeta^{a_i})^p \equiv h(\zeta^{a_i p}) \bmod \mathfrak{q} \tag{2.3}$$

which shows that $\mathfrak{q}$ divides $(h(\zeta_m^{a_i})^p - h(\zeta_m^{a_i p}))$.
Since $p \nmid \mathrm{disc}(f)$ and $p \nmid m$, we must have $\gcd(pa_i, m)$=1, forcing $h(\zeta_m^{a_i p}) = h(\zeta_m^{a_j})$ for some j, and in fact $i = j$. Otherwise, suppose $h(\zeta_m^{a_i p}) \neq h(\zeta_m^{a_i})$, then there exists j such that $\mathfrak{q} | (\alpha_i - \alpha_j)$ by (2.3). Since $\mathrm{disc}(f)$ is a rational integer, we also have $p \mid \mathrm{disc}(f)$, which contradicts with our choice of p.
Therefore, $\alpha_i = h\left(\zeta_m^{a_i}\right) = h\left(\zeta_m^{pa_i}\right) = \sigma_p\left(h\left(\zeta_m^{a_i}\right)\right) = \sigma_p(\alpha_i)$, implying that σ_p fixes the field $\mathbb{Q}(\alpha)$ and so p modulo m belongs to H. □

An immediate consequence of the theorem above is the infitude of primes in the arithmetic progression $1 \mod n$, providing us an alternative proof of Proposition 1.3.

Corollary 2.8. *There exist infinitely many rational prime numbers satisfying* $p \equiv 1 \bmod m$.

Proof. Set $H = \{1\}$, then the fixed field is the cyclotomic field $K = \mathbb{Q}(\zeta_m)$ itself, so $\alpha = \zeta_m$ in Theorem 2.7. Clearly, $f = \Phi_m$, the m-th cyclotomic polynomial. Let S be the set of all prime divisors of m, and S is clearly a finite set. Using previous results, we know $P(\Phi_m) \setminus S$ is infinite and it consists of primes $p \equiv 1 \bmod m$ only. □

This corollary has an important implication: in Proposition 1.3, the cyclotomic polynomial did not arise coincidently, but as the minimal polynomial of the m-th root of unity, which is adjoined to the rationals to give the cyclotomic extension. In fact, every finite abelian extension of the rationals $\mathbb{Q}$ lies in a cycltomic field $\mathbb{Q}(\zeta_m)$ for some natural number m. This is known as the Kronecker-Weber Theorem, announced in 1853 by Kronecker [4]. This explains why $\Phi_n(x)$ and $x^m - 1$ cannot have a common root modulo p for $m \mid n$ in the cyclotomic proof, because the cyclotomic field is the splitting field of the polynomial. Perhaps, a similar statement to the Kronecker-Weber Theorem may be needed to write down explicitly a similar polynomial for the Gaussian integers (to be discussed in later sections).

Nonetheless, in order to extend the result of Theorem 2.7 to other number fields, it is necessary to understand the underlying theory of the constructive Euclidean proof. Notice the proof relies heavily on prime powers appearing in the set of congruences, which corresponds to applying the automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ modulo a prime. By showing that σ_p fixes the fixed field of the subgroup H, we deduced that there are infinitely many primes belonging to H, which is the key trick of the proof. Instead of reducing the prime p modulo m directly via the usual map $\phi : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z})$, we used the isomorphism $\omega : \mathrm{Gal}(\mathbb{Q}(\zeta_m/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$ to assign each prime p to an automorphism σ_p, then mapped σ_p to its equivalence class $[p]$ in $H \leq (\mathbb{Z}/m\mathbb{Z})^\times$. This suggests a relationship between rational primes and the elements of the Galois group, pointing out the importance of understanding the structure of the Galois group in the proof.

Now consider the set of primes, S, that divide the discriminant of the polynomial f. These primes are excluded to avoid contradiction with the fact that the coset representatives of H are distinct, while in the cyclotomic proof, the exclusion of such primes is explained in terms of the roots of cyclotomic polynomial Φ_n modulo p. These explanations are limited to their respective proofs, so one might be curious about the theory behind them. It turns out there is an alternative explanation based on Galois extensions, specifically the splitting of primes in field extensions.

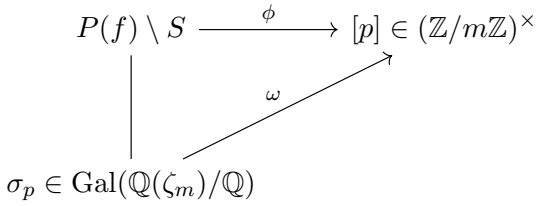

Figure 1: Illustration of the constructive Euclidean proof.

To summarise, we have the following questions to be answered:

1. How does the constructive Euclidean proof associate or map each rational prime to an element of the Galois group? What is the relationship explicitly?
2. If $(\mathbb{Z}/m\mathbb{Z})^\times$ is the Galois group of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, do we have a similar group structure for the Galois group of some extension $L/\mathbb{Q}(i)$?
3. If we can identify the group structure, what is the corresponding field extension for the Gaussian rationals $\mathbb{Q}(i)$?

3 Rational primes and the Frobenius element

3.1 Decomposition of primes in Galois extensions

In the previous section, we have suggested that primes are associated to a certian element in the Galois group. Now we want to make this relationship explicit. In this section, we take L/K to be a Galois extension of number fields. For a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ with $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1}...\mathfrak{q}_g^{e_g}$, where $e_1, ..., e_g$ are positive integers, we write $S_\mathfrak{p} = \{\mathfrak{q}_1, ..., \mathfrak{q}_g\}$ to be the set of prime factors of $\mathfrak{p}$ and we say $\mathfrak{q}_i$ lies over or divides $\mathfrak{p}$.

Now we consider a particular prime $\mathfrak{q} \in S_\mathfrak{p}$. It is clear that there is a natural embedding $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$, in which we can extend it to get $\mathcal{O}_K \hookrightarrow \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{q}$. Since $\mathfrak{q}$ lies over $\mathfrak{p}$, the kernel of this composite map is $\mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p}$. Then by the First Isomorphism Theorem, we have the embedding $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{q}$. By the definition of the Galois group $G = \mathrm{Gal}(L/K)$, the automorphisms act on L while fixing K, so they also act on $\mathcal{O}_L$ while fixing $\mathcal{O}_K$, so $(\mathcal{O}_L/\mathfrak{q}) \,/\, (\mathcal{O}_K/\mathfrak{p})$ is indeed a field extension.

Definition 3.1 (Residue class degree)**.** *Suppose $\mathfrak{q}$ is a prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$, then the residue class degree of $\mathfrak{q}$ is $f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$.*

By the above discussion, for any $\sigma \in \mathrm{Gal}(L/K)$, σ must fix $\mathfrak{p}$ and send its prime divisor $\mathfrak{q}_i$ to another divisor $\mathfrak{q}_j$, so G permutes the prime divisors of $\mathfrak{p}$. In fact, this is a a transitive action.

Proposition 3.2. *Suppose L/K is a Galois extension, $\mathfrak{p}$ prime of $\mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^g \mathfrak{q}_i^{e_i}$, $f_i = f_{\mathfrak{q}_i/\mathfrak{p}}$. Then $G = Gal(L/K)$ acts transitively on $S_\mathfrak{p}$ and $e = e_i, f = f_i$ for $1 \le i \le g$ and we have $[L : K] = efg$.*

Proof. Assume the opposite, that $G = \mathrm{Gal}(L/K)$ does not act on $S_\mathfrak{p}$ transitively. Say the image of $\mathfrak{q}_1$ under G is $\mathrm{Orb}_G(\mathfrak{q}_1) = \{\mathfrak{q}_1, ..., \mathfrak{q}_r\}$ with $r < g$. We set

$$A = \prod_{i=1}^{r} \mathfrak{q}_i, \qquad B = \prod_{j=r+1}^{g} \mathfrak{q}_j,$$

and then we have

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i} \subseteq \prod_{i=1}^{g} \mathfrak{q}_i = AB = A \cap B.$$

The last equality comes from the fact that A and B are coprime and in rings of integers, all prime ideals are maximal so A and B are comaximal (i.e. $A + B = \mathcal{O}_L$). In particular, $B \neq \mathcal{O}_L$. By construction, A and B are G invariant, or equivalently, $\sigma(A) = A, \sigma(B) = B$ for all $\sigma \in G$. Since $A + B = \mathcal{O}_L$, by the Chinese Remainder Theorem, there exists $a \in \mathcal{O}_L$ that satisfies the set of congruences

$$a \equiv 0 \bmod A, \quad a \equiv 1 \bmod B.$$

Let $a = 1 + b$ with $b \in B$, and consider the product of the conjugates of a. We can express it in two ways using the congruences above:

$$\begin{aligned} c &= \prod_{\sigma \in G} \sigma(a) \in K \cap A \subseteq \mathfrak{p} \subseteq A \cap B \subseteq B, \text{and} \\ c &= \prod_{\sigma \in G} \sigma(a) = \prod_{\sigma \in G} \sigma(1 + b) \in 1 + B. \end{aligned}$$

Therefore, we deduce that $c \in 1 + B$ and $c \in B$, meaning $1 \in B$. This contradicts the fact that $B \neq \mathcal{O}_L$, so G acts transitively on $S_\mathfrak{p}$ by contradiction.

By transitivity, we can rewrite the unique factorisation of the ideal $\mathfrak{p}$ as follows:

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{g} \sigma(\mathfrak{q}_i)^{e_i}.$$

Therefore, we conclude that $e = e_i$ for $1 \leq i \leq g$. Similarly, we also have for any $\sigma \in G, \mathfrak{q}_i \in S_\mathfrak{p}$, $\mathcal{O}_L/\mathfrak{q}_i \cong \mathcal{O}_L/\sigma(\mathfrak{q}_i)$. By transitivity again, we also conclude that $f = f_i$ for $1 \leq i \leq g$.

For the equality $[L : K] = efg$, the proof involves finding the dimension of $\mathcal{O}_L/\mathfrak{q}_i$ as a vector space over $\mathcal{O}_K/\mathfrak{p}$, which we refer readers to Chapter I.6, page 30–33 of [9]. □

Now that we know the Galois group acts transitively on $S_\mathfrak{p}$, if we fix a prime factor $\mathfrak{q} \in S_\mathfrak{p}$, it is natural to investigate the stabiliser of $\mathfrak{q} \in S_\mathfrak{p}$ in G.

Definition 3.3 (Decomposition Group)**.** *Let L/K be a Galois extension with $G = \mathrm{Gal}(L/K)$. The decomposition group of $\mathfrak{q} \in S_\mathfrak{p}$ is the subgroup $D_\mathfrak{q} = \{\sigma \in G \colon \sigma(\mathfrak{q}) = \mathfrak{q}\}$ of G (i.e. the*

stabiliser of $\mathfrak{q}$ *in* G*).*

Using the Orbit-Stabiliser Theorem, we know that $[G : D_\mathfrak{q}]$ equals the cardinality of the orbit of $\mathfrak{q}$. Recall 'transitive action' means that there is only one orbit, so the cardinality of the orbit must be the number of primes lying over $\mathfrak{p}$, so $[G : D_\mathfrak{q}] = \#S_\mathfrak{p} = g$.

Lemma 3.4. *The decomposition subgroups* $D_\mathfrak{q}$ *corresponding to primes* $\mathfrak{q}$ *lying over a given prime* $\mathfrak{p}$ *are all conjugate as subgroups of* G*.*

Proof. This proof is due to [13, page 104]. Let $\sigma, \tau \in G$. We have $\tau^{-1}\sigma\tau(\mathfrak{q}) = \mathfrak{q}$ if and only if $\sigma\tau(\mathfrak{q}) = \tau(\mathfrak{q})$, so $\tau\sigma\tau^{-1} \in D_{\tau\mathfrak{q}}$ if and only if $\tau\sigma\tau^{-1}(\tau(\mathfrak{q})) = \tau\sigma(\mathfrak{q}) = \tau(\mathfrak{q})$ if and only if $\sigma \in D_\mathfrak{q}$.

Similarly, we also have $\tau^{-1}\sigma\tau \in D_\mathfrak{q}$ if and only if $\tau^{-1}\sigma\tau(\mathfrak{q}) = \mathfrak{q}$. So $\tau^{-1}\sigma\tau \in D_\mathfrak{q}$ if and only if $\sigma\tau(\mathfrak{q}) = \tau(\mathfrak{q})$ if and only if $\sigma \in D_{\tau\mathfrak{q}}$. Hence, we have proved $\tau D_\mathfrak{q}\tau^{-1} = D_{\tau\mathfrak{q}}$. □

As previously mentioned, the quotient field $(\mathcal{O}_L/\mathfrak{q}) \,/\, (\mathcal{O}_K/\mathfrak{p}) = \mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}$ is a field extension. Furthermore, since the ideal $D_\mathfrak{q}$ fixes $\mathfrak{q}$, any $\sigma \in D_\mathfrak{q}$ induces a well-defined automorphism $\overline{\sigma}$ on $\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}$ given by $\overline{\sigma}(x + \mathfrak{q}) = \sigma(x) + \mathfrak{q}$ [9, page 123]. The map $\sigma \mapsto \overline{\sigma}$ is a reduction homomorphism from $\mathrm{Gal}(L/K)$ to the Galois group of the residue fields, $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$, denoted as $\pi_\mathfrak{q} \colon D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$. This is the first indication of associating primes with the Galois group $\mathrm{Gal}(L/K)$. It is worth noting that the map $\pi_\mathfrak{q}$ is surjective, but we will not provide a proof as it does not provide information about the pre-image, which is not useful for our purposes. For interested readers, further details can be found in Chapter 7, page 66 of [14].

3.2 The Frobenius element

Definition 3.5 (Inertia group)**.** *Let* $\pi_\mathfrak{q} \colon D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ *be the reduction homomorphism. The inertia group of* $\mathfrak{q}$ *is defined to be* $I_\mathfrak{q} = \mathrm{Ker}(\pi_\mathfrak{q})$*.*

The inertia group consists of those automorphisms of $D_\mathfrak{q}$ which induce the trivial automorphism on the residue class field $\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}$, so we can write

$$I_\mathfrak{q} = \{\sigma \in G \colon \sigma(a) = a \bmod \mathfrak{q} \text{ for all } a \in \mathcal{O}_K\}.$$

Since the reduction map is surjective, we have the following exact sequence of groups

$$1 \to I_\mathfrak{q} \to D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}) \to 1.$$

Together with the fact that $[L : K] = efg$ from Proposition 3.2 and $[G : D_\mathfrak{q}] = g$, we yield

$$\#I_\mathfrak{q} = \frac{\#D_\mathfrak{q}}{\#\,\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})} = \frac{\#\,\mathrm{Gal}(L/K)}{gf} = e.$$

Therefore, the inertia group actually measures how $\mathfrak{p}$ ramifies in L. In particular, if $\mathfrak{p}$ is unramified, we have $\#I_\mathfrak{q} = 1$ and therefore the isomorphism $D_\mathfrak{q} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$. It is a standard fact that the Galois group of finite fields is generated by the Frobenius automorphism $\sigma_\mathfrak{p}$, defined by $x \mapsto x^{\#\mathbb{F}_\mathfrak{p}}$, so in this case the decomposition group must be generated by the pre-image of the Frobenius automorphism.

Definition 3.6 (Frobenius element)**.** *Suppose $\mathfrak{q} \mid \mathfrak{p}$ is unramified with finite residue fields $\mathbb{F}_\mathfrak{q}, \mathbb{F}_\mathfrak{p}$. The inverse image of the Frobenius automorphism in* $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ *under the reduction homomorphism $\pi_\mathfrak{q} : D_\mathfrak{q} \xrightarrow{\sim} Gal(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is the Frobenius element $\sigma_\mathfrak{q} \in D_\mathfrak{q} \subseteq G =$* $\mathrm{Gal}(L/K)$.

Proposition 3.7. *Suppose $\mathfrak{q} \mid \mathfrak{p}$ is unramified with finite residue fields $\mathbb{F}_\mathfrak{q}, \mathbb{F}_\mathfrak{p}$.*

1. *The Frobenius element $\sigma_\mathfrak{q}$ is the unique element in $D_\mathfrak{q}$ such that for all $a \in L$,*

$$\sigma_\mathfrak{q}(a) \equiv a^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}.$$

2. *For $\mathfrak{q}_1, \mathfrak{q}_2 \in S_\mathfrak{p}$, the Frobenius elements $\sigma_{\mathfrak{q}_1}, \sigma_{\mathfrak{q}_2}$ are conjugates in G.*

Proof. (1): It is obvious that $\sigma_\mathfrak{q}$ has the required property, so remains to show uniqueness. Suppose $\sigma \in G$ also satisfies the property above. For any $x \in \mathfrak{q}$, we have $x \equiv 0 \bmod \mathfrak{q}$, so $\sigma(x) \equiv 0 \bmod \mathfrak{q}$ implies $\sigma(x) \in \mathfrak{q}$, therefore $\sigma \in D_\mathfrak{q}$.
By the isomorphism map $\pi_\mathfrak{q}$, both elements must be mapped to the Frobenius automorphism $x \mapsto x^{\#\mathbb{F}_\mathfrak{p}}$, so we have $\sigma = \sigma_\mathfrak{q}$.

(2): This part is due to [13, page 107]. Apply the definition of Frobenius element to $\sigma_{\mathfrak{q}_1}$, then for any $x \in \mathcal{O}_L$, we have $\sigma_{\mathfrak{q}_1}\sigma_{\mathfrak{q}_2}^{-1}(x) - \sigma_{\mathfrak{q}_2}^{-1}(x)^{\#\mathbb{F}_\mathfrak{p}} \in \mathfrak{q}$. Then apply $\sigma_{\mathfrak{q}_2}$ on both sides to yield

$$\sigma_{\mathfrak{q}_2}\sigma_{\mathfrak{q}_1}\sigma_{\mathfrak{q}_2}^{-1}(x) \equiv x^{\#\mathbb{F}_\mathfrak{p}} \bmod \sigma_{\mathfrak{q}_2}(\mathfrak{q})$$

which is equivalent to $\sigma_{\mathfrak{q}_2}\sigma_{\mathfrak{q}_1}\sigma_{\mathfrak{q}_2}^{-1} = \sigma_{\sigma_{\mathfrak{q}_2}(\mathfrak{q}_1)}$. The result follows from the uniqueness of the Frobenius element. □

In this context, the conjugacy class of the Frobenius element $\sigma_\mathfrak{q} \in G$ is the Frobenius class of $\mathfrak{p}$, denoted by $\mathrm{Frob}_\mathfrak{p}$. However, the previous proposition tells us that each conjugacy class is only a singleton set ($\mathrm{Frob}_\mathfrak{p} = \{\sigma_\mathfrak{q} \colon \mathfrak{q} \in S_\mathfrak{p}\}$) when L/K is an abelian extension, so there is no dependence on the choice of $\mathfrak{q}$. It follows that for each $\mathfrak{p}$ in $\mathcal{O}_K$, we can associate a uniquely determined element in $D_\mathfrak{q} \subseteq \mathrm{Gal}(L/K)$ which we denote by $\mathrm{Frob}_\mathfrak{p}$.

Definition 3.8 (Artin symbol)**.** *Suppose L/K is an abelian extension. Then given an unramified prime $\mathfrak{p}$ in K, and $\mathfrak{q} \in L$ dividing $\mathfrak{p}$, we denote the resulting Frobenius element*

$\mathrm{Frob}_{\mathfrak{p}}$ *by the Artin symbol*

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \mathrm{Frob}_{\mathfrak{p}}\,.$$

The purpose of this notation is to emphasise the independence of the Frobenius element from the choice of $\mathfrak{q}$ and the extension we are considering, which can also be viewed as a function that maps unramified primes $\mathfrak{p} \in K$ to $\mathrm{Frob}_{\mathfrak{p}} \in G$.

Remark 3.9. *The Artin symbol looks like the Legendre symbol, which is in fact intentional since the Artin symbol does generalise the (quadratic/cubic) Legendre symbol.*

Therefore, we have obtained the answers to our first question. By considering the residue fields, if all the primes we consider in the rationals $\mathbb{Q}$ are unramified in the field extension $\mathbb{Q}(\zeta_m)$, we can associate each rational prime p to a Frobenius element Frob_p. So when we consider the specific case $p \equiv 1 \bmod m$, this is also the same as requiring the Frobenius element Frob_p to be the identity map in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. On the other hand, the requirement for primes to be unramified also explains why there is a finite set of primes excluded in the polynomial proof and the constructive Euclidean proof of Dirichlet's Theorem, which are in both cases the primes that divide m. In addition, the set of congruences (2.3) in the constructive Euclidean proof is essentially applying Frob_p to α_i and a.

It is worth emphasising again that the theory developed above is limited to abelian extensions, otherwise we would need to consider Frobenius conjugacy classes instead, complicating our investigation.

4 Galois groups of abelian extensions of the Gaussian rationals

Now that we understand how to associate rational primes with the Frobenius element, we can apply this concept directly to give the constructive Euclidean proof for the Gaussian integers $\mathbb{Z}[i]$. However, this approach is not helpful in identifying the group structure $\mathrm{Gal}(L/\mathbb{Q}(i))$ for an abelian extension $L/\mathbb{Q}(i)$. Recall that the constructive Euclidean proof in Theorem 2.7 relies heavily on the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, so do we have a generalization of $(\mathbb{Z}/m\mathbb{Z})^\times$ for $\mathrm{Gal}(L/\mathbb{Q}(i))$? This motivates us to find an abelian extension for the Gaussian rationals. It fact, in algebraic number theory, the branch known as *class field theory* is about describing abelian extensions of global and local fields. We will use it to help us find an answer.

4.1 The Artin map

Previously we have introduced the Artin symbol to represent the Frobenius element, and we view it as a correspondence between unramified primes of the number field K and Frobenius elements in $G = \mathrm{Gal}(L/K)$. This can be extended further and in fact, this is

the first sign of relating Galois groups to generalised ideal class groups.

Definition 4.1 (First definition of the Artin map)**.** *Let S be the finite set of primes of K which ramifies in L, denote the ideal group of K by I_K (i.e. the group of non-zero fractional ideals of K), and let I_K^S be the subgroup of I_K generated by all the primes* ***outside*** *S. The Artin map is the homomorphism*

$$\left(\frac{L/K}{\cdot}\right) : I_K^S \to \mathrm{Gal}(L/K),$$

$$\prod_{i=1}^{t} \mathfrak{p}^{e_i} \mapsto \prod_{i=1}^{t} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}.$$

Remark 4.2. *Here we once again emphasise that we are considering the product of prime ideals that are* ***unramified*** *in L.*

This product is well defined since we have assumed $\mathrm{Gal}(L/K)$ to be abelian; and if $t = 1$, it is simply the Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$. Any ideal in a ring of integers admits a unique prime ideal factorisation, up to reordering, so this is establishing a relationship between the Galois group of a field extension and ideals even if the Artin map is not an isomorphism.

With regards to how we define the generalisation of Dirichlet's Theorem in the Gaussian integers, one might expect the role of the integer m in $p \equiv 1 \bmod m$ is simply played by an ideal $\mathfrak{m}$ in number fields. It turns out that this is not precise enough (we will see why later) and we need to introduce the notion of a *modulus*. The following definition is taken from [6, §8, page 144].

Definition 4.3 (Modulus)**.** *Let K be a number field. A modulus (or divisor) is a formal product $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ over all primes $\mathfrak{p}$, finite or infinite, of K, where the exponents must satisfy:*

1. *$n_{\mathfrak{p}} \geq 0$, and at most finitely many are non-zero;*
2. *$n_{\mathfrak{p}} = 0$ whenever $\mathfrak{p}$ is a complex infinite prime;*
3. *$n_{\mathfrak{p}} \leq 1$ whenever $\mathfrak{p}$ is a real infinite prime.*

This definition has abused some of the terminologies - here 'primes' actually refers to 'places', set of equivalence classes of absolute values induced by prime ideals. One can think of finite primes as $\mathfrak{p}$-adic absolute values, while an infinite prime is the usual Archimedean absolute value $|x|$ we use, but after applying an embedding $\sigma : K \to \mathbb{C}$ to an element x (i.e. $|\sigma(x)|$). Therefore, when it says 'formal product', one should think of the product as a way of listing primes with embeddings, since we do not really know what does multiplying ideals by embeddings mean. In this case, the exponent $n_{\mathfrak{p}}$ is really an indicator for finite, real and complex embeddings.

With the explanation above, one can also rewrite the definition of a K-modulus as a formal product $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$, where $\mathfrak{m}_\infty$ is a formal product of real embeddings of K (since when it is a complex embedding, the exponent is 0), and $\mathfrak{m}_0$ (the 'finite' part) is a nonzero ideal in $\mathcal{O}_K$. Therefore, for a purely imaginary field K, the definition of a modulus is the same as an ideal with $\mathfrak{m} = \mathfrak{m}_0$. Since the Gaussian rationals $\mathbb{Q}(i)$ are purely imaginary, we will omit the explanations involving places. Readers can refer to Chapter 3.1, page 45–47 of [2] or Chapter II.1, page 83-90 of [9].

Definition 4.4 (Second definition of the Artin map)**.** *For Galois extension L/K, let $\mathfrak{m}$ be a K-modulus divisible by all ramified primes in K, $I_K^{\mathfrak{m}}$ the subgroup of I_K generated by all the primes of K coprime with $\mathfrak{m}_0$. The Artin map is the homomorphism*

$$\Phi_{L/K}^{\mathfrak{m}} = \left(\frac{L/K}{\cdot}\right) : I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K); \qquad \prod_{\mathfrak{p} \nmid \mathfrak{m}} \mathfrak{p}^{n_\mathfrak{p}} \mapsto \prod_{\mathfrak{p} \nmid \mathfrak{m}} \left(\frac{L/K}{\mathfrak{p}}\right)^{n_\mathfrak{p}}.$$

Theorem 4.5 (Artin, 1927)**.** *Let L/K be an abelian Galois extension, and let $\mathfrak{m}$ be a modulus that is divisible by all primes that ramify in L. Then the Artin map $\Phi_{L/K}^{\mathfrak{m}} : I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective.*

This is the result of a lot of analytical materials, which are largely irrelevant from the objective of this dissertation. Readers may refer to Chapter IV, page 162–164 of [9] or Lecture 21, page 6–10 of [14], where the former uses the Frobenius Density Theorem to prove the result while the latter does not. Nevertheless, this is an extremely important property of the Artin map, because with certain restrictions on the choice of modulus $\mathfrak{m}$ (we will see later), we can apply the First Isomorphism Theorem to yield the isomorphism between the Galois group $\mathrm{Gal}(L/K)$ and $I_K^{\mathfrak{m}}$ quotient by the kernel. So for an abelian extension of the Gaussian rationals $\mathbb{Q}(i)$, the quotient group of $I_K^{\mathfrak{m}}$ is the generalisation of $(\mathbb{Z}/m\mathbb{Z})^\times$ that we are looking for.

Remark 4.6. *It is also possible to use an algebraic approach to prove the result above, but it will require far more complicated concepts such as ideles, which is considered to be the modern approach. Readers might refer to Chapter 4 of [2] or Chapter VI, X of [10].*

4.2 Ray class group of the Gaussian rationals

We will start by defining some subgroups of $K^\times$ associated with a modulus $\mathfrak{m}$.

- $I_K^{\mathfrak{m}} \subseteq I_K$, the subgroup of fractional ideals coprime to $\mathfrak{m}_0$.
- $K^{\mathfrak{m}} \subseteq K^\times$, the subgroup of $K^\times$ such that for $\alpha \in K^\times, (\alpha) \in I_K^{\mathfrak{m}}$.
- $K^{\mathfrak{m},1} \subseteq K^{\mathfrak{m}}$, the subgroup of $\alpha \in K^{\mathfrak{m}}$ that satisfies $a \equiv 1 \bmod \mathfrak{m}$, or equivalently
  1. $\alpha \equiv 1 \bmod \mathfrak{m}_0 \iff \mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{m}_0)$ for all $\mathfrak{p} \mid \mathfrak{m}_0$; and

2. $a \equiv 1 \bmod \mathfrak{m}_\infty \iff \sigma(\frac{\alpha}{1}) = \sigma(\alpha) > 0$ for all real embeddings $\sigma \mid \mathfrak{m}_\infty$ (i.e. the image of α under σ is positive).

- $P_K^{\mathfrak{m}} \subseteq I_K^{\mathfrak{m}}$, the subgroup of principal fractional ideals (α) with $\alpha \in K^{\mathfrak{m},1}$. This is sometimes called the *'rays' of principal ideals* or *ray group.*

Definition 4.7 (Ray class group)**.** *The ray class group of K for the modulus $\mathfrak{m}$ is the quotient $Cl_K^{\mathfrak{m}} \coloneqq I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ (when $\mathfrak{m} = 1$, this is just the usual class group of K).*

Remark 4.8. *In §1, we have mentioned the way how we view generalisation of Dirichlet's Theorem to other number fields differs from the usual convention. In fact, one possible way is interpreting it is 'there exist infinitely many prime ideals $\mathfrak{p} \in \mathcal{O}_K$ in each generalised ideal classes of $P_K^{\mathfrak{m}}$ for a number field K and modulus $\mathfrak{m}$'* [2, page 49].

Here we will give two examples to show why we need to use moduli instead of ideals in the definition of ray class group, although it does not really matter if the number field is purely imaginary as discussed before. Consider $K = \mathbb{Q}$, with the modulus $\mathfrak{m} = (5)$. We have

- $K^{\mathfrak{m}} = \{\frac{a}{b} \in \mathbb{Q}^\times : \gcd(\frac{a}{b}, 5) = 1\} = \{\frac{a}{b} : a, b \not\equiv 0 \bmod 5, a, b \in \mathbb{Z}\}$,
- $K^{\mathfrak{m},1} = \{\frac{a}{b}\mathbb{Z} : \frac{a}{b} \equiv 1 \bmod 5\} = \{\frac{a}{b} : a \equiv b \bmod 5\}$.

Note that in this example, the modulus $\mathfrak{m} = (5)$ does not include any real embeddings, so we have dropped the condition $\frac{a}{b} > 0$. This gives us

- $I_K^{\mathfrak{m}} = \{(1), \left(\frac{1}{2}\right), (2), \left(\frac{1}{3}\right), \left(\frac{2}{3}\right), \left(\frac{3}{2}\right), (3), \left(\frac{1}{4}\right), \left(\frac{3}{4}\right), \left(\frac{4}{3}\right), (4), \left(\frac{1}{6}\right), (6), ...\}$,
- $P_K^{\mathfrak{m}} = \{(1), \left(\frac{2}{3}\right), \left(\frac{3}{2}\right), \left(\frac{1}{4}\right), (4), \left(\frac{1}{6}\right), (6), \left(\frac{2}{7}\right), \left(\frac{7}{2}\right), ...\}$,
- $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} = \{\left(\frac{1}{2}\right), (2), \left(\frac{1}{3}\right), (3), \left(\frac{3}{4}\right), \left(\frac{4}{3}\right), ...\}$.

Notice we have $2 \equiv -3 \bmod 5$ and clearly $\left(\frac{2}{3}\right) = \left(-\frac{2}{3}\right)$, so $\left(\frac{2}{3}\right)$ is indeed an element of $P_K^{\mathfrak{m}}$. In fact, we are now dealing with *fractional ideals*, therefore multiplying the ideals by ± 1 does not change the equivalence class in the ray class group. Specfically, we have $-4 \equiv 1 \bmod 5$, so the ray class group mod $\mathfrak{m}$ is:

$$Cl_K^{\mathfrak{m}} = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} = \{[(1)], [(2)], [(3)], [(4)]\}/\{[(1)], [(4)]\} \cong (\mathbb{Z}/5\mathbb{Z})^\times/\{\pm 1\} \cong (\mathbb{Z}/2\mathbb{Z})^\times$$

If we consider $K = \mathbb{Q}, \mathfrak{m} = (5)\mathfrak{m}_\infty$ instead, we will need to consider the image of the principal ideals under the real embeddings. The only real embedding for $\mathbb{Q}$ is the identity element, so we are only allowed to consider the fractional ideals generated by positive elements. Equivalently, we now consider $K^{\mathfrak{m},1} = \{\frac{a}{b} : \frac{a}{b} > 0 \text{ and } a \equiv b \bmod 5\}$. This gives

- $P_K^{\mathfrak{m}} = \{(1), \left(\frac{1}{6}\right), (6), \left(\frac{2}{7}\right), \left(\frac{7}{2}\right), ...\}$,
- $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} = \{(1), \left(\frac{1}{2}\right), (2), \left(\frac{1}{3}\right), \left(\frac{2}{3}\right), \left(\frac{3}{2}\right), (3), \left(\frac{1}{4}\right), \left(\frac{3}{4}\right), \left(\frac{4}{3}\right), (4), ...\}$.

In this case, $[(-1)] \not\equiv [(1)]$, so the order of $\left(\frac{a}{b}\right) \cdot P_K^{\mathfrak{m}}$ is $\max\{\mathrm{ord}_5(a), \mathrm{ord}_5(b)\}$. Hence, we deduce that

$$Cl_K^{\mathfrak{m}} = I_K^{\mathfrak{m}} / P_K^{\mathfrak{m}} \cong (\mathbb{Z}/5\mathbb{Z})^{\times}.$$

One can see that when we use modulus instead of ideal in the definition of a ray class group, we allow a varying sign condition and this will produce a larger group as well. Even though it does not matter for any purely imaginary field as we emphasised, this might give us some insights in computing the ray class group when we do not have any other tools.

Now consider $K = \mathbb{Q}(i)$, with the modulus $\mathfrak{m} = (1 + 2i)$. Considering it is more difficult to compute the congruence classes, a geometric approach has been adopted.

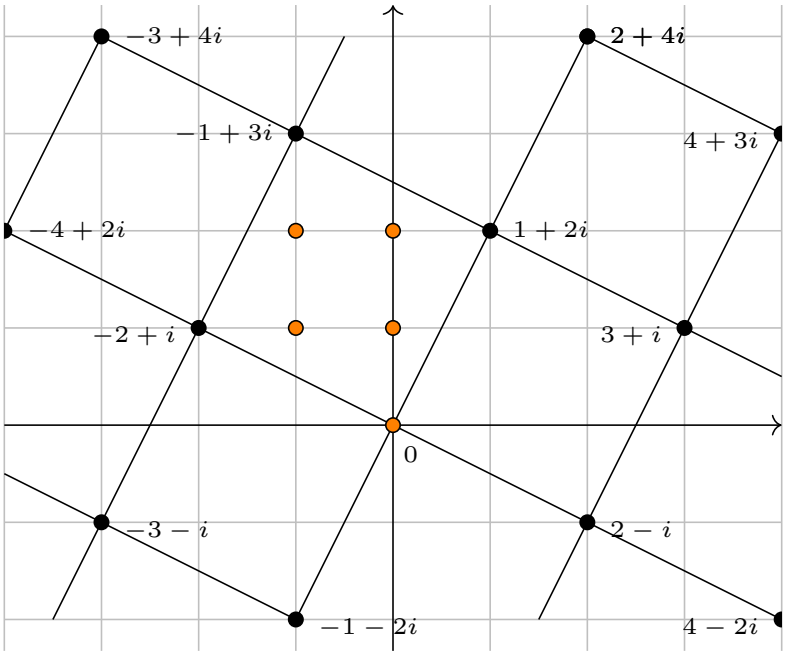

Figure 2: $\mathbb{Z}[i]$-multiples of $1 + 2i$, with representatives of $\mathbb{Z}[i]/(1 + 2i)$ in orange.

With reference to Figure 2, the equivalence classes of $\mathfrak{m}$ are

$$\mathbb{Z}[i]/(\mathfrak{m}) = \{[0] \equiv [1 + 2i], [i], [2i] \equiv [-1], [-1 + 2i] \equiv [-i], [-1 + i] \equiv [1]\} = \{\langle [i] \rangle\}.$$

With this piece of information, we can immediately identify that $I_K^{\mathfrak{m}} = P_K^{\mathfrak{m}}$. Notice for any fractional ideals of $\mathbb{Z}/\mathfrak{m}\mathbb{Z}[i]$, $\left[\left(\frac{a}{b}\right)\right] \equiv [i]^k$ for some integer k. Following the argument in the case of $K = \mathbb{Q}$, $\mathfrak{m} = (5)$, $\left(i^{-k} \cdot \frac{a}{b}\right) = \left(\frac{a}{b}\right)$ with $\left[\left(i^{-k} \cdot \frac{a}{b}\right)\right] \equiv [1]$. Therefore, the ray class group is just the trivial group, $Cl_{\mathbb{Q}(i)}^{\mathfrak{m}} = \{id\}$.

This example may look useless at first sight, but if we compare all these examples, one might notice the argument above is perhaps suggesting that for $K = \mathbb{Q}(i)$ with respect to a modulus $\mathfrak{m}$, the ray class group has the structure $Cl_K^{\mathfrak{m}} \cong (\mathbb{Z}[i]/(\mathfrak{m}))^{\times} / (\mathbb{Z}[i])^{\times}$. At least,

the cardinality argument works for the example above. Instead, this observation is true for any number field K.

Theorem 4.9. *Let $\mathfrak{m}$ be a modulus for a number field K. We have an isomorphism*

$$K^{\mathfrak{m}}/K^{\mathfrak{m},1} \cong \{\pm 1\}^{\#m_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times.$$

If K is a purely imaginary number field, then it simplifies to $K^{\mathfrak{m}}/K^{\mathfrak{m},1} \cong (\mathcal{O}_K/\mathfrak{m}_0)^\times$.

Proof. We will prove the latter case only, since the former involves the use of finite and infinite places which we have omitted for clarity. For full proof refer to Lecture 21, page 5 of [14]. Define the homomorphism

$$\psi : K^{\mathfrak{m}} \to (\mathcal{O}_K/\mathfrak{m}_0)^\times \quad ; \quad \alpha \mapsto [\alpha],$$

where $[\alpha] = [a][b]^{-1} \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$. By definition of $K^{\mathfrak{m}}$, (a) and (b) are coprime to $\mathfrak{m}_0$, so both lie in $(\mathcal{O}_K/\mathfrak{m}_0)^\times$. Therefore, this is a well-defined operation.
The kernel of the map is clearly $K^{\mathfrak{m},1}$, while surjectivity follows from the definition of equivalence classes being non-empty. Therefore, the isomorphism follows from the First Isomorphism Theorem. □

Recall from the previous examples of ray class groups, multiplying an ideal by units does not change the ideal. Since $K^{\mathfrak{m}}/K^{\mathfrak{m},1}$ is not invariant under unit multiplication, we must have $\left(K^{\mathfrak{m}}/K^{\mathfrak{m},1}\right)/\mathcal{O}_K^\times \cong I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. Therefore, we yield

$$I^{\mathfrak{m}}_{\mathbb{Q}(i)}/P^{\mathfrak{m}}_{\mathbb{Q}(i)} = Cl^{\mathfrak{m}}_{\mathbb{Q}(i)} \cong (\mathbb{Z}[i]/(\mathfrak{m}))^\times/(\mathbb{Z}[i])^\times.$$

Recall the discussion in Section 2.2, one of the reasons why the constructive Euclidean proof by Schur in Theorem 2.7 gives us the $1 \bmod p$ condition is because the group $\mathrm{Gal}(\mathbb{Q}(\zeta_m/\mathbb{Q})$ is isomorphic to the multiplicative group of integers modulo m. Hence, by showing the automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m/\mathbb{Q})$ fixes the fixed field H, this allows us to directly to reduce a prime p over a modulus we are interested in. Sadly, we now know that this is generally not true for the Gaussian rationals; it is not so clear what it means for a Gaussian prime π to satisfy $\pi \equiv 1 \in (\mathbb{Z}[i]/\mathfrak{m}\mathbb{Z}[i])^\times/\{\pm 1, \pm i\}$. Fortunately, we can perform the same trick if we choose our modulus $\mathfrak{m}$ carefully. We first give a definition to make the following process clearer to the reader:

Definition 4.10. *A Gaussian integer β is said to be odd if it is not divisible by $(1+i)$, and even otherwise.*

Proposition 4.11. *For any odd Gaussian integer β, $\beta \equiv i^\varepsilon \bmod 2(i+1)$ for some $\varepsilon \in$*

$\{0, 1, 2, 3\}$. *Furthermore, there is an isomorphism*

$$(\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i])^\times \cong (\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}.$$

Proof. Note that if β is odd, then it is necessarily a unit of $\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i]$, so we are left with proving the isomorphism. Note that $a+ib$ is not coprime with 2(1+i) if and only if $a+ib$ is divisible by $(1 \pm i)$, which happens when

$$\frac{a+ib}{1+i} = \frac{a+b}{2} + \frac{b-a}{2}i \quad \text{and} \quad \frac{a+ib}{1-i} = \frac{a+b}{2} + \frac{a+b}{2}i$$

are Gaussian integers and these will both require $a \equiv b \bmod 2$. Therefore, we have

$$\left| \left(\frac{\mathbb{Z}[i]}{(2+2i)\mathbb{Z}[i]} \right)^\times \right| = \frac{1}{2} \operatorname{Nm}(2+2i) = 4.$$

The units of Gaussian integers are $\{\pm 1, \pm i\}$, which are clearly distinct equivalent classes in $\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i]$. This yields the isomorphism. □

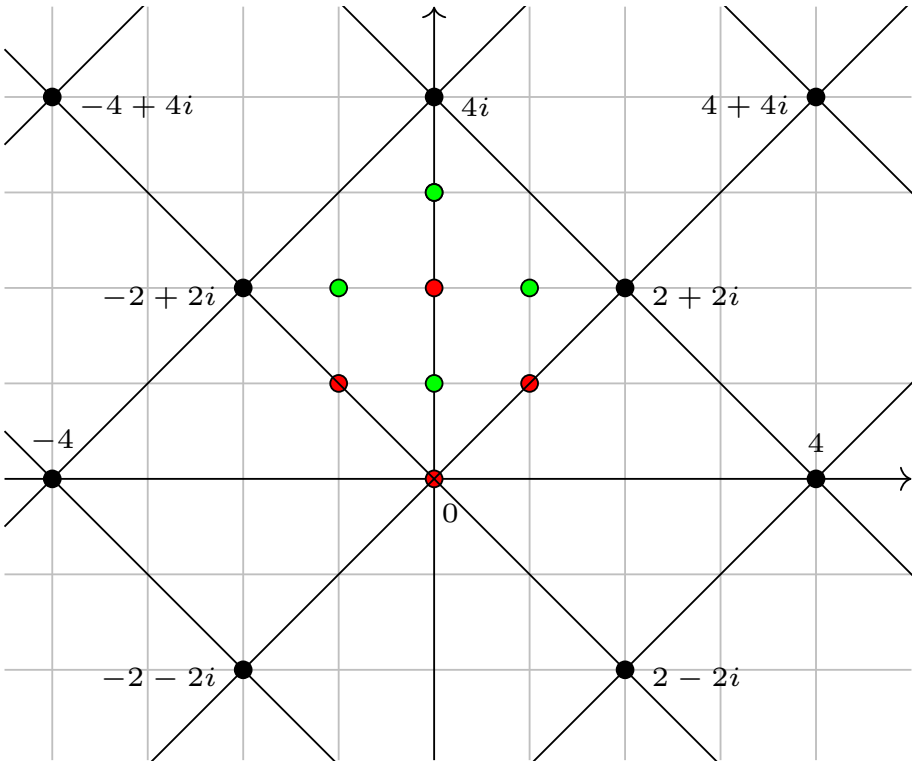

Figure 3: $\mathbb{Z}[i]$-multiples of $2+2i$, with odd representatives of $\mathbb{Z}[i]/(2+2i)$ in green.

This proposition is extremely useful: consider $\mathfrak{m} = 2(i+1)\beta$, where β is an odd Gaussian integer. By the Chinese Remainder Theorem, we have

$$(\mathbb{Z}[i]/(\mathfrak{m}))^\times/(\mathbb{Z}[i])^\times \cong (\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i])^\times/(\mathbb{Z}[i])^\times \times (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times \cong (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times.$$

We have now made significant progress towards obtaining the generalization of $(\mathbb{Z}/m\mathbb{Z})^\times$ in the Gaussian integers. To complete this generalisation, we must establish that the kernel of the Artin map $\Phi^{\mathfrak{m}}_{L/K}$ is the ray class group with respect to the modulus $\mathfrak{m} = (2+2i)\beta$, where β is an odd Gaussian integer. However, it should be noted that when we defined the Artin map in Definition 4.4, we assumed that the field extension L/K was given and that we could find a modulus $\mathfrak{m}$ containing all primes ramifying in L. Unfortunately, this presents a challenge in our current situation, as we cannot prove that the modulus $\mathfrak{m} = (2+2i)\beta$ contains all the primes that ramify, nor can we compute the kernel.

Despite these obstacles, we can rely on class field theory to overcome this challenge. It assures us that our concerns about the choice of modulus are unnecessary.

4.3 Class groups and class fields

The Galois correspondence provides a significant result in the bijection between groups and field extensions, with the conventional approach being to understand the Galois group as groups are generally easier to comprehend. In the same spirit of Galois theory, our discussion begins with an examination of certain subgroups of the fractional ideals $I_K^{\mathfrak{m}}$.

Definition 4.12 (Congruence subgroup)**.** *A subgroup* $\mathbf{H}$ *of* $I_K^{\mathfrak{m}}$ *is called a congruence subgroup with modulus* $\mathfrak{m}$ *if there is a modulus* $\mathfrak{m}$ *for* K *such that* $P_K^{\mathfrak{m}} \subseteq \mathbf{H} \subseteq I_K^{\mathfrak{m}}$*. We say* $\mathbf{H}$ *is defined mod* $\mathfrak{m}$ *in this context, denoted* $\mathbf{H}^{\mathfrak{m}}$*.*

One might observe that for two moduli $\mathfrak{m}, \mathfrak{n}$ satisfying $\mathfrak{n} \mid \mathfrak{m}$, we have $I_K^{\mathfrak{m}} \subseteq I_K^{\mathfrak{n}}$ by definition (if $\mathfrak{n} \mid \mathfrak{m}$, then there are more fractional ideals coprime with $\mathfrak{n}$ than with $\mathfrak{m}$), and similarly for $P_K^{\mathfrak{m}} \subseteq P_K^{\mathfrak{n}}$. Therefore, it might happen that $\mathbf{H}^{\mathfrak{m}} = I_K^{\mathfrak{m}} \cap \mathbf{H}^{\mathfrak{n}}$ for a congruence subgroup $\mathbf{H}^{\mathfrak{n}}$ defined mod $\mathfrak{n}$; in this case we say $\mathbf{H}^{\mathfrak{m}}$ is the restriction of $\mathbf{H}^{\mathfrak{n}}$ to $I_K^{\mathfrak{m}}$. This restriction provides us an equivalence relation on the set of congruence subgroups of I_K.

Definition 4.13. *Let* K *be a number field. Two congruence subrgoups* $\mathbf{H}_1, \mathbf{H}_2$ *have a common restriction, written* $\mathbf{H}_1 \sim \mathbf{H}_2$*, if there is a modulus* $\mathfrak{m}$ *for* K *such that*

$$\mathbf{H}_1 \cap I_K^{\mathfrak{m}} = \mathbf{H}_2 \cap I_K^{\mathfrak{m}}.$$

This is indeed an equivalence relation: reflexivity and symmetry are clear. Suppose $\mathbf{H}_1 \sim \mathbf{H}_2$ and $\mathbf{H}_2 \sim \mathbf{H}_3$, then there exist moduli $\mathfrak{m}$ and $\mathfrak{n}$ such that

$$\mathbf{H}_1 \cap I_K^{\mathfrak{m}} = \mathbf{H}_2 \cap I_K^{\mathfrak{m}} \text{ and } \mathbf{H}_2 \cap I_K^{\mathfrak{n}} = \mathbf{H}_3 \cap I_K^{\mathfrak{n}}$$

Let $\mathfrak{m}'$ be a modulus divisible by both moduli $\mathfrak{m}, \mathfrak{n}$ (so we can pick $\mathfrak{m}'$ to be the least common multiple of $\mathfrak{m}$ and $\mathfrak{n}$), then clearly

$$\mathbf{H}_1 \cap I_K^{\mathfrak{m}'} = \mathbf{H}_2 \cap I_K^{\mathfrak{m}'} \text{ and } \mathbf{H}_2 \cap I_K^{\mathfrak{m}'} = \mathbf{H}_3 \cap I_K^{\mathfrak{m}'}$$

Hence we have transitivity, $\mathbf{H}_1 \sim \mathbf{H}_3$, proving that $\sim$ is an equivalence relation [9, page 200]. We have shown that the least common multiple of two moduli is in the same equivalence class. Going the other way, the greatest common divisor of two moduli also has the same property, surprisingly.

Lemma 4.14. *Let $\mathbf{H}_1, \mathbf{H}_2$ be congruence subgroups defined modulo $\mathfrak{m}_1$ and $\mathfrak{m}_2$ respectively, which have a common restriction $\mathbf{H}_3 = \mathbf{H}_i \cap I_K^{\mathfrak{m}_i}$ for $i = 1, 2$. Let $\mathfrak{m}$ be the greatest common divisor of $\mathfrak{m}_1$ and $\mathfrak{m}_2$. Then there is a congruence subgroup $\mathbf{H}^{\mathfrak{m}}$ defined mod $\mathfrak{m}$ such that $\mathbf{H}^{\mathfrak{m}} \cap I_K^{\mathfrak{m}_i} = \mathbf{H}_i$ for $i = 1, 2$.*

Proof. Refer to Chapter V.6, page 200 of [9]. □

Combining these facts, we can now see that there is a unique modulus that represents each equivalence class. We formalise the ideas in the definition below.

Definition 4.15. *An equivalence class of congruence subgroups is called an ideal group. Further suppose an ideal group $\mathbf{H}$ contains congruence subgroups defined mod $\mathfrak{m}_1, ..., \mathfrak{m}_k$, then there is a unique modulus $\mathfrak{f}$ satisfying $\mathbf{H}^{\mathfrak{f}} \in \mathbf{H}$ and $\mathfrak{f} \mid \mathfrak{m}_i$ for all $i = 1, ..., k$. This modulus $\mathfrak{f}$ is called the conductor of $\mathbf{H}$.*

Earlier in §4.1, we have said that the Galois group of an abelian extension L/K is isomorphic to $I_K^{\mathfrak{m}} / \operatorname{Ker}\left(\Phi_{L/K}^{\mathfrak{m}}\right)$ under certain restrictions on the choice of modulus $\mathfrak{m}$. The main concern is if the kernel of the Artin map is not a congruence subgroup, then the quotient group does not make sense. By combining the idea of ideal group and conductor, we now would like to make the restrictions explicit by presenting one of the most important results in class field theory.

Theorem 4.16 (Artin Reciprocity Theorem - Artin, 1927)**.** *Let L/K be a **given** abelian extension. Then the conductor $\mathfrak{f}$ of L/K, divisible by exactly the primes of K ramifying in L, exists and for any modulus $\mathfrak{m}$ divisible by all finite and infinite primes of K that ramify in L, we have*

$$P_K^{\mathfrak{m}} \subseteq \operatorname{Ker}(\Phi_{L/K}^{\mathfrak{m}}) \subseteq I_K^{\mathfrak{m}} \text{ if and only if } \mathfrak{f} \mid \mathfrak{m}$$

Therefore, if $\mathfrak{f} \mid \mathfrak{m}$, the Artin map $\Phi_{L/K}^{\mathfrak{m}} : I_K^{\mathfrak{m}} \to \operatorname{Gal}(L/K)$ is surjective with $\operatorname{Ker}(\Phi_{L/K}^{\mathfrak{m}})$ satisfying $I_K^{\mathfrak{m}} / \operatorname{Ker}(\Phi_{L/K}^{\mathfrak{m}}) \cong \operatorname{Gal}(L/K)$.

Proof. Refer to Chapter V.5, page 190–198 of [9], although note that we have rephrased the statement according to [4, Theorem 6.3] to give a clearer version of the theorem. □

Again, this is not the condition we have. However, class field theory actually says that the converse to the Artin Reciprocity Theorem holds. Surprisingly, we do not even have to worry if the modulus $\mathfrak{m}$ is divisible by the conductor or not. This result is known as the Existence Theorem [4, Theorem 5.6].

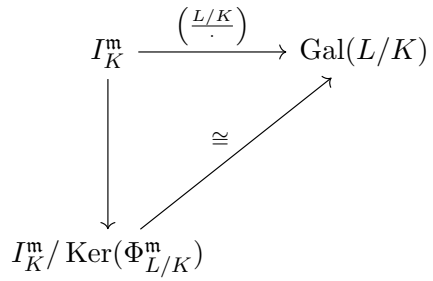

Figure 4: Illustration of the Artin Reciprocity theorem.

Theorem 4.17 (Existence Theorem - Takagi, 1920)**.** *Let* $\mathfrak{m}$ *be a modulus of* K *and* $\mathbf{H}$ *be a congruence subgroup for* $\mathfrak{m}$ ***given****. Then there is a unique abelian extension* L *of* K*, all of whose ramified primes, finite or infinite, divide* $\mathfrak{m}$*, such that if* $\Phi_{L/K}^{\mathfrak{m}} : I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ *is the Artin map of* $K \subset L$*, then* $\mathbf{H} = \mathrm{Ker}(\Phi_{\mathfrak{m}})$*.*

Proof. Refer to Chapter V.9, 208–214 of [9]. □

The Existence Theorem has quite a few remarkable consequences: the Existence theorem asserts that for any ideal class group, a corresponding abelian field extension of K must exist. We call such abelian field extension a *class field*. In particular, there are two types of class fields that are in our interest in this dissertation.

Definition 4.18. *Consider an abelian extension* L/K*.*

1. *If all primes of* K*, except the factors of the modulus* $\mathfrak{m}$*, are unramified in* L *for which* $\mathrm{Ker}\left(\Phi_{L/K}^{\mathfrak{m}}\right) = P_K^{\mathfrak{m}}$*, we call* L *the ray class field for the modulus* $\mathfrak{m}$*, denoted by* $K(\mathfrak{m})$*.*
2. *If* L *is the maximal unramified abelian extension of* K *(i.e. the primes of* K *are all unramified in* L*, or equivalently the conductor associated is* $\mathfrak{f} = (1)$*), we call* L *the Hilbert class field of* K*, denoted by* H/K*.*

Therefore, for any given modulus $\mathfrak{m}$, we can find a corresponding ideal class and the ray class field $K(\mathfrak{m})$ that contains some other smaller class fields. In other words, the Existence Theorem is a generalisation of the Kronecker-Weber Theorem to a number field K. While for the Hilbert class field, we will use it in the next section.

Historically, Takagi first discovered that for each ideal group $\mathbf{H}$, there is a corresponding class field L over K. However, he did not explicitly construct the isomorphism $I_K^{\mathfrak{m}}/\mathbf{H} \cong \mathrm{Gal}(L/K)$, as the concept of the Artin map had not yet been developed. The Artin Reciprocity Theorem, proved by Artin in 1927, provides a converse to Takagi's Existence Theorem, allowing for a more precise statement of the Existence Theorem to be used today and in this dissertation. The reason to introduce these two theorems in a reversed chronological order is because we would like to emphasise the fact that the kernel of the Artin map might not be a congruence group.

The deep connection between the Existence Theorem and the Artin Reciprocity Theorem provide complimentary perspectives on the structure of abelian extensions of number fields, which is why they are the most fundamental results in class field theory. Together, they give the main theorem in class field theory.

Theorem 4.19 (The classification theorem)**.** *Let K be any alegbraic number field, the correspondence $L_{\mathbf{H}} \to \mathbf{H}$ is a one-to-one, inclusion reversing, correspondence between finite dimensional, abelian extensions and ideal groups of K.*

Proof. Refer to Chapter V.9, page 215 of [9]. □

Figure 5: Correspondence between congruence subgroups and class fields $L_{\mathbf{H}}$.

4.4 Constructive Euclidean proof for the Gaussian rationals

Using the theory we have developed, we can now assure that with respect to the modulus $\mathfrak{m} = 2(1+i)\beta$, where β is an odd Gaussian integer, we can surely find a corresponding abelian Galois extension $L/\mathbb{Q}(i)$ with the Galois group being isomorphic to the multiplicative group of residue classes modulo β, $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$. Using Theorem 4.19, we can choose L to be the ray class field of $\mathbb{Q}(i)$ for the modulus $\mathfrak{m} = 2(1+i)\beta$, β odd, which must exist by Existence Theorem. By construction, we have $\mathrm{Ker}(\Phi^{\mathfrak{m}}_{L/\mathbb{Q}(i)}) = P^{\mathfrak{m}}_{\mathbb{Q}(i)}$, which is clearly a congruence subgroup. It then follows from the Artin Reciprocity Theorem that we have the isomorphism $\chi : I^{\mathfrak{m}}_{\mathbb{Q}(i)}/P^{\mathfrak{m}}_{\mathbb{Q}(i)} \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q}(i))$, induced by the Artin map $\Phi^{\mathfrak{m}}_{L/\mathbb{Q}(i)}$.

We do not know what the ray class field L actually looks like, so we are unable to define the isomorphism explicitly (this will require the material from the next section). However, Theorem 4.9 and Proposition 4.11 tell us that with respect to the same modulus $\mathfrak{m}$, we have the isomorphism

$$\rho : I^{\mathfrak{m}}_{\mathbb{Q}(i)}/P^{\mathfrak{m}}_{\mathbb{Q}(i)} \xrightarrow{\sim} (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times,\ \frac{a}{b}\mathbb{Z}[i] \mapsto [a][b]^{-1}.$$

Therefore, the two isomorphisms above allow us to identify $\mathrm{Gal}(L/\mathbb{Q}(i))$ with $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$ by $\rho \circ \chi^{-1} : \mathrm{Gal}(L/\mathbb{Q}(i)) \xrightarrow{\sim} (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$. In such a way, we can describe the Artin map for $K = \mathbb{Q}(i)$ as follows:

$$\Phi^{\mathfrak{m}}_{L/\mathbb{Q}(i)} : I^{\mathfrak{m}}_{\mathbb{Q}(i)} \to (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times,\ \Phi^{\mathfrak{m}}_{L/\mathbb{Q}(i)}\left(\frac{a}{b}\mathbb{Z}[i]\right) = [a][b]^{-1}.$$

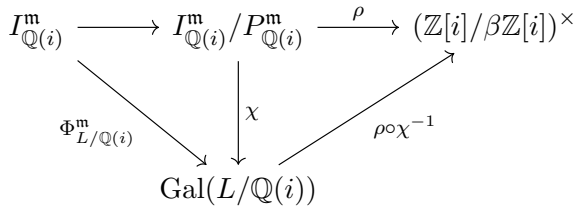

Figure 6: Illustration of identifying $\mathrm{Gal}(L/\mathbb{Q}(i))$ with $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$.

Gathering all the ingredients, we can now mimic the constructive Euclidean proof for Theorem 2.7 and write one for the Gaussian integers.

With respect to the modulus $\mathfrak{m} = 2(1+i)\beta$ where β is an odd Gaussian integer, the Artin map tells us that $\mathrm{Gal}(L/\mathbb{Q}(i))$ is isomorphic to $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$. By the Primitive Element Theorem, there exists an algebraic integer η such that $L = \mathbb{Q}(i)(\eta)$ is the ray class field of $\mathbb{Q}(i)$.

Theorem 4.20. *For any odd Gaussian integer β, let H be a subgroup of $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$, $\mathbb{Q}(i,\theta)$ be the fixed field of H in $\mathbb{Q}(i)(\eta)$. Then there is an irreducible polynomial f in $\mathbb{Q}(i)[x]$ such that if $\mathfrak{p}$ is a prime divisor of f, then either $\mathfrak{p}$ is a factor of β or $\mathfrak{p}$ modulo β belongs to H.*

Proof. Let $a_1, ..., a_n$ be the coset representatives of H in $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$ (so $n = [(\mathbb{Z}/\beta\mathbb{Z})^\times : H]$) and set $\theta_i = h(\eta_{a_i})$, where η_{a_i} is the image of η under the automorphism $\sigma_{a_i} \in \mathrm{Gal}(L/\mathbb{Q}(i))$. By the exact same argument in Lemma 2.5, $\theta_i = h(\eta_{a_i})$ are the distinct conjugates of θ. Define

$$f(x) := \prod_{j=1}^{n}(x - \theta_j).$$

Similar to the argument in Lemma 2.5, since the Galois group acts on the roots of f transitively and its coefficients as the identity, the polynomial f is irreducible over $\mathbb{Z}[i]$ as we want. Let $\mathfrak{p} \in P(f)$, which we know is non-empty by Theorem 2.4, such that $\mathfrak{p} \nmid \mathrm{disc}(f)$, then by Theorem 2.4, there exists $a \in \mathcal{O}_{\mathbb{Q}(i)}$ such that $\mathfrak{p}$ divides $f(a)$.

Now let $\mathfrak{q}$ be any prime ideal dividing $\mathfrak{p}$, then $\mathfrak{q} \mid \mathfrak{p} \mid f(a)$ for some Gaussian integer a. Since $\mathfrak{q}$ is a prime ideal in $\mathcal{O}_{\mathbb{Q}(i)}$, there exists j such that $\mathfrak{q} \mid (a - \theta_j) \implies a \equiv \theta_j \bmod \mathfrak{q}$.

From Proposition 3.7, the definition of the unique Frobenius element gives us $\mathrm{Frob}_{\mathfrak{p}}(\theta_j) \equiv \theta_j^{\#\mathbb{F}_{\mathfrak{p}}} \bmod \mathfrak{q}$. By transitivity of the Galois group, $\mathrm{Frob}_{\mathfrak{p}}$ must map θ_j to another coset representative; from the description of the Artin map, we also have $\mathrm{Frob}_{\mathfrak{p}}(\theta_j) = \theta_{j'}$ for some $1 \le j \le n$. Together, we have

$$\theta_{j'} \equiv \theta_j^{\#\mathbb{F}_{\mathfrak{p}}} \bmod \mathfrak{q}$$

With respect to the finite field $\mathbb{F}_{\mathfrak{p}}$, we apply the Frobenius automorphism to a, yielding $a \equiv a^{\#\mathbb{F}_{\mathfrak{p}}} \bmod \mathfrak{p} \implies a \equiv a^{\#\mathbb{F}_{\mathfrak{p}}} \bmod \mathfrak{q}$. Therefore, we have a set of congrueunces as

previously:

$$\theta_j \equiv a \equiv a^{\#\mathbb{F}_\mathfrak{p}} \equiv \theta_j^{\#\mathbb{F}_\mathfrak{p}} \equiv \theta_{j'} \bmod \mathfrak{q} \tag{4.1}$$

As argued in Theorem 2.7, the coset representatives θ_j and $\theta_{j'}$ must be the same. Equivalently, $\theta_j = \mathrm{Frob}_\mathfrak{p}(\theta_j)$, so $\mathrm{Frob}_\mathfrak{p}$ fixes the fixed field $\mathbb{Q}(i, \theta)$ and we deduce that $\mathfrak{p}$ modulo $\mathfrak{m}$ belongs to H. □

Corollary 4.21. *There exist infinitely many Gaussian primes satisfying* $\mathfrak{p} \equiv 1 \bmod \beta$.

Proof. Set $H = \{1\}$, then the fixed field is the ray class field $L = \mathbb{Q}(i, \eta)$ itself, so $\theta = \eta$ in Theorem 4.20 and we take f to be the minimal polynomial of η over the Gaussian rationals $\mathbb{Q}(i)$. The odd Gaussian integer β has a finite set of prime divisiors, so the set of primes $P(f)$ excluding all factors of $\mathfrak{m}$ is infinite and it consists of primes $\mathfrak{p} \equiv 1 \bmod \beta$ only. □

Thus far, it may have become apparent to readers that the constructive Euclidean proof relied solely on the connection between primes and Frobenius elements. This suggests that the constructive Euclidean proof can be extended to number fields with abelian Galois extensions more generally, by focusing on Frobenius elements instead of primes. The relevant statements will be presented in the following sections, and readers are encouraged to consult the article by Murty and Thain [11, page 8–10] for a more detailed treatment of the topic.

Theorem 4.22. *Let L, K be algebraic number fields, where L/K is abelian with Galois group* $\mathrm{Gal}(L/K)$. *Suppose $L = K(\alpha)$ and let H be a subgroup of* $\mathrm{Gal}(L/K)$, *then there exists an irreducible polynomial $f \in \mathcal{O}_K[x]$ such that all the prime divisors $\mathfrak{p}$ of f, with finitely many exceptions, have* $\mathrm{Frob}_\mathfrak{q} \in H$ *for all primes $\mathfrak{q}$ lying over $\mathfrak{p}$.*

Corollary 4.23. *If f is the minimal polynomial of α, then the prime divisors of f either divide the discriminant or have* $\mathrm{Frob}_\mathfrak{q} = id$.

Therefore, we can conclude that for the Gaussian integers, a polynomial proof for the arithmetic progression $1 \bmod n$ exists if n is a Gaussian integer coprime with $1+i$, showing that our guess in the beginning to be partially correct. This is surprising because simply judging from the Eucldiean proofs in integers, they do not hint any connection between the infinitude of primes and prime ramification.

5 The lemniscatic extension

5.1 Abelian extension of imaginary quadratic fields

Now we would like to write down explicitly the polynomial suggested by the constructive Euclidean proof in Corollary 4.21, which will require us to compute an explicit field extension of the Gaussian rationals. Recall that the Kronecker-Weber Theorem says that every finite abelian extension of the rationals lies in a cyclotomic field $\mathbb{Q}(\zeta_m)$ for some natural

number m. In other words, adjoining the m-th root of unity, which are the *m-division points* of the unit circle, to the rationals generates abelian extensions of the rationals. It turns out that something similar happens for imaginary quadratic fields:

Definition 5.1 (Group of $\mathfrak{c}$-torsion points)**.** *Let K be a number field, $\mathfrak{c}$ be an ideal in $\mathcal{O}_K$. For an elliptic curve E with complex multiplication by $\mathcal{O}_K$, we define the group of $\mathfrak{c}$-torsion points of E to be*

$$E[\mathfrak{c}] = \{P \in E : [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{c}\}.$$

Theorem 5.2. *Let K be a quadratic imaginary field, E be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and $h : E \to \mathbb{P}^1$ be a Weber function for the curve E defined over H, the Hilbert class field of K. Let $\mathfrak{c}$ be an integral ideal of $\mathcal{O}_K$, the the field $K\left(j(E), h(E[\mathfrak{c}])\right)$ is the ray class field of K modulo $\mathfrak{c}$.*

We have not defined what a Weber function is, but to put it in simple terms, it is a function that gives the x-coordinates of the torsion points of E/H. One way to define it is as follows: Take the Weierstrass equation for E/H of the form $y^2 = x^3 + Ax + B$ with $A, B \in H$, then the following is a Weber function for E/H:

$$h(P) = h(x, y) = \begin{cases} x, & \text{if } AB \neq 0, \\ x^2, & \text{if } B = 0, \\ x^3, & \text{if } A = 0. \end{cases}$$

Examining the cyclotomic extension again, one can consider the map $\mathbb{C}^* \to \mathbb{C}^*$, defined by $z \mapsto z^m$, then the kernel is precisely the group of m-th roots of unity. In other words, they are the group of 'm-torsion points' of $\mathbb{C}^*$. Therefore, the theorem above is an analogous result of the Kronecker-Weber Theorem and did not come out of nowhere. One can refer to Chapter II, §5 of [12] for more details and the proof of Theorem 5.2.

In our case, the set of Gaussian rationals $\mathbb{Q}(i)$ is an imaginary quadratic field, in fact it is also its own Hilbert class field since $\mathbb{Q}(i)$ has class number 1. Therefore, this theorem tells us that we should look for an elliptic curve defined over $\mathbb{Q}(i)$. Surprisingly, the associated elliptic curve is induced by considering the division points of an algebraic curve called the *lemniscate (of Bernoulli)*, similar to how we considered the division points of the unit circle. This was first investigated by the mathematician Niels Henrik Abel (1802–29), where he showed the n-division points of the lemniscate can be constructed using straightedge and compass. Following the work of David A. Cox [5, Chapter 15], we will try to find the field extension for the Gaussian rationals, and hence find the desired polynomial.

5.2 The lemniscate and lemniscatic function

Definition 5.3 (Lemniscate)**.** *The lemniscate, or the lemniscate of Bernoulli, is the plane curve defined by the equation* $(x^2 + y^2)^2 = x^2 - y^2$*, or the polar equation* $r^2 = \cos(2\theta)$*.*

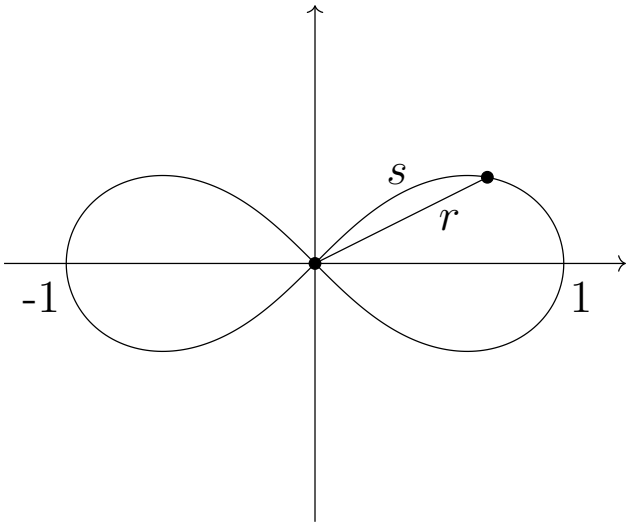

Figure 7: The lemniscate of Bernoulli, defined by $r^2 = \cos 2\theta$.

Unlike circles, the division points of the lemniscate are defined in terms of arc length, so we need to find a formula for the arc length of the lemniscate. Since the lemniscate is symmetric in the x-axis and y-axis, we can consider the first quadrant only. Using the polar equation, we have $\theta = \frac{1}{2}\cos^{-1}(r^2)$. Then by the arc length formula (with respect to polar coordinates), we have

$$\text{arc length } = s = \int_0^r \frac{1}{\sqrt{1-t^4}}dt, \tag{5.1}$$

where s is the arc length along the lemniscate from the origin to the point in the first quadrant. This integral is improper when $r = 1$, but since it converges, $\int_0^1 \frac{1}{\sqrt{1-t^4}}dt$ is the arc length of the lemniscate in the first quadrant.

Definition 5.4 (Lemniscate constant)**.** *The lemniscate constant,* ϖ*, is the ratio of the perimeter of the lemniscate to its diameter, defined to be*

$$\varpi := 2\int_0^1 \frac{1}{\sqrt{1-t^4}}.$$

Now it follows that the arc length of the lemniscate is 2ϖ and the distance between consecutive n-division points is $\frac{2\varpi}{n}$. By definition, s is an increasing function in r defined on a closed interval, so the inverse function exists, written as

$$r = \varphi(s), 0 \le s \le \frac{\varpi}{2} \iff s = \int_0^r \frac{1}{\sqrt{1-t^t}}dt.$$

This function is now only defined on the first quadrant, but it is not hard to extend the notion of arc length parameterisation. We follow the notion of [5, page 465–466].

Definition 5.5. *The arc length paramterisation of the lemniscate is defined by sending a real number s to a point P on the lemniscate such that*

- *If $s = 0$, then P is the origin.*
- *If $s > 0$, then move from the origin into the first quadrant portion of the lemniscate and continue along the curve until we reach the point P whose cumulative arc length from the origin is s.*
- *If $s < 0$, then move from the origin into the third quadrant portion and continue until we reach the point P whose cumulative arc length from the origin is $-s$.*

We call s the signed arc length variable of the lemniscate.

The polar distance paramterisation of the lemniscate is defined by sending $r \in [-1, 1]$ to a point P on the lemniscate such that

- *If $0 \leq r \leq 1$, then P is on the right half of the lemniscate;*
- *If $-1 \leq r \leq 0$, then P is on the left half of the lemniscate.*

We call r the signed polar distance of the corresponding point on the lemniscate.

In such way, we can now see that the signed arc length s satisfies (5.1) for $-\frac{\varpi}{2} \leq s \leq \frac{\varpi}{2}$ and $-1 \leq r \leq 1$. We call the resulting function $\varphi(s)$ the *lemniscatic function*. It is obvious that when $|s|$ is large, it is just looping around the lemniscate. Similar to measuring angles on the unit circle, we also have $\varphi(s) = \varphi(s + 2\varpi)$. Therefore, not only now we have extended φ to all of $\mathbb{R}$, but we have also shown that $\psi(s)$ is a function of period 2ϖ. In particular, one can also deduce the identities

$$\varphi(-s) = -\varphi(s), \quad \varphi(\varpi - s) = \varphi(s), \tag{5.2}$$

where the first follows from the symmetry in y-axis, and the second follows from the symmetry in the x-axis, according to how we define the arc length above. Other identities are listed below.

Proposition 5.6. *For $x, y \in \mathbb{R}$, the lemniscatic function satisfies*

- $\varphi'(x) = \sqrt{1 - \varphi^4(x)}$,
- $\varphi(x \pm y) = \frac{\varphi(x)\varphi'(y) \pm \varphi(y)\varphi'(y)}{1+\varphi^2(x)\varphi^2(y)}$ *(this is called the addition law).*

Proof. Refer to Chapter 15.2, page 467 of [5]. □

Theorem 5.7 (Multiplication by integers)**.** *Given an integer $n > 0$, there are relatively prime polynomals $P_n(x), Q_n(x) \in \mathbb{Z}[x]$ such that if n is odd, then*

$$\varphi(nx) = \varphi(x)\frac{P_n(\varphi^4(x))}{Q_n(\varphi^4(x))},$$

and if n is even, then

$$\varphi(nx) = \varphi(x)\frac{P_n\varphi^4(x))}{Q_n(\varphi^4(x))}\varphi'(x).$$

Furthermore, $Q_n(0) = 1$.

Proof. Refer to Chapter 15.2, page 470–471 of [5]. □

Recall that the primary motivation for defining the lemniscatic function is to study the n-division points of the lemniscate, and the theorem above is the key to it. By construction, the polar distances of the n-division points are $\varphi\left(m\frac{2\overline{\omega}}{n}\right)$ for $m = 0, 1, ..., n-1$. When n is odd,

$$0 = \varphi(m \cdot 2\overline{\omega}) = \varphi\left(n \cdot m\frac{2\overline{\omega}}{n}\right) = \varphi(m\frac{2\overline{\omega}}{n})\frac{P_n(\varphi^4(m\frac{2\overline{\omega}}{n}))}{Q_n(\varphi^4(m\frac{2\overline{\omega}}{n}))}$$

where we have used the periodicity of the lemniscatic function in the first equality. Therefore, the polar distance $\varphi\left(m\frac{2\overline{\omega}}{n}\right)$ is a root of the polynomial $xP_n(x^4) \in \mathbb{Z}[x]$ when n is odd.

Corollary 5.8. *Let n be an odd integer and define $xP_n(x^4) \in \mathbb{Z}[x]$ to be the n-division polynomial. Then the polar distances of the n-divison points of the lemniscate are roots of the n-division polynomial.*

5.3 The complex lemniscatic function

To describe the roots of the n-division polynomial in a nice way, Abel wanted to represent all roots of the polynomial using the lemiscatic function φ. However, most of the roots are complex numbers and a 'complex polar distance' does not make sense at all. Therefore, one approach is to extend φ to a function defined on the complex plane $\mathbb{C}$. This can be achieved by using change of variable $t = iu$ in (5.1), which shows that

$$\int_0^{ir} \frac{1}{\sqrt{1-t^4}}dt = i\int_0^r \frac{1}{\sqrt{1-u^4}}du = iy, \text{ where } r = \varphi(y)$$

Therefore, for a real number y, we can define $\varphi(iy)$ to be $\varphi(iy) = ir = i\varphi(y)$. Using the addition law and the fact that $\varphi'(iy) = \varphi'(y)$, we can define φ over $\mathbb{C}$.

Definition 5.9. *For $z = x + iy \in \mathbb{C}$, the complex lemniscatic function is defined to be*

$$\varphi(z) = \varphi(x + iy) = \frac{\varphi(x)\varphi'(y) + i\varphi(y)\varphi'(x)}{1 - \varphi^2(x)\varphi^2(y)}.$$

Proposition 5.10. *The function $\varphi(z)$ satisfies the following properties:*

1. *For $z \in \mathbb{C}$ and $m, n \in \mathbb{Z}$, we have*

$$\varphi(z + (m + in)\overline{\omega}) = (-1)^{m+n}\varphi(z).$$

2. *The addition law*

$$\varphi(z + w) = \frac{\varphi(z)\varphi'(w) + \varphi(w)\varphi'(z)}{1 - \varphi^2(z)\varphi^2(w)}.$$

   holds for all $z, w \in \mathbb{C}$ such that both sides are defined.

3. *$\varphi(z)$ is analytic for all $z \neq (m + in)\frac{\overline{\omega}}{2}$, where m, n are odd integers. In particular:*

   - *For $m, n \in \mathbb{Z}$, $\varphi(z)$ has simple zeros at $z = (m + in)\overline{\omega}$.*
   - *For m, n odd integers, $\varphi(z)$ has simple poles at $z = (m + in)\frac{\overline{\omega}}{2}$.*

4. *Fix a complex number w_0. Then the equation $\varphi(z) = w_0$ has a solution $z_0 \in \mathbb{C}$. Furthermore, if z_0 is one solution, then all solutions are given by*

$$z = (-1)^{m+n}z_0 + (m + in)\overline{\omega}, m, n \in \mathbb{Z}.$$

Proof. Refer to Chapter 15.3, page 477–481 of [5]. □

This is a series of remarkable properties, particularly the first one since it tells us that $\varphi(z)$ is doubly periodic: $\varphi(z) = \varphi(z + (1 + i)\overline{\omega}) = \varphi(z + (1 - i)\overline{\omega})$, in which the periods $(1 + i)\overline{\omega}, (1 - i)\overline{\omega}$ are clearly linearly independent over $\mathbb{R}$.

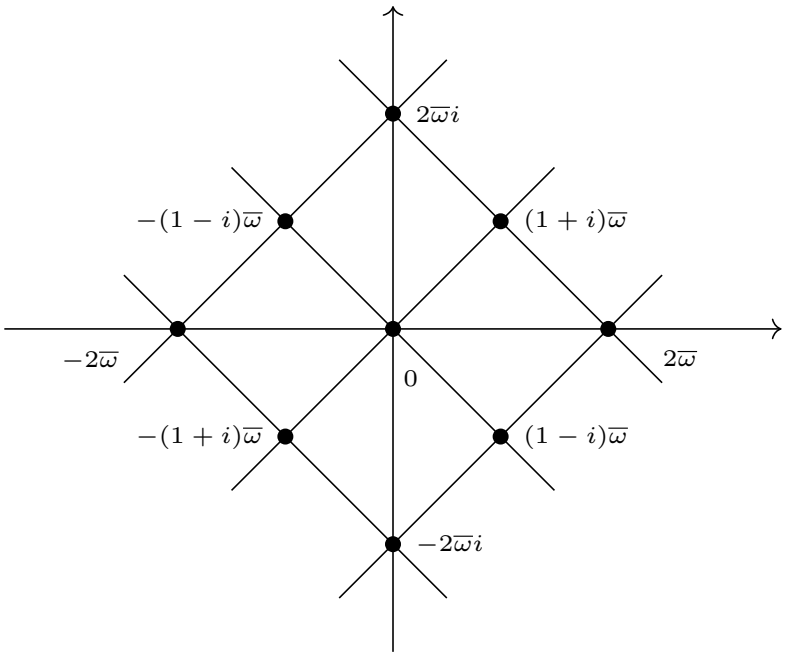

Figure 8: Period lattice of $\varphi(z)$.

Remark 5.11. *One should notice that the identity (5.2) follows from $\varphi(iz) = i\varphi(z)$ by taking $(m, n) = (1, 0)$ in (1) in the proposition above. Therefore, the complex lemniscate function agrees with itself over the reals.*

While (3) of Proposition 5.10 tells us that $\varphi(z)$ is a meromorphic function on $\mathbb{C}$. All together, $\varphi(z)$ is an elliptic function on $\mathbb{C}$ for the lattice $\Lambda = \mathbb{Z}(1+i)\overline{\omega} + \mathbb{Z}(1-i)\overline{\omega}$, producing the elliptic curve $E = \mathbb{C}/\Lambda$.

Proposition 5.12. *The Weierstrass equation of E is $y^2 = 4x^3 + x$ and E has complex multiplication by $\mathbb{Z}[i]$.*

Proof. Refer to page 47 of [7]. □

In particular, the second property allows us to generalise the notion of multiplication by integers in Theorem 5.7 to Gaussian integers for the $\varphi(z)$.

Theorem 5.13 (Multiplication by Gaussian integers)**.** *Let β be an odd Gaussian integer, $d = \frac{1}{4}(\mathrm{Nm}(\beta) - 1)$, where $\mathrm{Nm}(\beta)$ is the norm of β. Then there exists relatively prime polynomals $P_n(x), Q_n(x)$ in the polynomial ring $\mathbb{Z}[i][x]$ and $\varepsilon \in \{0, 1, 2, 3\}$ such that:*

1. *For all $z \in \mathbb{C}$, we have*
$$\varphi(\beta z) = i^{\varepsilon}\varphi(z)\frac{P_\beta(\varphi^4(z))}{Q_\beta(\varphi^4(z))}.$$
2. *$P_\beta(x)$ and $Q_\beta(x)$ have degree d.*
3. *The roots of the β-**division polynomial** $xP_\beta(x^4)$ are the complex numbers $\varphi(\alpha\frac{\overline{\omega}}{\beta})$ for odd Gaussian integers α.*
4. *$P_\beta(x)$ is monic, $Q_\beta(0) = 1$ and $Q_\beta(x) = x^d P_\beta\left(\frac{1}{x}\right)$.*
5. *Suppose $\beta = \pi$ is an odd Gaussian prime, then*
$$P_\pi(x) = x^d + x_1 x^{d-1} + ... + a_d,$$
such that each a_j is divisible by π and $a_d = i^{-\varepsilon}\pi$. Furthermore, $P_\pi(x^4)$ is irreducible.

Proof. Refer to Chapter 15.4, page 486–495 of [5]. □

Readers might find other sources saying the roots of the β-division polynomial $xP_\beta(x^4)$ are of the form $\varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right)$ for odd α, particularly in [7]. This is just another way of writing (3) in Theorem 5.13: using the identities in (5.2), we have

$$\varphi\left(\frac{2\overline{\omega}}{\beta}\right) = \varphi\left(\overline{\omega} - \frac{2\overline{\omega}}{\beta}\right) = \varphi\left((\beta - 2)\frac{\overline{\omega}}{\beta}\right).$$

Since β is an odd Gaussian integer, $\beta - 2$ is odd as well and we are back to (3) in Theorem 5.13. In particular, one may also replace 2 with any other even Gaussian integer in the argument above. Alternatively, one may also argue that since $\varphi(2\overline{\omega}) = 0$, $\varphi\left(\frac{2\overline{\omega}}{\beta}\right)$ must be a root of the β-division polynomial (simply substitute $z = \frac{2\overline{\omega}}{\beta}$ in the first result of Theorem 5.13). In order to align with Abel's original motive, we will write the roots of $xP_\beta(x)$ as $\varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right)$ for odd α from now onwards.

5.4 Computation of the field extension

With all the theory of the lemniscate (function), we can finally show that the field $K_\beta = \mathbb{Q}\left(i, \varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right)$ is the ray class field of the modulus $\mathfrak{m} = 2(1+i)\beta$ we have chosen in §4.

Theorem 5.14. *Let $\beta \in \mathbb{Z}[i]$ be odd and consider $K_\beta = \mathbb{Q}\left(i, \varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right)$. Then $K_\beta/\mathbb{Q}(i)$ is an abelian Galois extension.*

Proof. We will follow [5, page 499]. In Theorem 5.13, we were told that the roots of $xP_\beta(x^4)$ are of the form $\varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right)$ for odd α. We claim the associated $\alpha \in \mathbb{Z}[i]$ is unique modulo $\beta \in \mathbb{Z}[i]$:

Suppose $\varphi(\alpha\frac{2\overline{\omega}}{\beta}) = \varphi(\widetilde{\alpha}\frac{2\overline{\omega}}{\beta})$ for some odd Gaussian integers $\alpha, \widetilde{\alpha}$, then both $\alpha\frac{2\overline{\omega}}{\beta}$ and $\widetilde{\alpha}\frac{2\overline{\omega}}{\beta}$ are solutions to the equation $\varphi(z) = w_0, w_0 \in \mathbb{C}$. Using property 4 in Proposition 5.10, there exists $(a+ib) \in \mathbb{Z}[i]$ such that

$$\widetilde{\alpha}\frac{2\overline{\omega}}{\beta} = (-1)^{a+b}\alpha\frac{2\overline{\omega}}{\beta} + (a+ib)\overline{\omega}.$$

Simplifying gives

$$\widetilde{\alpha} = (-1)^{a+b}\alpha + (a+ib)\beta.$$

Since $\alpha, \widetilde{\alpha}, \beta$ are all odd Gaussian integers and sum of two odd Gaussian integers is even, $(a+ib)$ is even so $(-1)^{a+b} = 1$ by Proposition 4.11 and hence

$$\widetilde{\alpha} = \alpha + (a+ib)\beta.$$

This shows that $\widetilde{\alpha}$ and α belong to the same coset, proving uniqueness.

Since α is odd, Theorem 5.13 shows that $\varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right)$ is a rational function in $\varphi\left(2\frac{\overline{\omega}}{\beta}\right)$ with coefficients in $\mathbb{Q}(i)$. Together with the uniqueness of α it follows that the β-division polynomial $xP_\beta(x^4)$ splits completely in K_β. Clearly one of the roots is $\varphi\left(\frac{2\overline{\omega}}{\beta}\right)$, so K_β is the splitting field of $xP_\beta(x^4)$ over $\mathbb{Q}(i)$ and $K_\beta/\mathbb{Q}(i)$ is a Galois extension. □

Remark 5.15. *This proofs tells us that we can rewrite (3) in Theorem 5.13 as follows: the β-division polynomial $xP_\beta(x^4)$ has $\mathrm{Nm}(\beta)$ distinct roots given by $\varphi(\alpha\frac{2\overline{\omega}}{\beta})$ for $\alpha \in \mathbb{Z}[i]/\beta\mathbb{Z}[i]$.*

The next lemma will help us in the main proof to be presented.

Lemma 5.16. *Let β be odd, then the fields $K_\beta = \mathbb{Q}\left(i, \varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right)$ and $\mathbb{Q}\left(i, \varphi\left(\frac{(1+i)\overline{\omega}}{\beta}\right)\right)$ are equivalent.*

Proof. We shall use a trick similar to that of page 47 of [7]. Since β is odd, by Bézout's lemma we know there exists Gaussian integers u, v such that $u\beta + v(1-i) = 1$. Multiply both sides by $\frac{(1+i)\overline{\omega}}{\beta}$ gives

$$u(1+i)\overline{\omega} + v\frac{2\overline{\omega}}{\beta} = \frac{(1+i)\overline{\omega}}{\beta}$$

Recall φ is doubly periodic with respect to the lattice Λ (Proposition 5.10), so we obtain

$$\varphi\left(v\frac{2\overline{\omega}}{\beta}\right) = \varphi\left(\frac{(1+i)\overline{\omega}}{\beta} + (-u-ui)\overline{\omega}\right) = \varphi\left(\frac{(1+i)\overline{\omega}}{\beta}\right).$$

Theorem 5.13 tells us that $\varphi\left(v\frac{2\overline{\omega}}{\beta}\right) = \varphi\left(\frac{(1+i)\overline{\omega}}{\beta}\right)$ is a rational function in $\varphi\left(\frac{2\overline{\omega}}{\beta}\right)$, showing that $\mathbb{Q}\left(i, \varphi\left(\frac{(1+i)\overline{\omega}}{\beta}\right)\right) \subseteq K_\beta$.

Conversely, using the addition law from Proposition 5.10 together with $\varphi'(iz) = \varphi'(z)$ and $\varphi(iz) = i\varphi(z)$,

$$\varphi((1-i)z) = \varphi(z - iz) = \frac{\varphi(z)\varphi'(-iz) + \varphi(-iz)\varphi'(z)}{1 - \varphi^2(z)\varphi^2(-iz)} = \frac{(1-i)\varphi(z)\varphi'(z)}{1-\varphi^4(z)}.$$

Substituting $z = \frac{(1+i)\overline{\omega}}{\beta}$ then shows that $\varphi\left(\frac{2\overline{\omega}}{\beta}\right)$ is a rational function in $\varphi\left(\frac{(1+i)\overline{\omega}}{\beta}\right)$, proving the other inclusion. □

Proposition 5.17. *Let $\beta \in \mathbb{Z}[i]$ be odd. For any $\sigma_\alpha \in \mathrm{Gal}(K_\beta/\mathbb{Q}(i))$, there is a unique $[\alpha] \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$ such that $\sigma_\alpha(\varphi\left(\frac{2\overline{\omega}}{\beta}\right)) = \varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right)$. Furthermore, the map $\sigma_\alpha \mapsto [\alpha]$ defines an isomorphism*

$$\mathrm{Gal}(K_\beta/\mathbb{Q}(i)) \cong (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times.$$

Proof. The first part of the proof follows from Chapter 15.5, page 499 of [5]. It is a standard fact that the Galois group of an irreducible polynomial permutes its roots transitively. Therefore, for $\sigma_\alpha \in \mathrm{Gal}(K_\beta/\mathbb{Q}(i))$, there exists an odd Gaussian integer α, unique modulo β, such that

$$\sigma_\alpha\left(\varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right) = \varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right).$$

Now consider the map $\mathrm{Gal}(K_\beta/\mathbb{Q}(i)) \hookrightarrow (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$, defined by $\sigma_\alpha \mapsto [\alpha]$.

Well-defined.
Since $\mathbb{Z}[i]$ is a principal domain, $[\alpha] \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$ if and only if α, β are coprime. Let m

be the order of σ_α in $\mathrm{Gal}(K_\beta/\mathbb{Q}(i))$, then

$$\varphi\left(\frac{2\overline{\omega}}{\beta}\right) = \sigma_\alpha^m\left(\varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right) = \varphi\left(\alpha^m\frac{2\overline{\omega}}{\beta}\right),$$

where the last equality follows from repeatedly applying σ_α to (1) of Theorem 5.13 with $z = \frac{\overline{\omega}}{\beta}$. By uniquess of α, we conclude that $\alpha^m \equiv 1 \bmod \beta$.

Group homomorphism.
Let $\alpha, \gamma \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$. Then

$$\sigma_\alpha\sigma_\gamma\left(\varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right) = \sigma_\alpha\left(\varphi\left(\gamma\frac{2\overline{\omega}}{\beta}\right)\right) = \varphi\left(\alpha\gamma\frac{2\overline{\omega}}{\beta}\right) = \sigma_{\alpha\gamma}\left(\varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right).$$

Injection.
Suppose $\sigma_\alpha\left(\varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right) = \sigma_\gamma\left(\varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right)$, then we have $\varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right) = \varphi\left(\gamma\frac{2\overline{\omega}}{\beta}\right)$ with which we have shown that α, γ must belong to the same coset in $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$ as in Theorem 5.14.

Surjection.
There is a proof that fully utilises class field theory, but with lots of tedious calculations. Therefore, we will only outline the main procedures, for details one may refer to [7, page 48–49].

Apply Theorem 5.2 to the elliptic curve $E/\mathbb{Q}(i)$ in Proposition 5.12 and choose our modulus to be $\mathfrak{m} = 2(1+i)\beta$, this tells us that the ray class field of $\mathbb{Q}(i)$ for the modulus $\mathfrak{m} = 2(1+i)\beta$ is $L = \mathbb{Q}\left(i, \wp\left(\frac{\overline{\omega}}{2\beta}\right)^2\right)$ (this is based on another way of analytically defining a Weber function, see [12, page 135]). Using the results in Section 4, we know

$$L = \mathbb{Q}\left(i, \wp\left(\frac{\overline{\omega}}{2\beta}\right)^2\right) \cong (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times.$$

According to Cox, φ satisfies

$$\varphi(z) = -2\frac{\wp(z)}{\wp'(z)}, \quad \varphi'(z) = \frac{4\wp(z)^2 - 1}{4\wp(z)^2 + 1}.$$

These identities can be used to replace the Weierstrass $\wp$-function with Abel's lemniscate function in the expression of L, giving

$$L = \mathbb{Q}\left(i, \varphi'\left(\frac{\overline{\omega}}{2\beta}\right)\right).$$

If we differentiate the addition law in Proposition 5.10 for $\varphi\left(z - \frac{\overline{\omega}}{2}\right)$, we get

$$\varphi'\left(z - \frac{\overline{\omega}}{2}\right) = 2\frac{\varphi(z)}{1 + \varphi(z)^2}. \tag{5.3}$$

Using Proposition 4.11, there exists $v \in \mathbb{Z}[i]$ such that $2(1+i)v - \beta = i^\varepsilon$. Multiply both sides by $\frac{\overline{\omega}}{2\beta}$ to give $\frac{(1+i)\overline{\omega}}{\beta}v - \frac{\overline{\omega}}{2} = \frac{\overline{\omega}}{2\beta}i^\varepsilon$. Together with $\varphi'(iz) = \varphi'(z)$ (which is how we defined φ over $\mathbb{C}$) and the fact that $K_\beta = \mathbb{Q}\left(i, \varphi\left(\frac{(1+i)\overline{\omega}}{\beta}\right)\right)$ as proved in Lemma 5.16, we obtain

$$\begin{aligned}\varphi'\left(\frac{\overline{\omega}}{2\beta}\right) &= \varphi'\left(i^\varepsilon \frac{\overline{\omega}}{2\beta}\right) \\ &= \varphi'\left(\frac{(1+i)\overline{\omega}}{\beta}v - \frac{\overline{\omega}}{2}\right) \\ &= 2\frac{\varphi(\frac{(1+i)\overline{\omega}}{\beta}v)}{1+\varphi(\frac{(1+i)\overline{\omega}}{\beta}v)^2}\end{aligned}$$

by the identity given in (5.3)

$$\begin{aligned}&\in \mathbb{Q}\left(i, \varphi\left(\frac{(1+i)\overline{\omega}}{\beta}\right)\right) \\ &= K_\beta.\end{aligned}$$

Hence, $\mathbb{Q}(i) \subseteq L \subseteq K_\beta$ and $|\operatorname{Gal}(K_\beta/\mathbb{Q}(i))| \geq |\operatorname{Gal}(L/\mathbb{Q}(i))| = |(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times|$. Since we have shown the injection $\operatorname{Gal}(K_\beta/\mathbb{Q}(i)) \hookrightarrow (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$, we must have $L = K_\beta$, proving the isomorphism. □

Hence, if we take $\left\{\varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right) : \alpha \in (\mathbb{Z}[i]/\mathbb{Z}[i])^\times\right\}$ to be the roots of a monic polynomial, then all the results we have developed in this section along with standard Galois theory results tell us that such a polynomial has to be irreducible over $\mathbb{Z}[i]$. We use the definition from [7, page 49].

Definition 5.18 (Lemnatomic polynomial)**.** *Let β be an odd Gaussian integer, we define the β-th lemnatomic polynomial to be the product*

$$\Lambda_\beta(x) \coloneqq \prod_{[\alpha]\in(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times} \left(x - \varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right)\right) \in \mathbb{Z}[i][x].$$

This is the minimal polynomial required in Corollary 4.21. In particular, it is monic of degree $|(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times|$ in particular. As we conclude this section, we would like to highlight a few properties of the lemnatomic polynomial. These properties are similar to those of cyclotomic polynomials, and may be useful in finding a Euclidean proof for the statement 'there are infinitely many Gaussian primes satisfying $\pi \equiv 1 \bmod \beta$ for odd β'.

Proposition 5.19. *Let $\beta \in \mathbb{Z}[i]$ be odd and $xP_\beta(x^4) \in \mathbb{Z}[i][x]$ be the β-division polynomial from Theorem 5.13, then the lemnatomic polynomial satisfies the following properties:*

1. *If β is a unit, then $\Lambda_\beta(x) = x$ (this follows from the definition immediately).*

2. *$xP_\beta(x^4) = \prod_{\gamma|\beta} \Lambda_\gamma(x)$, where the product is over all divisors γ of β and without loss of generality, we assume $\gamma \equiv 1 \bmod 2(1+i)$.*

3. *Suppose β is not a unit. If $\beta = u\pi^k$ where u is a unit, π is a Gaussian prime and $k \geq 1$, then $\Lambda_\beta(0) = \pi$. Otherwise, $\Lambda_\beta(0) = 1$.*

Proof. See page 50–51 in [7]. □

6 Conclusion

The objective of this dissertation was to determine whether it is true or not that for any Gaussian integer z, we can show the existence of infinitely many Gaussian primes π that satisfy $\pi \equiv 1 \bmod z$ using a Euclidean proof. It turns out that this guess is partially correct: such a proof does exist and we even managed to find the required polynomial explicitly, but it only works for odd Gaussian integers (i.e. coprime with $1+i$).

The investigation began by examining the polynomial proofs for Dirichlet's Theorem, in the hope of producing a similar constructive Euclidean proof for the Gaussian integers to show our guess in §1 to be correct. It was then observed that the proof relies heavily on the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, which associates rational primes $\mathfrak{p}$ that are *unramified* in $\mathbb{Q}(\zeta_m)$ to the Frobenius element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. This observation led to demonstrating the theory behind Frobenius elements, as presented in §3. The investigation then looked into possible structures of $\mathrm{Gal}(L/\mathbb{Q}(i))$ for some abelian extension $L/\mathbb{Q}(i)$. By utilising class field theory, it was shown that for an odd Gaussian integer β, choosing the modulus $\mathfrak{m} = 2(1+i)\beta$ guarantees the ray class field modulo $\mathfrak{m}$ to exist. In particular, $\mathrm{Gal}(\mathbb{Q}(i)(\mathfrak{m})/\mathbb{Q}(i)) \cong (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$, as given by the Artin map.

Whilst the results we have obtained above allow us to prove the existence of a Euclidean proof for Dirichlet's Theorem in the Gaussian integers, we decided to conclude the investigation by computing the polynomial explicitly, therefore finding the ray class field modulo $\mathfrak{m}$, $\mathbb{Q}(i)(\mathfrak{m})$, explicitly (note that here $\mathbb{Q}(i)(\mathfrak{m})$ does not mean adjoining $\mathfrak{m}$ to $\mathbb{Q}(i)$). It turns out that $\mathbb{Q}(i)(\mathfrak{m})/\mathbb{Q}(i)$ is called the lemniscatic extension, related to the division points on the lemniscate of Bernoulli, similar to how cyclotomic extensions are related to division points on the unit circle. By examining the properties of the complex lemniscatic function $\varphi(s)$ and using existing class field theory results, we have demonstrated that $\mathbb{Q}(i)(\mathfrak{m}) = \mathbb{Q}\left(i, \varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right)$ and deduced that the required polynomial is the β-th lemnatomic polynomial, defined by

$$\Lambda_\beta(x) = \prod_{[\alpha] \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times} \left(x - \varphi\left(\alpha\frac{2\overline{\omega}}{\beta}\right)\right).$$

The findings of this dissertation have connected different branches of number theory, namely Galois theory, class field theory, and the theory of elliptic curves. Yet, the starting point of this investigation was a specific case of a theorem in number theory that is typically considered elementary and within the reach of high school students, which is what makes the results of this dissertation surprising. In comparison with the usual analytic methods used to prove Dirichlet's Theorem, the algebraic approach in this dissertation has uncovered the underlying meaning or theories behind results that we might have taken for granted nowadays. The connections made between different areas of number theory in this dissertation could inspire new techniques and approaches that could be used to tackle related problems, where the analytic approaches might be too specific to the problem to achieve the same effect.

Readers might also recall that the primary motive of this investigation is to generalise 'elementary tricks' for Dirichlet's Theorem in other number fields. In Cox's work [5, page 49–54], an 'elementary' proof was provided to demonstrate that $\mathbb{Q}\left(i, \varphi\left(\frac{2\overline{\omega}}{\beta}\right)\right)$ is the ray class field modulo $\mathfrak{m} = 2(1+i)\beta$, where β is odd. To be precise, this was achieved by showing that the β-th lemnatomic polynomial is irreducible over the Gaussian rationals $\mathbb{Q}(i)$. However, we did not adopt this approach in our work as it requires prior knowledge of the existence of this polynomial, which is precisely what we were trying to prove. Additionally, this method relies on advanced results such as Theorem 5.13, and thus is ironically an 'elementary result' based on non-elementary results. Similarly, most results in this dissertation have gone beyond the scope of what might be considered elementary. Therefore, even if one can use the lemnatomic polynomial to give a Euclidean proof of the infinitude of Gaussian primes satisfying $\pi \equiv 1 \bmod z, \gcd(1+i, z) = 1$, we would hardly consider it elementary, or at least equivalently as difficult as the analytical approach.

In addition, there are still limitations that must be addressed. The focus has been on purely imaginary fields, specifically, imaginary quadratic fields in §5. As a result, the methods or tricks employed lack generalisability to most number fields. Furthermore, the heavy reliance on class field theory restricts the computation to abelian extensions only. It is worth noting that this limitation prompts the question of whether a constructive, non-elementary proof such as Theorem 4.20 exists for non-abelian extensions. Although the answer to this question is unknown, it is anticipated that solving such a problem would be extremely complex. In conclusion, this dissertation provides an introduction to problems associated with field extensions and class field theory, while also accomplishing the original objectives.

References

[1] Kumar, A. *Cyclotomic Polynomials, Primes Congruent to 1 mod n.* Massachusetts Institute of Technology: MIT OpenCouseWare, https://ocw.mit.edu/courses/18-781-theory-of-numbers-spring-2012/resources/mit18_781s12_lec12/. (2012).

[2] Childress, N. *Class field theory.* Springer. https://doi.org/10.1007/978-0-387-72490-4. (2009).

[3] Conrad, K. *Euclidean proofs of Dirichlet's Theorem.* https://kconrad.math.uconn.edu/blurbs/gradnumthy/dirichleteuclid.pdf. (2010).

[4] Conrad, K., Lemmermeyer, F., Roquette, P.J., & Serre J., *History of Class Field History.* https://kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf. (2009)

[5] Cox, D. A. *Galois theory.* John Wiley & Sons, Incorporated. (2012).

[6] Cox, D. A. *Primes of the form $x^2 + ny$: Fermat, class field theory, and complex multiplication (Second ed.).* John Wiley & Sons, Inc. (2013).

[7] Cox, D., Hyde, T. *The Galois theory of the lemniscate.* Journal of Number Theory 135, page 43-59. (2014)

[8] I. Schur, *Uber die Existenz unendlich vieler Primzahlen in einiger speziellen arithmetischen Progressionen.* S-B Berlin. Math. Ges., 11, page 40–50. (1912).

[9] Janusz, G. J. *Algebraic number fields (2nd ed.).* American Mathematical Society. (1996).

[10] Lang, S. *Algebraic number theory (2nd ed.).* Springer-Verlag. https://doi.org/10.1007/978-1-4612-0853-2. (1994).

[11] Murty, R. and Thain, N. *Prime Numbers in Certain Arithmetic Progressions.* Functiones Et Approximatio Commentarii Mathematici, Volume 35, page 249-259. (2006).

[12] Silverman, J. H. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag. https://doi.org/10.1007/978-1-4612-0851-8. (1994).

[13] Stein, W. *Introduction to Algebraic Number Theory.* https://wstein.org/129-05/notes/129.pdf. (2005).

[14] Sutherland, A. *Number Theory I.* Massachusetts Institute of Technology: MIT OpenCouseWare, https://ocw.mit.edu/courses/18-785-number-theory-i-fall-2021/resources/mit18_785f21_full_lec/. (2021).