Exploring the 2-Part of Class Groups in Quadratic Fields Perspectives on the Cohen-Lenstra Conjectures

YONG WANG , Huili Zhang , Ying Zhou , Haopeng Deng , Lingyue Li *

Posted Date: 10 October 2024

doi: 10.20944/preprints202410.0808.v1

Keywords: quadratic fields; class numbers; class groups; Cohen-Lenstra conjecture

Article

Exploring the 2-Part of Class Groups in Quadratic Fields: Perspectives on the Cohen-Lenstra Conjectures

Yong Wang [1], Huili Zhang [1], Ying Zhou [2], Haopeng Deng [3], Lingyue Li [1,*]

[1] School of Arts and Science, Guangzhou Maritime University, Guangzhou, 510725, China
[2] Institute of Visual Informatics (IVI), Universiti Kebangsaan Malaysia (UKM)
[3] School of Intelligent Transportation and Engineering, Guangzhou Jiaotong University, Guangzhou, 510725, China
* Correspondence: lilingyue17@mails.ucas.ac.cn

Abstract: Cohen and Lenstra introduced conjectures concerning the distribution of class numbers in quadratic fields, though many of these conjectures remain unproven. This paper investigates the 2-part of class groups in imaginary quadratic fields and examines their alignment with the Cohen-Lenstra heuristics. We provide detailed proofs of key theorems related to ideal decompositions and modular homomorphisms, and we explore the distribution of class groups of imaginary quadratic fields. Our analysis includes constructing imaginary quadratic fields with prescribed 2-class groups and discussing the implications of these findings on the Cohen-Lenstra conjecture.

Keywords: quadratic fields; class numbers; class groups; Cohen-Lenstra conjecture

1. Introduction

The class numbers of number fields are fundamental invariants with significant importance in number theory. The class numbers of quadratic fields, in particular, have been extensively studied. For instance, Gauss famously conjectured that there are infinitely many real quadratic fields with class number 1, while only a finite number (specifically 9) of imaginary quadratic fields share this property. For an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, where $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$, the class number $h(K) = 1$ were later proven by Baker and Stark [7,11].

While Gauss's conjecture on imaginary quadratic fields has been resolved, the corresponding question for real quadratic fields remains open. Whether there are infinitely many real quadratic fields with class number 1 is an unsolved problem [9]. One difficulty lies in the fact that the class number of a real quadratic field is closely related to its fundamental unit group, making the determination of class numbers for real quadratic fields more challenging compared to their imaginary counterparts. This problem is also related to the growth of the regulator in real quadratic fields, which can become quite large.

Determining class numbers for general number fields is often challenging. Cohen and Lenstra proposed several conjectures regarding the distribution of class numbers in number fields, including their famous conjectures on real and imaginary quadratic fields [6,12]. Their conjectures predict that for a fixed discriminant, the distribution of class numbers follows certain probabilistic laws, favoring the existence of class groups with small order.

Our Contribution: This paper focuses on the 2-part of class groups in imaginary quadratic fields. While the Cohen-Lenstra heuristics were originally formulated for odd primes, the behavior of the 2-part is influenced by genus theory, leading to deviations from the heuristics. We provide a detailed analysis of the 2-part of class groups, including theoretical results and numerical data, to explore these deviations and their implications.

Before presenting these conjectures, we provide several foundational concepts and properties to facilitate understanding. We recall that for an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, the class number is related to the Dedekind zeta function $\zeta_K(s)$ and the Minkowski bound, which gives a lower bound on the size of the class group. In particular, the 2-part of the class group is closely connected to the structure of the quadratic form class group.

 doi:10.20944/preprints202410.0808.v1

2. Fractional Ideals and Class Groups

Definition 1. *([2,3]) Let K be a number field and $\mathbb{Z}_K$ be the ring of integers of K. A subset I of K is called a fractional ideal of the number field K, if there exists a non-zero element $u \in K$, such that uI is a non-zero ideal of $\mathbb{Z}_K$.*

Definition 2. *([4,5]) Let A be a Dedekind ring. A principal fractional ideal is a fractional ideal of the form αA, generated by a single element α in the quotient field of A, where $\alpha \neq 0$ unless otherwise specified. The group of fractional ideals modulo the group of principal ideals (i.e., non-zero principal fractional ideals) is called the ideal class group of A. Denote by $P(K)$ the set of all principal fractional ideals. The principal fractional ideals form a group called the principal fractional ideal group.*

Let $I(K)$ denote the set of fractional ideals of the number field K, then $\mathbb{Z}_K$ is the integer ideal in $I(K)$. The fractional ideals of K form a group under multiplication, with the identity element being $\mathbb{Z}_K$.

The quotient group $Cl(K) = I(K)/P(K)$ is called the ideal class group (or simply the class group) of K. An ideal class of K is an element of $Cl(K)$. Therefore, two fractional ideals are equivalent in K if they lie in the same coset of $I(K)/P(K)$. Both $I(K)$ and $P(K)$ are infinite abelian groups, but the quotient group $Cl(K)$ is a finite abelian group. The order of this group, $h(K) = |Cl(K)|$, is called the ideal class number (or simply the class number) of K.

It can be observed that $h(K)$ is an important invariant of K. From the definition of $Cl(K)$, we have:

$$\begin{aligned} h(K) = 1 &\iff I(K) = P(K) \text{ (i.e., every fractional ideal is a principal fractional ideal);} \\ &\iff \text{every ideal in } \mathbb{Z}_K \text{ is a principal ideal;} \\ &\iff \mathbb{Z}_K \text{ is a principal ideal domain;} \\ &\iff \mathbb{Z}_K \text{ is a unique factorization domain.} \end{aligned}$$

Thus, the size of the class number $h(K)$ measures the difference between the Dedekind domain $\mathbb{Z}_K$ and a unique factorization domain.

Definition 3. *([4,5]) Let K be a field and O_K be a domain. A set $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of O_K (or K) if for every element $\alpha \in O_K$, there is a unique representation:*

$$\alpha = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n, \quad \lambda_i \in \mathbb{Z}.$$

Theorem 1. *(Hermite) For every given $d \in \mathbb{Z}$, there are only finitely many quadratic fields K such that $d(K) = d$, where $d(K)$ is the discriminant of K.*

Using Dirichlet's class number formula [7] and Theorem 1, one can develop a method to calculate class groups and class numbers. The first step is to calculate Minkowski's constant for the field K:

$$M(K) = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d(K)|^{1/2}.$$

In this equation, $n = [K : \mathbb{Q}] = r_1 + 2r_2$, where r_1 is the number of real embeddings of K, $2r_2$ is the number of complex embeddings of K, and $d(K)$ is the discriminant of K. The second step is to factor each rational prime $p \leq M(K)$ into prime ideals in O_K, i.e.,

$$pO_K = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct prime ideals and $a_1, \ldots, a_n$ are positive integers uniquely determined by pO_K. Thus, $Cl(K)$ is generated by the set $I = \{[\mathfrak{p}] : \mathfrak{p} \mid pO_K, p \leq M(K)\}$, where $[\mathfrak{p}]$ is the ideal class of $\mathfrak{p}$. Hence, $Cl(K)$ and $h(K)$ can be determined when the size of I is manageable.

 doi:10.20944/preprints202410.0808.v1

Example 1. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field and $d > 0$ a square-free integer. Then $n = 2$, $r_1 = 0$, $r_2 = 1$, and*

$$M(K) = \frac{2}{\pi}\sqrt{|d(K)|}.$$

For $K = \mathbb{Q}(\sqrt{-23})$, we have $O_K = \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-23})\right]$ and $M(K) = \frac{2}{\pi}\sqrt{23} < 4$. As $-23 \equiv 1 \pmod 8$ and $\left(\frac{-23}{3}\right) = 1$, the primes 2 and 3 split in K as follows:

$$2O_K = \mathfrak{p}_2\overline{\mathfrak{p}_2}, \quad N(\mathfrak{p}_2) = N(\overline{\mathfrak{p}_2}), \quad [\mathfrak{p}_2] = [\overline{\mathfrak{p}_2}]^{-1};$$

$$3O_K = \mathfrak{p}_3\overline{\mathfrak{p}_3}, \quad N(\mathfrak{p}_3) = N(\overline{\mathfrak{p}_3}), \quad [\mathfrak{p}_3] = [\overline{\mathfrak{p}_3}]^{-1}.$$

Thus, $Cl(K)$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$. Let's calculate the order of $[\mathfrak{p}_2]$:

$$\begin{aligned}
[\mathfrak{p}_2] = 1 &\iff [\mathfrak{p}_2] = (\alpha), \quad \alpha = \frac{a+b\sqrt{-23}}{2}, \quad a,b \in \mathbb{Z}, \quad 2 \mid (a-b), \\
&\iff \frac{a^2+23b^2}{4} = N(\mathfrak{p}_2) = 2, \quad a,b \in \mathbb{Z}, \\
&\implies a^2 + 23b^2 = 8.
\end{aligned}$$

Since the equation $x^2 + 23y^2 = 8$ has no integer solutions, we conclude that $[\mathfrak{p}_2] \neq 1$.

Next, consider the equation $x^2 + 23y^2 = 32$, which has a solution $(x, y) = (3, 1)$. Let $\beta = \frac{3+\sqrt{-23}}{2} \in O_K$. Then $N(\beta) = 8$, and there are four decompositions of (β):

$$(\beta) = \mathfrak{p}_2^3, \mathfrak{p}_2^2\overline{\mathfrak{p}_2}, \mathfrak{p}_2\overline{\mathfrak{p}_2}^2, \overline{\mathfrak{p}_2}^3.$$

Since $\mathfrak{p}_2\overline{\mathfrak{p}_2} = (2)$ is not a factor of (β) (because $\frac{\beta}{2} \notin O_K$), the only possibilities are $(\beta) = \mathfrak{p}_2^3$ or $(\beta) = \overline{\mathfrak{p}_2}^3$. Hence, $[\mathfrak{p}_2]^3 = 1$, and $[\mathfrak{p}_2]$ has order 3.

Moreover, the equation $x^2 + 23y^2 = 24$ has a solution $(x, y) = (1, 1)$. Let $\gamma = \frac{1+\sqrt{-23}}{2} \in O_K$. The norm of (γ) is 6, and it is an integral ideal. There are four decompositions of (γ):

$$(\gamma) = \mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2\overline{\mathfrak{p}_3}, \overline{\mathfrak{p}_2}\mathfrak{p}_3, \quad \overline{\mathfrak{p}_2\mathfrak{p}_3},$$

which implies $[\mathfrak{p}_2] = [\mathfrak{p}_3]$ or $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1}$. Therefore, $Cl(K)$ is generated only by $[\mathfrak{p}_2]$, and it is a cyclic group of order 3, so $h(K) = 3$.

This example demonstrates simple calculations of class numbers for real and imaginary quadratic fields. However, when $M(K)$ is large, the above method becomes cumbersome. In such cases, more efficient tools, such as analytic techniques, are needed to study the class number problem.

Definition 4. *If $\mathfrak{p} \in \Gamma$, the norm of $\mathfrak{p}$ is $N(\mathfrak{p}) = |A/\mathfrak{p}|$.*

Definition 5. *If G_1 and G_2 are A-modules, $G_1 \subseteq G_2$ means that G_1 is a submodule of G_2. If $\mathfrak{p} \in \Gamma$ and G is a finite A-module, then $r_\mathfrak{p}(G)$ is the $\mathfrak{p}$-rank of G, i.e., it is the dimension of the vector space $G/\mathfrak{p}G$ over $A/\mathfrak{p}$.*

Definition 6. *Let k be a positive integer or ∞. If $k \neq \infty$ and G is a finite A-module, then $s_k(G)$ (or $s_k^A(G)$) represents the number of A-epimorphisms from A^k to G. Define:*

$$S_k(G) := \{\varphi \in \mathrm{Hom}_A(A^k, G) : \varphi \text{ is an epimorphism}\}, \quad s_k(G) = |S_k(G)|.$$

 doi:10.20944/preprints202410.0808.v1

If G is a finite A-module, then $w_k(G) = s_k(G)|G|^{-k}|\mathrm{Aut}(G)|^{-1}$ is the k-weight, and $w(G) = w_\infty(G) = |\mathrm{Aut}(G)|^{-1}$. If $\mathfrak{p} \in \Gamma$, let:

$$\eta_k(\mathfrak{p}) = \prod_{1\le i\le k}\Big(1-(N\mathfrak{p})^{-i}\Big), \quad \eta_\infty(\mathfrak{p}) = \prod_{i\ge 1}\Big(1-(N\mathfrak{p})^{-i}\Big).$$

Definition 7. *Since every finite A-module G can be written as $G = \bigoplus_i A/\mathfrak{p}_i^{a_i}$, define:*

$$\chi_A(G) = \prod_i \mathfrak{p}_i^{a_i}.$$

If $A = \mathbb{Z}$, then $\chi_{\mathbb{Z}}(G) = n\mathbb{Z}$, where $n = |G|$. Let α be an integral ideal, and define the k-weight $w_k(\alpha)$ of α as:

$$w_k(\alpha) = \sum_{G(\alpha)} w_k(G), \quad w(\alpha) = w_\infty(\alpha),$$

where $\sum_{G(\alpha)}$ denotes summation over G up to A-isomorphism with $\chi_A(G) = \alpha$.

Definition 8. *Let G be an abelian group and p a prime number. If for every $a \in G$ there exists $n \ge 1$ such that $p^n a = 0$, then G is called a p-primary group. For a general abelian group G, let $G_p = \{a \in G : n \ge 1, p^n a = 0\}$ denote the p-part of G.*

Theorem 2. *Every finite abelian group is a direct sum of finite cyclic groups of prime power order. More generally, every finite abelian group is a direct sum of finite cyclic groups [8].*

Definition 9. *We call J a projective module if it is a direct summand of a free module.*

Theorem 3. *If J is a projective module over a principal ideal domain (PID), then J is free [8].*

Definition 10. *Let S be a subset of A. Then S is called a multiplicatively closed set in A, if S satisfies the following two conditions:*

1. $1 \in S$;
2. *If $a, b \in S$, then $ab \in S$,*

Suppose A is a domain and S is a multiplicatively closed set of A. Then $S^{-1}A$ represents the localization of A with respect to S, and is defined as:

$$S^{-1}A := \left\{\frac{r}{s} : r \in A, s \in S, \quad \frac{r}{s} = \frac{r'}{s'} \Leftrightarrow \exists u \in S \text{ such that } u(rs' - sr') = 0\right\}.$$

Addition and multiplication in $S^{-1}A$ are defined as follows:

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}, \quad \left(\frac{a}{s}\right)\left(\frac{b}{t}\right) = \frac{ab}{st}.$$

Let $\mathfrak{p}$ be a prime ideal of A, and let $S_\mathfrak{p} = A \setminus \mathfrak{p}$. Then $S_\mathfrak{p}^{-1}A$ is called the *localization* of A at $\mathfrak{p}$, and is denoted $A_\mathfrak{p}$. It is a local ring.

If J is a projective A-module, define the localization of J at S as $S^{-1}J$. In this case, $S^{-1}J$ is a projective module over $S^{-1}A$. The localization of a Dedekind domain is a principal ideal domain. Moreover, projective modules over a principal ideal domain are free, so projective modules over a Dedekind domain are locally free [11].

Definition 11. *Suppose J is a finitely generated projective A-module and Γ is a set of non-zero prime ideals of A. If $\mathfrak{p} \in \Gamma$, the rank of J at $\mathfrak{p}$ is defined as the rank of $J_\mathfrak{p}$ as a free module over $A_\mathfrak{p}$, where $J_\mathfrak{p}$ and $A_\mathfrak{p}$ are the*

 doi:10.20944/preprints202410.0808.v1

localizations of J and A at $\mathfrak{p}$. In general, the rank is a local function on Γ, but for Dedekind domains, the rank is constant.

Theorem 4. *([11]) If A is a Dedekind domain and J is a projective module, then $J \cong A \oplus I$, where I is a non-zero ideal and* $\mathrm{rank}(J) = n + 1$.

Note. *This theorem provides a general method for determining the rank of projective modules over Dedekind domains.*

3. Ideal Decompositions and Modular Homomorphisms

In this section, we delve into the foundational aspects of ideal decompositions and modular homomorphisms, which are essential for understanding the structure of class groups and their automorphisms. We provide detailed proofs of key theorems, following the exposition in [6].

Let $A = \mathcal{O}_K$ denote the ring of integers of a number field K, and let Γ represent the set of non-zero prime ideals of A.

3.1. Main Theorem and Proof

Theorem 5. *Suppose J is a projective A-module with rank k, and G is a finite A-module with $\chi_A(G) =$, then:*
(i) The number of A-module epimorphisms from J to G is equal to $s_k(G)$;
(ii) $s_k(G) = (N)^k \prod_{\mathfrak{p}|} \left(\frac{\eta_k(\mathfrak{p})}{\eta_{k-r_{\mathfrak{p}}(G)}(\mathfrak{p})} \right)$ and $w_k(G) = \prod_{\mathfrak{p}|} \frac{\eta_k(\mathfrak{p})}{\eta_{k-r_{\mathfrak{p}}(G)}(\mathfrak{p})} \cdot \frac{1}{|\mathrm{Aut}(G)|}$;
(iii) $\#\{H \leq J : J/H \cong G\} = (N)^k w_k(G)$;
(iv) $\lim_{k \to +\infty} w_k(G) = w(G)$.

Proof. (i) Let S_α be the set of prime ideals in A excluding all prime ideals that are not divisible by α. Define $S_\alpha^{-1}A$, $S_\alpha^{-1}J$, and $S_\alpha^{-1}G$ as the localization of A, J, and G, respectively. For convenience, denote A_α, J_α, and G_α as $S_\alpha^{-1}A$, $S_\alpha^{-1}J$, and $S_\alpha^{-1}G$, respectively.

At this time, A_α is a semi-local Dedekind domain, and a semi-local Dedekind domain is a principal ideal domain. Therefore, J_α as an A_α-module is a free module, so we have $J_\alpha \cong A_\alpha^k$, and there exists a module isomorphism $\psi : J_\alpha \to A_\alpha^k$.

Thus, any A_α-module surjection from J_α to G_α can be transformed into a surjection from A_α^k to G_α via this isomorphism. Conversely, any A_α-module surjection from A_α^k to G_α can be transformed into a surjection from J_α to G_α via the isomorphism. Therefore, the number of A_α-module epimorphisms from J_α to G_α is equal to $s_k(G_\alpha)$. □

To prove (i) in general, the following concepts and theorems are needed.

Definition 12. ***Localization of mapping:*** *Let $\varphi : M \to N$ be an A-module homomorphism. Then the localization of φ at α is defined as:*

$$\varphi_\alpha : S_\alpha^{-1}M \to S_\alpha^{-1}N, \quad m/u \mapsto \varphi(m)/u, \quad u \in S_\alpha.$$

Proposition 1. *Suppose $\psi : A \to A_\alpha$ is the natural localization mapping. Then it has the following properties:*
(i) For any ideal $I \subseteq A_\alpha$, $I = \psi^{-1}(I)A_\alpha$, and the mapping $I \to \psi^{-1}(I)$ is an injection from the set of ideals of A_α to the set of ideals of A, and maps prime ideals to prime ideals.
(ii) Suppose N is an ideal of A. Then N has the form $\psi^{-1}(I)$, where $I \subseteq A_\alpha$ if and only if $N = \psi^{-1}(NA_\alpha)$. That is, if $a \in A$ and $au \in N$ for some $u \in A$, then $a \in N$. This correspondence $I \to \psi^{-1}(I)$ is an isomorphism from the prime ideals of A_α to the prime ideals of A that are not contained in α. A similar result holds for any module and its submodules.

For the proof, see [2, p. 61-63].

 doi:10.20944/preprints202410.0808.v1

This property indicates the existence of a natural mapping between a ring and its localization, which establishes a correspondence between ideals in the ring and ideals in the local ring. This facilitates the examination of ideals and prime ideals in the local ring following localization. Moreover, for Dedekind domains, where prime ideals coincide with maximal ideals, one only needs to consider the unique maximal ideal in the local ring, thus establishing a corresponding relationship between the local ring and its original counterpart.

Theorem 6. *If $\varphi : M \to N$ is an A-module isomorphism, then φ is injective, surjective, or bijective if and only if for every maximal ideal α of A, the localized mapping $\varphi_\alpha : S_\alpha^{-1}M \to S_\alpha^{-1}N$ is injective, surjective, or bijective, respectively.*

For the proof of the theorem, see [2, p. 67-68].

By applying Theorem 3.2 and Proposition 3.1, one can prove Theorem 3.1(i) by replacing M with A^k and N with G.

Lemma 1. *If $\varphi \in \mathrm{Hom}_A(A^k, G)$, let $\overline{\varphi} : (A/\mathfrak{p})^k \to G/\mathfrak{p}G$ be defined as $\overline{\varphi}(\overline{g}) = \overline{\varphi(g)}$, where $g \in A^k$ and $\overline{g} \in (A/\mathfrak{p})^k$. Then φ is surjective if and only if $\overline{\varphi}$ is surjective.*

Proof. First, we prove that the definition of $\overline{\varphi}$ is reasonable. Suppose $\overline{g_1} = \overline{g_2}$, so $\overline{g_2 - g_1} = 0$, and we have:

$$\overline{\varphi}(\overline{g_2}) - \overline{\varphi}(\overline{g_1}) = \overline{\varphi(g_2)} - \overline{\varphi(g_1)} = \overline{\varphi(g_2 - g_1)} = \overline{0}.$$

It is obvious that $\overline{\varphi}$ is an $A/\mathfrak{p}$-module homomorphism.

Now, since G is a p-group, we can express $G = \oplus_i A/\mathfrak{p}^{a_i}$ and $\mathfrak{p}G = \oplus_i \mathfrak{p}A/\mathfrak{p}^{a_i}$. Thus, for any $\varphi \in \mathrm{Hom}_A(A^k, G)$, we have:

$$\varphi \cong \oplus_i \mathrm{Hom}_A(A^k, A/\mathfrak{p}^{a_i}).$$

Therefore, we can write $\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_t)$ and $\overline{\varphi} = (\overline{\varphi_1}, \overline{\varphi_2}, \ldots, \overline{\varphi_t})$, where each $\varphi_i = \pi \circ \varphi$. It follows that $\overline{\varphi}$ is surjective if and only if each $\overline{\varphi_i}$ is surjective. □

Theorem 7. *The equality $s_k^A(G) = s_k^{A/\mathfrak{p}}(G/\mathfrak{p}G) \cdot \#\{\varphi \in \mathrm{Hom}_A(A^k, G) : \overline{\varphi} = 0\}$ holds.*

Proof. Define:

$$\Phi : S_k(G) \longrightarrow S_k^{A/\mathfrak{p}}(G/\mathfrak{p}G), \quad \varphi \longrightarrow \overline{\varphi}.$$

It is clear that Φ is surjective. By the fundamental theorem of homomorphisms, we have:

$$S_k(G)/\mathrm{Ker}\Phi \cong S_k^{A/\mathfrak{p}}(G/\mathfrak{p}G),$$

where $\mathrm{Ker}\Phi = \{\varphi \in \mathrm{Hom}_A(A^k, G) : \overline{\varphi} = 0\}$.

Thus, we conclude that:

$$s_k^A(G) = s_k^{A/\mathfrak{p}}(G/\mathfrak{p}G) \cdot \#\{\varphi \in \mathrm{Hom}_A(A^k, G) : \overline{\varphi} = 0\}.$$

This proves Theorem 3.3. □

Choose a set of basis $\{e_1, e_2, \cdots, e_k\}$ for A^k. Since $\overline{\varphi} = 0 \iff \mathrm{Im}\varphi \subset \mathfrak{p}G \iff \varphi(e_i) \in \mathfrak{p}G$ for every i and each e_i, the number of φ is given by $|\mathfrak{p}G|$. Therefore,

$$\#\{\varphi \in \mathrm{Hom}_A(A^k, G) : \overline{\varphi} = 0\} = |\mathfrak{p}G|^k = \frac{|G|^k}{|G/\mathfrak{p}G|^k}.$$

 doi:10.20944/preprints202410.0808.v1

Let $r = r_{\mathfrak{p}}(G)$, then $G/\mathfrak{p}G$ is a vector space over $A/\mathfrak{p}$ of dimension r. Thus, $G/\mathfrak{p}G \cong (A/\mathfrak{p})^r$, and consequently $|G/\mathfrak{p}G| = (N\mathfrak{p})^r$. Therefore,

$$|\mathfrak{p}G|^k = \frac{|G|^k}{(N\mathfrak{p})^{kr}} = \frac{(N\alpha)^k}{(N\mathfrak{p})^{kr}}.$$

On the other hand, $s_k^{A/\mathfrak{p}}(G/\mathfrak{p}G)$ represents the number of $k \times r$ matrices with rank r over $A/\mathfrak{p}$. This is equivalent to counting the number of linearly independent r-dimensional vectors $(v_1, v_2, \ldots, v_r)$ in $(A/\mathfrak{p})^k$.
Since a vector space of dimension i has $(N\mathfrak{p})^i$ elements over $A/\mathfrak{p}$, it follows that:

$$s_k^{A/\mathfrak{p}}(G/\mathfrak{p}G) = ((N\mathfrak{p})^k - 1)(N\mathfrak{p}^k - N\mathfrak{p}) \cdots ((N\mathfrak{p})^k - (N\mathfrak{p})^{r-1}) = \frac{(N\mathfrak{p})^{kr}\eta_k(\mathfrak{p})}{\eta_{k-r}(\mathfrak{p})}.$$

Hence, Theorem 3.1 (ii) is established.
Proof of Theorem 3.1(iii):
Let $Y = \{H \subseteq J : J/H \cong G\}$ and $X = \{\mathrm{Ker}\varphi : \varphi \in \mathrm{Hom}_A(J, G), \varphi \text{ is surjective}\}$. We assert that $Y = X$.
Clearly, $X \subseteq Y$. To complete the proof, we need only show that $Y \subseteq X$.
Suppose $H \in Y$. Then there exists an A-module isomorphism $\varphi_0 : J/H \to G$. Combining this with the natural projection $\pi : J \to J/H$, we obtain $\varphi = \varphi_0 \circ \pi \in \mathrm{Hom}_A(J, G)$, which is surjective, and

$$\mathrm{Ker}\varphi = \mathrm{Ker}\pi = H.$$

Thus, $Y \subseteq X$, proving that $Y = X$. Therefore, we have

$$\#\{H \leq J : J/H \cong G\} = \#\{\mathrm{Ker}\varphi : \varphi \in \mathrm{Hom}_A(J, G), \varphi \text{ is surjective}\}.$$

Since $\mathrm{Ker}\varphi_1 = \mathrm{Ker}\varphi_2 \iff \exists \sigma \in \mathrm{Aut}(J)$ such that $\varphi_2 = \sigma \circ \varphi_1$, we deduce that

$$\#\{\mathrm{Ker}\varphi : \varphi \in \mathrm{Hom}_A(J, G), \varphi \text{ is surjective}\} = \frac{s_k(G)}{|\mathrm{Aut}(G)|} = w_k(G) \cdot |G|^{-k} = (N\alpha)^k w_k(G).$$

Thus, Theorem 3.1 (iii) is proved.
Proof of Theorem 3.1(iv): From Theorem 3.1(ii), taking the limit as $k \to +\infty$, we obtain:

$$\lim_{k\to+\infty} w_k(G) = \frac{1}{|\mathrm{Aut}(G)|} \lim_{k\to+\infty} \prod_{\mathfrak{p}|\alpha} \frac{\eta_k(\mathfrak{p})}{\eta_{k-r_{\mathfrak{p}}(G)}(\mathfrak{p})} = \frac{1}{|\mathrm{Aut}(G)|}.$$

Thus, Theorem 3.1 (iv) holds.

Lemma 2. *If $\varphi_1 \in \mathrm{Hom}_A(A^{k_1}, G_1)$ is surjective, then*

$$\#\{\varphi \in \mathrm{Hom}_A(A^{k_1+k_2}, G) : \varphi \text{ is surjective and } \varphi|_{A^{k_1}} = \varphi_1\} = s_{k_2}(G/G_1)|G_1|^{k_2}.$$

For a proof, see [6].

Theorem 8. *When $k_1, k_2 \neq \infty$ and G is a finite A-module, we have*

$$s_{k_1+k_2}(G) = \sum_{G_1 \subseteq G} s_{k_1}(G_1) s_{k_2}(G/G_1)|G_1|^{k_2}.$$

 doi:10.20944/preprints202410.0808.v1

Proof. Suppose $A^{k_1\times k_2} = A^{k_1} \times A^{k_2}$. For a given $a = (a_1, a_2) \in A^{k_1} \times A^{k_2}$ and $\varphi \in \mathrm{Hom}_A(A^{k_1\times k_2}, G)$, define

$$\varphi_1 : A^{k_1} \to G, \quad \varphi_1(a) = \varphi(a_1, 0);$$
$$\varphi_2 : A^{k_2} \to G, \quad \varphi_2(a) = \varphi(0, a_2).$$

Thus, $\varphi(a_1, a_2) = \varphi(a_1, 0) + \varphi(0, a_2) = \varphi_1(a_1) + \varphi_2(a_2)$, and we conclude that

$$s_{k_1+k_2}(G) = \sum_{G_1\subseteq G} \#\{\varphi \in \mathrm{Hom}_A(A^{k_1+k_2}, G) : \varphi \text{ is surjective and } \varphi(A^{k_1}) = G_1\}.$$

Thus, we have

$$s_{k_1+k_2}(G) = \sum_{G_1\subseteq G} \sum_{\varphi_1\in S_{k_1}(G)} \#\{\varphi \in \mathrm{Hom}_A(A^{k_1+k_2}, G) : \varphi \text{ is surjective and } \varphi|_{A^{k_1}} = \varphi_1\}.$$

□

From Lemma 3.2, we can now prove the theorem.

Theorem 9. *Let α be a non-zero ideal of A. For any $k_2 \neq \infty$, we have*

$$w_{k_1+k_2} = \sum_{\beta|\alpha} (N\beta)^{-k_2} w_{k_1}(\beta) w_{k_2}(\alpha\beta^{-1}).$$

For a proof, see [6].

Theorem 10. *Let α be a non-zero ideal of A. For any k, we have*

$$\sum_{\beta|\alpha} w_k(\beta) = (N\alpha) w_{k+1}(\alpha).$$

In particular, $\sum_{\beta|\alpha} w(\beta) = N(\alpha)w(\alpha)$.

Proof. Note that $s_1(G) \neq 0$ if and only if $G \cong A/\alpha$, where α is a non-zero ideal of A. According to the fundamental theorem of modular homomorphisms, we have $G \cong A/\mathrm{Ker}\varphi$ where $\varphi \in s_1(G)$ and $s_1(A/\alpha) \cong \mathrm{Aut}(A/\alpha)$. Therefore, $s_1(A/\alpha) = |\mathrm{Aut}(A/\alpha)|$. By Theorem 3.5, setting $k_1 = k$ and $k_2 = 1$, we obtain:

$$\begin{aligned} w_1(\alpha) &= \sum_{G(\alpha)} \frac{s_1(G)}{|G| \cdot |\mathrm{Aut}(G)|} = |G|^{-1} = \frac{1}{N\alpha}, \\ w_{k+1}(\alpha) &= \sum_{\beta|\alpha} (N\beta)^{-1} w_k(\beta) w_1(\alpha\beta^{-1}) \\ &= \sum_{\beta|\alpha} (N\beta)^{-1} w_k(\beta) (N(\alpha\beta^{-1}))^{-1} \\ &= \sum_{\beta|\alpha} (N\beta)^{-1} w_k(\beta) N(\alpha)^{-1} N(\beta). \end{aligned}$$

Thus, we conclude that $\sum_{\beta|\alpha} w_k(\beta) = (N\alpha) w_{k+1}(\alpha)$. Taking the limit as $k \to \infty$, we find $\sum_{\beta|\alpha} w(\beta) = N(\alpha)w(\alpha)$. □

Theorem 11. *Let $\mathfrak{p} \in \Gamma$ be a prime ideal.*

 doi:10.20944/preprints202410.0808.v1

(i) When $\mathrm{Re}(s) > -1$, *we have:*

$$\sum_{i\geq 0} w_k(\mathfrak{p}^i)N(\mathfrak{p})^{-is} = \prod_{1\leq j\leq k}\left(1-(N\mathfrak{p})^{-j-s}\right)^{-1}.$$

(ii) If $\zeta_{k,A}(s) = \zeta_k(s) = \sum_\alpha w_k(\alpha)(N\alpha)^{-s}$ *where* $\mathrm{Re}(s) > 0$, *then:*

$$\zeta_k(s) = \prod_{1\leq j\leq k}\zeta_A(s+j),$$

where $\zeta_A(s)$ *is the Dedekind zeta function of* A.

Proof. (i) For $k = 1$, since $w_1(\alpha) = 1/N\alpha$ and $N(\mathfrak{p}^m) = (N\mathfrak{p})^m$, we have:

$$\begin{aligned}\sum_{i\geq 0} w_1(\mathfrak{p}^i)(N\mathfrak{p})^{-is} &= \sum_{i\geq 0}(N\mathfrak{p})^{-i}(N\mathfrak{p})^{-is}\\ &= \sum_{i\geq 0}(N\mathfrak{p})^{-i(1+s)}\\ &= (1-(N\mathfrak{p})^{-1-s})^{-1}.\end{aligned}$$

For $k \geq 2$, using Theorems 3.5 and 3.6 and the fact that $N(\mathfrak{p}^m) = (N\mathfrak{p})^m$, we obtain:

$$\begin{aligned}\sum_{i\geq 0} w_k(\mathfrak{p}^i)(N\mathfrak{p})^{-is} &= \sum_{i\geq 0}\sum_{l\leq i} w_{k-1}(\mathfrak{p}^l)(N\mathfrak{p})^{-i}(N\mathfrak{p})^{-is}\\ &= \sum_{i\geq 0}(N\mathfrak{p})^{-i(1+s)}\sum_{l\leq i} w_{k-1}(\mathfrak{p}^l)\\ &= \sum_{l\geq 0}\sum_{i\geq l}(N\mathfrak{p})^{-i(1+s)} w_{k-1}(\mathfrak{p}^l)\\ &= \sum_{l\geq 0} w_{k-1}(\mathfrak{p}^l)(N\mathfrak{p})^{-l(s+1)}\left(1-(N\mathfrak{p})^{-(1+s)}\right)^{-1}. \qquad \star\end{aligned}$$

Continuing this process, we have:

$$\begin{aligned}\star &= \sum_{l\geq 0} w_1(\mathfrak{p}^l)(N\mathfrak{p})^{-l(s+k)}\prod_{1\leq j\leq k}\left(1-(N\mathfrak{p})^{-(j+s)}\right)^{-1}\\ &= \prod_{1\leq j\leq k}\left(1-(N\mathfrak{p})^{-(j+s)}\right)^{-1}\cdot\sum_{l\geq 0}(N\mathfrak{p})^{-l(s+k+1)}\\ &= \prod_{1\leq j\leq k}\left(1-(N\mathfrak{p})^{-(j+s)}\right)^{-1}\cdot(1-(N\mathfrak{p})^{-(s+k+1)})^{-1}\\ &= \prod_{1\leq j\leq k}\left(1-(N\mathfrak{p})^{-j-s}\right)^{-1}.\end{aligned}$$

(ii) For $k = 1$, we have:

$$\zeta_1(s) = \sum_\alpha w_1(\alpha)(N\alpha)^{-s} = \sum_\alpha (N\alpha)^{-(1+s)} = \zeta_A(s+1).$$

 doi:10.20944/preprints202410.0808.v1

For $k \geq 2$, we calculate:

$$\begin{aligned}
\zeta_k(s) &= \sum_{\alpha} w_k(\alpha)(N\alpha)^{-s} = \sum_{\alpha}\sum_{\beta|\alpha} w_{k-1}(\beta)(N\alpha)^{-(1+s)} \\
&= \sum_{\beta}\sum_{\gamma} w_{k-1}(\beta)(N\beta)^{-(1+s)}(N\gamma)^{-(1+s)}, \quad (\alpha = \beta\gamma) \\
&= \sum_{\beta} w_{k-1}(\beta)(N\beta)^{-(1+s)}\zeta_A(s+1) \\
&= \zeta_A(s+1)\sum_{\beta} w_{k-2}(\beta)(N\beta)^{-(2+s)}\zeta_A(s+2), \ldots \\
&= \zeta_A(s+1)\zeta_A(s+2)\cdots\zeta_A(s+k-1)\sum_{\beta} w_1(\beta)(N\beta)^{-(k+s-1)}.
\end{aligned}$$

Since $w_1(\beta) = (N\beta)^{-1}$, we conclude that:

$$\zeta_k(s) = \prod_{1\leq j\leq k} \zeta_A(s+j).$$

Thus, the theorem is proved. □

4. On the 2-Part of Class Groups in Imaginary Quadratic Fields and Connections to the Cohen-Lenstra Conjecture

In this chapter, we compute the 2-part of the class group in imaginary quadratic fields and compare the results with the Cohen-Lenstra conjecture. From these calculations, we derive new conjectures. Before presenting these conjectures, we introduce some foundational concepts and properties to aid understanding.

We begin with the concept of partitions. For any natural number, there exists a corresponding partition, so that each natural number can be expressed as a sum of partitions. For example:

$$6 = 6+0 = 5+1 = 4+2 = 4+1+1 = \cdots.$$

Thus, a partition can represent a natural number $n = (n_i), n_1 \geq n_2 \geq \cdots \geq n_k > 0$.

Let Ω represent the set of partitions of natural numbers, and define $\mathcal{G}_p$ as the set of all finite Abelian p-groups (up to isomorphism). For any finite Abelian p-group, it can be expressed as $\bigoplus_i (\mathbb{Z}/p^{e_i})^{r_i}$, where $1 \leq i \leq k$, $k > 0$, $e_1 > e_2 > \cdots > e_k > 0$, and $r_i > 0$. There is a natural isomorphism between these two sets: $\mathcal{G}_p \cong \Omega$.

4.1. Theorem and Conjectures

Theorem 12. *Let $G = \bigoplus_i (\mathbb{Z}/p^{e_i})^{r_i}$, $(1 \leq i \leq k)$, where $k > 0$, $e_1 > e_2 > \cdots > e_k > 0$, and $r_i > 0$. Then the order of the automorphism group $\mathrm{Aut}(G)$ is given by:*

$$|\mathrm{Aut}(G)| = \left(\prod_{1\leq i\leq k}\prod_{1\leq s\leq r_i}(1-p^{-s})\right)\prod_{1\leq i,j\leq k} p^{\min(e_i,e_j)r_i r_j}.$$

In particular, if $H = \mathrm{Aut}((\mathbb{Z}/p^e)^r)$, then $|H| = p^{r^2e}\prod_{1\leq s\leq r}(1-p^{-s})$.

For a detailed proof, see [12, Theorem 1.2.10].

 doi:10.20944/preprints202410.0808.v1

Conjecture 4.1 (Cohen-Lenstra). *Suppose p is an odd prime, and let $D^{\pm}(X)$ denote the number of real or imaginary quadratic fields whose absolute discriminant is less than X. Let G be a finite Abelian p-group. Then:*

$$\lambda^{\pm}(G) = \lim_{X\to\infty} \frac{|\{K \in D^{\pm}(X) : Cl_p(K) \cong G\}|}{|D^{\pm}(X)|}$$

exists, and $\lambda^{+}(G) = c^{+}|\mathrm{Aut}(G)|^{-1}|G|^{-1}$, while $\lambda^{-}(G) = c^{-}|\mathrm{Aut}(G)|^{-1}$, where c^{+} and c^{-} are constants independent of G.

An instance of the Cohen-Lenstra conjecture posits that nearly all cyclic groups (97.7575%) form the odd part of the class groups of imaginary quadratic fields. Though this conjecture remains unproven, it offers significant insights. Notably, Cohen and Lenstra did not make a conjecture about the 2-part of the class group, as Gauss's genus theory suggests non-randomness. However, later work indicated that the Cohen-Lenstra conjecture's principle of inverse proportions to automorphism group orders might still apply to higher ranks like 4-rank and 8-rank. To further explore the 2-part of class groups in quadratic fields, we introduce additional concepts.

4.2. Directed Graphs and the 2-Rank of Class Groups

Definition 13. *Let $G = (V, E)$ be a directed graph, where $V = V_1 \cup V_2$ is a partition of V. The partition is odd if there exists $v_1 \in V_1$ such that the number of arcs from v_1 to vertices in V_2 is odd, or there exists $v_2 \in V_2$ such that the number of arcs from v_2 to vertices in V_1 is odd. Otherwise, the partition is even. A graph G is said to be odd if every non-trivial partition of V is odd.*

Let $K = \mathbb{Q}(\sqrt{-D})$, where $D \geq 2$ is an imaginary quadratic field, and let r_2 be the 2-rank of the class group $Cl(K)$. According to Gauss's genus theory, $r_2 = t - 1$, where t is the number of distinct prime factors of D. Define the directed graph $G(D)$, where the vertices are the prime factors of D, and there exists an arc $\overrightarrow{p_i p_j}$ if $\left(\frac{p_j}{p_i}\right) = -1$, where $\left(\frac{p_j}{p_i}\right)$ is the Legendre symbol.

Definition 14. *Let $M(G) = \mathrm{diag}(d_1, \ldots, d_m) - A(G)$, where $d_{ij} = \sum_{j=1}^{m} a_{ij}$ and $A(G)$ is the adjacency matrix. Define $r = \mathrm{rank}_{\mathbb{F}_2}(M(G))$.*

Lemma 3. *[13] The graph G is odd if and only if $r = m - 1$.*

Theorem 13. *[13] Let $K = \mathbb{Q}(\sqrt{-D})$ with $D \geq 2$, and let t be the number of distinct prime factors of D. Then $2^{t-1}||h_K$ if and only if the directed graph $G(D)$ is odd.*

Proposition 2. *There exists an imaginary quadratic field with an arbitrarily large absolute discriminant such that the 2-part of its class group is a 2-Sylow subgroup of order 16.*

Proof. According to Theorem 14, we know that if the directed graph $G(D)$ is odd for $t = 5$, we can obtain a 2-Sylow subgroup of order 16.

Let $K = \mathbb{Q}(\sqrt{-D})$, with $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $p_4 = 11$, and $p_5 = p$. Then $D = 3 \times 5 \times 7 \times 11 \times p$, and $-D \equiv 1 \pmod 4$. The matrix is given by:

$$M(G) = \begin{pmatrix} 0 & 0 & 0 & 0 & a_{15} \\ 0 & 0 & 1 & 0 & a_{25} \\ 1 & 1 & 0 & 0 & a_{35} \\ 0 & 0 & 1 & 0 & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & 0 \end{pmatrix}.$$

 doi:10.20944/preprints202410.0808.v1

According to Lemma 2, to make the graph $G(D)$ odd, we need the rank of the matrix $M(G)$ to be 4. Take a special case: let $a_{15} = 0, a_{25} = 0, a_{51} = 0, a_{52} = 0, a_{53} = 1, a_{54} = 1$. That is, $\left(\frac{3}{p}\right) = 1$, $\left(\frac{5}{p}\right) = 1$, $\left(\frac{p}{3}\right) = 1$, $\left(\frac{p}{5}\right) = 1$, $\left(\frac{7}{p}\right) = -1$, and $\left(\frac{11}{p}\right) = -1$.

For the congruence equation $\left(\frac{3}{p}\right) = 1$ and $\left(\frac{p}{3}\right) = 1$, we get the solution $p \equiv 1 \pmod{12}$. For $\left(\frac{5}{p}\right) = 1$ and $\left(\frac{p}{5}\right) = 1$, we get $p \equiv 1, 49 \pmod{60}$. Taking $p \equiv 1 \pmod{60}$, and combining this with $\left(\frac{7}{p}\right) = -1$ and $\left(\frac{p}{7}\right) = -1$, we get $p \equiv 61, 481, 901 \pmod{4620}$. At this time, $-D = 3 \times 5 \times 7 \times 11 \equiv 1 \pmod{4}$. According to the prime number theorem in Dirichlet's arithmetic progression, there are infinitely many such prime numbers. Thus, the proposition is proved. □

By Proposition 4.1, one can construct an infinite number of imaginary quadratic fields where the 2-part of the class group forms a 2-Sylow subgroup of order 16. Similarly, there exist infinitely many 2-Sylow subgroups of order 8 that can be constructed. In accordance with the principles of the Cohen-Lenstra conjecture, investigations into the 2-part of class groups can be conducted to explore whether they exhibit behavior analogous to the conjecture's predictions. Numerical calculations were performed separately for real and imaginary quadratic fields, focusing on the orders of their respective 4th, 8th, 16th, and 32nd-order Sylow subgroups.

4.3. Numerical Results

The 4th-order 2-Sylow group has the following situations:

$$\mathbb{Z}/4,\ \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

The 8th-order 2-Sylow group has the following situations:

$$\mathbb{Z}/8,\ \mathbb{Z}/4 \oplus \mathbb{Z}/2,\ (\mathbb{Z}/2)^3$$

We can calculate that the orders of their corresponding automorphism groups are 4, 8, and 168, respectively.

For the 16th-order 2-Sylow group, there are the following situations:

$$\mathbb{Z}/16,\ \mathbb{Z}/8 \oplus \mathbb{Z}/2,\ (\mathbb{Z}/4)^2,\ \mathbb{Z}/4 \oplus (\mathbb{Z}/2)^2,\ (\mathbb{Z}/2)^4$$

We can calculate that the orders of their corresponding automorphism groups are 8, 16, 96, 192, and 20160, respectively.

For the 32nd-order 2-Sylow subgroup, there are the following situations:

$$\mathbb{Z}/32, \mathbb{Z}/16 \oplus \mathbb{Z}/2,\ \mathbb{Z}/8 \oplus \mathbb{Z}/4,\ \mathbb{Z}/8 \oplus (\mathbb{Z}/2)^2,\ (\mathbb{Z}/4)^2 \oplus \mathbb{Z}/2,\ \mathbb{Z}/4 \oplus (\mathbb{Z}/2)^3,\ (\mathbb{Z}/2)^5$$

The following tables present numerical results for the different orders of 2-Sylow subgroups.

 doi:10.20944/preprints202410.0808.v1

Table 1. The 2-part of class group of 4th-order 2-Sylow subgroup

X	[4]	[2,2]
10^2	4	1
10^3	35	40
3×10^3	103	129
5×10^3	181	176
8×10^3	292	379
10^4	349	480
3×10^4	941	1438
5×10^4	1513	2334
8×10^4	2402	3878
10^5	2967	4889
3×10^5	8257	14657
5×10^5	13898	24459
8×10^5	21469	39115
10^6	26559	48931
3×10^6	76146	145945
5×10^6	124395	242094

Table 2. The 2-part of class group of 8th-order 2-Sylow subgroup

X	[8]	[4,2]	[2,2,2]
10^3	20	16	3
3×10^3	47	47	11
5×10^3	59	53	13
6×10^3	62	55	13
6306	62	55	13
6307	62	55	13
10^4	62	55	13
5×10^4	62	55	13
10^5	62	55	13
3×10^5	62	55	13
5×10^5	62	55	13
10^6	62	55	13
3×10^6	62	55	13
5×10^6	62	55	13
10^7	62	55	13
10^8	62	55	13

Table 3. The 2-part of class group of 16th-order 2-Sylow subgroup

X	[16]	[8,2]	[4,4]	[4,2,2]	[2,2,2,2]
10^2	0	0	0	0	0
10^3	7	6	0	0	0
10^4	60	103	8	54	1
1.5×10^4	82	126	14	59	1
31242	100	143	16	60	1
31243	100	143	16	60	1
10^5	100	143	16	60	1
5×10^5	100	143	16	60	1
8×10^5	100	143	16	60	1
10^6	100	143	16	60	1
3×10^6	100	143	16	60	1
5×10^6	100	143	16	60	1
8×10^6	100	143	16	60	1
10^7	100	143	16	60	1
3×10^7	100	143	16	60	1
10^8	100	143	16	60	1

 doi:10.20944/preprints202410.0808.v1

Table 4. The 2-part of class group of 32th-order 2-Sylow subgroup

X	[32]	[16,2]	[8,4]	[8,2,2]	[4,4,2]	[4,2,2,2,2]	[2,2,2,2,2]
10^3	1	0	0	0	0	0	0
3×10^3	6	9	0	0	0	0	0
5×10^3	17	18	0	4	0	0	0
10^4	32	47	5	26	1	3	0
3×10^4	98	165	22	117	5	12	0
5×10^4	145	222	42	147	10	15	0
10^5	181	266	60	160	13	15	0
1.6×10^5	186	273	60	160	13	15	0
164802	186	273	60	160	13	15	0
164803	187	273	60	160	13	15	0
3×10^5	187	273	60	160	13	15	0
5×10^5	187	273	60	160	13	15	0
10^6	187	273	60	160	13	15	0
5×10^6	187	273	60	160	13	15	0
10^7	187	273	60	160	13	15	0
5×10^7	187	273	60	160	13	15	0
10^8	187	273	60	160	13	15	0

For real quadratic fields, some similar conclusions are given as follows:

Table 5. The 2-part of class group of 8th-order 2-Sylow subgroup

X	[8]	[4,2]	[2,2,2]
10^3	1	0	0
3×10^3	5	3	0
5×10^3	11	9	11
10^4	34	28	5
3×10^4	118	136	43
5×10^4	212	267	93
10^5	437	641	287
5×10^5	2224	3971	2354
10^6	4432	8561	5627
10^7	43074	101697	85661
10^8	412562	1131993	1131993

Table 6. The 2-part of class group of 16th-order 2-Sylow subgroup

X	[16]	[8,2]	[4,4]	[4,2,2]	[2,2,2,2]
10^3	0	0	0	0	0
5×10^3	0	0	0	0	0
10^4	1	0	0	0	0
5×10^4	38	46	2	21	0
10^5	84	137	10	63	2
3×10^5	126	569	56	312	29
5×10^5	545	1073	101	640	81
10^6	1106	2260	254	1529	249
5×10^6	5431	12180	1654	10983	2695
10^7	10771	25400	3654	25012	7590
10^8	103719	283124	48799	352085	148636

 doi:10.20944/preprints202410.0808.v1

Table 7. The 2-part of class group of 32th-order 2-Sylow subgroup

X	[32]	[16,2]	[8,4]	[8,2,2]	[4,4,2]	[4,2,2,2,2]	[2,2,2,2,2]
10^3	0	0	0	0	0	0	0
3×10^3	0	0	0	0	0	0	0
5×10^3	0	0	0	0	0	0	0
10^4	0	0	0	0	0	0	0
3×10^4	1	1	0	0	0	0	0
5×10^4	3	3	0	0	0	0	0
10^5	15	7	1	3	0	0	0
5×10^5	89	188	33	128	4	19	0
10^6	225	464	94	385	23	75	0
10^7	2689	6310	1505	6363	675	2285	142
10^8	25888	70594	18728	88398	12891	47300	6980

From the aforementioned chart, it is evident that the occurrence of 2-Sylow subgroups with class numbers 16 and 32 is relatively infrequent, and their fluctuation remains gradual as the absolute discriminant increases.

Claim 4.1. *The observations depicted in the chart do not align well with the fundamental principles of the Cohen-Lenstra conjecture as X increases. For instance, in the case of the 16th-order 2-Sylow subgroup in the class groups of imaginary quadratic fields, its frequency is notably lower for* $[16]$ *compared to* $[8,2]$.

We propose that this phenomenon may be explained by the fact that for $\mathbb{Z}/16$*, the absolute discriminant tends to have fewer prime factors than* $\mathbb{Z}/8 \oplus \mathbb{Z}/2$*. This difference in prime factorization leads to a lower frequency of occurrence for the former compared to the latter. It is crucial to distinguish between real and imaginary quadratic fields, as they exhibit significantly different characteristics. Our calculations further support this distinction, showing that only nine imaginary quadratic fields have a class number of 1. In contrast, there appears to be an infinite number of real quadratic fields (approximately 75%) with a class number of 1.*

The class number $h(K)$ of a number field is given by the following equation:

$$h(K) = \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K \sqrt{|d(K)|}},$$

where $\zeta_K(s)$ is the Dedekind zeta function, and:

$$\rho_K = \frac{\mathrm{Res}_{s=1}\zeta_K(s)}{h_K},$$

w_K is the order of the unit group of the field, and R_K is the regulator of the field K. In the case of imaginary quadratic fields, $R_K = 1$.
However, for real quadratic fields, R_K depends on the fundamental unit of the number field. For a general number field K, determining its unit group can be challenging, making the calculation of R_K difficult when using the analytical formula for class numbers. This complexity contributes to the greater uncertainties and challenges encountered with real quadratic fields compared to imaginary quadratic fields.
More generally, if p divides the order of the Galois group of the field, Cohen-Lenstra's prediction does not hold. However, in the case of an imaginary quadratic field F, Gerth provided a useful theorem for the quadratic extension of F, which can be found in [10].

4.4. On the Cohen-Lenstra Conjectures in Higher-Order Algebraic Extensions of Fields

In the previous chapter, we derived several conclusions and conjectures from analyzing and computing the 2-part of the class group in quadratic fields. In this chapter, we extend this analysis to higher-order field extensions. When the extension degree $n > 2$, there exist Cohen-Lenstra-type

 doi:10.20944/preprints202410.0808.v1

conjectures for these cases [14–16]. Here, we present the Cohen-Lenstra conjecture for algebraic field extensions of degree n.

Conjecture 4.2. ***(Proto-Cohen-Lenstra)*** *Let n be a positive integer, and let S be a permutation group acting on a set of n elements. Let r_1, r_2 satisfy $r_1 + r_2 = n$, where r_1 denotes the number of real embeddings and r_2 denotes the number of pairs of complex conjugate embeddings. Let $D(X)$ denote the set of fields K with absolute discriminant less than X and with an extension degree n, such that $n = r_1 + 2r_2$. Let p be a prime number such that p does not divide $|S|$, and let G be an Abelian p-group. Then:*

$$\lim_{X\to\infty} \frac{|\{K \in D(X) : Cl_p(K) \cong G\}|}{|D(X)|}$$

exists, and is inversely proportional to $|\mathrm{Aut}(G)| \times |G|^{r_1+r_2-1}$, where $Cl_p(K)$ denotes the p-part of the class group. However, in certain cases, this conjecture may not hold.

A Special Case: $n = 3$

Theorem 14. *Let $n = 3$ and $G = C_3$. Applying the above conjecture to this case, if $p \equiv 2 \pmod 3$, then $r_p(K) := \dim_{\mathbb{F}_p}(Cl(K)/pCl(K))$ is even for all conditions.*

Proof: Let $\mathrm{Gal}(K/\mathbb{Q}) = C_3 = \langle\sigma\rangle$ be the third-order cyclic group acting on $Cl_p(K)$. The number of ideal classes of order p is $p^{r_p(K)} - 1 \equiv 0 \pmod 3$ if and only if $r_p(K)$ is even. Therefore, if p is odd, there must be a non-trivial p-torsion ideal class C fixed by the Galois action. Hence, if $r_p(K)$ is odd, then there must be a non-trivial p-torsion ideal class C fixed by the Galois action.

In particular, there exists a non-principal ideal α of order p such that $\alpha, \alpha^\sigma, \alpha^{\sigma^2}$ are in the same ideal class. The product $\alpha^{1+\sigma+\sigma^2}$ is a principal ideal, $(N\alpha)\mathcal{O}_K$. For any $a \in \alpha$, $N\alpha = a^{1+\sigma+\sigma^2}$, and $(N\alpha)\mathcal{O}_K$ is generated as an $\mathcal{O}_K$-module.

Thus, $(N\alpha)\mathcal{O}_K \subset \alpha^{1+\sigma+\sigma^2}$. Now, the ideal $\alpha^{1+\sigma+\sigma^2}$ and $(N\alpha)\mathcal{O}_K$ have the same norm $N\alpha^3$, and therefore, they are equal. Furthermore, $(N\alpha)\mathcal{O}_K$ is principal because it is generated by $N\alpha$, and $C^3 = 1$ in $Cl_p(K)$. This contradicts $3 \nmid p$, concluding the proof.

This theorem suggests that for allowable G, the automorphism must be compatible with the Galois action, and in this case, K is a Galois field.

Refinements of the Conjecture:

Conjecture 4.3. ***(Refined Cohen-Lenstra)*** *Let ℓ be an odd prime number, and $S = C_\ell$. Let $D(X)$ be the set of C_ℓ-fields with absolute discriminant less than X. Let p be a prime different from ℓ, and let G be a finite Abelian p-group that is $\mathbb{Z}[\zeta_\ell]$-modular. Then:*

$$\lim_{X\to\infty} \frac{|\{K \in D(X) : Cl_p(K) \cong G\}|}{|D(X)|}$$

exists, and is inversely proportional to

$$|\mathrm{Aut}_{\mathbb{Z}[\zeta_\ell]}(G)| \times |G|^{\ell-1}.$$

Consider a special case where $n = 3$ and $S = C_3$. In this case, the conjecture simplifies to:

$$\lim_{X\to\infty} \frac{\sum_{K\in D(X)} p^{r_p(K)}}{|D(X)|} = \begin{cases} (1+p^{-1})^2 & \text{if } p \equiv 1 \pmod 3, \\ 1 + \frac{1}{p^2} & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

 doi:10.20944/preprints202410.0808.v1

Therefore, we have:

$$E\left[\left|\mathrm{Sur}_{\zeta_\ell}(Cl(K),G)\right|\right] = \lim_{X\to\infty} \frac{\sum_{K\in D(X)} p^{r_p(K)-1}}{|D(X)|}.$$

This study extends the Cohen-Lenstra conjecture to infinite algebraic extensions $K/\mathbb{Q}$, demonstrating that the distribution of finite p-class groups is significantly influenced by the structure of the automorphism group $\mathrm{Aut}_{\mathbb{Z}[\zeta_\ell]}(G)$. Specifically, for a finite group G, the probability that the p-class group $Cl_p(K)$ of a number field K from a set $D(X)$ is isomorphic to G adheres to:

$$\lim_{X\to\infty} \frac{|\{K \in D(X) : Cl_p(K) \cong G\}|}{|D(X)|} = \frac{1}{|\mathrm{Aut}_{\mathbb{Z}[\zeta_\ell]}(G)| \times |G|^{\ell-1}}.$$

This result highlights that the distribution of p-class groups depends not only on the order and structure of G, but also on the size of its automorphism group. Specifically, as the size of the automorphism group $\mathrm{Aut}_{\mathbb{Z}[\zeta_\ell]}(G)$ increases, the likelihood of finding $Cl_p(K) \cong G$ decreases, with this probability diminishing rapidly with the increasing order of G.

We predict that the Cohen-Lenstra conjecture will continue to hold in broader algebraic settings, particularly in infinite Galois extensions, though several factors will influence the distribution of p-class groups:

1. **Ramification of Primes**: The behavior of primes, particularly p, in the extension will critically affect the class group structure. In extensions where p splits or ramifies completely, deviations from the conjecture's predictions may occur.
2. **Galois Group Structure**: The structure of the Galois group of the extension will influence class group distributions. Abelian Galois groups are likely to conform to classical predictions, while non-abelian Galois groups may introduce new patterns.
3. **Effect of Automorphism Groups**: The significance of automorphism groups $\mathrm{Aut}_{\mathbb{Z}[\zeta_\ell]}(G)$ increases in infinite extensions. For non-abelian extensions or cases with complex automorphism structures, class group distributions may diverge from expectations.

Overall, while the distribution of p-class groups is expected to follow the inverse proportionality described above, factors such as ramification and Galois group structure will play crucial roles. These insights generalize the Cohen-Lenstra conjecture to more complex algebraic extensions, providing new perspectives on class group distributions.

5. Conclusions

The exploration of the 2-part of class groups in imaginary quadratic fields reveals intricate patterns influenced by genus theory and the splitting behavior of primes. While the Cohen-Lenstra heuristics provide a valuable framework, deviations occur due to these underlying arithmetic factors.

Further research could involve:

1. Extending computational data to larger discriminants and other families of number fields.
2. Investigating the impact of higher-order residue symbols on the structure of class groups.
3. Developing refined heuristics that account for the influence of genus theory and other arithmetic invariants.

Determining the class number of general number fields remains a significant challenge in algebraic number theory. The Cohen-Lenstra conjectures address class numbers for various number fields, including real and imaginary quadratic fields, but remain largely unproven, especially for higher-order extensions.

This study investigates the 2-part of class groups in imaginary quadratic fields, providing both theoretical and computational insights. We have examined the extent to which the Cohen-Lenstra heuristics apply to these fields, noting deviations due to genus theory and other arithmetic properties.

 doi:10.20944/preprints202410.0808.v1

Our results contribute to a deeper understanding of class group distributions and highlight areas for future exploration.

Funding: This work was supported by the (K42022003) Shi Haiping Research Start-up Fund for Talent Introduction, Guangzhou Jiaotong University.

References

1. K. Q. Feng, *Algebraic Number Theory*, Harbin Institute of Technology Press, 2018.
2. K. J. Fukuzaki, "Definability of the ring of integers in some infinite algebraic extensions of the rationals," *Mathematical Logic Quarterly*, vol. 58, no. 4-5, pp. 317-332, 2012.
3. J. A. Buchmann and H. W. Lenstra, "Approximating rings of integers in number fields," *Journal de théorie des nombres de Bordeaux*, vol. 6, no. 2, pp. 221-260, 1994.
4. A. Quadrat, "On a generalization of the Youla–Kučera parametrization. Part I: The fractional ideal approach to SISO systems," *Systems & Control Letters*, vol. 50, no. 2, pp. 135-148, 2003.
5. W. Heinzer, "Integral domains in which each non-zero ideal is divisorial," *Mathematika*, vol. 15, no. 2, pp. 164-170, 1968.
6. H. Cohen and H. Lenstra, "Heuristics on class groups of number fields," in *Number Theory*, vol. 1068, Lecture Notes in Mathematics, pp. 33-62, Springer, Berlin, 1984.
7. H. M. Stark, "A Complete Solution of the Class Number Problem for Imaginary Quadratic Fields with Class Number 1," *Journal of Number Theory*, vol. 2, no. 1, pp. 51-76, 1970.
8. J. Rotman, *A Basic Course of Modern Algebra*, China Machine Press, 2007.
9. E. T. Hecke, *Lectures on the Theory of Algebraic Numbers*, Vol. 77, Springer Science & Business Media, 2013.
10. F. Gerth, "The 4-class ranks of quadratic extensions of certain imaginary quadratic fields," *Annals of Mathematics*, 1989.
11. A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1970.
12. J. Lengler, "The Cohen–Lenstra heuristic: methodology and results," *Annals of Mathematics*, 2007.
13. K. Q. Feng, "Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture."
14. H. Cohen and H. W. Lenstra Jr., "Heuristics on class groups of number fields," in *Number Theory Noordwijkerhout 1983: Proceedings of the Journées Arithmétiques held at Noordwijkerhout, The Netherlands July 11–15, 1983*, Springer Berlin Heidelberg, 2006, pp. 33-62.
15. M. Bhargava, "The density of discriminants of quintic rings and fields," *Annals of Mathematics*, 2010, pp. 1559-1591.
16. J. S. Ellenberg and A. Venkatesh, "The number of extensions of a number field with fixed degree and bounded discriminant," *Annals of Mathematics*, 2006, pp. 723-741.