On the 2-part of class groups and Diophantine equations

Yik Tung Chan

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
of
University College London.

Department of Mathematics
University College London

10^{th} August, 2020

I, Yik Tung Chan, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the work.

Abstract

This thesis contains several pieces of work related to the 2-part of class groups and Diophantine equations. We first give an overview of some techniques known in computing the 2-part of the class groups of quadratic number fields, including the use of the Rédei symbol and Rédei reciprocity in the study of the 8-rank of the class groups of quadratic fields. We review the construction of governing fields for the 8-rank by Corsman and extend a proof of Smith on the distribution of the 8-rank for imaginary quadratic fields, to real quadratic fields, conditional on the general Riemann hypothesis.

In joint work with Peter Koymans, Djordjo Milovic, and Carlo Pagano, we improve a previous lower bound by Fouvry and Klüners, on the density of the solvability of the negative Pell equation over the set of squarefree positive integers with no prime factors congruent to 3 mod 4. We show how Rédei reciprocity allows us to apply techniques introduced by Smith to obtain this improvement.

In joint work with Djordjo Milovic, using Kuroda's formula, we study the average behaviour of the unit group index in certain families of totally real biquadratic fields $\mathbb{Q}(\sqrt{p}, \sqrt{d})$ parametrised by the prime p.

In joint work with Christine McMeekin and Djordjo Milovic, we study certain cyclic totally real number fields K, in which we attach a quadratic symbol $\mathrm{spin}(\mathfrak{a}, \sigma)$ to each odd prime ideal $\mathfrak{a}$ and each non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. We prove a formula for the density of primes ideals $\mathfrak{p}$ such that $\mathrm{spin}(\mathfrak{p}, \sigma) = 1$ for all non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Finally, we study integral points on the quadratic twists $\mathcal{E}_D : y^2 = x^3 - D^2x$ of the congruent number curve. We show that the number of non-torsion integral points on $\mathcal{E}_D$ is $\ll (3.8)^{\mathrm{rank}\, \mathcal{E}_D(\mathbb{Q})}$ and its average is bounded above by 2. We deduce that the system of simultaneous Pell equations $aX^2 - bY^2 = d,\ bY^2 - cZ^2 = d$

for pairwise coprime positive integers a, b, c, d, has at most $\ll (3.6)^{\omega(abcd)}$ integer solutions.

Impact Statement

This thesis showcases several pieces of work relating to the arithmetic statistics of class groups, elliptic curves, and Diophantine equations. We hope that this could lead to new insights in investigating other connections between different objects in number theory that have not been fully explored.

We study several interesting questions in arithmetic statistics. We show how some new results in the area can be applied to existing unsolved problems in the field. For example, we apply recent work by Smith on the distribution of the 2-part of class groups to improve a current lower bound to the density of the solvability of the negative Pell equation, working towards a conjecture by Stevenhagen in the field. We ask a new question on the arithmetic statistics of the unit group of biquadratic fields, and provide an answer in a special case using Kuroda's formula and our understanding of the 2-part of class groups.

In the study of the 8-rank of class groups of quadratic fields, we give explicit constructions of minimally unramified C_4-extensions, which may facilitate further study in class fields.

Furthermore, we give applications of the study of elliptic curves to Diophantine equations. We apply methods from Diophantine approximation to study the number integral points on elliptic curves, and show how results obtained for elliptic curves have implications for Diophantine equations such as simultaneous Pell equations.

Acknowledgements

I am grateful to my supervisor, Andrew Granville, for providing the guidance, support and encouragement I needed throughout my research.

I thank Djordjo Milovic for introducing me to the research of class groups, and led me to numerous interesting problems in the area. I would also like to thank Peter Koymans and Carlo Pagano for many insightful discussions that improved my understanding on the subject. My gratitude extends to my academic siblings Ardavan Afshar, Sam Porritt and Niki Kalaydzhieva for always being there to exchange ideas. I also thank my examiners Samir Siksek and Vladimir Dokchitser for their careful reading and useful comments.

My studies were funded by European Research Council grant agreement No. 670239 and UCL John Hawkes Scholarship. I am grateful to everyone at UCL mathematics department and LSGNT for providing the atmosphere and community that facilitated my reaserch.

Contents

Introduction

The Pell equation is the quadratic Diophantine equation having the form

$$x^2 - Dy^2 = 1, \tag{0.1}$$

where $D > 0$ is a given squarefree integer and we are interested in finding integer solutions x, y. The negative Pell equation is the analogous equation

$$x^2 - Dy^2 = -1. \tag{0.2}$$

With the factorisation $x^2 - Dy^2 = (x + y\sqrt{D})(x - y\sqrt{D})$, it is natural to study the unit group of $\mathbb{Q}(\sqrt{D})$. We know from Dirichlet's unit theorem, that the unit group of a real quadratic field $\mathbb{Q}(\sqrt{D})$ must have the form

$$\langle -1 \rangle \times \langle \epsilon_D \rangle,$$

where ϵ_D is the *fundamental unit*, i.e. the minimal unit in K greater than 1. Therefore (0.1) is always solvable and possesses infinitely many solutions.

However this is not the case for (0.2). Taking (0.2) modulo any prime $p \mid D$, we see that -1 has to be a quadratic residue modulo p, so D cannot be divisible by any prime $p \equiv 3 \bmod 4$ if (0.2) is solvable. However the condition that any $p \mid D$ is not congruent to 3 mod 4 is not sufficient in determining the solvability of (0.2). For example, there are no solutions when D is $34, 146, 178, 194, 205, 221, \cdots$. The equation (0.2) is solvable if and only if there is an element with norm -1 in the unit group of $\mathbb{Q}(\sqrt{D})$. This happens precisely when the ordinary class group $\mathbf{Cl}_D$ and the narrow class group $\mathbf{C}_D$ of $\mathbb{Q}(\sqrt{D})$ coincide. The odd parts of $\mathbf{Cl}_D$ and $\mathbf{C}_D$ are always isomorphic, so it suffices to study the 2-parts of $\mathbf{Cl}_D$ and $\mathbf{C}_D$. In recent

years, much progress has been made in the study of the distribution of 2-parts of class groups of quadratic number fields, most notably by Fouvry and Klüners [30] and Smith [81].

We start off in Chapter 1, by giving an overview of some of the techniques known in computing the 2-part of the class groups of quadratic number fields. Class field theory establishes the existence of the class field H_D and the narrow class field H_D^+, which are the fields that satisfy $\mathbf{Cl}_D \cong \mathrm{Gal}(H_D/\mathbb{Q}(\sqrt{D}))$ and $\mathbf{C}_D \cong \mathrm{Gal}(H_D^+/\mathbb{Q}(\sqrt{D}))$. The field H_D^+ is the maximal abelian extension of $\mathbb{Q}(\sqrt{D})$ that is unramified at all finite places, and H_D is maximal totally real subfield of H_D^+. Therefore we can study the 2-part of the class group by constructing unramified 2-power extensions of $\mathbb{Q}(\sqrt{D})$.

In Chapter 2, we give an explicit construction of minimally ramified cyclic degree 4 extensions of quadratic fields. This generalises the construction of cyclic degree 4 extensions of $\mathbb{Q}(\sqrt{D})$ that lie in its narrow class field H_D^+, considered in the study of the 4-rank of $\mathbf{C}_D$. With this we define the Rédei symbol and give a proof of Rédei reciprocity. The Rédei symbol, together with Rédei reciprocity, originated from Rédei's [65] classical work on the 8-rank of $\mathbf{C}_D$, and were generalised by Corsman [27]. The Rédei symbol is a triple $[a, b, c]$, taking values in $\{\pm 1\}$, where (a, b) defines a cyclic degree 4 extension $L_{a,b}/\mathbb{Q}(\sqrt{D})$ that is minimally ramified, i.e. unramified at all prime ideals not dividing $2ab$, and c specifies an class in $\mathbf{C}_D[2]$, represented by an ideal $\mathbf{c}$ of norm $|c|$. The Rédei symbol is by definition multiplicative in its last entry, and the value of $[a, b, c]$ depends on the splitting of $\mathbf{c}$ in $L_{a,b}/\mathbb{Q}(\sqrt{D})$ when $\mathbf{c}$ is a prime ideal. Rédei reciprocity shows that the entries of the Rédei symbol are symmetric, and this allows us to extend multiplicativity to all three entries.

In Chapter 3, we show how Rédei reciprocity can be applied to the study of the 8-rank of the narrow class groups of quadratic fields. It allows us to construct minimal governing fields for the 8-rank, as shown by Corsman [27], which are fields $\Omega_3(d)$ such that the 8-rank of $\mathbf{C}_{dp}$ is determined by the splitting of p in $\Omega_3(d)/\mathbb{Q}$. Then we extend a proof of Smith [80] in obtaining the distribution of the 8-rank for imaginary quadratic fields, to real quadratic fields, conditional on the general Riemann hypothesis. Let $\mathcal{D}(N)$ be the set of positive squarefree integer less than N.

Theorem 3.1. *Assume the general Riemann hypothesis. For any $m \geq j \geq 0$ and any $\delta \in \{\pm 1\}$, we have*

$$\lim_{N\to\infty} \frac{\#\{\delta \cdot D \in \mathcal{D}(N) : \operatorname{rk}_4 \mathbf{C}_D = m,\ \operatorname{rk}_8 \mathbf{C}_D = j\}}{\#\{\delta \cdot D \in \mathcal{D}(N) : \operatorname{rk}_4 \mathbf{C}_D = m\}} = \begin{cases} \operatorname{Prob}(j \mid m, m+1) & \text{if } \delta = 1, \\ \operatorname{Prob}(j \mid m, m) & \text{if } \delta = -1, \end{cases}$$

where

$$\operatorname{Prob}(j \mid m, n) \coloneqq \frac{\#\{M \in \operatorname{Mat}_{m\times n}(\mathbb{F}_2) : \operatorname{corank}(M) = j\}}{\#\operatorname{Mat}_{m\times n}(\mathbb{F}_2)}$$

and $\operatorname{Mat}_{m\times n}(\mathbb{F}_2)$ denotes the space of $m \times n$ matrices over $\mathbb{F}_2$.

In Chapter 4, we consider the solvability of the negative Pell equation over the set

$$\mathcal{P} \coloneqq \{D \text{ positive squarefree integer} : p \not\equiv 3 \bmod 4 \text{ for all primes } p \mid D\}.$$

This is the set of squarefree $D > 0$ such that $\operatorname{rk}_2 \mathbf{C}_D = \operatorname{rk}_2 \mathbf{Cl}_D$. Stevenhagen [86] conjectured that the natural density of $D \in \mathcal{P}$ such that the negative Pell equation is solvable, is $58.057\ldots\%$. Fouvry and Klüners [31, 32] showed that the density lies between $52.427\ldots\%$ and $\frac{2}{3}$. Their lower bound comes from the density of $D \in \mathcal{P}$ such that such that

$$\operatorname{rk}_4 \mathbf{Cl}_D = \operatorname{rk}_4 \mathbf{C}_D \in \{0, 1\} \text{ and } \operatorname{rk}_8 \mathbf{C}_D = 0,$$

and their upper bound comes from the density of $D \in \mathcal{P}$ such that

$$\operatorname{rk}_4 \mathbf{C}_D = \operatorname{rk}_4 \mathbf{Cl}_D + 1.$$

In joint work with Peter Koymans, Djordjo Milovic, and Carlo Pagano [19], we improve the lower bound using new techniques introduced by Smith [81], together with some new algebraic results relying on Rédei reciprocity. More precisely, let $\mathcal{P}(N) \coloneqq \{D < N : D \in \mathcal{P}\}$, $\mathcal{P}^-(N) \coloneqq \{D \in \mathcal{P}(N) : (0.2) \text{ is solvable for } D\}$, and $\alpha \coloneqq \prod_{j=1}^{\infty}(1 + 2^{-j})^{-1} = 0.41942\ldots$, we prove the following.

Theorem 4.1. *We have*

$$\liminf_{N\to\infty} \frac{|\mathcal{P}^-(N)|}{|\mathcal{P}(N)|} \geq \alpha\beta = 0.53822\ldots,$$

where

$$\beta = \sum_{n=0}^{\infty} 2^{-n(n+3)/2} = 1.28325\ldots > 5/4.$$

Our improved lower bound comes from the density of $D \in \mathcal{P}$ such that

$$\mathrm{rk}_4\, \mathbf{Cl}_D = \mathrm{rk}_4\, \mathbf{C}_D = n \text{ and } \mathrm{rk}_8\, \mathbf{C}_D = 0.$$

In Chapter 5, we proceed to study a generalisation of the Pell equation. This chapter contains results from joint work with Djordjo Milovic [21]. Fixing any d in the set

$$\mathcal{R} \coloneqq \{d \in \mathbb{Z}_{>0} \text{ squarefree} : \mathrm{rk}_2\, \mathbf{Cl}_d = \mathrm{rk}_2\, \mathbf{C}_d,\ \mathrm{rk}_4\, \mathbf{C}_d = 0\},$$

we study how often an equation

$$x^2 - dy^2 = 4\epsilon_p \tag{0.3}$$

is solvable for $x, y \in \mathcal{O}_{\mathbb{Q}(\sqrt{p})}$, where ϵ_p is the fundamental unit of $\mathbb{Q}(\sqrt{p})$, as we vary p in certain congruence classes. This involves studying the unit groups of the fields $k_1 = \mathbb{Q}(\sqrt{p})$, $k_2 = \mathbb{Q}(\sqrt{d})$, $k_3 = \mathbb{Q}(\sqrt{dp})$, $K = \mathbb{Q}(\sqrt{d}, \sqrt{p})$. Under our choices of d and p, the unit group index of K is $Q(K) \coloneqq [\mathcal{O}_K^\times : \mathcal{O}_{k_1}^\times \mathcal{O}_{k_2}^\times \mathcal{O}_{k_3}^\times] \in \{1, 2\}$, and (0.3) is solvable if and only if $Q(K) = 2$. We make use of Kuroda's class number formula [51, 48, 49] to translate this problem to the setting of class groups. The formula states that

$$\hbar(K) = \frac{1}{4} Q(K) \cdot \hbar(k_1)\hbar(k_2)\hbar(k_3),$$

where $\hbar(K)$ denotes the size of the 2-part of $\mathbf{Cl}_K$. We use techniques similar to that used in Chapter 2, to construct the maximal 2-power subfield $\mathcal{H}_{d,p}^+$ of the narrow Hilbert class field of K. Define $m_{d,p} \coloneqq \#\{q \mid d : q \text{ splits completely in } \mathbb{Q}(\sqrt{p})\}$, and take

$$\mathcal{P}_{d,m} \coloneqq \{p \equiv 1 \bmod 4 \text{ prime} : p \nmid d,\ \mathrm{rk}_4\, \mathbf{C}_{dp} = 0,\ m_{d,p} = m\},$$

and $\mathcal{P}_{d,m}(N) \coloneqq \{p \in \mathcal{P}_{d,m} : p < N\}$. Writing $\mathcal{K}_{d,p} \coloneqq \mathbb{Q}(\sqrt{d}, \sqrt{p})$, we expect that the density of $p \in \mathcal{P}_{d,m}$ such that $Q(\mathcal{K}_{d,p}) = 2$ to behave as follows.

Conjecture 5.2. *For $d \in \mathcal{R}$, we have*

$$\lim_{N\to\infty} \frac{\#\{p \in \mathcal{P}_{d,m}(N) : \ Q(\mathcal{K}_{d,p}) = 2\}}{\#\mathcal{P}_{d,m}(N)} = \frac{1}{2^{t-1}},$$

where $t = \omega(d)$.

We are able to prove our conjecture in the cases $m = t - 1$ and $m = t - 2$.

Theorem 5.3. *Suppose $d \in \mathcal{R}$ and let $t = \omega(d)$. Then the map*

$$\mathcal{P}_{d,m} \to \{1, 2\}, \qquad p \mapsto Q(\mathcal{K}_{d,p})$$

is Frobenian for $m = t - 1$ and $m = t - 2$. Moreover, Conjecture 5.2 holds for $m = t - 1$ and $m = t - 2$, and, for all $m \in \{0, 1, \ldots, t - 3\}$, we have

$$\lim_{N\to\infty} \frac{\#\{p \in \mathcal{P}_{d,m}(N) : \ Q(\mathcal{K}_{d,p}) = 2\}}{\#\mathcal{P}_{d,m}(N)} \leq \frac{1}{2^m}.$$

Chapter 6 is based on joint work with Christine McMeekin and Djordjo Milovic [20]. We study totally real cyclic odd degree extensions $K/\mathbb{Q}$, which have odd class number, and such that every totally positive unit is the square of a unit. Given a non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and an odd ideal $\mathfrak{a}$, the *spin* of $\mathfrak{a}$ (with respect to σ), is defined as the quadratic residue symbol

$$\mathrm{spin}(\mathfrak{a}, \sigma) \coloneqq \left(\frac{\alpha}{\mathfrak{a}^\sigma}\right),$$

where α is any totally positive generator of the principal ideal $\mathfrak{a}^h$, and h is the class number of K. The spin was previously studied by Friedlander, Iwaniec, Mazur, and Rubin [33]. Conditional on a standard conjecture on short character sums (Conjecture C_η in Chapter 6), we prove a formula depending only on the degree $n = [K : \mathbb{Q}]$, for the density of primes p such that $\mathrm{spin}(\mathfrak{p}, \sigma) = 1$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}$ holds for some prime ideal $\mathfrak{p}$ lying above p, over the set of primes that split

completely in $K/\mathbb{Q}$. We can state our theorem more precisely. Define

$$\begin{aligned} S &\coloneqq \{p \text{ prime} : p \text{ splits completely in } K/\mathbb{Q}\},\\ S_{\pm} &\coloneqq \{p \in S : p \equiv \pm 1 \bmod 4\mathbb{Z}\},\\ F &\coloneqq \{p \in S : \operatorname{spin}(\mathfrak{p}, \sigma) = 1 \text{ for all } \sigma \in \operatorname{Gal}(K/\mathbb{Q}) \setminus \{1\}\},\\ F_{\pm} &\coloneqq S_{\pm} \cap F, \end{aligned}$$

where $\mathfrak{p}$ denotes a prime ideal in K lying above p. For sets of primes $A \subseteq B$, we define the restricted density of A (restricted to B) to be

$$d(A|B) \coloneqq \lim_{N\to\infty} \frac{\#\{p < N : p \in A\}}{\#\{p < N : p \in B\}}.$$

Theorem 6.4. *Let K be a cyclic totally real number field of odd degree n over $\mathbb{Q}$ with odd class number, such that every totally positive unit is the square of a unit, and such that 2 is inert in $K/\mathbb{Q}$. Assume Conjecture C_η holds for $\eta = \frac{2}{n(n-1)}$. For $k \neq 1$ dividing n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Then for a fixed sign $\pm$,*

$$d(F_{\pm}|S_{\pm}) = \frac{s_{\pm}}{2^{3(n-1)/2}}, \quad \text{and} \quad d(F|S) = \frac{s_+ + s_-}{2^{(3n-1)/2}}$$

where

$$s_+ \coloneqq 1 + \prod_{\substack{k|n,\ k\neq 1\\ d_k \text{ odd}}} 2^{\frac{\phi(k)}{2d_k}} \left(\prod_{\substack{k|n,\ k\neq 1\\ d_k \text{ odd}}} 2^{\frac{\phi(k)}{2}} - 1 \right),$$

and

$$s_- \coloneqq \prod_{\substack{k|n,\ k\neq 1\\ d_k \text{ even}}} (2^{\frac{d_k}{2}} + 1)^{\frac{\phi(k)}{d_k}} \prod_{\substack{k|n,\ k\neq 1\\ d_k \text{ odd}}} (2^{d_k} - 1)^{\frac{\phi(k)}{2d_k}},$$

where ϕ denotes the Euler's totient function.

At first sight, it might seem that the probability that $\operatorname{spin}(\mathfrak{p}, \sigma) = 1$ holds for all $\sigma \in \operatorname{Gal}(K/\mathbb{Q}) \setminus \{1\}$, should be $1/2^{n-1}$, since there are $n-1$ quadratic symbol conditions to satisfy. However, it turns out that not all of these symbols behave independently. More precisely, it was shown in [33] that $\operatorname{spin}(\mathfrak{p}, \sigma)\operatorname{spin}(\mathfrak{p}, \sigma^{-1})$ depends on the Hilbert symbols $(\alpha, \alpha^\sigma)_v$ at even places v, where α is any totally positive generator of $\mathfrak{p}^h$. Assuming that 2 is inert in $K/\mathbb{Q}$, we are able to give a combinatorial argument to study the behaviour of the condition $(\alpha, \alpha^\sigma)_2 = 1$.

In Chapter 7, we explore an application of the study of elliptic curves to a special type of simultaneous generalised Pell equations.

Theorem 7.6. *Let a, b, c, d be pairwise coprime positive integers and set $D = abcd$. Then for any sufficiently large D, the system of equations*

$$aX^2 - bY^2 = d, \qquad bY^2 - cZ^2 = d$$

has at most $15+(1.89)^{r+19r^{1/3}} \leq 15+(3.58)^{\omega(D)+12\omega(D)^{1/3}}$ *solutions* $(X, Y, Z) \in \mathbb{Z}^3_{>0}$, *where* $r \coloneqq \operatorname{rank} \mathcal{E}_D(\mathbb{Q})$.

The solutions to the system of equations in Theorem 7.6 can be mapped explicitly to integral points on the congruent number curve

$$\mathcal{E}_D : y^2 = x^3 - D^2x.$$

Then Theorem 7.6 follows from an upper bound on the number of integral points on $\mathcal{E}_D$.

Theorem 7.1. *We have*

$$\#\mathcal{E}_D(\mathbb{Z}) \ll (3.8)^{\operatorname{rank} \mathcal{E}_D(\mathbb{Q})}.$$

We also prove an average result on the number of integral points. Let $\mathcal{T}_D$ denote the set of torsion points in $\mathcal{E}_D(\mathbb{Q})$, and $\mathcal{D}(N)$ denote the set of squarefree integers less than N.

Theorem 7.5. *We have*

$$\limsup_{N\to\infty} \frac{1}{\#\mathcal{D}(N)} \sum_{D\in\mathcal{D}(N)} \#(\mathcal{E}_D(\mathbb{Z}) \setminus \mathcal{T}_D) \leq 2.$$

If we further assume the abc conjecture, the upper bound can be improved to 1.

Non-torsion integral points come in pairs of the form $(x, \pm y)$. It follows from Smith's work [81] that almost all $\mathcal{E}_D$ has rank 0 or 1. The upper bound in Theorem 7.5 comes from the possible existence of a pair of small points in the range $D^2/(\log D)^{12+\epsilon} < x < D^{2+\epsilon}$, and a pair of large points of size $x >$

$\exp(\exp(\frac{23}{12}\sqrt{\log D}))$ left from an application of Roth's Theorem, which we are unable to eliminate on most curves of rank 1, except by using the *abc*-conjecture.

Chapter 1

The 2-part of class groups of quadratic number fields

Class groups first appeared in the theory of binary quadratic forms. An integral quadratic form has discriminant $D := b^2 - 4ac$. Gauss defined a composition law on quadratic forms of a fixed discriminant. The set of equivalence classes of quadratic forms is then a finite abelian group. The formulation of the concept of ideals by Dedekind, allows class groups to be described in terms of ideals. The class group measures how far a ring is from being a principal ideal domain.

Gauss made several conjectures in *Disquisitiones Arithmeticae* [34]. The first being the following statement later proved by Heilbronn [39].

Theorem. *The class number of $\mathbb{Q}(\sqrt{D})$ tends to infinity as $D \to -\infty$.*

This implies that there are only finitely many imaginary quadratic fields with any given number. For low class numbers, Gauss gave tables of fields, which he conjectured to contain all the possible imaginary quadratic fields with the given class numbers. Providing a complete list of imaginary quadratic fields with a given class number became known as the "class number problem". For class number 1, this was solved independently by Baker [4], Heegner [38] and Stark [84].

In contrast, much less is known for real quadratic fields. The following conjecture is still open.

Conjecture. *There are infinitely many real quadratic fields with class number one.*

The p-part of an abelian group is the subgroup containing all elements with p-power order. The fundamental theorem of finite abelian groups states that any

finite abelian group is isomorphic to a direct product of cyclic groups of prime-power order. Therefore the isomorphism class of a given abelian group is determined by its p-parts. Given a finite abelian group G and an integer $k \geq 1$, the p^k-rank of G is defined as $\mathrm{rk}_{p^k} G = \dim_{\mathbb{F}_p}(p^{k-1}G/p^kG)$. The non-increasing sequence of non-negative integers $\{\mathrm{rk}_{p^k} G\}_{k\geq 1}$ determines the isomorphism class of the p-primary part of G.

We are mainly interested in studying the 2-part of the class groups of quadratic fields. We review the techniques known in computing the 2^k-ranks of the class group of quadratic fields.

Let C_n denote the cyclic subgroup of order n, V_4 denote the Klein four group, and D_8 denote the Dihedral group of order 8.

1.1 Class groups

For a number field K, the narrow class group is defined as $\mathbf{C}_K = J_K/P_K^+$ and the ordinary class group is defined as $\mathbf{Cl}_K = J_K/P_K$, where

$$\begin{aligned} J_K &\coloneqq \{\text{fractional ideals of } K\}, \\ P_K &\coloneqq \{\text{principal fractional ideals of } K\}, \text{ and} \\ P_K^+ &\coloneqq \{\text{totally positive principal fractional ideals of } K\}. \end{aligned}$$

The class groups $\mathbf{C}_K$ and $\mathbf{Cl}_K$ are both finite abelian groups. There exists the following short exact sequence

$$0 \to P_K/P_K^+ \to \mathbf{C}_K \to \mathbf{Cl}_K \to 0. \tag{1.1}$$

We say $\alpha \in K$ is *totally positive*, if $\sigma(\alpha) > 0$ for all real embeddings $\sigma : K \hookrightarrow \mathbb{R}$. A principal ideal is *totally positive* if it has a generator that is totally positive.

1.1.1 Some class field theory

Suppose L/K is a Galois extension. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ unramified in L and $\mathfrak{P}$ be a prime in $\mathcal{O}_L$ containing $\mathfrak{p}$. The Artin symbol is the unique Frobenius element $\left(\frac{L/K}{\mathfrak{P}}\right)$ in $\mathrm{Gal}(L/K)$ [28, Lemma 5.19, p.95] such that for any $\alpha \in \mathcal{O}_L$, we have

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) = \alpha^{\mathrm{Norm}(\mathfrak{p})} \bmod \mathfrak{P}.$$

The Artin symbol satisfies some useful properties [28, Corollary 5.21, p.95]. First of all, it encodes information about the splitting of a given prime. A prime $\mathfrak{p}$ splits completely in L/K if and only if $\left(\frac{L/K}{\mathfrak{P}}\right) = 1$. Moreover, for any $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\left(\frac{L/K}{\sigma\mathfrak{P}}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}.$$

We denote by $\left(\frac{L/K}{\mathfrak{p}}\right)$ the Frobenius conjugacy class of $\left(\frac{L/K}{\mathfrak{P}}\right)$ in the Galois group $\mathrm{Gal}(L/K)$. When $\left(\frac{L/K}{\mathfrak{p}}\right)$ contains only one element, by abuse of notation we write $\left(\frac{L/K}{\mathfrak{p}}\right)$ to stand for the unique element in the conjugacy class. For example, when L/K is an abelian extension, $\left(\frac{L/K}{\mathfrak{P}}\right)$ is the only element in $\left(\frac{L/K}{\mathfrak{p}}\right)$, and we write

$$\left(\frac{L/K}{\mathfrak{p}}\right) \coloneqq \left(\frac{L/K}{\mathfrak{P}}\right).$$

If L/K is abelian and p splits completely in $K/\mathbb{Q}$, $\left(\frac{L/\mathbb{Q}}{p}\right)$ contains only one element, so we write

$$\left(\frac{L/\mathbb{Q}}{p}\right) \coloneqq \left(\frac{L/K}{\mathfrak{P}}\right),$$

where $(p) = \mathfrak{P} \cap \mathcal{O}_L$.

When K is totally real, the Artin symbol $\left(\frac{L/K}{\infty}\right)$ is defined as the Frobenius at infinity, i.e. the identity map if L/K is totally real, and complex conjugation otherwise.

1.1.2 Hilbert class field

Suppose L/K is a abelian extension unramified at all finite places. Then we can extend the Artin symbol to all ideals in $\mathcal{O}_K$ by multiplicativity

$$\left(\frac{L/K}{\cdot}\right) : J_K \to \mathrm{Gal}(L/K) \qquad \prod_j \mathfrak{p}_j^{e_j} \mapsto \prod_j \left(\frac{L/K}{\mathfrak{p}_j}\right)^{e_j}.$$

Class field theory tells us that the Artin symbol induces isomorphisms between class groups and Galois groups.

Proposition 1.1 (Artin reciprocity)**.** *[43, p.228, 242] Let K be a number field. Denote H^+ the maximal abelian extension of K unramified at all finite primes and H the maximal abelian extension of K unramified at all finite and infinite primes.*

Then

$$\left(\frac{H^+/K}{\cdot}\right) : \mathbf{C}_K \xrightarrow{\cong} \mathrm{Gal}(H^+/K)$$

and

$$\left(\frac{H/K}{\cdot}\right) : \mathbf{Cl}_K \xrightarrow{\cong} \mathrm{Gal}(H/K).$$

We call H^+ the *narrow Hilbert class field* and H the *ordinary Hilbert class field*. Given any Galois extension $K/\mathbb{Q}$, the class fields H^+ and H are always Galois over $\mathbb{Q}$ since any conjugate fields are also unramified.

The following proposition is useful for constructing unramified extensions.

Proposition 1.2 ([37, Chapter V, Theorem 120])**.** *Let L be a number field and suppose that $\beta \in \mathcal{O}_L \setminus \mathcal{O}_L^2$ is coprime to 2. Given a rational prime p, $L(\sqrt{\beta})/L$ is unramified at any prime $\mathfrak{p}$ in L above p if and only if the following are satisfied:*

(i) $\mathrm{ord}_{\mathfrak{p}}\, \beta\mathcal{O}_L$ *is even at every $\mathfrak{p}$ above p, and*

(ii) further that $X^2 \equiv \beta \bmod 4$ is solvable for some $X \in \mathcal{O}_L$ if $p = 2$.

Theorem 1.3 (Monodromy theorem [59, p. 265, Corollary 2 of Proposition 6.8])**.** *Let L/K be a normal finite extension of an algebraic number field. The subgroup of* $\mathrm{Gal}(L/K)$ *generated by all inertia groups of prime ideals of $\mathcal{O}_L$ corresponds to the maximal subfield of L, unramified over K.*

1.1.3 Dual class group

The dual class group $\hat{\mathbf{C}}_K$ is defined as $\mathrm{Hom}(\mathbf{C}_K, \mathbb{T})$, where $\mathbb{T}$ is the circle group $\{z \in \mathbb{C} : |z| = 1\}$. Since $\mathbf{C}_K$ is a finite abelian group, we have $\hat{\mathbf{C}}_K \cong \mathbf{C}_K$.

Given some $\psi \in \hat{\mathbf{C}}_K$, since $\ker \psi$ is a subgroup of the abelian group $\mathrm{Gal}(H^+/K)$, we can take L to be the subfield of H^+ such that $\ker \psi \cong \mathrm{Gal}(H^+/L)$. If ψ has exact order m, then $\mathrm{Gal}(L/K) \cong C_m$. We call L the *field of definition* of ψ. In other words, L is the smallest field such that one can write

$$\psi : \mathbf{C}_K \xrightarrow{\cong} \mathrm{Gal}(H^+/K) \twoheadrightarrow \mathrm{Gal}(L/K) \cong C_m \hookrightarrow \mathbb{T},$$

where the first isomorphism is Artin reciprocity. For ease of notation we simply write $\psi = \left(\frac{L/K}{\cdot}\right)$ as an element in $\hat{\mathbf{C}}_K$ by identifying the image of $\left(\frac{L/K}{\cdot}\right)$ with $\{z \in \mathbb{C} : |z| = 1,\ z^m = 1\} \subset \mathbb{T}$.

1.2 Quadratic number fields

Here and henceforth, take K to be the quadratic number field $\mathbb{Q}(\sqrt{D})$, where $D \neq 1$ is a squarefree integer. The discriminant of $K/\mathbb{Q}$ is given by

$$\Delta_K = \begin{cases} D & \text{if } D \equiv 1 \bmod 4, \\ 4D & \text{if } D \equiv 2 \text{ or } 3 \bmod 4. \end{cases}$$

A discriminant of a quadratic field is a *fundamental discriminant*. For simplicity, we write $\mathbf{C}_D$ and $\mathbf{Cl}_D$ for $\mathbf{C}_{\mathbb{Q}(\sqrt{D})}$ and $\mathbf{Cl}_{\mathbb{Q}(\sqrt{D})}$ respectively.

1.2.1 Imaginary quadratic fields

For imaginary quadratic fields K, i.e. $D < 0$, every element has positive norm, so $P_K^+ = P_K$ and $\mathbf{C}_D = \mathbf{Cl}_D$. Hence also $H = H^+$. The unit group is simply $\langle -1 \rangle$.

1.2.2 Real quadratic fields

For real quadratic fields K, i.e. $D > 0$, there exist elements with negative norms, for example $\sqrt{D}$. Principal ideals generated by such an element is only totally positive if there exists a unit with negative norm. In (1.1), the quotient P_K/P_K^+ is generated by the class $[(\sqrt{D})]$,

$$0 \to \langle [(\sqrt{D})] \rangle \to \mathbf{C}_D \to \mathbf{Cl}_D \to 0. \tag{1.2}$$

Dirichlet's unit theorem states that the unit group of a number field is finitely generated and has rank $r + s - 1$, where r is the number of real embeddings and s is the number of conjugate pairs of complex embeddings of K. Therefore, we can express the unit group of K in the form

$$\langle -1 \rangle \times \langle \epsilon_D \rangle, \tag{1.3}$$

where ϵ_D is taken as the minimal unit in K greater than 1, which is called the *fundamental unit*. Therefore, $\mathbf{Cl}_K = \mathbf{C}_K$ holds precisely when ϵ_D has norm -1. A field extension of a totally real field is unramified at all places in infinity, if and only if it is totally real. Therefore H is the maximal totally real subfield of H^+. Also $[H^+ : H] \leq 2$. There is the following short exact sequence

$$0 \to \mathrm{Gal}(H^+/H) \cong \left\langle \left(\frac{H^+/K}{\infty} \right) \right\rangle \to \mathrm{Gal}(H^+/K) \to \mathrm{Gal}(H/K) \to 0. \tag{1.4}$$

Relating (1.1) and (1.4) by Artin reciprocity, we see that

$$\left(\frac{H^+/K}{\infty}\right) = \left(\frac{H^+/K}{(\sqrt{D})}\right)$$

generates $\mathrm{Gal}(H^+/H)$.

1.2.3 Quadratic symbols

Suppose E is a number field. For any nonzero $a \in \mathcal{O}_E$ and $\mathfrak{p}$ a prime in E, we write $\left(\frac{a}{\mathfrak{p}}\right)$ to denote the Kronecker symbol, and extend this multiplicatively. We define $\left(\frac{a}{\mathfrak{p}}\right)_+$ to be $c \in \{0,1\}$ such that $(-1)^c = \left(\frac{a}{\mathfrak{p}}\right)$. If $\mathfrak{p}$ is unramified in $E(\sqrt{a})/E$, we can equate the Artin symbol and the Kronecker symbol by

$$\left(\frac{a}{\mathfrak{p}}\right) = \left(\frac{E(\sqrt{a})/E}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits in } E(\sqrt{a})/E, \\ -1 & \text{if } \mathfrak{p} \text{ is inert in } E(\sqrt{a})/E. \end{cases}$$

We write $\mathcal{M}_E$ to be the set of places of E, for example

$$\mathcal{M}_{\mathbb{Q}} = \{\text{prime numbers}\} \cup \{\infty\}.$$

We call a prime ideal $\mathfrak{p}$ in $\mathcal{O}_E$ even if $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$, and odd otherwise. If $\mathfrak{p} \in \mathcal{M}_E$, we write $E_{\mathfrak{p}}$ for the completion of E with respect to $\mathfrak{p}$. For any $\mathfrak{p} \in \mathcal{M}_E$, and any $a, b \in E^\times$, we define the local Hilbert symbol at $\mathfrak{p}$ to be

$$(a,b)_{\mathfrak{p}} = \begin{cases} 1 & \text{if } x^2 - ay^2 = bz^2 \text{ has a solution } (x,y,z) \in E_{\mathfrak{p}}^3 \setminus \{(0,0,0)\}, \\ -1 & \text{otherwise.} \end{cases}$$

By the Hasse-Minkowski theorem, $x^2 - ay^2 = bz^2$ is solvable by some $(x,y,z) \in E^3 \setminus \{(0,0,0)\}$ if and only if $(a,b)_{\mathfrak{p}} = 1$ for all $p \in \mathcal{M}_E$.

We can relate Artin symbols of quadratic extensions with Hilbert symbols.

Lemma 1.4. *Suppose E is a number field and let $a, b \in \mathcal{O}_E$. If a prime $\mathfrak{p}$ is unramified over $E(\sqrt{a})/E$, then*

$$(a,b)_{\mathfrak{p}} = \left(\frac{E(\sqrt{a})/E}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}\, b}.$$

Proof. This follows from results from local class field theory, see for example [61,

Proposition 3.1 p.333], [17, Exercise 2.8, p.352] and [17, Chapter VI.2, Proposition 2, p.141]. Since the global Artin map at a prime is the corresponding local Artin map, we have

$$(a,b)_{\mathfrak{p}} = \left(\frac{E_{\mathfrak{p}}(\sqrt{a})/E_{\mathfrak{p}}}{b}\right) = \left(\frac{E(\sqrt{a})/E}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}} b}. \qquad \square$$

1.2.4 Splitting of primes in biquadratic extensions

Lemma 1.5. *Suppose F and E are number fields such that $\mathrm{Gal}(F/E) \cong V_4$. Let E_1, E_2, E_3 be the three quadratic subfields. If $\mathfrak{v}$ is unramified in F/E_1 and $\mathfrak{v} \cap \mathcal{O}_E$ is unramified in E_2/E, then*

$$\left(\frac{F/E_1}{\mathfrak{v}}\right) = \left(\frac{E_2/E}{\operatorname{Norm}_{E_1/E}\mathfrak{v}}\right).$$

Proof. Let $\mathfrak{p} = \mathfrak{v} \cap \mathcal{O}_E$. If $\mathfrak{p}$ ramifies or splits in E_1/E, then $\mathfrak{p} = \operatorname{Norm}_{E_1/E}\mathfrak{v}$ and the splitting of $\mathfrak{v}$ in F/E_1 is the same as the splitting of $\mathfrak{p}$ in E_2/E.

If $\mathfrak{p}$ is inert in E_1/E, then $\mathfrak{p}^2 = \operatorname{Norm}_{E_1/E}\mathfrak{v}$ and $\mathfrak{p}$ must split in one of E_2/E and E_3/E. Therefore $\left(\frac{F/E_1}{\mathfrak{v}}\right) = 1$. $\square$

Lemma 1.5 also follows from more general theory of Artin symbols, see for example [17, Chapter VII, Proposition 3.2, p.166].

Lemma 1.6. *Suppose F and E are number fields such that $\mathrm{Gal}(F/E) \cong V_4$. Let E_1, E_2, E_3 be the three quadratic subfields. If $\mathfrak{p}$ is unramified in E_1/E, then F/E_2 and F/E_3 must be unramified at any prime above $\mathfrak{p}$.*

Proof. By symmetry it suffices to show that F/E_2 must be unramified. If $\mathfrak{p}$ ramifies in E_2/E, then since the inertia degree of $\mathfrak{p}$ in F/E is 2, any prime in E_2 above $\mathfrak{p}$ must be unramified. If $\mathfrak{p}$ is unramified in E_2/E, then since $F = E_1 \cdot E_2$, $\mathfrak{p}$ is unramified in F/E. $\square$

Lemma 1.7. *Let $a, b \neq 1$ be distinct squarefree integers. A prime ideal ramifies in $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{ab})$ if and only if it divides $\gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})})$.*

Proof. First suppose that $p \mid \gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})})$, then p ramifies in both $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$. If $p \nmid \Delta_{\mathbb{Q}(\sqrt{ab})}$, i.e. p is unramified in $\mathbb{Q}(\sqrt{ab})/\mathbb{Q}$, which is always the case when p is odd, then it must ramify in $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{ab})$. If $p \mid \Delta_{\mathbb{Q}(\sqrt{ab})}$, then p is totally ramified in $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$.

Suppose instead $p \nmid \gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})})$. If $p \nmid \Delta_{\mathbb{Q}(\sqrt{a})}$ and $p \nmid \Delta_{\mathbb{Q}(\sqrt{b})}$, p is unramified in both $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$, hence also in their compositum $\mathbb{Q}(\sqrt{a}, \sqrt{b})$.

If p divides exactly one of $\Delta_{\mathbb{Q}(\sqrt{a})}$ and $\Delta_{\mathbb{Q}(\sqrt{b})}$, then $p \mid \Delta_{\mathbb{Q}(\sqrt{ab})}$. In this case p is unramified in one of $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{b})/\mathbb{Q}$, but ramifies in $\mathbb{Q}(\sqrt{ab})/\mathbb{Q}$, so the prime ideal above p must be unramified in $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{ab})$. □

When we have quadratic extension of a quadratic extension, the following lemma allows us to determine its Galois closure.

Lemma 1.8 ([54, Chapter VI, Exercise 4, p.321])**.** *Let K be a number field. Let $E = K(\sqrt{a})$, where $a \in K^\times \setminus (K^\times)^2$, and let $F = E(\sqrt{\beta})$, where $\beta \in E^\times \setminus (E^\times)^2$. Let $N = \mathrm{Norm}_{E/K}(\beta)$.*

(i) If $N \in (K^\times)^2$, then F/K is normal and $\mathrm{Gal}(F/K) \cong V_4$.

(ii) If $N \in a \cdot (K^\times)^2$, then F/K is normal and $\mathrm{Gal}(F/K) \cong C_4$.

(iii) If $N \notin (K^\times)^2 \cup a \cdot (K^\times)^2$, then F/K has normal closure $F(\sqrt{N})$ and $\mathrm{Gal}(F(\sqrt{N})/K) \cong D_8$.

1.3 Inductively computing the 2^k-rank

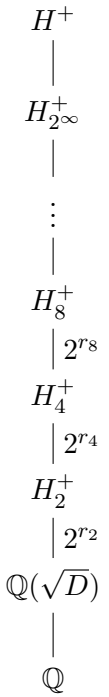
To find the size of the 2-part of $\mathbf{C}_D$, we can either work with $\mathbf{C}_D$ directly or its dual $\hat{\mathbf{C}}_D$, by constructing 2-power extensions of K contained in the narrow class field H^+. Let $r_{2^k} \coloneqq \mathrm{rk}_{2^k} \mathbf{C}_D$, so $2^{r_{2^k}} = \#\, \mathbf{C}_D^{2^{k-1}}[2] = \#(\mathbf{C}_D^{2^{k-1}} \,/\, \mathbf{C}_D^{2^k})$.

Since $\mathbf{C}_D^{2^k}$ is a subgroup of $\mathbf{C}_D$, there exists some field $H_{2^k}^+ \subseteq H^+$ such that $\mathbf{C}_D^{2^k} \cong \mathrm{Gal}(H^+/H_{2^k}^+)$ under Artin reciprocity. Then we have $\mathrm{Gal}(H_{2^k}^+/K) \cong \mathrm{Gal}(H^+/K)/\,\mathrm{Gal}(H^+/H_{2^k}^+) \cong \mathbf{C}_D \,/\, \mathbf{C}_D^{2^k}$. We see that

$$\left(\frac{H_{2^k}^+/K}{\cdot}\right) : \mathbf{C}_D \,/\, \mathbf{C}_D^{2^k} \to \mathrm{Gal}(H_{2^k}^+/K) \qquad [\mathfrak{m}] \mapsto \left(\frac{H_{2^k}^+/K}{\mathfrak{m}}\right).$$

Therefore

$$\mathbf{C}_D^{2^k} = \ker\left(\frac{H_{2^k}^+/K}{\cdot}\right) = \bigcap_{\Psi \in \hat{\mathbf{C}}_D[2^k]} \ker \Psi. \tag{1.5}$$



We see that $H_{2^k}^+$ is the compositum of the fields of definition of all $\Psi \in \hat{\mathbf{C}}_D[2^k]$. The field $H_{2^k}^+$ is constructed as the maximal abelian at finite places unramified extension of K of exponent 2^k. We can repeat this until we obtain $H_{2^\infty}^+$, the maximal abelian at finite places unramified 2-power extension of K. This is a finite process since the class group is finite.

The field H_2^+ is called the *genus field* of K. It follows from Gauss genus theory [28, Theorem 6.1] that

$$H_2^+ = K(\sqrt{p^*} : p \mid \Delta_K), \tag{1.6}$$

where $p^* = (-1)^{\frac{p-1}{2}} p$ for odd p and

$$2^* = \frac{D}{\prod\limits_{\text{odd } p \mid D} p^*} = \begin{cases} 2 & \text{if } D \equiv 2 \bmod 8, \\ -2 & \text{if } D \equiv -2 \bmod 8, \\ -1 & \text{if } D \equiv 3 \bmod 4. \end{cases}$$

We can also show directly that the field we defined is indeed the genus field of K. It is straightforward to check that the H_2^+/K is indeed unramified, for example we can apply Lemma 1.6. We prove the following more general lemma which implies that the genus field must have degree bounded by 2^{t-1} over K, where $t = \omega(\Delta_K)$. Then since we have constructed an unramified extension H_2^+/K with degree 2^{t-1}, we see that $r_2 = \operatorname{rk}_2 \hat{\mathbf{C}}_D = t - 1$.

Lemma 1.9. *Suppose E is a number field with odd narrow class number, and let K/E be a quadratic extension. Let $H_{2^k}^+$ be the maximal abelian at finite places unramified extension of K of exponent 2^k. Let $\sigma \in \operatorname{Gal}(H_{2^k}^+/E)$ be a lift of the generator of $\operatorname{Gal}(K/E)$. Then for any subfield $L \subseteq H_{2^k}^+$ containing K, L/E is Galois and $\sigma g \sigma^{-1} = g^{-1}$ for any $g \in \operatorname{Gal}(L/K)$. Furthermore, $\operatorname{Gal}(H_2^+/E)$ is abelian and of exponent 2, and $\operatorname{rk}_2 \mathbf{C}_K \leq \#\{\mathfrak{p} \text{ prime in } E : \mathfrak{p} \text{ ramifies in } K/E\} - 1$.*

Proof. Consider the short exact sequence

$$1 \to \mathbf{C}_K \,/\, \mathbf{C}_K^{2^k} \cong \operatorname{Gal}(H_{2^k}^+/K) \to \operatorname{Gal}(H_{2^k}^+/E) \to \langle \sigma \rangle \to 1.$$

Each class in $\mathbf{C}_K \,/\, \mathbf{C}_K^{2^k}$ contains a prime ideal $\mathfrak{v}$ in K by Chebotarev density theorem.

Suppose $\mathfrak{p}$ is the prime in E lying below $\mathfrak{v}$. Since E has odd narrow class number, $[\mathfrak{p}]$ is trivial in $\mathbf{C}_E \,/\, \mathbf{C}_E^{2^k}$, and so $[\mathfrak{p}\mathcal{O}_K]$ is trivial in $\mathbf{C}_K \,/\, \mathbf{C}_K^{2^k}$. If $\mathfrak{p}$ splits or ramifies in K/E, then $\mathfrak{v}\mathfrak{v}^\sigma = \mathfrak{p}\mathcal{O}_K$, so $[\mathfrak{v}]^{-1} = [\mathfrak{v}]^\sigma$ in $\mathbf{C}_K \,/\, \mathbf{C}_K^{2^k}$. If $\mathfrak{p}$ is inert, then $[\mathfrak{v}]$ is trivial in $\mathbf{C}_K \,/\, \mathbf{C}_K^{2^k}$. Since the isomorphism $\mathbf{C}_K \,/\, \mathbf{C}_K^{2^k} \cong \mathrm{Gal}(H_{2^k}^+/K)$ respects the action of σ, this implies that $\sigma g \sigma^{-1} = g^{-1}$ for any $g \in \mathrm{Gal}(H_{2^k}^+/K)$. Now every subgroup of $\mathrm{Gal}(H_{2^k}^+/K)$ is stable under σ, so any $L \subseteq H_{2^k}^+$ containing K is Galois over E. The same argument for L/K shows that $\sigma g \sigma^{-1} = g^{-1}$ holds for any $g \in \mathrm{Gal}(L/K)$.

When $k = 1$, any $g \in \mathrm{Gal}(H_2^+/K)$ has order dividing 2, so $g = g^{-1}$ and since $\sigma g \sigma^{-1} = g^{-1}$, we see that g commutes with σ. Therefore $\mathrm{Gal}(H_2^+/E)$ is abelian and of exponent 2. It follows from the monodromy theorem (Theorem 1.3), since E has no unramified at all finite prime abelian extension of even degree, that $\mathrm{Gal}(H_2^+/E)$ is generated by the inertia groups of ramified primes. Since $\mathrm{Gal}(H_2^+/E)$ is abelian, the inertia group does not depend on the choice of prime above a given prime $\mathfrak{p}$ in E, so the number of generators is bounded by the number of primes ramifying in K/E. □

Let $p_1, \ldots, p_t$ be the distinct prime factors of Δ_K. These are precisely the primes that ramify in $K/\mathbb{Q}$. Denote $\mathfrak{p}_j$ the ideal in $\mathcal{O}_K$ that is above p_j, so $(p_j) = \mathfrak{p}_j^2$ and $[\mathfrak{p}_j]^2 = 1$. It is well known (see for example [85, Corollary 9.9(a)]) that $\mathbf{C}_D[2]$ can be generated by the classes $[\mathfrak{p}_j]$, so we can express any element in $\mathbf{C}_D[2]$ as $\prod_j [\mathfrak{p}_j]^{e_j}$, for some $e_j \in \{0, 1\}$.

Define a t-dimensional $\mathbb{F}_2$-vector space

$$\mathcal{V}_1 \coloneqq \begin{cases} \{\pm b \mid \Delta_K\} \subset \mathbb{Q}^\times / \{1, -D\}(\mathbb{Q}^\times)^2 & \text{if } D > 0, \\ \{b \mid \Delta_K : b > 0\} \subset \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 & \text{if } D < 0. \end{cases} \tag{1.7}$$

Since $\#\mathcal{V}_1 = 2^t$ and $\#\,\mathbf{C}_D[2] = 2^{t-1}$, there is a two-to-one projection

$$P : \mathcal{V}_1 \twoheadrightarrow \mathbf{C}_D[2] \qquad m \mapsto \begin{cases} [\mathfrak{m}] & \text{if } m > 0, \\ [\mathfrak{m}(\sqrt{D})] & \text{if } m < 0, \end{cases}$$

where $\mathfrak{m}$ is an ideal in K with norm $|m|$. One set of representatives for $\mathcal{V}_1$ is

$$\{p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t} : (e_1, e_2, \ldots, e_t) \in \mathbb{F}_2^t\}.$$

Since $\#\ker P = 2$, there exist exactly one non-trivial positive representative $R \mid \Delta_K$ in $\ker P$. If $D < 0$, we always have $R = D$, since $(\sqrt{D})$ is a totally positive principal ideal. Define $\mathcal{V}_k$ to be the set of elements $b \in \mathcal{V}_1$ such that $P(b) \in \mathbf{C}_D^{2^{k-1}}[2]$.

Define another t-dimensional $\mathbb{F}_2$-vector space

$$\mathcal{U}_1 \coloneqq \{(p_1^*)^{e_1}(p_2^*)^{e_2}\dots(p_t^*)^{e_t} : (e_1, e_2, \dots, e_t) \in \mathbb{F}_2^t\} \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2. \tag{1.8}$$

The field of definition of any $\Psi \in \hat{\mathbf{C}}_D[2]$ is contained in H_2^+, so we can write $\Psi = \left(\frac{K(\sqrt{a})/K}{\cdot}\right)$ for some $a \in \mathcal{U}_1$. Then there is a two-to-one projection

$$\psi_1 : \mathcal{U}_1 \twoheadrightarrow \hat{\mathbf{C}}_D[2] \qquad a \mapsto \left(\frac{K(\sqrt{a})/K}{\cdot}\right).$$

Since $K(\sqrt{a}) = K(\sqrt{D/a})$, we see that $\ker\psi_1 = \{1, D\}$. Define $\mathcal{U}_k$ to be the set of $a \in \mathcal{U}_1$ such that $\psi_1(a) \in \hat{\mathbf{C}}_D^{2^{k-1}}[2]$.

For any $a \in \mathcal{U}_k$, there exists some $\Psi \in \hat{\mathbf{C}}_D[2^k]$ such that $\Psi^{2^{k-1}} = \psi_1(a)$. Since $\Psi \in \hat{\mathbf{C}}_D[2^k]$, we can write $\Psi = \left(\frac{L/K}{\cdot}\right)$, where $L \subseteq H^+$ and $\mathrm{Gal}(L/K) \cong C_{2^i}$ for some $i \le k$. From $\Psi^{2^{k-1}} = \psi_1(a)$, we deduce that the field of definition of $\psi_1(a)$ must be contained in L. Also if $\psi_1(a)$ is non-trivial, then Ψ must have exact order 2^k, so $i = k$. Therefore $L \subseteq H_{2^k}^+$ is a C_{2^k}-extension of K containing $K(\sqrt{a})$. We see that any two choices of $\left(\frac{L/K}{\cdot}\right)$ defer by an element in $\hat{\mathbf{C}}_D[2^{k-1}]$. If $\psi_1(a)$ is trivial then $\Psi \in \hat{\mathbf{C}}_D[2^{k-1}]$. Therefore we can define

$$\psi_k : \mathcal{U}_k \to \hat{\mathbf{C}}_D[2^k]/\hat{\mathbf{C}}_D[2^{k-1}] \qquad \psi_k(a)^{2^{k-1}} = \psi_1(a).$$

The following is now clear.

Theorem 1.10. *Let $a \in \mathcal{U}_1 \setminus \{1, D\}$. Then $a \in \mathcal{U}_k$ if and only if there exists a field L such that $K \subseteq K(\sqrt{a}) \subseteq L \subseteq H^+$ and $\mathrm{Gal}(L/K) \cong C_{2^k}$.*

We see that

$$\bigcap_{\Psi \in \hat{\mathbf{C}}_D[2^k]} \ker\Psi = \bigcap_{i \le k} \bigcap_{a \in \mathcal{U}_i} \ker\psi_i(a).$$

From (1.5), we deduce that

$$\mathbf{C}_D^{2^k} = \ker\left(\frac{H_{2^{k-1}}^+/K}{\cdot}\right) \bigcap_{a \in \mathcal{U}_k} \ker\psi_k(a) = \mathbf{C}_D^{2^{k-1}} \bigcap_{a \in \mathcal{U}_k} \ker\psi_k(a).$$

Define a pairing

$$\langle \quad , \quad \rangle_k : \mathcal{U}_k \times \mathcal{V}_k \to \{\pm 1\} \qquad \langle a, m \rangle_k \mapsto \psi_k(a)(P(m)). \tag{1.9}$$

Since $\hat{\mathbf{C}}_D[2^{k-1}]$ is trivial on $\mathbf{C}_D^{2^{k-1}}$, $\langle \quad , \quad \rangle_k$ is well defined. It is straightforward to check that the pairing factors through $\hat{\mathbf{C}}_D^{2^{k-1}}[2] \times \mathbf{C}_D^{2^{k-1}}[2]$. This pairing arises from the natural pairing $\hat{\mathbf{C}}_D \times \mathbf{C}_D \to \mathbb{T}$. The important property of this pairing $\langle \quad , \quad \rangle_k$ is that its left kernel (i.e. cokernel) is $\mathcal{U}_{k+1}$ and right kernel is $\mathcal{V}_{k+1}$, which both have size $2^{1+r_{2^{k+1}}}$. Starting with $\mathcal{U}_1$ and $\mathcal{V}_1$, we inductively obtain the $r_4, r_8, r_{16}, \ldots$ via this pairing. We have sequences of subspaces

$$\{1, D\} \subseteq \cdots \subseteq \mathcal{U}_{k+1} \subseteq \mathcal{U}_k \subseteq \cdots \subseteq \mathcal{U}_1 \quad \{1, R\} \subseteq \cdots \subseteq \mathcal{V}_{k+1} \subseteq \mathcal{V}_k \subseteq \cdots \subseteq \mathcal{V}_1,$$

such that $\psi_1(\mathcal{U}_k) = \hat{\mathbf{C}}_D^{2^{k-1}}[2]$, $P(\mathcal{V}_k) = \mathbf{C}_D^{2^{k-1}}[2]$ and $\dim_{\mathbb{F}_2} \mathcal{U}_k = \dim_{\mathbb{F}_2} \mathcal{V}_k = r_{2^k} + 1$. Define

$$\overline{\mathcal{U}}_k = \mathcal{U}_k / \{1, D\} \text{ and } \overline{\mathcal{V}}_k = \mathcal{V}_k / \{1, R\}. \tag{1.10}$$

The pairing is also well-defined on $\overline{\mathcal{U}}_k$ and $\overline{\mathcal{V}}_k$.

For any $S = \{s_1, \ldots, s_m\} \subseteq \mathcal{U}_k$ and $T = \{t_1, \ldots, t_n\} \subseteq \mathcal{V}_k$, define $R_{k,S,T}(D)$ to be the $m \times n$ matrix $(c_{i,j})$ over $\mathbb{F}_2$, such that $(-1)^{c_{i,j}} = \langle s_i, t_j \rangle_k$. If S is a basis for $\mathcal{U}_k$ and T is a basis for $\mathcal{V}_k$, then $R_{k,S,T}(D)$ is the matrix representation of $\langle \quad , \quad \rangle_k$, and we have $\operatorname{coker} R_{k,S,T}(D) \cong \mathcal{U}_{k+1}$ and $\ker R_{k,S,T}(D) \cong \mathcal{V}_{k+1}$, under the maps $(e_1, \ldots, e_m) \mapsto s_1^{e_1} \ldots s_m^{e_m}$ and $(e_1, \ldots, e_n) \mapsto t_1^{e_1} \ldots t_n^{e_n}$, respectively.

We will discuss this idea in computing r_4 and r_8 in the following sections.

1.4 Computing 4-rank

We can find $r_4 = \operatorname{rk}_4 \mathbf{C}_D$ from the dimension of the right kernel of $\langle \quad , \quad \rangle_1$. We attempt to obtain a matrix representation of the pairing $\langle \quad , \quad \rangle_1$ with respect to the basis $S = \{p_1^*, \ldots, p_t^*\}$ for $\mathcal{U}_1$ and the basis $T = \{p_1, \ldots, p_t\}$ for $\mathcal{V}_1$. Taking norms, we obtain an expression in terms of the Kronecker symbols at each prime $\mathfrak{p}_j$,

$$\langle p_i^*, p_j \rangle_1 = \left(\frac{K(\sqrt{p_i^*})/K}{\mathfrak{p}_j} \right) = \begin{cases} \left(\frac{\mathbb{Q}(\sqrt{p_i^*})/\mathbb{Q}}{p_j} \right) = \left(\frac{p_i^*}{p_j} \right) & \text{if } i \neq j, \\ \left(\frac{\mathbb{Q}(\sqrt{D/p_i^*})/\mathbb{Q}}{p_i} \right) = \left(\frac{D/p_i^*}{p_i} \right) & \text{if } i = j. \end{cases}$$

We see that the matrix representation for $\langle \quad , \quad \rangle_1$ with respect to the bases S and T, is given by $R_{1,S,T}(D) \coloneqq (c_{ij})_{1\le i,j\le t}$, where

$$c_{ij} = \begin{cases} \left(\frac{p_i^*}{p_j}\right)_+ & \text{if } i \neq j, \\ \left(\frac{D/p_i^*}{p_i}\right)_+ & \text{if } i = j. \end{cases}$$

Note that the entries have been converted from $\{\pm 1\}$ to $\{0,1\}$, as $\langle \quad , \quad \rangle_1$ is multiplicative, while the matrix space acts on additive structures. We call $R_1 \coloneqq R_{1,S,T}(D)$ the Rédei matrix, since it was first given by Rédei [64]. Then $\mathcal{V}_2$ is the left kernel of R_1, $\mathcal{U}_2$ is the right kernel of R_1, and $\operatorname{corank} R_1 = r_4 + 1$.

We can convert the Kronecker symbols into Hilbert symbols, so alternatively, for any p_i and odd p_j,

$$\langle p_i^*, p_j\rangle_1 = (D, p_j)_{p_i} = (-D, p_i^*)_{p_j}.$$

If $p_j = 2$, we see that exactly one of p_i^* or D/p_i^* is congruent to 1 mod 4, and

$$\langle p_i^*, 2\rangle_1 = (D,2)_{p_i} = \begin{cases} 1 & \text{if } p_i^* \text{ or } D/p_i^* \equiv 1 \bmod 8 \\ -1 & \text{if } p_i^* \text{ or } D/p_i^* \equiv 5 \bmod 8 \end{cases}.$$

Therefore checking also the Hilbert symbol at ∞, and noting that $(-D,a)_p = (D,b)_p = 1$ for any $a, b \mid D$ and $p \nmid \Delta_{\sqrt{D}}$, we have

$$\mathcal{U}_2 = \{a \in \mathcal{U}_1 : (-D,a)_p = 1 \text{ for all } p \in \mathcal{M}_{\mathbb{Q}}, \\ \text{and } a \text{ or } D/a \equiv 1 \bmod 8 \text{ if } 2 \in \mathcal{V}_1\}, \quad (1.11)$$

$$\mathcal{V}_2 = \{b \in \mathcal{V}_1 : (D,b)_p = 1 \text{ for all } p \in \mathcal{M}_{\mathbb{Q}}\}. \quad (1.12)$$

1.4.1 Decomposition of second type

Rédei and Reichardt [66] showed that we can find the 4-rank by constructing the unramified C_4-extensions. Fouvry and Klüners [31] described the construction in more detail and applied this idea to the negative Pell equation. They gave the following definition.

Definition 1.11 (decomposition of second type)**.** *Given a squarefree integer D, we call $\{D_1, D_2\}$ a decomposition of second type if the following holds*

- $D = D_1 D_2$;
- $(D_1, D_2)_p = 1$ *for all* $p \in \mathcal{M}_{\mathbb{Q}}$;
- *if one of* $\Delta_{\mathbb{Q}(\sqrt{D_1})}, \Delta_{\mathbb{Q}(\sqrt{D_2})}$ *is even, the other is* $1 \bmod 8$.

In terms of Kronecker symbols, an equivalent formulation of the last two conditions in the definition is $\left(\frac{D_2}{p}\right) = 1$ for all $p \mid D_1$ and $\left(\frac{D_1}{p}\right) = 1$ for all $p \mid D_2$. We treat $\{D_1, D_2\}$ and $\{D_2, D_1\}$ as the same decomposition since they define the same extensions.

It is straightforward to check from (1.11) that this is an alternative description of elements in $\mathcal{U}_2$.

Theorem 1.12. *We have $a \in \mathcal{U}_2$ if and only if $\{a, D/a\}$ is a decomposition of second type. Therefore $\mathbb{Q}(\sqrt{D})$ has 2^{r_4} decomposition of second type.*

For $a \in \mathcal{U}_2 \notin \{1, D\}$, the field of definition of $\psi_2(a) \in \hat{\mathbf{C}}_D[2^k]$ turns out to be D_8-extensions of $\mathbb{Q}$. We will show in Section 2.1 that such extensions can be constructed explicitly. Here we prove a slightly more general lemma. The case when $E = \mathbb{Q}$ is known by Rédei and Reichardt [66].

Lemma 1.13. *Let E be a number field with odd class number, and let K/E be a quadratic extension. Suppose L/K is a C_4-extension unramified at all finite places. Then* $\mathrm{Gal}(L/E) \cong C_2 \rtimes C_4 = D_8$.

Proof. By Lemma 1.9, $\sigma g \sigma^{-1} = g^{-1}$ for any $g \in \mathrm{Gal}(L/K)$, and L/E is a Galois extension. Since $\mathrm{Gal}(L/E)$ has order 8, the only group that satisfy the conditions is D_8. □

1.5 Computing the 8-rank

To compute the 8-rank, we find the right kernel of the pairing $\langle \quad , \quad \rangle_2$.

Definition 1.14 (Rédei symbol for decomposition of second type)**.** *Let $a \in \mathcal{U}_2$ and $b \in \mathcal{V}_2$. Define the Rédei symbol as*

$$[a, D/a, b] \coloneqq \langle a, b \rangle_2.$$

and the additive Rédei symbol, which takes values in $\mathbb{F}_2$*, as*

$$[a, D/a, b]_+ = \begin{cases} 0 & \text{if } [a, D/a, b] = 1, \\ 1 & \text{if } [a, D/a, b] = -1. \end{cases}$$

Take a basis $S = \{a_1, \ldots, a_{r_4+1}\}$ for $\mathcal{U}_2 = \operatorname{coker} R_1$ and a basis $T = \{b_1, \ldots, b_{r_4+1}\}$ for $\mathcal{V}_2 = \ker R_1$. Then the matrix representation of $\langle \quad , \quad \rangle_2$ is $R_{2,S,T}(D) \coloneqq ([a_i, D/a_i, b_j]_+)_{1 \le i,j \le r_4+1}$, and $\operatorname{corank} R_2 = r_8 + 1$.

In the next chapter we will study the Rédei symbol in a more general setting.

Chapter 2

A new look at Rédei reciprocity

In 1939, Rédei defined a symbol in terms of some power residue symbol [65] to study the 8-rank of the class group, with a similar meaning to the symbol we defined in Definition 1.14, but with more restrictions on the entries. He showed that his symbol satisfies some form of symmetry in the entries. More recently, in a more class field theoretic setting, Corsman [27] extended the Rédei symbol to include the infinite places, and discovered a more general form of the symmetry, which we will call Rédei reciprocity. Smith also provided a proof of Rédei reciprocity in [80]. However, as pointed out in [87], both Corman and Smith's proofs did not account for subtleties arising from the primes above 2 and ∞ correctly. Stevenhagen gave more careful versions of the definition and proof of Rédei reciprocity in [87, Theorem 1].

The proofs involve applying Hilbert reciprocity to an appropriate field and relating the Hilbert symbols with the Artin symbol defining the Rédei symbol. We will give a proof following a similar approach, but taking a more explicit route when constructing minimally ramified extensions, where the Rédei symbol is defined.

For any principal ideal (d) in a field K, let $[d]$ denote the squarefree ideal dividing (d) such that $(d)[d]$ is the square of an ideal. In contrast to the previous chapters, here K will denote some V_4-extension of $\mathbb{Q}$.

2.1 Constructing minimally ramified C_4-extensions

In this section, let $a, b \neq 1$ be nonzero integers satisfying

$$(a, b)_p = 1 \text{ for all } p \in \mathcal{M}_{\mathbb{Q}}. \tag{2.1}$$

Note that $(a,b)_\infty = 1$ implies that at least one of a and b is positive. Define

$$S_{a,b} = \begin{cases} 2\gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}) & \text{if } \{a,b\} \equiv \{5 \bmod 8,\ 3 \bmod 4\}, \\ \gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}) & \text{otherwise.} \end{cases}$$

Define $\mathcal{F}_{a,b}$ to be the set containing all $\beta \in \mathbb{Q}(\sqrt{a})$ such that

(i) $L = \mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{\beta})$ is a Galois extension of $\mathbb{Q}$,

(ii) $L/\mathbb{Q}(\sqrt{ab})$ is a C_4-extension that is unramified at any prime ideal not dividing $S_{a,b}$.

We will show that given (2.1), $\mathcal{F}_{a,b}$ is non-empty. Fouvry and Klüners [31, Section 3.2] constructed elements in $\mathcal{F}_{a,b}$ when $\{a,b\}$ is a decomposition of second type of ab. We extend their construction to this more general setting.

2.1.1 Choosing a generator

We will construct some $\beta \in \mathcal{F}_{a,b}$. By the Hasse-Minkowski theorem, condition (2.1) implies that there exists some $(x,y,z) \in \mathbb{Q}^3 \setminus \{(0,0,0)\}$ satisfying

$$x^2 - ay^2 = bz^2. \tag{2.2}$$

Clearing denominators and removing any common factors if necessary, we take

$$x, y, z \in \mathbb{Z} \text{ not all zero and pairwise coprime satisfying (2.2).} \tag{2.3}$$

When a or b is congruent to 1 mod 4, we also require that either

$$\begin{cases} (x,y,z) \equiv (1,1,0) \bmod 2 \ \text{ and } \ x - z \equiv 1 \bmod 4, \text{ or} & \text{(2.4a)} \\ (x,y,z) \equiv (1,0,1) \bmod 2 \ \text{ and } \ x - y \equiv 1 \bmod 4. & \text{(2.4b)} \end{cases}$$

Note that (2.4a) implies that $a \equiv 1 \bmod 4$ and (2.4b) implies that $b \equiv 1 \bmod 4$. The existence of such (x,y,z) is guaranteed by the following lemma.

Lemma 2.1. *If a or b is congruent to* 1 mod 4*, there exists (x,y,z) satisfying* (2.3) *and one of* (2.4b) *and* (2.4a)*.*

Proof. From the preceding discussion, it is clear that hypothesis (2.7) implies the existence of some (x,y,z) satisfying (2.3). Without loss of generality, assume that

$b \equiv 1 \bmod 4$. It suffices to show that x is odd and and exactly one of y and z is even, because then switching the sign of x gives $x - y \equiv 1 \bmod 4$ or $x - z \equiv 1 \bmod 4$.

Suppose $a \equiv 1 \bmod 4$. Notice that $x^2 \equiv z^2 + y^2 \bmod 4$, so x is odd and exactly one of y and z is even.

Suppose $a \equiv 2 \bmod 4$. Then from $x^2 - 2y^2 \equiv z^2 \bmod 4$, we see that x is odd, y is even and z is odd.

Suppose $a \equiv 3 \bmod 4$. From $x^2 + y^2 \equiv z^2 \bmod 4$, we see that z is odd and exactly one of x and y is odd. If x is even and y is odd, we can take $(X, Y, Z) = (x(1+b) - 2bz,\ y(1-b),\ 2x - z(1+b))$, which satisfies $X^2 - aY^2 = bZ^2$. Then X and Z are both exactly divisible by 2 and Y is divisible by 4. Therefore removing any common factors of X, Y and Z reduces to the case where x is odd and y is even. □

Fix some (x, y, z) satisfying (2.3) and in addition (2.4b) or (2.4a) if a or b is congruent to 1 mod 4, we define

$$\begin{cases} \alpha = x + z\sqrt{b}, & \beta = \frac{x+y\sqrt{a}}{2} \quad \text{if } a \equiv 1 \bmod 4 \text{ and } 2 \mid z, \\ \alpha = 2(x + z\sqrt{b}), & \beta = x + y\sqrt{a} \quad \text{otherwise.} \end{cases} \tag{2.5}$$

Let $\mathcal{F}'_{a,b}$ be the set of all $\beta \in \mathbb{Q}(\sqrt{a})$ that arise from (2.5).

Note that β is defined as a *primitive* element in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{a})}$, i.e. $p \nmid \beta$ for any rational prime p. Moreover, $\alpha = (\sqrt{\beta} + \mathrm{sgn}(z)\sqrt{\bar{\beta}})^2$, where $\bar{\beta}$ is the conjugate of β in $\mathbb{Q}(\sqrt{a})$ and $\mathrm{sgn}(z) \in \{\pm 1\}$ is the sign of z.

We will show the following.

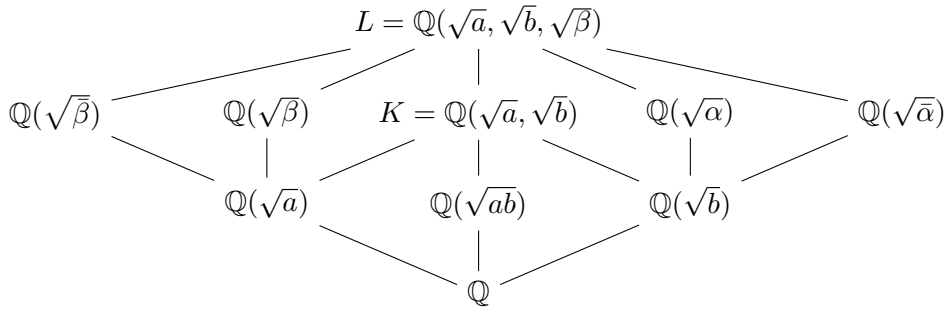
Theorem 2.2. $\mathcal{F}'_{a,b} \subseteq \mathcal{F}_{a,b}$.

Define $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ and $L = \mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{\beta})$. To prove Theorem 2.2, we need to check L satisfies the conditions set out in the definition of $\mathcal{F}_{a,b}$.

Applying Lemma 1.8 shows that $\mathrm{Gal}(L/\mathbb{Q}) \cong D_8$, unless $ab \in (\mathbb{Q}^\times)^2$, when $\mathbb{Q} = \mathbb{Q}(\sqrt{ab})$ and $\mathrm{Gal}(L/\mathbb{Q}) \cong C_4$.

In our case N is bz^2 and the normal closure $F(\sqrt{N})$ in the theorem is L.

We obtain the following field diagram, where $\bar{\alpha}$ denotes the conjugate of α in $\mathbb{Q}(\sqrt{b})$. Here $L/\mathbb{Q}(\sqrt{ab})$ is a cyclic extension of degree 4 which is central in $L/\mathbb{Q}$.



To prove Theorem 2.2, it remains to show that $L/\mathbb{Q}(\sqrt{ab})$ is unramified at any prime ideal not dividing $S_{a,b}$.

With Proposition 1.2 in mind, we first show that L/K is unramified at odd primes not dividing $S_{a,b}$.

Lemma 2.3. *The following holds.*

(i) $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ *is unramified at any odd prime not dividing* b*, and*

(ii) $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}(\sqrt{b})$ *is unramified at any odd prime not dividing* a*.*

It follows that L/K *is unramified at any odd prime not dividing* $\gcd(a, b)$*.*

Proof. Suppose $\mathfrak{p}$ is a prime in $\mathbb{Q}(\sqrt{a})$ lying above an odd prime $p \nmid \Delta_{\mathbb{Q}(\sqrt{b})}$. Note that $\mathfrak{p}$ ramifies in $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ if and only if $\mathfrak{p} \mid \beta$. If $\mathfrak{p} \mid \beta$, then $\mathfrak{p} \mid x + y\sqrt{a}$. Taking norms gives $p \mid bz^2$, but $p \nmid b$, so $p \mid z$. The condition $\gcd(x, y) = 1$ implies that $p \nmid \beta$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{a})}$, so $\mathfrak{p}$ is the only prime above p that divides β. Now $\operatorname{ord}_{\mathfrak{p}} \beta$ is even, hence $\mathfrak{p}$ is unramified over $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$. Applying Lemma 1.6 to the V_4-extension $L/\mathbb{Q}(\sqrt{a})$, we see that L/K is unramified at any prime above $\mathfrak{p}$.

If $p \nmid \Delta_{\mathbb{Q}(\sqrt{a})}$, a symmetric argument with β replaced with α shows that $\mathfrak{p}$ is unramified over $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}(\sqrt{b})$ and L/K is unramified at any prime above $\mathfrak{p}$. □

To handle ramification over the prime 2, we require $\alpha \in \mathbb{Q}(\sqrt{b})$ or $\beta \in \mathbb{Q}(\sqrt{a})$ to be a square modulo 4 when $2 \notin S$. Indeed, suppose $a \equiv 1 \bmod 8$, then if $\beta \equiv X^2 \bmod 4$ and is odd in $\mathbb{Q}(\sqrt{a})$, then 1 and $(X + \sqrt{\beta})/2$ forms an integral basis of $\mathcal{O}_{\mathbb{Q}(\sqrt{\beta})}$ over $\mathcal{O}_{\mathbb{Q}(\sqrt{a})}$. This basis has discriminant β, which is odd, so 2 is unramified.

Lemma 2.4. *Suppose* $2 \notin S_{a,b}$*. Then the following holds:*

(i) $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ *is unramified at any even prime if* (2.4b) *holds, and*

(ii) $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}(\sqrt{b})$ *is unramified at any even prime if* (2.4a) *holds.*

Furthermore, L/K *is unramified at any even prime.*

Proof. The assumption $2 \nmid S_{a,b}$ implies that $a \equiv 1 \bmod 8$, or $b \equiv 1 \bmod 8$, or $a \equiv b \equiv 1 \bmod 4$. We first show that (2.4b) implies that β is a square modulo 4 in $\mathcal{O}_{\mathbb{Q}(\sqrt{a})}$, so that $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ is unramified at any even prime. Assuming (2.4b) holds, we have $b \equiv 1 \bmod 4$.

If $a \equiv 1 \bmod 4$, then $\beta = x + y\sqrt{a} \equiv (x-y) + 2y(\frac{1+\sqrt{a}}{2}) \equiv 1 \bmod 4$.

Suppose $a \equiv 2 \bmod 4$. If $y \equiv 0 \bmod 4$, then $\beta = x + y\sqrt{a} \equiv 1 \bmod 4$. If $y \equiv 2 \bmod 4$, then $\beta = x + y\sqrt{a} \equiv 3 + 2\sqrt{a} \equiv (1+\sqrt{a})^2 \bmod 4$.

Suppose $a \equiv 3 \bmod 4$. Then $b \equiv 1 \bmod 8$. From $x^2 - ay^2 \equiv z^2 \bmod 8$, we must have $y \equiv 0 \bmod 4$, so $\beta = x + y\sqrt{a} \equiv 1 \bmod 4$.

Therefore $L/\mathbb{Q}(\sqrt{a})$ is unramified at any even prime. Applying Lemma 1.6 to the V_4-extension $L/\mathbb{Q}(\sqrt{a})$, we see that L/K is also unramified at any even prime.

If (2.4a) holds instead of (2.4b), then $a \equiv 1 \bmod 4$ and z is even, so $\alpha = x + z\sqrt{b}$. A symmetric argument shows that α is a square modulo 4, so that $L/\mathbb{Q}(\sqrt{b})$ and hence L/K are unramified at any even prime. □

By Lemma 2.3 and Lemma 2.4, L/K is unramified at any finite prime not dividing $S_{a,b}$. Together with Lemma 1.7, we see that $L/\mathbb{Q}(\sqrt{ab})$ is unramified at any finite prime not dividing $S_{a,b}$. This proves Theorem 2.2.

2.2 Defining the Rédei symbol

To define the Rédei symbol, take $a, b, c \neq 1$ to be nonzero squarefree integers satisfying

$$\gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}, \Delta_{\mathbb{Q}(\sqrt{c})}) = 1, \text{ and} \tag{2.6}$$

$$(a,b)_p = (a,c)_p = (b,c)_p = 1 \text{ for all } p \in \mathcal{M}_{\mathbb{Q}}. \tag{2.7}$$

Our goal is to define an Artin symbol $\left(\frac{K(\sqrt{\beta})/K}{\mathbf{c}}\right)$ that only depends on a, b and c.

Fix some $\beta \in \mathcal{F}'_{a,b}$ and define $L = K(\sqrt{\beta})$. By Theorem 2.2, L/K is unramified at any odd prime dividing c, since it must be coprime to $S_{a,b}$ by (2.6). When c is even, at least one of a and b is congruent to 1 mod 4 by (2.6) so must be congruent to 1 mod 8 by (2.7), so L/K is unramified at any prime at 2. Any $p \mid c$ splits or

ramifies in $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{b})/\mathbb{Q}$ from condition (2.7), so we can always find an ideal $\mathbf{c}$ in K with norm $|c|$.

2.2.1 Removing the dependency on the choice of field extensions

Now that we know where this Artin symbol exists, we need to check where it is independent of the choice of β and $\mathbf{c}$.

Since $\mathrm{Gal}(L/K)$ is in the centre of $\mathrm{Gal}(L/\mathbb{Q})$, for each prime $p \mid c$, the symbol $\left(\frac{L/K}{\mathfrak{v}}\right)$ does not depend on the choice of prime ideal $\mathfrak{v}$ above p. Therefore taking a different $\mathbf{c}$ does not change the value of $\left(\frac{L/K}{\mathbf{c}}\right)$.

Theorem 2.5. *Let $a, b, c \neq 1$ be nonzero squarefree integers satisfying the conditions* (2.6) *and* (2.7). *Define $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Let $\beta, \beta' \in \mathcal{F}_{a,b}$. Let $\mathbf{c}$ be an ideal in K of norm $|c|$. Futher assume for any even prime $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{a})$,*

$$\mathrm{ord}_{\mathfrak{p}}\, \beta \text{ is even if } \{a, b\} \equiv \{3 \bmod 4,\ 5 \bmod 8\} \text{ and } c \equiv 5 \bmod 8. \tag{2.8}$$

Then

$$\begin{cases} \left(\frac{K(\sqrt{\beta})/K}{\mathbf{c}}\right) = \left(\frac{K(\sqrt{\beta'})/K}{\mathbf{c}}\right) & \text{if } c > 0, \\ \left(\frac{K(\sqrt{\beta})/K}{\mathbf{c}\infty}\right) = \left(\frac{K(\sqrt{\beta'})/K}{\mathbf{c}\infty}\right) & \text{if } c < 0. \end{cases}$$

Lemma 2.6. *Let $a, b \neq 1$ be nonzero squarefree integers satisfying* (2.1). *Define $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Suppose $\beta, \beta' \in \mathcal{F}_{a,b}$. Then $K(\sqrt{\beta'}) = K(\sqrt{d\beta})$ for some squarefree integer d. Furthermore, $K(\sqrt{d})/\mathbb{Q}(\sqrt{ab})$ is also unramified at any finite prime not dividing $S_{a,b}$, and*

$$\gcd(\Delta_{\mathbb{Q}(\sqrt{ab/d})}, \Delta_{\mathbb{Q}(\sqrt{d})}) \mid S_{a,b}. \tag{2.9}$$

Proof. Since $K(\sqrt{\beta'})$ and $K(\sqrt{\beta'})$ are both C_4-extensions of $\mathbb{Q}(\sqrt{ab})$, by Lemma 1.8, we must have $\mathrm{Norm}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}\, \beta = bz^2$ and $\mathrm{Norm}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}\, \beta' = bz'^2$ for some $z, z' \in \mathbb{Q}^\times$. Now $\mathrm{Norm}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}\, \beta\beta' = (bzz')^2$, so $\mathbb{Q}(\sqrt{\beta\beta'})/\mathbb{Q}$ is a V_4-extension. Hence $\mathbb{Q}(\sqrt{\beta\beta'}) = \mathbb{Q}(\sqrt{a}, \sqrt{d})$ for some squarefree integer d, and $\beta\beta' \in d \cdot (\mathbb{Q}(\sqrt{a})^\times)^2$. Therefore $K(\sqrt{\beta'}) = K(\sqrt{d\beta})$. Since $K(\sqrt{d}) \subset K(\sqrt{\beta}) \cdot K(\sqrt{\beta'})$, we know that $K(\sqrt{d})/\mathbb{Q}(\sqrt{ab})$ must be unramified where $K(\sqrt{\beta})/\mathbb{Q}(\sqrt{ab})$ and $K(\sqrt{\beta'})/\mathbb{Q}(\sqrt{ab})$ are both unramified, i.e. outside $S_{a,b}$. In particular $\mathbb{Q}(\sqrt{d}, \sqrt{ab})/\mathbb{Q}(\sqrt{ab})$ is unramified outside $S_{a,b}$. Now (2.9) follows from Lemma 1.7. □

Proof of Theorem 2.5. Suppose d is a squarefree integer such that $K(\sqrt{\beta'}) =$

$K(\sqrt{d\beta})$ as in Lemma 2.6. If $\left(\frac{K(\sqrt{d})/K}{\mathbf{c}}\right) = 1$, since $\mathrm{Gal}(K(\sqrt{\beta},\sqrt{\beta'})/K) \cong V_4$, we have

$$\left(\frac{K(\sqrt{\beta'})/K}{\mathbf{c}}\right) = \left(\frac{K(\sqrt{\beta})/K}{\mathbf{c}}\right)\left(\frac{K(\sqrt{d})/K}{\mathbf{c}}\right) = \left(\frac{K(\sqrt{\beta})/K}{\mathbf{c}}\right).$$

Therefore it suffices to show that $\left(\frac{K(\sqrt{d})/K}{\mathbf{c}}\right) = 1$.

Suppose $p \mid c$. Then (2.6) implies that $p \nmid S_{a,b}$. The condition $(a,c)_p = (b,c)_p = 1$ in (2.7) implies that any p either splits or ramify in the extensions $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{b})/\mathbb{Q}$. Suppose $\mathfrak{v} \mid \mathbf{c}$ is the prime in K above p. Apply Lemma 1.5 to $K(\sqrt{d})/\mathbb{Q}(\sqrt{ab})$, then to $\mathbb{Q}(\sqrt{ab},\sqrt{d})/\mathbb{Q}$, then

$$\left(\frac{K(\sqrt{d})/K}{\mathfrak{v}}\right) = \left(\frac{\mathbb{Q}(\sqrt{ab},\sqrt{d})/\mathbb{Q}(\sqrt{ab})}{\mathrm{Norm}_{K/\mathbb{Q}(\sqrt{ab})}\,\mathfrak{v}}\right) = \begin{cases} \left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{p}\right) & \text{if } p \nmid \Delta_{\mathbb{Q}(\sqrt{d})}, \\ \left(\frac{\mathbb{Q}(\sqrt{ab/d})/\mathbb{Q}}{p}\right) & \text{if } p \nmid \Delta_{\mathbb{Q}(\sqrt{ab/d})}. \end{cases}$$

We must be in at least one of the two cases by (2.9). Converting to the Hilbert symbol,

$$\left(\frac{K(\sqrt{d})/K}{\mathfrak{v}}\right) = (d,c)_p. \tag{2.10}$$

since by assumption $(ab,c)_p = (a,c)_p(b,c)_p = 1$.

Since c is squarefree, multiplying the symbols (2.10) over $\mathfrak{v} \mid \mathbf{c}$ then applying Hilbert reciprocity, we have

$$\left(\frac{K(\sqrt{d})/K}{\mathbf{c}}\right) = \prod_{p|c}(d,c)_p = (d,c)_\infty \prod_{p\nmid c}(d,c)_p.$$

If $c > 0$ then $(d,c)_\infty = 1$. If c is negative, then

$$\left(\frac{K(\sqrt{d})/K}{\infty}\right) = (d,c)_\infty.$$

Therefore it remains to show that

$$\prod_{p\nmid c}(d,c)_p = 1. \tag{2.11}$$

For any odd p dividing d but not c, p must divide a or b because of (2.9), so

$$(d,c)_p = \left(\frac{\mathbb{Q}(\sqrt{c})/\mathbb{Q}}{p}\right) = \begin{cases} (a,c)_p & \text{if } p \mid a, \\ (b,c)_p & \text{if } p \mid b \end{cases} = 1.$$

If $p \nmid 2cd$, we have $(d,c)_p = 1$.

The term $(d,c)_2$ only appear in (2.11) when c is odd. If c is odd and $2 \nmid S_{a,b}$, then from (2.9), $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ or $\mathbb{Q}(\sqrt{ab/d})/\mathbb{Q}$ is unramified at 2, so $(d,c)_2 = 1$. The remaining case is when c is odd and $2 \mid S_{a,b}$. Since $\Delta_{\mathbb{Q}(\sqrt{c})}$ is coprime to $S_{a,b}$, we must have $c \equiv 1 \bmod 4$. If $c \equiv 1 \bmod 8$, then $(d,c)_2 = 1$, so the remaining case is $c \equiv 5 \bmod 8$. To satisfy (2.7), we are left with the case in (2.8), but our assumption ensures d is odd, so $(d,c)_2 = 1$. □

We see from the following example that the value of the Artin symbol depends on the choice of β if (2.8) is not assumed.

Example 2.7. *Take $a = 23 \equiv 3 \bmod 4$, $b = 13 \equiv 5 \bmod 8$ and $c = 29 \equiv 5 \bmod 8$, which satisfy (2.6) and (2.7). We find that $(x,y,z) = (6,1,1)$ and $(29,1,6)$ are both solutions to $x^2 - ay^2 = bz^2$. Set $\beta = 6+\sqrt{13}$ and $\beta' = 29+\sqrt{13}$, then $K(\sqrt{\beta})/\mathbb{Q}$ and $K(\sqrt{\beta'})/\mathbb{Q}$ are both unramified at 29, but $\left(\frac{K(\sqrt{\beta})/K}{\mathbf{c}}\right) = 1$ and $\left(\frac{K(\sqrt{\beta'})/K}{\mathbf{c}}\right) = -1$ for any ideal $\mathbf{c}$ in K with norm 29.*

We now define the Rédei symbol.

Definition 2.8 (Rédei symbol)**.** *For any triple $(A,B,C) \in \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q}^\times$ satisfying conditions (2.6) and (2.7), take a,b,c to be the squarefree integers such that $(a,b,c) = (r^2A, s^2B, t^2C)$ for some $r,s,t \in \mathbb{Q}^\times$. Define $K = \mathbb{Q}(\sqrt{a},\sqrt{b})$. If $a,b,c \neq 1$, take any $\beta \in \mathcal{F}_{a,b}$ which satisfies (2.8), and any ideal $\mathbf{c}$ in K of norm $|c|$. The Rédei symbol is defined by*

$$[A,B,C] = \begin{cases} \left(\frac{K(\sqrt{\beta})/K}{\mathbf{c}}\right) & \text{if } c > 0 \text{ and } 1 \notin \{a,b,c\}, \\ \left(\frac{K(\sqrt{\beta})/K}{\mathbf{c}\infty}\right) & \text{if } c < 0 \text{ and } 1 \notin \{a,b,c\}, \\ 1 & \text{if } 1 \in \{a,b,c\}. \end{cases}$$

2.3 Proof of Rédei reciprocity

Our aim is to prove the following theorem using Hilbert reciprocity.

Theorem 2.9 (Rédei reciprocity)**.** *For $a, b, c \in \mathbb{Q}^\times$ satisfying the conditions* (2.6), (2.7)*, we have*

$$[a, b, c] = [a, c, b].$$

It suffices to prove Theorem 2.9 assuming $a, b, c \neq 1$ are nonzero squarefree integers. We can also fix $\beta \in \mathcal{F}'_{a,b}$ and $\gamma \in \mathcal{F}'_{a,c}$, since they automatically satisfy (2.8), and the Rédei symbols are independent of such choices. Define $K_{a,b} = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, $K_{a,c} = \mathbb{Q}(\sqrt{a}, \sqrt{c})$, $L_{a,b} = \mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{\beta})$ and $L_{a,c} = \mathbb{Q}(\sqrt{a}, \sqrt{c}, \sqrt{\gamma})$.

We will prove the following more explicit version of Theorem 2.9.

Theorem 2.10. *Let $a, b, c \neq 1$ be nonzero squarefree integers satisfying* (2.6) *and* (2.7)*. Take $\mathbf{c}$ to be an ideal in $K_{a,b}$ which has norm $|c|$ and $\mathbf{b}$ to be an ideal in $K_{a,c}$ which has norm $|b|$. Then*

$$\left(\frac{L_{a,b}/K_{a,b}}{\mathbf{c}}\right)\left(\frac{L_{a,c}/K_{a,c}}{\mathbf{b}}\right) = \begin{cases} \left(\frac{L_{a,b}/K_{a,b}}{\infty}\right) & \text{if } c < 0, \\ \left(\frac{L_{a,c}/K_{a,c}}{\infty}\right) & \text{if } b < 0, \\ 1 & \text{if } b > 0 \text{ and } c > 0. \end{cases}$$

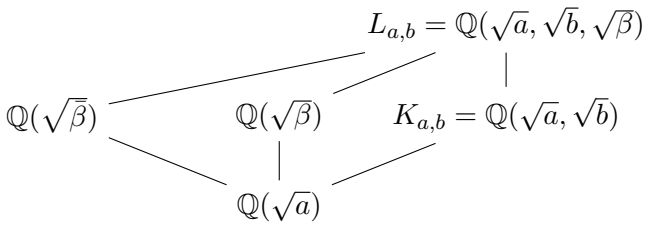
Theorem 2.9 is immediate from Theorem 2.10.

Now $L_{a,b}/K_{a,b}$ and $L_{a,c}/K_{a,c}$ are unramified at primes outside $S_{a,b}$ and $S_{a,c}$ respectively. Take $\mathbf{c}$ to be an ideal in $K_{a,b}$ which divides γ, and has norm $|c|$. Take $\mathbf{b}$ to be an ideal in $K_{a,c}$ which divides β, and has norm $|b|$. It is possible to pick such $\mathbf{b}$ and $\mathbf{c}$ by the following lemma.

Lemma 2.11. *There exists an ideal $\mathbf{c}$ in $K_{a,b}$ such that* $\mathrm{Norm}_{K_{a,b}/\mathbb{Q}(\sqrt{a})}(\mathbf{c}) = [\gamma]$*, and* $\mathrm{Norm}(\mathbf{c}) = |c|$*.*

Proof. Let $\mathfrak{p}$ be a prime in $\mathbb{Q}(\sqrt{a})$ above some prime p in $\mathbb{Q}$. Only at most one prime $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{a})$ above p can divide γ, since $p \nmid \gamma$. From the defining equation for γ, we get $\gamma\bar{\gamma} = cz^2$ or $c(z/2)^2$ for some $z \in \mathbb{Z}$, if $\mathfrak{p} \mid [\gamma]$, then $p \mid c$. Any $p \mid c$ must either ramify or split in $\mathbb{Q}(\sqrt{b})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ by (2.7). Since c is squarefree, we have $\mathrm{ord}_{\mathfrak{p}}[\gamma] = \mathrm{ord}_p c$. For each $p \mid c$, we can take a prime $\mathfrak{v}$ in $K_{a,b}$ above $\mathfrak{p}$ so that $\mathrm{Norm}_{K_{a,b}/\mathbb{Q}} \mathfrak{v} = p$. We take $\mathbf{c}$ to be a product of such $\mathfrak{v}$ over all $p \mid c$, then $\mathbf{c}$ satisfies the required properties. □

For any prime $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{a})$, we study the Hilbert symbol $(\beta, \gamma)_{\mathfrak{p}}$ according to



the ramification of $\mathfrak{p}$ in the extensions $\mathbb{Q}(\sqrt{\beta})$, $\mathbb{Q}(\sqrt{\bar{\beta}})$, $\mathbb{Q}(\sqrt{\gamma})$ and $\mathbb{Q}(\sqrt{\bar{\gamma}})$. Notice that $L_{a,b}/\mathbb{Q}(\sqrt{a})$ and $L_{a,c}/\mathbb{Q}(\sqrt{a})$ are V_4-extensions.

Lemma 2.12. *If $\mathfrak{p}$ is unramified in $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$, then*

$$(\beta, \gamma)_{\mathfrak{p}} = \left(\frac{L_{a,b}/K_{a,b}}{\mathfrak{v}}\right)^{\mathrm{ord}_{\mathfrak{p}}[\gamma]},$$

where $\mathfrak{v}$ is any prime in $K_{a,b}$ lying above $\mathfrak{p}$.

Proof. Note that $\mathfrak{p}$ being unramified in $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ implies that $\mathfrak{v}$ is unramified in $L_{a,b}/K_{a,b}$ by Lemma 1.6.

By Lemma 1.4,

$$(\beta, \gamma)_{\mathfrak{p}} = \left(\frac{\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}[\gamma]}.$$

We are done if $\mathrm{ord}_{\mathfrak{p}}[\gamma] = 0$, so assume $\mathrm{ord}_{\mathfrak{p}}[\gamma] = 1$. By Lemma 2.11, we have $\mathrm{Norm}_{K_{a,b}/\mathbb{Q}(\sqrt{a})}\,\mathfrak{v} = \mathfrak{p}$. Since $\mathrm{Gal}(L_{a,b}/\mathbb{Q}(\sqrt{a})) \cong V_4$, we can apply Lemma 1.5 to get

$$\left(\frac{\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})}{\mathrm{Norm}_{K_{a,b}/\mathbb{Q}(\sqrt{a})}\,\mathfrak{v}}\right) = \left(\frac{L_{a,b}/K_{a,b}}{\mathfrak{v}}\right). \qquad \square$$

If $\mathfrak{p}$ is odd and $\mathfrak{p} \mid [\beta]$ and $\mathfrak{p} \mid [\gamma]$. By Lemma 2.11, we can find $\mathfrak{v}$ and $\mathfrak{u}$ that are unramified in $L_{a,c}/K_{a,c}$ and $L_{a,b}/K_{a,b}$ respectively.

Lemma 2.13. *Suppose $\mathfrak{p}$ ramifies in both $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}(\sqrt{a})$. If $\{a, b\} \equiv \{3 \bmod 4,\ 5 \bmod 8\}$ or $\{a, c\} \equiv \{3 \bmod 4,\ 5 \bmod 8\}$, assume further that $\mathfrak{p}$ is odd. Let $\mathfrak{v}$ be a prime in $K_{a,b}$ lying above $\mathfrak{p}$, and $\mathfrak{u}$ be a prime in $K_{a,c}$ lying above $\mathfrak{p}$. Then*

$$(\beta, \gamma)_{\mathfrak{p}} = \left(\frac{L_{a,c}/K_{a,c}}{\mathfrak{u}}\right)^{\mathrm{ord}_{\mathfrak{p}}[\beta]} \left(\frac{L_{a,b}/K_{a,b}}{\mathfrak{v}}\right)^{\mathrm{ord}_{\mathfrak{p}}[\gamma]},$$

Proof. Since $\mathbb{Q}_p \subseteq \mathbb{Q}(\sqrt{a})_{\mathfrak{p}}$, we have $(b, c)_{\mathfrak{p}} = 1$ from the assumption $(b, c)_p = 1$. By

the multiplicativity of the Hilbert symbol, we have

$$1 = (b,c)_{\mathfrak{p}} = (\beta,\gamma)_{\mathfrak{p}}(\bar{\beta},\gamma)_{\mathfrak{p}}(\beta,\bar{\gamma})_{\mathfrak{p}}(\bar{\beta},\bar{\gamma})_{\mathfrak{p}}.$$

Since $\mathfrak{p}$ ramifies in both $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}(\sqrt{a})$, by Lemma 2.3 and Lemma 2.4, $\mathfrak{p} \mid \Delta_{\mathbb{Q}(\sqrt{b})}$ and $\mathfrak{p} \mid \Delta_{\mathbb{Q}(\sqrt{c})}$. By (2.6), $\mathfrak{p} \nmid \Delta_{\mathbb{Q}(\sqrt{a})}$, so $\mathfrak{p} \nmid S_{a,b}$ and $\mathfrak{p} \nmid S_{a,c}$, so $\mathfrak{v}$ is unramified in $L_{a,b}/K_{a,b}$, and $\mathfrak{u}$ is unramified in $L_{a,c}/K_{a,c}$. Taking the inertia field of $\mathfrak{p}$ in in $L_{a,b}/\mathbb{Q}(\sqrt{a})$, we see that $\mathfrak{p}$ must be unramified in $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$. Similarly we see that $\mathfrak{p}$ is unramified in $\mathbb{Q}(\sqrt{\bar{\gamma}})/\mathbb{Q}(\sqrt{a})$.

Now we can apply Lemma 2.12 to $(\bar{\beta},\gamma)_{\mathfrak{p}}$, $(\beta,\bar{\gamma})_{\mathfrak{p}}$ and $(\bar{\beta},\bar{\gamma})_{\mathfrak{p}}$. □

If $\mathfrak{p}$ is unramified in $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ or $\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}(\sqrt{a})$, we can apply Lemma 2.12. Otherwise $\mathfrak{p}$ is ramified in both $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}(\sqrt{a})$, then we can apply Lemma 2.13, except when $\mathfrak{p}$ is even and $\{a,b,c\} \equiv \{3 \bmod 4,\ 5 \bmod 8,\ 5 \bmod 8\}$ or $\{3 \bmod 4,\ 1 \bmod 8,\ 5 \bmod 8\}$. If $a \equiv b \equiv 1 \bmod 4$ or $a \equiv c \equiv 1 \bmod 4$, or one of a,b,c is congruent to $1 \bmod 8$, then $\mathfrak{p}$ is unramified in $\mathbb{Q}(\sqrt{\beta})/\mathbb{Q}(\sqrt{a})$ or $\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}(\sqrt{a})$ by Lemma 2.4, so we we are covered by Lemma 2.12. Therefore the remaining case is when $\mathfrak{p}$ is even and $a \equiv 3 \bmod 4$, and $b \equiv c \equiv 5 \bmod 8$.

Lemma 2.14. *Suppose $a \equiv 3 \bmod 4$, and $b \equiv c \equiv 5 \bmod 8$. Let $\mathfrak{p}$ be an even prime in $\mathbb{Q}(\sqrt{a})$. Then $(\beta,\gamma)_{\mathfrak{p}} = 1$.*

Proof. By (2.4b) and from the equation $x^2 - ay^2 \equiv 5z^2 \bmod 8$, we see that $\beta \equiv \gamma \equiv 3+2\sqrt{a} \bmod 4$, so each of β and γ is congruent to one of $\{3\pm2\sqrt{a}, -1\pm2\sqrt{a}\} \bmod 8$. Since $(3+2\sqrt{a})(1+2\sqrt{a}) \equiv -1 \bmod 8$ and $(3+2\sqrt{a})(3-2\sqrt{a}) = (1+2\sqrt{a})(1-2\sqrt{a}) \equiv 5 \bmod 8$, it suffices to compute the Hilbert symbol between $3+2\sqrt{a}$, -1 and 5. The fact that $(5,5)_{\mathfrak{p}} = (5,-1)_{\mathfrak{p}} = 1$ follows from the Hilbert symbol at the rational prime 2. Since $(\sqrt{a})^2$ is congruent to either -5 or $-1 \bmod 8$, we also have $(-1,-1)_{\mathfrak{p}} = 1$. Notice that

$$\begin{aligned}(\sqrt{a})^2 &\equiv (3+2\sqrt{a}) + (3+2\sqrt{a})(1+\sqrt{a})^2 \bmod 8,\\ (2+\sqrt{a})^2 &\equiv (3+2\sqrt{a}) + 5(1+\sqrt{a})^2 \bmod 8, \text{ and}\\ (2+\sqrt{a})^2 &\equiv (3+2\sqrt{a}) - (1-\sqrt{a})^2 \bmod 8.\end{aligned}$$

Hensel's Lemma implies that $(3+2\sqrt{a}, 3+2\sqrt{a})_{\mathfrak{p}} = (3+2\sqrt{a}, 5)_{\mathfrak{p}} = (3+2\sqrt{a}, -1)_{\mathfrak{p}} = 1$. By the multiplicativity of the Hilbert symbol, we have $(\beta,\gamma)_{\mathfrak{p}} = 1$. □

From Lemma 2.12, Lemma 2.13, and Lemma 2.14, we conclude the following.

Lemma 2.15. *Let $\mathfrak{p}$ be a prime in $\mathbb{Q}(\sqrt{a})$. Let $\mathfrak{v}$ be a prime in $K_{a,b}$ lying above $\mathfrak{p}$, and $\mathfrak{u}$ be a prime in $K_{a,c}$ lying above $\mathfrak{p}$. Then*

$$(\beta,\gamma)_{\mathfrak{p}} = \begin{cases} \left(\frac{L_{a,c}/K_{a,c}}{\mathfrak{u}}\right)\left(\frac{L_{a,b}/K_{a,b}}{\mathfrak{v}}\right) & \text{if } \operatorname{ord}_{\mathfrak{p}}[\beta] = \operatorname{ord}_{\mathfrak{p}}[\gamma] = 1, \\ \left(\frac{L_{a,c}/K_{a,c}}{\mathfrak{u}}\right) & \text{if } \operatorname{ord}_{\mathfrak{p}}[\beta] = 1 \text{ and } \operatorname{ord}_{\mathfrak{p}}[\gamma] = 0, \\ \left(\frac{L_{a,b}/K_{a,b}}{\mathfrak{v}}\right) & \text{if } \operatorname{ord}_{\mathfrak{p}}[\beta] = 0 \text{ and } \operatorname{ord}_{\mathfrak{p}}[\gamma] = 1, \\ 1 & \text{if } \operatorname{ord}_{\mathfrak{p}}[\beta] = \operatorname{ord}_{\mathfrak{p}}[\gamma] = 0. \end{cases}$$

We now look at the places at infinity.

Lemma 2.16. *We have*

$$\prod_{\mathfrak{p}|\infty}(\beta,\gamma)_{\mathfrak{p}} = \begin{cases} \left(\frac{L_{a,b}/K_{a,b}}{\infty}\right) & \text{if } c < 0, \\ \left(\frac{L_{a,c}/K_{a,c}}{\infty}\right) & \text{if } b < 0, \\ 1 & \text{if } b > 0 \text{ and } c > 0. \end{cases}$$

Proof. Suppose $\mathfrak{p}$ is a place at infinity in $K_{a,b}$. Note that $(\beta,\gamma)_{\mathfrak{p}} = -1$ is only possible when $\mathbb{Q}(\sqrt{a})$ is real and β,γ are both negative in $\mathbb{Q}(\sqrt{a})_{\mathfrak{p}}$. If $a > 0$, then there are two embeddings of $\mathbb{Q}(\sqrt{a})$. Now $\prod_{\mathfrak{p}|\infty}(\beta,\gamma)_{\mathfrak{p}} = -1$ if and only if exactly one of $\{\beta,\gamma\}, \{\bar{\beta},\bar{\gamma}\}$ contains all negative elements. This can only happen when $b < 0$ or $c < 0$. Note that b and c cannot both be negative since $(b,c)_{\infty} = 1$.

By symmetry we only need to prove one of the two cases $b < 0$ and $c < 0$. Suppose $c < 0$, so exactly one of $\gamma, \bar{\gamma}$ is negative and $a, b > 0$. Then $\left(\frac{L_{a,b}/K_{a,b}}{\infty}\right) = -1$ if and only if $\beta, \bar{\beta} < 0$ and this holds precisely when $\prod_{\mathfrak{p}|\infty}(\beta,\gamma)_{\mathfrak{p}} = -1$. □

Hilbert reciprocity formula in $\mathbb{Q}(\sqrt{a})$ states that

$$\prod_{\mathfrak{p}\in\mathcal{M}_{\mathbb{Q}(\sqrt{a})}} (\beta,\gamma)_{\mathfrak{p}} = 1.$$

Substitute each term $(\beta,\gamma)_{\mathfrak{p}}$ with the expressions in Lemma 2.15 and Lemma 2.16, then Theorem 2.10 follows from Lemma 2.11.

2.4 Symmetry in entries

The Rédei symbol, where it is defined, is symmetric in its first two entries by construction. It follows from Rédei reciprocity that any two entries are symmetric.

Rédei reciprocity also allows multiplicativity to hold at any entry. Since the Rédei symbol is defined as an Artin symbol, it is multiplicative in the last entry. We get $[a,b,c][a,b,c'] = [a,b,cc']$ where the symbols are defined. By Rédei reciprocity, we have

$$[a,b,c][a,b',c] = [a,c,b][a,c,b'] = [a,c,bb'] = [a,bb',c].$$

2.5 Rédei symbol for decompositions of second type

We now check that the Rédei symbol defined in Definition 2.8 is actually a more general version of Definition 1.14.

We use the description of the elements in $\mathcal{U}_2$ as decompositions of second type in Theorem 1.12. Suppose $D = ab$ and $\{a,b\}$ is a decomposition of second type for $\mathbb{Q}(\sqrt{D})$. Take $c \in \mathcal{V}_2$. We proceed to check the conditions in Definition 2.8 holds for a, b and c.

It is immediate from the definition of decomposition of second type that $(a,b)_p = 1$ for all primes $p \leq \infty$. We also have $\gcd(a,b) = 1$, which implies $S(a) \cap S(b) = \varnothing$, so (2.6) always holds. Since if one of a, b is even, the other has to be 1 mod 8, (2.8) does not apply to decomposition of second type.

We still need to check $(a,c)_p = (b,c)_p = 1$ for all primes $p \leq \infty$. By (1.12), we have $(D,c)_p = 1$ for all primes $p \leq \infty$. Note that $(D,c)_p = (a,c)_p(b,c)_p$, so it suffices to show that for each p, one of $(a,c)_p$ and $(b,c)_p$ is 1. Suppose $p \nmid c$. Since $\gcd(a,b) = 1$, we have $p \nmid a$ or $p \nmid b$, which implies $(a,c)_p = 1$ or $(b,c)_p = 1$. Now suppose $p \mid c$, since c must split in at least one of $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$, then either $(a,c)_p = \left(\frac{a}{p}\right) = 1$ or $(b,c)_p = \left(\frac{b}{p}\right) = 1$.

Chapter 3

Governing fields and the distribution of the 8-rank

In this chapter, we will present an application of Rédei reciprocity. Corsman [27] used Rédei reciprocity to construct a minimal governing field for the 8-rank of class groups of quadratic fields, that is, a Galois extension $\Omega(d)/\mathbb{Q}$ such that the splitting of primes p in $\Omega(d)/\mathbb{Q}$ determines $\mathrm{rk}_8 \mathbf{C}_{dp}$. Governing fields are useful because Chebotarev density theorem allows us to determine the density of different splitting behaviour of primes.

The distribution of the 4-rank was predicted by an extension of Cohen-Lenstra heuristics [22] by Gerth [35]. Fouvry and Klüners [30] proved that the 4-rank of class groups of quadratic number fields behaves as predicted. Using Corsman's construction, Smith [80] found the distribution of the 8-rank of the class groups of imaginary quadratic fields, assuming the general Riemann hypothesis. Subsequently Smith proved unconditionally the distribution of the full 2-primary part of class groups of imaginary quadratic field [81].

In Theorem 3.21, we extend Smith's initial conditional result to real quadratic fields. Let $\mathcal{D}(N)$ be the set of positive squarefree integer less than N. We will prove the following.

Theorem 3.1. *Assume the general Riemann hypothesis. For any $m \geq j \geq 0$ and*

any $\delta \in \{\pm 1\}$*, we have*

$$\lim_{N\to\infty} \frac{\#\{\delta \cdot D \in \mathcal{D}(N) : \mathrm{rk}_4 \mathbf{C}_D = m,\ \mathrm{rk}_8 \mathbf{C}_D = j\}}{\#\{\delta \cdot D \in \mathcal{D}(N) : \mathrm{rk}_4 \mathbf{C}_D = m\}} = \begin{cases} \mathrm{Prob}(j \mid m, m+1) & \text{if } \delta = 1, \\ \mathrm{Prob}(j \mid m, m) & \text{if } \delta = -1, \end{cases}$$

where

$$\mathrm{Prob}(j \mid m, n) := \frac{\#\{M \in \mathrm{Mat}_{m\times n}(\mathbb{F}_2) : \mathrm{corank}(M) = j\}}{\#\,\mathrm{Mat}_{m\times n}(\mathbb{F}_2)} \tag{3.1}$$

and $\mathrm{Mat}_{m\times n}(\mathbb{F}_2)$ *denotes the space of* $m \times n$ *matrices over* $\mathbb{F}_2$*.*

The $\delta = -1$ case is due to Smith [80].

3.1 Frobenian maps

Let X be a discrete set. A map $f : \mathcal{M}_K \to X$ is called *Frobenian* [70, Section 3.3] if there exists a Galois extension E/K, and a map $\varphi : \mathrm{Gal}(E/K) \to X$ such that

(i) φ is invariant under conjugation, and

(ii) $f(\mathfrak{p}) = \varphi(\left(\frac{E/K}{\mathfrak{p}}\right))$ for any $\mathfrak{p} \in \mathcal{M}_K$ that is unramified in E/K.

When f is a Frobenian map, we call any field E satisfying the above a governing field of f. Since the Chebotarev Density Theorem is a ready-made tool for studying densities of prime numbers, it is of particular interest to determine when a map is Frobenian.

3.1.1 Chebotarev density theorem

Chebotarev density theorem is a useful tool in studying splitting behaviour of primes.

Theorem 3.2 (Chebotarev density theorem, [43, Chapter V, Theorem 10.4], [60, Chapter V, Theorem 6.4])**.** *Let* L/K *be an abelian extension. Then given any conjugacy class* C *in* $\mathrm{Gal}(L/K)$*,*

$$\lim_{n\to\infty} \frac{\#\{\mathfrak{p} \text{ prime in } K : \mathrm{Norm}(\mathfrak{p}) < n,\ \left(\frac{L/K}{\mathfrak{p}}\right) = C\}}{\#\{\mathfrak{p} \text{ prime in } K : \mathrm{Norm}(\mathfrak{p}) < n\}} = \frac{\#C}{[L:K]}.$$

Lagarias and Odlyzko also proved an effective form of Chebotarev density theorem [52, Corollary 1.3]. However, their result only holds for $n \geq \exp(10 \cdot [L :$

$\mathbb{Q}](\log \Delta_{L/\mathbb{Q}})^2)$, which is not applicable when the discriminant of the field is too large relative to n. If we are allowed to assume the generalised Riemann hypothesis, such requirement can be weakened. The following conditional result was proved by Lagarias and Odlyzko, and refined by Serre.

Theorem 3.3 (Effective Chebotarev density theorem, [52, Theorem 1.1], [69, Théorème 4])**.** *Let L/K be a Galois extension. Assume that the generalised Riemann hypothesis holds for the Dedekind zeta function associated to L. Then given any conjugacy class C in* $\mathrm{Gal}(L/K)$*, we have*

$$\begin{aligned}&\#\left\{\mathfrak{p} \text{ prime in } K : \mathrm{Norm}(\mathfrak{p}) < n,\ \left(\frac{L/K}{\mathfrak{p}}\right) = C\right\}\\ &= \frac{\mathrm{Li}(n)\#C}{[L:K]}\left(1 + O\left(\frac{\log n}{\sqrt{n}}\left(\log \Delta_{L/\mathbb{Q}} + [L:\mathbb{Q}]\log n\right)\right)\right).\end{aligned}$$

In Theorem 3.3, having $n \geq (\log \Delta_{L/\mathbb{Q}})^{2+\epsilon} + [L:\mathbb{Q}]^{2+\epsilon}$ is enough to give us our desired asymptotics as $n \to \infty$.

We can show that the density of primes in $\mathfrak{p}$ in K with inertia degree 1 over $\mathbb{Q}$ has density 1. Let p be the rational prime below $\mathfrak{p}$. If p does not split completely in $K/\mathbb{Q}$, then $p^2 \leq \mathrm{Norm}(\mathfrak{p}) < n$. There are $\ll \sqrt{\mathrm{Li}(n)}$ such p by the prime number theorem. Therefore the set of prime $\mathfrak{p}$ in K such that $\mathbb{Z} \cap \mathfrak{p}$ splits completely in $K/\mathbb{Q}$ has density 1, more precisely

$$\frac{\#\{\mathfrak{p} \text{ prime in } K : \mathrm{Norm}(\mathfrak{p}) < n,\ \left(\frac{K/\mathbb{Q}}{\mathbb{Z}\cap\mathfrak{p}}\right) = \mathrm{id}\}}{\#\{\mathfrak{p} \text{ prime in } K : \mathrm{Norm}(\mathfrak{p}) < n\}} = 1 + O\left(\frac{1}{\sqrt{\mathrm{Li}(n)}}\right).$$

Moreover, when $L/\mathbb{Q}$ is Galois and L/K is an abelian, if p splits completely in $K/\mathbb{Q}$, the conjugacy class $\left(\frac{L/\mathbb{Q}}{p}\right)$ contains exactly 1 element. This allows us to deduce the following from Theorem 3.2 and Theorem 3.3.

Corollary 3.4. *Let L/K be an abelian extension and $L/\mathbb{Q}$ be a Galois extension. Then given any $\sigma \in \mathrm{Gal}(L/K)$,*

$$\lim_{n\to\infty} \frac{\#\{p < n \text{ prime} : \left(\frac{L/\mathbb{Q}}{p}\right) = \sigma\}}{\#\{p < n \text{ prime} : p \text{ splits completely in } L/\mathbb{Q}\}} = \frac{1}{[L:K]}.$$

Corollary 3.5. *Let L/K be an abelian extension and $L/\mathbb{Q}$ be a Galois extension. Assume that the generalised Riemann hypothesis holds for the Dedekind zeta function*

associated to L. Then given any $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\begin{aligned}&\#\left\{p < n \text{ prime} : \left(\frac{L/\mathbb{Q}}{p}\right) = \sigma\right\}\\ &= \frac{\mathrm{Li}(n)}{[L:\mathbb{Q}]}\left(1 + O\left(\frac{\log n}{\sqrt{n}}\left(\log \Delta_{L/\mathbb{Q}} + [L:\mathbb{Q}]\log n\right)\right)\right).\end{aligned}$$

3.2 Governing fields for the 2^k-rank of class groups

Cohn and Lagarias [23] conjectured that governing fields exists for the 2^k-rank of class groups of quadratic fields. In other words, more precisely, for fixed d and j, the map f_d sending primes p to the sequence $\{\mathrm{rk}_{2^k}\mathbf{C}_{dp}\}_{k\le j}$ is Frobenian.

Conjecture 3.6. *Given integers d and j, there exists a normal extension $\Omega_j(d)$ of $\mathbb{Q}$ having the following property. If p and p_0 are primes such that $\left(\frac{\Omega_j(d)/\mathbb{Q}}{p}\right) = \left(\frac{\Omega_j(d)/\mathbb{Q}}{p_0}\right)$, then $\mathrm{rk}_{2^k}\mathbf{C}_{dp} = \mathrm{rk}_{2^k}\mathbf{C}_{dp_0}$ for $1 \le k \le j$.*

If such a field $\Omega_j(d)$ exits, we call it a governing field for the 2^j-rank. Cohn and Lagarias also showed that the conjecture holds for $j = 1$ and $j = 2$. The cases $j = 1$ and $j = 2$ are relatively straightforward. The existence of governing fields for $j = 3$ was first proved by Stevenhagen in [85]. Corsman [27] gave a different proof by constructing the governing fields explicitly using Rédei reciprocity. We will present the construction of governing fields $\Omega_3(d)$, following Corsman's approach. No governing field has been found for $j \ge 4$ so far.

3.2.1 Building on a common basis

The case $j = 1$ follows from genus theory.

Theorem 3.7. *$\Omega_1(d) = \mathbb{Q}(\sqrt{-1}, \sqrt{d})$ is a governing field for the 2-rank.*

Proof. Suppose $\left(\frac{\Omega_j(d)/\mathbb{Q}}{p}\right) = \left(\frac{\Omega_j(d)/\mathbb{Q}}{p_0}\right)$. Then p has to be unramified in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$, so $p, p_0 \nmid 2d$. Also $\left(\frac{-1}{p}\right) = \left(\frac{-1}{p_0}\right)$ implies that $p \equiv p_0 \bmod 4$, so $dp \equiv dp_0 \bmod 4$ and $\omega(\Delta_{\mathbb{Q}(\sqrt{dp})}) = \omega(\Delta_{\mathbb{Q}(\sqrt{dp_0})})$, where ω denotes the number of distinct prime factors. Since $\mathrm{rk}_2(dp) = \omega(\Delta_{\mathbb{Q}(\sqrt{dp})}) - 1$, we have $\mathrm{rk}_2\mathbf{C}_{dp} = \mathrm{rk}_2\mathbf{C}_{dp_0}$. □

Suppose $\Delta_{\mathbb{Q}(\sqrt{dp_0})}$ has prime factors $p_0, \ldots, p_{t-1}$, where $p_0 \ne 2$. Observe that for the set of fields $\{\mathbb{Q}(\sqrt{dp}) : \left(\frac{\Omega_1(d)/\mathbb{Q}}{p}\right) = \left(\frac{\Omega_1(d)/\mathbb{Q}}{p_0}\right)\}$, we can take a common bases

$S = \{p_1^*, \ldots, p_{t-1}^*\}$ for $\overline{\mathcal{U}}_1$ and

$$T = \begin{cases} \{p_1, \ldots, p_{t-1}, -1\} \text{ for } \mathcal{V}_1 & \text{if } d > 0, \\ \{p_1, \ldots, p_{t-1}\} \text{ for } \overline{\mathcal{V}}_1 & \text{if } d < 0. \end{cases}$$

The existence of $\Omega_2(d)$ follows from the Rédei's work. Given fields with the same $\overline{\mathcal{U}}_1$ and $\mathcal{V}_1$, we look for those which have the same $\mathcal{V}_2$, hence the same 4-rank.

Proposition 3.8 (Governing field for 4-rank)**.** *Fix a squarefree integer d. Let $p_1, \ldots, p_r$ be distinct odd prime factors of d. Let*

$$\Omega_2(d) = \mathbb{Q}\Big(\sqrt{-1}, \sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_r}\Big).$$

Suppose p and p_0 are primes that satisfy $\left(\frac{\Omega_2(d)/\mathbb{Q}}{p}\right) = \left(\frac{\Omega_2(d)/\mathbb{Q}}{p_0}\right)$. Then $R_{1,S,T}(dp) = R_{1,S,T}(dp_0)$ and hence $\operatorname{rk}_4 \mathbf{C}_{dp} = \operatorname{rk}_4 \mathbf{C}_{dp_0}$. In particular, $\Omega_2(d)$ is a governing field for the 4-rank of $\{\mathbf{C}_{dp}\}_p$.

Proof. Suppose p and p_0 are primes so that $\left(\frac{\Omega_2(d)/\mathbb{Q}}{p}\right) = \left(\frac{\Omega_2(d)/\mathbb{Q}}{p_0}\right)$. Since $\Omega_1(d) \subseteq \Omega_2(d)$, we see that p and p_0 must be odd, $dp_0 \equiv dp \bmod 4$, and $p, p_0 \nmid d$. Suppose $p_0, p_1, \ldots, p_{t-1}$ are the distinct prime factors of $\Delta_{\mathbb{Q}(\sqrt{dp_0})}$. Restricting to subfields of $\Omega_2(d)$, we see that $\left(\frac{-1}{p}\right) = \left(\frac{-1}{p_0}\right)$ and $\left(\frac{2}{p}\right) = \left(\frac{2}{p_0}\right)$. This implies that $p \equiv p_0 \bmod 8$. We also see that $\left(\frac{p_j}{p}\right) = \left(\frac{p_j}{p_0}\right)$, for odd p_j and $j \in \{1, \ldots, t-1\}$. The only possible difference in the entries of $R_{1,S,T}(dp)$ and $R_{1,S,T}(dp_0)$ are on the diagonal. The diagonal entries of $R_{1,S,T}(dp_0)$ are $\left(\frac{\prod_{i \in \{0,\ldots,t-1\} \setminus j} p_i^*}{p_j}\right)_+$ for $j = 1, \ldots, t-1$. Therefore it suffices to show that $\left(\frac{p_0^*}{p_j}\right) = \left(\frac{p^*}{p_j}\right)$ and $\left(\frac{\prod_{1 \le i \le t-1} p_i^*}{p_0}\right) = \left(\frac{\prod_{1 \le i \le t-1} p_i^*}{p}\right)$. This follows from quadratic reciprocity. Therefore $R_{1,S,T}(dp) = R_{1,S,T}(dp_0)$. □

For odd primes $p_0 \nmid d$, define

$$A_{d,p_0} = \{p \text{ prime} : p \nmid 2d \text{ and } p_0 p \text{ square modulo } 8d\}.$$

Let $A_{d,p_0}(n) = \{p \in A_{d,p_0} : p < n\}$.

From the proof of Proposition 3.8, we see the following by restricting to quadratic subfields of $\Omega_2(d)/\mathbb{Q}$.

Lemma 3.9. *Suppose p and p_0 are primes. Then the following are equivalent*

(i) $p \in A_{d,p_0}$,

(ii) $\left(\frac{\Omega_2(d)/\mathbb{Q}}{p}\right) = \left(\frac{\Omega_2(d)/\mathbb{Q}}{p_0}\right)$.

Proposition 3.8 gives us a condition that is enough for $R_{1,S,T}(dp) = R_{1,S,T}(dp_0)$ to hold. Therefore we can find a basis for $\overline{\mathcal{U}}_2 = \operatorname{coker} R_1$ that is common for $\mathbb{Q}(\sqrt{dp})$ and $\mathbb{Q}(\sqrt{dp_0})$, and also for $\ker R_1$, which is $\mathcal{V}_2$ if $d > 0$ and $\overline{\mathcal{V}}_2$ if $d < 0$. Our aim is to determine the fields $\mathbb{Q}(\sqrt{dp})$ that have the same matrix representation of the paring $\langle \quad , \quad \rangle_2$ on this basis.

Lemma 3.10. *Let d be a squarefree integer and let $p_0 \nmid 2d$ be a prime. Take a basis $\{a_i : i\}$ for $\operatorname{coker} R_{1,S,T}(dp_0)$ and a basis $\{b_j : j\}$ for $\ker R_{1,S,T}(dp_0)$. Define*

$$F_{p_0}(d) \coloneqq \prod_{i,j} L_{a_i,b_j},$$

where $L_{a_i,b_j} = \mathbb{Q}(\sqrt{a_i}, \sqrt{b_i}, \sqrt{\beta_{ij}})$ for some fixed choice of $\beta_{ij} \in \mathcal{F}_{a_i,b_j}$ and $\mathcal{F}_{a,b}$ is as defined in Section 2.1. Then if $p \in A_{d,p_0}$ satisfy $\left(\frac{F_{p_0}(d)/\mathbb{Q}}{p_0}\right) = \left(\frac{F_{p_0}(d)/\mathbb{Q}}{p_0}\right)$, we have $\operatorname{rk}_8 \mathbf{C}_{dp} = \operatorname{rk}_8 \mathbf{C}_{dp_0}$.

Proposition 3.11 (Governing field for 8-rank)**.** *Let d be a squarefree integer. Take $\mathcal{I}(d)$ to be a set containing a prime in each class in $(\mathbb{Z}/8d\mathbb{Z})^\times/((\mathbb{Z}/8d\mathbb{Z})^\times)^2$. Then*

$$\Omega_3(d) = \Omega_2(d) \cdot \prod_{p_0 \in \mathcal{I}(d)} F_{p_0}(d)$$

is a governing field for the 8-rank of $\{\mathbf{C}_{dp}\}_p$.

It suffices to show that such a field $F_{p_0}(d)$ exists for any odd prime p_0. We fix a prime p_0 and take any $p \in A_{d,p_0}$. Let m be the 4-rank of $\mathbf{C}_{dp_0}$. Let t be number of distinct prime factors of $\Delta_{\mathbb{Q}(\sqrt{dp_0})}$ so $t \geq r$. List the distinct prime factors of $\Delta_{\mathbb{Q}(\sqrt{dp_0})}$ as $p_0, \ldots, p_{t-1}$.

3.2.2 Governing fields for the 8-rank

Now take $S_2 \subseteq \operatorname{span}_{\mathbb{F}_2} S$ so that $S_2 = \{a_1, \ldots, a_m\}$ is a basis for $\overline{\mathcal{U}}_2 = \operatorname{coker} R_{1,S,T}(dp_0)$. Also take a basis

$$T_2 = \begin{cases} \{b_1, \ldots, b_{m+1}\} \subseteq \operatorname{span}_{\mathbb{F}_2} T \text{ for } \mathcal{V}_2 = \ker R_{1,S,T}(dp_0) & \text{if } d > 0 \\ \{b_1, \ldots, b_m\} \subseteq \operatorname{span}_{\mathbb{F}_2} T \text{ for } \overline{\mathcal{V}}_2 = \ker R_{1,S,T}(dp_0) & \text{if } d < 0. \end{cases}$$

By construction $p_0 \nmid a_j$ and $p_0 \nmid b_j$. The matrix $R_{2,S_2,T_2}(dp_0)$ is the $\mathbb{F}_2$-matrix $([a_i, dp_0/a_i, b_j]_+)_{i,j}$. By the multiplicativity of the Rédei symbol and Rédei reciprocity, we have

$$\begin{aligned}[a_i, dp/a_i, b_j][a_i, dp_0/a_i, b_j] = [a_i, p_0 p, b_j] = [a_i, b_j, p_0 p] \\ = \left(\frac{L_{a_i,b_j}/K_{a_i,b_j}}{\mathfrak{p}}\right)\left(\frac{L_{a_i,b_j}/K_{a_i,b_j}}{\mathfrak{p}_0}\right),\end{aligned}$$

where $\mathfrak{p}$ and $\mathfrak{p}_0$ are primes in K_{a_i,b_j} with norm p and p_0 respectively. Since $\left(\frac{L_{a_i,b_j}/K_{a_i,b_j}}{\mathfrak{p}_0}\right)$ and $[a_i, dp_0/a_i, b_j]$ are fixed, $R_{2,S_2,T_2}(dp)$ only depends on $\left(\frac{L_{a_i,b_j}/K_{a_i,b_j}}{\mathfrak{p}}\right)$.

Lemma 3.12. *Suppose $p \nmid 2abd$. If $a \in \mathcal{U}_2$ and $b \in \mathcal{V}_2$, then p splits in both $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{b})/\mathbb{Q}$.*

Proof. Since $(a, dp/a)_p = (dp, b)_p = 1$, this implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$, so p splits in $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{b})/\mathbb{Q}$. □

By construction, any $p \in A_{d,p_0}$ is coprime with any a_i, b_j. By Lemma 3.12, p splits completely in the compositum

$$E_{p_0}(d) \coloneqq \prod_{i,j} K_{a_i,b_j}$$

and $\left(\frac{L_{a_i,b_j}/K_{a_i,b_j}}{\mathfrak{p}}\right) = \left(\frac{L_{a_i,b_j}/\mathbb{Q}}{p}\right)$.

By Lemma 1.5, $\left(\frac{L_{a_i,b_j}/K_{a_i,b_j}}{\mathfrak{p}}\right) = \left(\frac{E_{p_0}(d)\cdot L_{a_i,b_j}/E_{p_0}(d)}{\mathfrak{v}}\right)$, where $\mathfrak{v}$ is a prime in $E_{p_0}(d)$ above $\mathfrak{p}$. Therefore there is the following one-to-one correspondence between

$$\begin{aligned}\left\{\left(\frac{F_{p_0}(d)/\mathbb{Q}}{p}\right) : p \in A_{d,p_0}\right\} &\to \{R_{2,S_2,T_2}(dp) : p \in A_{d,p_0}\} \subseteq \mathrm{Mat}_{m\times s}(\mathbb{F}_2) \\ \tau &\mapsto \left(\tau \restriction_{L_{a_i,b_i}}\right)_{i,j},\end{aligned}$$

where s is m when $d < 0$ and $m+1$ when $d > 0$. Therefore $F_{p_0}(d)$ is the field required by Proposition 3.11. The 8-rank of $\mathbf{C}_{dp}$ only depends on the splitting of p in $F_{p_0}(d)/E_{p_0}(d)$. This proves Lemma 3.10.

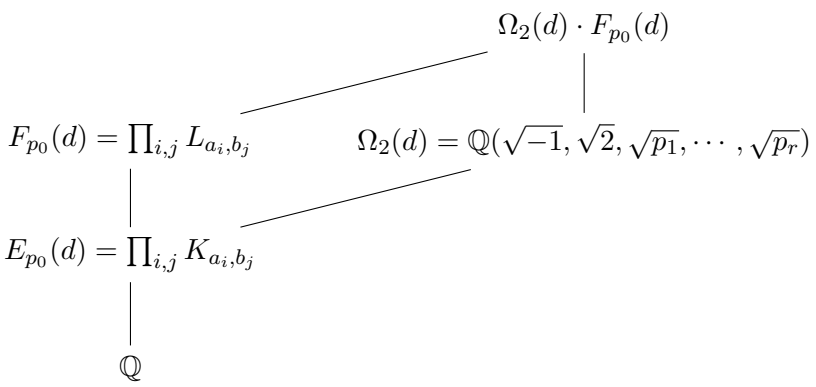
3.3 Distribution of the 8-rank in congruence classes

Lemma 3.13. *Suppose p and $p_0 \nmid 2d$ are primes. Then*

(i) $\left(\frac{\Omega_2(d)/\mathbb{Q}}{p}\right) = \left(\frac{\Omega_2(d)/\mathbb{Q}}{p_0}\right)$ *if and only if* $p \in A_{d,p_0}$*;*

(ii) if $p \in A_{d,p_0}$*, then* $\left(\frac{F_{p_0}(d)/\mathbb{Q}}{p}\right) = \left(\frac{F_{p_0}(d)/\mathbb{Q}}{p_0}\right)$ *if and only if* $R_{2,S_2,T_2}(dp) = R_{2,S_2,T_2}(dp_0)$*;*

(iii) $\left(\frac{\Omega_2(d)\cdot F_{p_0}(d)/\mathbb{Q}}{p}\right) = \left(\frac{\Omega_2(d)\cdot F_{p_0}(d)/\mathbb{Q}}{p_0}\right)$ *if and only if* $p \in A_{d,p_0}$ *and* $R_{2,S_2,T_2}(dp) = R_{2,S_2,T_2}(dp_0)$.



To obtain the distribution over all imaginary quadratic field, an effective form of Chebotarev density theorem is needed to allow summing over all squarefree integers d. However, the unconditional form of Chebotarev density theorem requires N/d to be relatively large with respect to the discriminant of the field being applied to. Without this, we have to assume the Riemann hypothesis to obtain a good enough error term.

Assumption 3.14 (GRH)**.** *The generalised Riemann hypothesis holds for Dedekind zeta function associated to any Galois extension $L/\mathbb{Q}$, with Galois group* $\mathrm{Gal}(L/\mathbb{Q}) \cong C_2^s \times (C_2^m \rtimes C_2^n)$ *for some positive integers $m \leq n$ and s.*

We apply the Chebotarev density theorem as stated in Corollary 3.4, over the extension $\Omega_2(d)\cdot F_{p_0}(d)/E_{p_0}(d)$ and $\Omega_2(d)/E_{p_0}(d)$, noting that p splits completely in $E_{p_0}(d)/\mathbb{Q}$.

Theorem 3.15. *Take $R \in \{R_{2,S_2,T_2}(dp) : p \in A_{d,p_0}\}$. Then*

$$\lim_{n\to\infty} \frac{\#\{p \in A_{d,p_0}(n) : R_{2,S_2,T_2}(dp) = R\}}{\#A_{d,p_0}(n)} = \frac{1}{[F_{p_0}(d) : E_{p_0}(d)]}.$$

If we assume (GRH), then

$$\frac{\#\{p \in A_{d,p_0}(n) : R_{2,S_2,T_2}(dp) = R\}}{\#A_{d,p_0}(n)} = \frac{1}{[F_{p_0}(d) : E_{p_0}(d)]} + O\left(\frac{2^r \log n \log d}{\sqrt{n}}\right), \quad (3.2)$$

where r is the number of odd prime factors of d.

Proof. Let $E \coloneqq E_{p_0}(d)$, $F \coloneqq F_{p_0}(d)$, and $M \coloneqq \Omega_2(d) \cdot F_{p_0}(d)$. Assuming (GRH), we can apply an effective form of Chebotarev density theorem over the abelian extensions M/E and $\Omega_2(d)/E$, as in Corollary 3.3, then for $\sigma \in \mathrm{Gal}(M/E)$ and $\tau \in \mathrm{Gal}(\Omega_2(d)/E)$.

$$\frac{\#\left\{p < n \text{ prime} : \left(\frac{M/\mathbb{Q}}{p}\right) = \sigma\right\}}{\#\left\{p < n \text{ prime} : \left(\frac{\Omega_2(d)/\mathbb{Q}}{p}\right) = \tau\right\}} = \frac{1}{[M : \Omega_2(d)]}\left(1 + O\left(\frac{\log n}{\sqrt{n}}\left(\log \Delta_M + [M : \mathbb{Q}] \log n\right)\right)\right). \quad (3.3)$$

Observe that $[M : \Omega_2(d)] = [F : E]$, $[\Omega_2(d) : \mathbb{Q}] = 2^{r+2}$ and $[M : \mathbb{Q}] = 2^{r+2} \cdot [F : E]$. The prime that ramifies in $M/\mathbb{Q}$ must divide $2d$. Therefore by [69, Proposition 6, p.130], we have

$$\log \Delta_M \le ([M : \mathbb{Q}] - 1) \sum_{p \mid \Delta_M} \log p + ([M : \mathbb{Q}] \log [M : \mathbb{Q}]) \omega(\Delta_M) = O(2^r [F : E] \log d).$$

Then (3.2) follows from (3.3) and Lemma 3.13. □

3.4 Prime divisors

Define $S_r(N) \coloneqq \{n \in \mathcal{D}(N) : \omega(n) = r\}$ and $\mu \coloneqq \mu(N) \coloneqq \log \log N$. Sathé–Selberg theorem [67] shows that, uniformly in the range $r < 2\mu$, we have

$$\#S_r(N) \asymp \frac{N}{\log N} \frac{(\log \log N)^{r-1}}{(r-1)!}.$$

This shows that the number of distinct prime factors is Poisson distributed in $\mathcal{D}(N)$. Let $T(N) \coloneqq \{(d_0, p) : 0 < d_0 p < N,\ d \text{ odd squarefree integer},\ p \nmid 2d_0 \text{ prime}\}$, and

$T_r(N) \coloneqq \{(d_0, p) \in T(N) : \omega(d_0) = r - 1\}$. Observe that

$$\#T_r(N) \asymp r\#S_r(N)$$

Lemma 3.16. *The number of elements in $(d_0, p) \in T(N)$ so that $|r - \mu| > \mu^{2/3}$ is $\ll \exp(-\frac{1}{2}\mu^{1/3})\#T(N)$.*

Proof. By the Erdős–Kac theorem [88, Chapter 111.4, Theorem 8], the limit distribution of $\omega(n)$ is the normal distribution with mean $\log\log n$ and variance $\log\log n$. Therefore the density of integers in $\mathcal{D}(N)$ with $|r - \mu| > \mu^{2/3}$, is $\ll \mu^{-1/6}\exp\left(-\frac{1}{2}\mu^{1/3}\right) \ll \exp\left(-\frac{1}{2}\mu^{1/3}\right)$. □

Now we show that we can make assumptions on the size of p in $T_r(N)$ without affecting the resulting density.

Lemma 3.17. *[80, Lemma 4.5] Suppose $|r - \mu| < \mu^{2/3}$. The number of elements in $(d, p) \in T_r(N)$ so that $\log\log p < \mu^\epsilon$ is $\ll \mu^{-(1-\epsilon)}\#T_r(N)$.*

Proof. Suppose n is such that $\log\log n = \mu^\epsilon$.

$$\frac{\sum_{p<n}\#S_{r-1}(N/p)}{r\#S_r(N)} \ll \frac{r-1}{r\log\log N}\sum_{p<n}\frac{\log N}{p\log(N/p)}$$
$$\ll \frac{1}{\log\log N}\sum_{p<n}\frac{1}{p} \ll \frac{\log\log n}{\log\log N} \quad \square$$

3.5 Genericity

The result on the distribution of the 8-rank of class groups of imaginary quadratic fields is due to Smith [80]. Where $F_{p_0}(d)/E_{p_0}(d)$ has maximum degree, we expect

$$\mathrm{Gal}(F_{p_0}(d)/E_{p_0}(d)) \cong C_2^{m^2},$$

where $m = \mathrm{rk}_4\,\mathbf{C}(dp_0)$. This shows that each matrix in $\mathrm{Mat}_{m\times(m+1)}(\mathbb{F}_2)$ occurs equally likely, i.e. with density $\frac{1}{[F_{p_0}(d):E_{p_0}(d)]} = \frac{1}{2^{m(m+1)}}$.

We call (d, p) *generic* if

(i) d is a squarefree integer,

(ii) $p \nmid 2d$ is a prime, and

(iii) there exists non-trivial $a \mid d$ such that $(a, -dp)_v = (a, dp)_v = 1$ for all $v \in \mathcal{M}_{\mathbb{Q}}$.

It is straighforward to check that if (d, p_0) is generic, then (d, p) is automatically generic for any $p \in A_{d,p_0}$.

Lemma 3.18. *If (d, p_0) is generic, then*

$$\mathrm{Gal}(F_{p_0}(d)/E_{p_0}(d)) \cong \begin{cases} C_2^{m^2} & \text{if } d < 0, \\ C_2^{m(m+1)} & \text{if } d > 0. \end{cases}$$

Proof. Let $E = E_{p_0}(d)$ and $F = F_{p_0}(d)$. In this case, the sets $\mathcal{U}_2$ and $\mathcal{V}_2$ are disjoint subspaces in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. This implies that E is a C_2^{2m}-extension of $\mathbb{Q}$ when $d < 0$ and C_2^{2m+1}-extension when $d > 0$. Let σ_i (resp. τ_j) be the element in $\mathrm{Gal}(F/\mathbb{Q})$ that sends $\sqrt{a_i} \mapsto -\sqrt{a_i}$ (resp. $\sqrt{b_j} \mapsto -\sqrt{b_j}$) and fixes all other generators. The the commutator $[\sigma_i, \tau_j]$ is the unique non-trivial automorphism of $L_{a_i,b_j}/K_{a_i,b_j}$ and fixes all other L_{a_l,b_k}. The commutator subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ is generated by all $[\sigma_i, \tau_j]$, therefore has order 2^{m^2} when $d < 0$ and order $2^{m(m+1)}$ when $d > 0$. The maximal abelian subextension of $F/\mathbb{Q}$ is $E/\mathbb{Q}$, so the commutator subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ is $\mathrm{Gal}(F/E)$. Since F/E has exponent 2, this proves the lemma. □

Smith showed that almost all (d, p_0) are generic in [80, Lemma 4.6].

Lemma 3.19. *Suppose $|r - \mu| < \mu^{2/3}$. The number of $(d_0, p) \in T_r(N)$ such that (d_0, p) or $(2d_0, p)$ is not generic, is $\ll \left(\frac{3}{4}\right)^r \#T_r(N)$.*

Proof. Suppose $(d, p) \in T_r(N)$ and (d, p) is not generic. Suppose $a \mid d$ has k prime factors and satisfy $(a, -dp_0)_v = (a, dp_0)_v = 1$ for all $v \in \mathcal{M}_{\mathbb{Q}}$. Then we have $\left(\frac{-1}{v}\right) = \left(\frac{dp_0/a}{v}\right) = 1$ for $v \mid a$ and $\left(\frac{a}{v}\right) = 1$ for $v \mid dp_0/a$. These are $r+k$ independent Legendre symbols. The probability that a satisfies the requirements is $\ll 2^{-r-k}$. Making use of [45, Proposition 9], we can convert this probability to natural density. Therefore the probability that some $a \mid d$ satisfies the equations is $\ll \sum_{k \geq 0} \binom{r}{k} 2^{-s-k} \ll 2^{-r}(1 + \frac{1}{2})^r \ll (\frac{3}{4})^r$. For the case when $(2d_0, p)$ is not generic, replacing d with $2d_0$ we get the same estimate up to a multiplicative constant. □

3.6 Distribution of the 8-rank in natural densities

The expression for $\mathrm{Prob}(j \mid m,n)$ in (3.1) can be evaluated more explicitly [83, Chapter 1 Exercise 192],

$$\mathrm{Prob}(j \mid m,n) = \frac{\prod_{i=j+1}^{m}(1-2^{-i})\prod_{i=n-m+j+1}^{n}(1-2^{-i})}{2^{j(n-m+j)}\prod_{i=1}^{m-j}(1-2^{-i})}.$$

The imaginary case is in [80, Proposition 2.5].

Lemma 3.20. *Suppose (d,p_0) is generic. Let $m \coloneqq \mathrm{rk}_4\,\mathbf{C}_{dp_0}$. Then for any $j \le m$, we have*

$$\lim_{n\to\infty}\frac{\#\{p \in A_{d,p_0}(n) : \mathrm{rk}_8\,\mathbf{C}_{dp} = j\}}{\#A_{d,p_0}(n)} = \begin{cases} \mathrm{Prob}(j \mid m,m) & \text{if } d<0 \\ \mathrm{Prob}(j \mid m,m+1) & \text{if } d>0. \end{cases}$$

If we assume (GRH), and further that (d,p_0) satisfies $|\omega(d)-\mu| < \mu^{2/3}$, $dp_0 < N$, $\log\log\frac{N}{d} > \mu^{1/2}$, then for any $c<1/2$ and $j \le m$, we have

$$\frac{\#\{p \in A_{d,p}(n) : \mathrm{rk}_8\,\mathbf{C}_{dp_0} = j\}}{\#A_{d,p}(n)} = \begin{cases} \mathrm{Prob}(j \mid m,m) + O\left(\exp(-ce^{\mu^{1/\epsilon}})\right) & \text{if } d<0 \\ \mathrm{Prob}(j \mid m,m+1) + O\left(\exp(-ce^{\mu^{1/\epsilon}})\right) & \text{if } d>0. \end{cases}$$

Proof. The lemma follows from summing Theorem 3.15 over all R of corank j. The lower bound of n gives the required error term. Lemma 3.18 shows that every element in $\mathrm{Mat}_{m\times m}(\mathbb{F}_2)$ or $\mathrm{Mat}_{m\times m+1}(\mathbb{F}_2)$ are attained with the same density. □

We are now ready to prove our main theorem. We will prove the following effective version of Theorem 3.1.

Theorem 3.21. *Assume (GRH). For any $m \ge j \ge 0$ and $\delta \in \{\pm 1\}$, we have*

$$\frac{\#\{\delta\cdot D \in \mathcal{D}(N) : \mathrm{rk}_4\,\mathbf{C}_D = m,\ \mathrm{rk}_8\,\mathbf{C}_D = j\}}{\#\{\delta\cdot D \in \mathcal{D}(N) : \mathrm{rk}_4\,\mathbf{C}_D = m\}} = \begin{cases} \mathrm{Prob}(j \mid m,m+1) + O\left((\log\log N)^{-(1-\epsilon)}\right) & \text{if } \delta = 1, \\ \mathrm{Prob}(j \mid m,m) + O\left((\log\log N)^{-(1-\epsilon)}\right) & \text{if } \delta = -1. \end{cases}$$

Proof. We first fix $\eta \in \{\pm 1, \pm 2\}$, and sum over $(\eta \cdot d_0, p)$, where $(d_0, p) \in T(N)$, i.e.

$$\frac{\#\{(d_0,p) \in T(N) : \mathrm{rk}_4\, \mathbf{C}_{\eta \cdot d_0 p} = m, \mathrm{rk}_8\, \mathbf{C}_{\eta \cdot d_0 p} = j\}}{\#\{(d_0,p) \in T(N) : \mathrm{rk}_4\, \mathbf{C}_{\eta \cdot d_0 p} = m\}}.$$

Write $d = \eta \cdot d_0$, where d_0 is an odd positive integer. By Lemma 3.16, we only need to consider the sum over r in the range $|r - \mu| < \mu^{2/3}$. Also by Lemma 3.19, we can assume (d, p_0) is generic.

It suffices to consider the sum

$$\sum_{|r-\mu|<\mu^{2/3}} \sum_{d<N} \sum_{\substack{p_0 \in \mathcal{I}(d) \\ \mathrm{rk}_4\, \mathbf{C}_{dp_0} = m \\ (d,p_0) \text{ generic}}} \frac{\#\{(d_0,p) \in T_r(N) : p \in A_{d,p_0}(\frac{N}{d}),\ \mathrm{rk}_8\, \mathbf{C}_{dp} = j\}}{\#\{(d_0,p) \in T_r(N) : p \in A_{d,p_0}(\frac{N}{d})\}},$$

where $\mathcal{I}(d)$ is taken as in Proposition 3.11. When $\log\log N/d < \sqrt{\log\log N}$, apply Lemma 3.17, otherwise apply Lemma 3.20. Combining the sums for $\eta \in \{1, 2\}$ when $\delta = 1$ and $\eta \in \{-1, -2\}$ when $\delta = -1$, and keeping track of the error terms coming from Lemma 3.16, Lemma 3.17, Lemma 3.19 and Lemma 3.20. This proves the theorem. □

Chapter 4

The negative Pell equation

This chapter is based on joint work with Peter Koymans, Djordjo Milovic, and Carlo Pagano [19].

We consider the solvability over $\mathbb{Z}$ of the negative Pell equation

$$x^2 - Dy^2 = -1, \tag{4.1}$$

where D is a positive integer. A necessary but insufficient condition for (4.1) to be solvable is that D is not divisible by any prime congruent to 3 mod 4. To see this, simply take the equation (4.1) modulo any prime $p \mid D$, then -1 must be a quadratic residue modulo p, which is impossible if $p \equiv 3 \bmod 4$.

Recall from (1.3) that the unit group of K has the form

$$\langle -1 \rangle \times \langle \epsilon_D \rangle,$$

where ϵ_D is the fundamental unit in $\mathbb{Q}(\sqrt{D})$. If (4.1) is solvable, we see that $x+y\sqrt{D}$ is a unit in $\mathbb{Q}(\sqrt{D})$ with norm -1, so $\operatorname{Norm} \epsilon_D = -1$. Conversely, if $\operatorname{Norm} \epsilon_D = -1$, then ϵ_D^3 can be written as $x + y\sqrt{D}$, where $x, y \in \mathbb{Z}$, which corresponds to a solution to (4.1). Therefore (4.1) is solvable if and only if $\operatorname{Norm} \epsilon_D = -1$.

Since $\sqrt{D}$ has negative norm, the ideal $(\sqrt{D})$ is totally positive if and only there exists a unit of norm -1. From (1.2), this happens precisely when the narrow and ordinary class groups coincide. Altogether, we see that (4.1) is solvable if and only if $\mathbf{Cl}_D \cong \mathbf{C}_D$.

Since $\# \mathbf{C}_D / \# \mathbf{Cl}_D$ can only be either 1 or 2, the odd parts of $\mathbf{Cl}_D$ and $\mathbf{C}_D$

are always isomorphic, so it suffices to compare the 2-parts of $\mathbf{Cl}_D$ and $\mathbf{C}_D$. Hence

$$(4.1) \text{ is solvable} \iff \mathrm{rk}_{2^k}\,\mathbf{Cl}_D = \mathrm{rk}_{2^k}\,\mathbf{C}_D \text{ for all integers } k \geq 1.$$

The frequency of solvability of (4.1) is intricately related to the joint distribution of 2-primary parts $\mathbf{Cl}_D$ and $\mathbf{C}_D$.

Note that $\mathrm{rk}_2\,\mathbf{Cl}_D = \mathrm{rk}_2\,\mathbf{C}_D$ if and only if D is in the *Pell family*

$$\mathcal{P} = \{D \text{ positive squarefree integer} : p \not\equiv 3 \bmod 4 \text{ for all primes } p \mid D\}.$$

This can be seen by observing that the genus field H_2^+ as discussed in (1.6) is totally real if and only if $D \in \mathcal{P}$.

As $\mathcal{P}$ has natural density 0 in the set of all positive squarefree integers, it is more meaningful to study density questions concerning the solvability of (4.1) relative to $\mathcal{P}$. There exists $D \in \mathcal{P}$ such that (4.1) is not solvable, for example:

$$34, 146, 178, 194, 205, 221, 305, 377, 386, 410, 466, 482, \ldots.$$

Stevenhagen [86] conjectured that

$$\lim_{N\to\infty} \frac{|\mathcal{P}^-(N)|}{|\mathcal{P}(N)|} = 1 - \alpha = 0.58057\ldots,$$

where

$$\mathcal{P}(N) = \{D \in \mathcal{P} : D \leq N\},$$

$$\mathcal{P}^-(N) = \{D \in \mathcal{P}(N) : \ (4.1) \text{ is solvable over } \mathbb{Z}\},$$

and

$$\alpha = \prod_{j \text{ odd}} (1 - 2^{-j}) = \prod_{j=1}^{\infty} (1 + 2^{-j})^{-1} = 0.41942\ldots.$$

Until now, the best bounds in the direction of Stevenhagen's conjecture are due to Fouvry and Klüners [31, 32]. They proved that

$$0.52427\ldots = \frac{5}{4}\alpha \leq \liminf_{N\to\infty} \frac{|\mathcal{P}^-(N)|}{|\mathcal{P}(N)|} \leq \limsup_{N\to\infty} \frac{|\mathcal{P}^-(N)|}{|\mathcal{P}(N)|} \leq \frac{2}{3}. \tag{4.2}$$

The lower bound in (4.2) comes from proving that the density of $D \in \mathcal{P}$ such that

$$\mathrm{rk}_4 \mathbf{C}_D = 0$$

is equal to α and the density of $D \in \mathcal{P}$ such that

$$\mathrm{rk}_4 \mathbf{Cl}_D = \mathrm{rk}_4 \mathbf{C}_D = 1 \text{ and } \mathrm{rk}_8 \mathbf{C}_D = 0$$

is equal to $\alpha/4$.

By incorporating the methods developed by Smith [81], we can improve the lower bound.

Theorem 4.1 ([19, Theorem 1.1])**.** *We have*

$$\liminf_{N\to\infty} \frac{|\mathcal{P}^-(N)|}{|\mathcal{P}(N)|} \geq \alpha\beta = 0.53822\ldots,$$

where

$$\beta = \sum_{n=0}^{\infty} 2^{-n(n+3)/2} = 1.28325\ldots > 5/4.$$

We obtain our lower bound by proving that the density of $D \in \mathcal{P}$ such that

$$\mathrm{rk}_4 \mathbf{Cl}_D = \mathrm{rk}_4 \mathbf{C}_D = n \text{ and } \mathrm{rk}_8 \mathbf{C}_D = 0.$$

is equal to $2^{-n(n+3)/4}\alpha$.

In fact, we prove more. For integers $n \geq m \geq 0$, let

$$\mathcal{P}_{n,m}(N) = \{D \in \mathcal{P}(N) : \mathrm{rk}_4 \mathbf{Cl}_D = \mathrm{rk}_4 \mathbf{C}_D = n \text{ and } \mathrm{rk}_8 \mathbf{C}_D = m\},$$

and

$$\mathcal{P}_n(N) = \{D \in \mathcal{P}(N) : \mathrm{rk}_4 \mathbf{C}_D = n\}.$$

Theorem 4.2 ([19, Theorem 1.2])**.** *For integers $n \geq m \geq 0$, we have*

$$\lim_{N\to\infty} \frac{|\mathcal{P}_{n,m}(N)|}{|\mathcal{P}(N)|} = \alpha \cdot 2^{-n(n+1)} \frac{\prod_{j=m+1}^{n}(2^n - 2^{n-j})}{\prod_{k=1}^{m}(2^k - 1)\prod_{l=1}^{n-m}(2^l - 1)}. \tag{4.3}$$

Similar to (3.1), define

$$\mathrm{Prob}_{\mathrm{Sym}}(j \mid m) \coloneqq \frac{\#\{M \in \mathrm{Sym}_m(\mathbb{F}_2) : \mathrm{corank}(M) = j\}}{\#\,\mathrm{Sym}_m(\mathbb{F}_2)},$$

where $\mathrm{Sym}_m(\mathbb{F}_2)$ denotes the space of $m \times m$ symmetric matrices over $\mathbb{F}_2$. The limit in (4.3) can be interpreted as

$$\frac{1}{2^n}\,\mathrm{Prob}(m \mid n, n) \lim_{r\to\infty} \mathrm{Prob}_{\mathrm{Sym}}(n \mid r).$$

By [86, Proposition 2.8],

$$\lim_{r\to\infty} \mathrm{Prob}_{\mathrm{Sym}}(n \mid r) = \frac{\alpha}{\prod_{i=1}^{n}(2^i - 1)}.$$

Proved by Fouvry and Klüners in [31], this is the density of $D \in \mathcal{P}$ such that $\mathrm{rk}_4\,\mathbf{C}_D = n$. Then Theorem 4.2 follows from proving that

(i) $\frac{1}{2^n}$ is the density of D in $\mathcal{P}$ such that $\mathrm{rk}_4\,\mathbf{Cl}_D = \mathrm{rk}_4\,\mathbf{C}_D$ given that $\mathrm{rk}_4\,\mathbf{C}_D = n$; and

(ii) $\mathrm{Prob}(m \mid n, n)$ is the density of D in $\mathcal{P}$ such that $\mathrm{rk}_8\,\mathbf{C}_D = n$ given that $\mathrm{rk}_4\,\mathbf{C}_D = \mathrm{rk}_4\,\mathbf{Cl}_D = n$.

More precisely, the following is the main result in [19] used to deduce Theorem 4.2.

Theorem 4.3 ([19, Theorem 6.1])**.** *For any integers $n \geq m \geq 0$ Then*

$$\left|\#\mathcal{P}_{n,m}(N) - \frac{1}{2^n}\,\mathrm{Prob}(m \mid n, n)\#\mathcal{P}_n(N)\right| \ll \frac{N}{\log\log\log N}$$

Similar to (1.4), writing $K = \mathbb{Q}(\sqrt{D})$, we have

$$0 \to \left\langle \left(\frac{H_{2^k}^+/K}{(\sqrt{D})}\right) \right\rangle \to \mathrm{Gal}(H_{2^k}^+/K) \to \mathrm{Gal}(H_{2^k}/K) \to 0.$$

From this we see that $H_{2^k}^+ = H_{2^k}$ if and only if $\left(\frac{H_{2^k}^+/K}{(\sqrt{D})}\right)$ is trivial. Therefore $\mathrm{rk}_{2^k}\,\mathbf{Cl}_D = \mathrm{rk}_{2^k}\,\mathbf{C}_D$ holds if and only if -1 is in the right kernel of $\langle\ \ ,\ \ \rangle_{k+1}$. To check that $\mathrm{rk}_4\,\mathbf{Cl}_D = \mathrm{rk}_4\,\mathbf{C}_D$ holds, for all $a \in \overline{\mathcal{U}}_2$, we need to have $\langle a, -1\rangle_2 =$

$[a, \frac{D}{a}, -1] = 1$, where $[\cdot, \cdot, \cdot]$ is the Rédei symbol defined in Section 1.5. Since $\dim_{\mathbb{F}_2} \overline{\mathcal{U}}_2 = \mathrm{rk}_4 \mathbf{C}(D) = n$, we expect there to be n independent symbols, which should give a probability of $\frac{1}{2^n}$ for all of them to be trivial.

For $D \in \mathcal{P}$, $\{b \mid D : b > 0\}$ is a set of representatives for both $\mathcal{V}_1$ and $\mathcal{U}_1$. By quadratic reciprocity, we see that the Rédei matrix discussed in Section 1.4, with respect to a basis of this set is symmetric. Therefore $\langle \quad , \quad \rangle_1$ is a symmetric pairing on this set of representatives. This leads to the same set of positive representatives for $\mathcal{U}_2$ and $\mathcal{V}_2$, given by

$$\{a \mid D : a > 0,\ a \text{ squarefree},\ (a, D/a) = 1\}.$$

This also follows from comparing the sets given in (1.11) and (1.12). This leads to a major novel difficulty with working in the Pell family. The reason for this is that the algebraic results break down in this case since there is no valid choice of "variable indices". In particular, all discriminants $D \in \mathcal{P}$ end up in the error term of Smith's theorem [81]. Considering up to the 8-rank, we are able to extend Smith's algebraic results to mitigate this issue using Rédei reciprocity.

We will discuss some of the ideas used in proving Theorem 4.3.

4.1 Reflection principles

The Rédei symbol plays a prominent role in the proof of Theorem 4.2. We prove several identities on the product of Rédei symbols, which serve as the algebraic input for our analytic machinery in proving equidistribution.

Write $\mathcal{U}_k(D)$, $\mathcal{V}_k(D)$, $\overline{\mathcal{U}}_k(D)$, $\overline{\mathcal{V}}_k(D)$, and $\langle \quad , \quad \rangle_{k,D}$ to stand for spaces defined in (1.8), (1.7), (1.10), and the pairing defined in (1.9), respectively, for the field $\mathbb{Q}(\sqrt{D})$.

We call a triple of nonzero integers $\{a, b, c\}$ *admissible* if abc is not divisible by any prime that is congruent to 3 mod 4, and the Rédei symbol $[a, b, c]$ is defined, i.e. $\{a, b, c\}$ satisfies conditions (2.6) and (2.7). It is straightforward to check that admissibility of $\{a, b, c\}$ does not depend on the ordering of the triple. Also if $\{a, b, c\}$ and $\{a, b, c'\}$ are admissible then so is $\{a, b, cc'\}$. Recall from Definition 1.14, that $\langle a, b \rangle_{2,D}$ is the Rédei symbol $[a, \frac{D}{a}, b]$.

We now prove our main algebraic results.

Theorem 4.4. *Let $d \in \mathcal{P}$. Let p_1, p_2, q_1, q_2 be primes congruent to $1 \bmod 4$ and coprime to d. Let a and b be divisors of d, where $a > 0$ and b is possibly negative. Assume that $b \in \mathcal{V}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$.*

(i) If $a \in \mathcal{U}_2(p_i q_j d)$ for all $(i, j) \in \{(1, 2), (2, 1), (2, 2)\}$, then $a \in \mathcal{U}(p_1 q_1 d)$ and

$$\langle a, b\rangle_{2,p_1q_1d}\langle a, b\rangle_{2,p_1q_2d}\langle a, b\rangle_{2,p_2q_1d}\langle a, b\rangle_{2,p_2q_2d} = 0. \tag{4.4}$$

(ii) If instead $p_i a \in \mathcal{U}_2(p_i q_j d)$ for all $(i, j) \in \{(1, 2), (2, 1), (2, 2)\}$ and $\left(\frac{q_1 q_2}{p_1}\right) = \left(\frac{p_1 p_2}{q_1}\right) = 1$, then $p_1 a \in \mathcal{U}_2(p_1 q_1 d)$, $\{p_1 p_2, q_1 q_2, b\}$ is admissible and

$$\langle p_1 a, b\rangle_{2,p_1q_1d}\langle p_1 a, b\rangle_{2,p_1q_2d}\langle p_2 a, b\rangle_{2,p_2q_1d}\langle p_2 a, b\rangle_{2,p_2q_2d} = [p_1 p_2, q_1 q_2, b]. \tag{4.5}$$

Proof. (i) We can check that the assumptions implies that $(a, -p_1 q_1 d)_v = 1$ for all $v \in \mathcal{M}_{\mathbb{Q}}$, so $a \in \mathcal{U}(p_1 q_1 d)$. Writing the terms as Rédei symbols, the left-hand side of (4.4) equals

$$[a, p_1 q_1 \frac{d}{a}, b][a, p_1 q_2 \frac{d}{a}, b][a, p_2 q_1 \frac{d}{a}, b][a, p_2 q_2 \frac{d}{a}, b].$$

By the multiplicativity of Rédei symbols, this product equals

$$[a, q_1 q_2, b][a, q_1 q_2, b] = 1.$$

(ii) It is straightforward to check that the assumptions ensures that $(p_1 a, -p_1 q_1 d)_v = 1$ for all $v \in \mathcal{M}_{\mathbb{Q}}$, so $p_1 a \in \mathcal{U}(p_1 q_1 d)$. Writing the terms as Rédei symbols, the left-hand side of (4.5) equals

$$[p_1 a, q_1 \frac{d}{a}, b][p_1 a, q_2 \frac{d}{a}, b][p_2 a, q_1 \frac{d}{a}, b][p_2 a, q_2 \frac{d}{a}, b]$$

Applying the multiplicativity of Rédei symbols, this product equals

$$[p_1 a, q_1 q_2, b][p_2 a, q_1 q_2, b] = [p_1 p_2, q_1 q_2, b]. \qquad \square$$

Theorem 4.5. *Let $d \in \mathcal{P}$. Take primes p_1, p_2, q_1, q_2 that are 1 modulo 4 and coprime to d. Let a be a positive divisor of d. Assume that $p_i a \in \mathcal{V}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$.*

Then $p_i a \in \mathcal{U}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$, $\{p_1 p_2, q_1 q_2, p_1 p_2\}$ is admissible and

$$\langle p_1 a, p_1 a\rangle_{2,p_1 q_1 d}\langle p_1 a, p_1 a\rangle_{2,p_1 q_2 d}\langle p_2 a, p_2 a\rangle_{2,p_2 q_1 d}\langle p_2 a, p_2 a\rangle_{2,p_2 q_2 d} = [p_1 p_2, p_1 p_2, q_1 q_2]. \quad (4.6)$$

Proof. Since $p_i a$ is not divisible by primes congruent to $3 \bmod 4$, the assumption $p_i a \in \mathcal{V}_2(p_i q_j d)$ implies that $(p_i a, p_i q_j d)_v = (p_i a, -p_i q_j d)_v = 1$ for all $v \in \mathcal{M}_{\mathbb{Q}}$, so $p_i a \in \mathcal{U}_2(p_i q_j d)$. Therefore the left-hand side of (4.6) is

$$[p_1 a, q_1 \frac{d}{a}, p_1 a][p_1 a, q_2 \frac{d}{a}, p_1 a][p_2 a, q_1 \frac{d}{a}, p_2 a][p_2 a, q_2 \frac{d}{a}, p_2 a].$$

The product becomes

$$[p_1 a, q_1 q_2, p_1 a][p_2 a, q_1 q_2, p_2 a] = [p_1 a, q_1 q_2, -q_1 q_2][p_2 a, q_1 q_2, -q_1 q_2] = [p_1 p_2, q_1 q_2, -q_1 q_2].$$

By Lemma 4.6, we have

$$[p_1 p_2, q_1 q_2, -q_1 q_2] = [p_1 p_2, q_1 q_2, p_1 p_2].$$

Then the desired result follows from Rédei reciprocity. □

Lemma 4.6. *Suppose $a, b \in \mathcal{P}$ are coprime integers such that $(a, b)_v = 1$ for all $v \in \mathcal{M}_{\mathbb{Q}}$. Then*

$$[a, b, -ab] = 1.$$

Proof. Since $a \in \mathcal{U}_2(ab)$, we have $[a, b, -ab] = \langle a, -ab\rangle_{2,ab} = \langle a, 1\rangle_{2,ab} = 1$ by definition. □

Theorem 4.7. *Let $d \in \mathcal{P}$. Let p_1, p_2, q_1, q_2 be distinct primes congruent to $1 \bmod 4$ and coprime to d. Let a, b be a positive divisors of d. Assume that $b, p_i a \in \mathcal{V}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$. Then $b, p_i a \in \mathcal{U}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$, and*

$$\prod_{i=1}^{2}\prod_{j=1}^{2}\langle p_i a, b\rangle_{2,p_i q_j d}\langle b, p_i a\rangle_{2,p_i q_j d} = 0. \quad (4.7)$$

Proof. The assumptions implies that $b, p_i a \in \mathcal{U}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$. The product (4.7) can be rewritten as

$$\prod_{i=1}^{2}\prod_{j=1}^{2}[p_i a, \frac{d}{a}q_j, b][b, \frac{d}{b}p_i q_j, a p_i].$$

By the multiplicativity of Rédei symbols and Rédei recirocity (Theorem 2.9), we have

$$[p_1 a, q_1 q_2, b][p_2 a, q_1 q_2, b][b, q_1 q_2, a p_1][b, q_1 q_2, a p_2]$$
$$= [p_1 p_2, q_1 q_2, b][b, q_1 q_2, p_1 p_2] = 0. \quad \square$$

Theorem 4.8. *Let d be a positive squarefree integer composed of primes that are 1 or 2 modulo 4. Let p_1, p_2, q_1, q_2 be distinct primes that are 1 modulo 4 and coprime to d. Let a, b be positive divisors of d. We assume that $q_j b, p_i a \in \mathcal{V}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$. Then we have $q_j b, p_i a \in \mathcal{U}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$, $\{p_1 p_2, q_1 q_2, -1\}$ is admissible and*

$$\prod_{i=1}^{2}\prod_{j=1}^{2}\langle p_i a, q_j b\rangle_{2,p_i q_j d}\langle q_j b, p_i a\rangle_{2,p_i q_j d} = [p_1 p_2, -1, q_1 q_2]. \tag{4.8}$$

Proof. The assumptions implies that $p_i a, q_j b \in \mathcal{V}_2(p_i q_j d)$ for all $i, j \in \{1, 2\}$. The left-hand side of (4.8) equals

$$\prod_{i=1}^{2}\prod_{j=1}^{2}[p_i a, \frac{d}{a}q_j, q_j b][q_j b, \frac{d}{b}p_i, p_i a].$$

By the multiplicativity of Rédei symbols, we can rewrite the product as

$$[p_1 p_2, \frac{d}{a}q_1, b q_1][p_1 p_2, \frac{d}{a}q_2, b q_2][q_1 q_2, \frac{d}{b}p_1, a p_1][q_1 q_2, \frac{d}{b}p_2, a p_2].$$

One readily checks that $p_i \frac{d}{b}$ is coprime to $q_1 q_2$ and that $q_j \frac{d}{a}$ is coprime to $p_1 p_2$. Therefore we can apply Lemma 4.6 to each of the terms in the above sum

$$[p_1 p_2, \frac{d}{a}q_1, -dab p_1 p_2][p_1 p_2, \frac{d}{a}q_2, -dab p_1 p_2][q_1 q_2, \frac{d}{b}p_1, -dab q_1 q_2][q_1 q_2, \frac{d}{b}p_2, -dab q_1 q_2].$$

We can further simplify this by multiplicativity and get

$$[p_1p_2, q_1q_2, -dabp_1p_2][p_1p_2, q_1q_2, -dabq_1q_2] = [p_1p_2, q_1q_2, p_1p_2q_1q_2].$$

Since p_1p_2 and q_1q_2 are coprime, we can apply Lemma 4.6 and get that the above equals

$$[p_1p_2, q_1q_2, -1],$$

and the result follows from Rédei reciprocity. □

4.2 Equidistribution

For a squarefree integer D, write the distinct prime factors of D as $p_1 < p_2 < \cdots < p_r$, where $r \coloneqq \omega(D)$. Define

$$\mu_D : \mathbb{F}_2^{r-1} \to \overline{\mathcal{U}}_1(D) \qquad (e_1, \dots, e_{r-1}) \mapsto p_1^{e_1} \dots p_{r-1}^{e_{r-1}}.$$

Take $S_1 = \{p_1, p_2, \dots, p_{r-1}\}$, which is a basis for $\overline{\mathcal{U}}_1(D)$. Then $S_1 \cup \{-1\}$ is a basis for $\mathcal{V}_1(D)$. For $D \in \mathcal{P}$, we always have -1 in the kernel of $\langle \quad , \quad \rangle_1$, so we can always take -1 in the basis of $\mathcal{V}_2(D)$. In particular $\mathcal{V}_2(D) \cong \operatorname{span}_{\mathbb{F}_2}(\ker R_{1,S_1,S_1}(D) \cup \{-1\})$. In the following, write $R_1(D) \coloneqq R_{1,S_1,S_1}(D)$.

Given a matrix $A \in \operatorname{Sym}_{r-1}(\mathbb{F}_2)$ with corank n, take a basis $\mathcal{B}$ for $\ker A$, then $S \coloneqq \mu_D(\mathcal{B})$ is a basis for $\overline{\mathcal{U}}_2(D)$ and $T \coloneqq \mu_D(\mathcal{B}) \cup \{-1\}$ is a basis for $\mathcal{V}_2(D)$. We need to show that $R_2(D, \mathcal{B}) \coloneqq R_{2,S,T}(D)$ is equidistibuted in $\operatorname{Mat}_{n,n+1}(\mathbb{F}_2)$, over the set of $D \in \mathcal{P}$ such that $R_1(D) = A$.

Define $\mathcal{P}_A(N) \coloneqq \{D \in \mathcal{P} : R_1(D) = A\}$. The goal is to show that for most A that appear as $R_1(D)$ for some $D \in \mathcal{P}(N)$, fixing a basis $\mathcal{B}$ for $\ker A$, for any non-trivial (multiplicative) character $F : \operatorname{Mat}_{n,n+1}(\mathbb{F}_2) \to \{\pm 1\}$, we have

$$\sum_{D \in \mathcal{P}_A(N)} F(R_2(D, \mathcal{B})) \ll \frac{\#\mathcal{P}_A(N)}{(\log\log\log N)^3}. \tag{4.9}$$

For if we take $B = (b_{i,j}) \in \operatorname{Mat}_{n,n+1}(\mathbb{F}_2)$, then

$$\frac{1}{2^{n(n+1)}} \prod_{i,j} \left(1 + (-1)^{b_{i,j}} F_{i,j}\right)$$

is an indicator function of the subset $\{B\}$ of $\mathrm{Mat}_{n,n+1}(\mathbb{F}_2)$, where $F_{i,j} : \mathrm{Mat}_{n,n+1}(\mathbb{F}_2) \to \{\pm 1\}$ is the character such that $F_{i,j}(M) = 1$ if and only if the (i,j) entry of M is -1, for $1 \le i \le n$ and $1 \le j \le n+1$. Expanding the product, we can rewrite the indicator function as

$$\frac{1}{2^{n(n+1)}} \sum_{H} \prod_{(i,j)\in H} (-1)^{b_{i,j}} F_{i,j},$$

where the sum is taken over all subsets H of $\{1,\dots,n\} \times \{1,\dots,n+1\}$. When $H = \varnothing$, the product is 1 by convention. Now summing up the indicator function evaluated at $R_2(D,\mathcal{B})$, over $D \in \mathcal{P}_A(N)$, we get

$$\begin{aligned}&\#\{D \in \mathcal{P}_A(N) : R_2(D,\mathcal{B}) = B\}\\ &\quad = \frac{1}{2^{n(n+1)}} \left(1 + \sum_{H\neq\varnothing} \left(\prod_{(i,j)\in H} (-1)^{b_{i,j}}\right) \sum_{D\in\mathcal{P}_A(N)} \left(\prod_{(i,j)\in H} F_{i,j}\right)(R_2(D,\mathcal{B}))\right).\end{aligned}$$

Each $\prod_{(i,j)\in H} F_{i,j}\,\mathrm{Mat}_{n,n+1}(\mathbb{F}_2) \to \{\pm 1\}$ is a character, so we can deduce from (4.9), that

$$\left|\#\{D \in \mathcal{P}_A(N) : R_2(D,\mathcal{B}) = B\} - \frac{1}{2^{n(n+1)}}\right| \ll \frac{\#\mathcal{P}_A(N)}{(\log\log\log N)^3}.$$

4.2.1 Variable indices

We work with $D \in \mathcal{P}_A$ and $\mathcal{B}$ fixed according to A. List the elements in $\mu_D(\mathcal{B})$ as $s_1,\dots,s_n$. Then the entries of $R_2(D,\mathcal{B}) = (a_{i,j})$ satisfy $(-1)^{a_{i,j}} = \langle s_i, s_j\rangle_2 = [s_i, D/s_i, s_j]$ for $1 \le i,j \le n$ and $(-1)^{a_{i,n+1}} = \langle s_i, -1\rangle_2 = [s_i, D/s_i, -1]$ for $1 \le i \le n$. Write p_i as the i-th largest prime of D.

The set $\{F_{i,j} : 1 \le i \le n,\ 1 \le j \le n+1\}$ is a basis of the dual space of $\mathrm{Mat}_{n,n+1}(\mathbb{F}_2)$. Any character $F : \mathrm{Mat}_{n,n+1}(\mathbb{F}_2) \to \{\pm 1\}$ can be written as

$$F = \prod_{i,j} F_{i,j}^{c_{i,j}},$$

where $c_{i,j} \in \{0,1\}$. Define $B_0 := (c_{i,j})_{1\le i,j\le n}$ and $B_1 := (c_{i,n+1})_{1\le i\le n}$. For each non-trivial F, we take a subset W of $\{1,2,\dots,r-1\}$ with size 2 or 3 as follows.

(V1) If $B_0 \neq 0$ is symmetric with diagonal entries all 0, and $B_1 = 0$, take $1 \le j_1, j_2 \le n$ so that $c_{j_1,j_2} = 1$. Then take $W = \{k_1, k_2\}$, so that

- $p_{k_1} \mid s_{j_1}$ and $p_{k_1} \nmid s_i$ for all $i \neq j_1$;
- $p_{k_2} \mid s_{j_2}$ and $p_{k_2} \nmid s_i$ for all $i \neq j_2$.

(V2) If B_0 is not symmetric, take $1 \leq j_1, j_2 \leq n$ so that $c_{j_1,j_2} = 1$ and $c_{j_2,j_1} = 0$. Then take $W = \{k_1, k_2, k_3\}$, so that

- $p_{k_1} \mid s_{j_1}$ and $p_{k_1} \nmid s_i$ for all $i \neq j_1$;
- $p_{k_2} \mid s_{j_2}$ and $p_{k_2} \nmid s_i$ for all $i \neq j_2$;
- $p_{k_3} \nmid s_i$ for all i.

(V3) Otherwise, B_0 is diagonal or $B_1 \neq 0$. Take $1 \leq j \leq n$ such that $c_{j,j} = 1$ or $c_{j,n+1} = 1$. Then take $W = \{k_1, k_2\}$, so that

- $p_{k_1} \mid s_j$ and $p_{k_1} \nmid s_i$ for all $i \neq j$;
- $p_{k_2} \nmid s_i$ for all $i \neq j$.

Any choice of W is universal for any $D \in \mathcal{P}_A$ when A and $\mathcal{B}$ are fixed.

For most A that appear as $R_1(D)$, the existence of a choice of W is guaranteed when r is large enough by [19, Lemma 6.9].

4.2.2 A combinatorial result

Instead of working with $F : \mathrm{Mat}_{n,n+1}(\mathbb{F}_2) \to \{\pm 1\}$ directly, we consider a product of F evaluated at a certain set of integers.

Let $X = X_1 \times X_2 \times \cdots \times X_k$. Define a map $d : \{X \to \{\pm 1\}\} \to \{X \times X \to \{\pm 1\}\}$. For $\tilde{F} : X \to \{\pm 1\}$, define

$$d\tilde{F}(x^{(1)}, x^{(2)}) = \prod_{(v_1,\ldots,v_k) \in \{1,2\}^k} \tilde{F}((x_1^{(v_1)}, \ldots, x_k^{(v_k)})),$$

where $x^{(i)} = (x_1^{(i)}, \ldots, x_k^{(i)})$. Let $\mathcal{A}(X) = \operatorname{im} d$.

We expect that it is rare to have

$$\left|\tilde{F}^{-1}(1)\right| \geq \epsilon \# X. \tag{4.10}$$

We say that g is ϵ-bad if (4.10) holds for some $\tilde{F}$ such that $d\tilde{F} = g$. Then [19,

Theorem 3.3] implies that

$$\frac{\#\{g \in \mathcal{A}(X) : \text{g is } \epsilon\text{-bad}\}}{\#\mathcal{A}(X)}.$$

is small.

Let $M \coloneqq \lfloor (\log\log\log N)^{10} \rfloor$. Fixing a choice of W, we take a collection of subsets of elements in $\mathcal{P}_A(N)$ (described in [19, Section 6]). Each $D \in \mathcal{P}_A(N)$ appear in the same number of subsets, other than a small proportion collected in the error term.

The subsets of the collection take the following forms. If we are in (V1) or (V3), a subset has the form

$$\{a\} \times Y \times Z \coloneqq \{a\} \times \{p^{(i)} : i\} \times \{q^{(j)} : j\}$$

(viewed as a subset of $\mathcal{P}_A(N)$ via the map $(a, p^{(i)}, q^{(j)}) \mapsto ap^{(i)}q^{(j)}$), where $p^{(i)}$ and $q^{(j)}$ are respectively the k_1-th and k_2-th largest primes of $ap^{(i)}q^{(j)}$, for all $i, j \in \{1, 2\}$, $\#Y = M$, and Z is the largest possible set such that all the above conditions are satisfied.

If we are in (V2), take subsets of the form

$$\{a\} \times Y_1 \times Y_2 \times Z \coloneqq \{a\} \times \{p^{(i)} : i\} \times \{q^{(j)} : j\} \times \{r^{(k)} : k\},$$

where $p^{(i)}$, $q^{(j)}$, $r^{(k)}$ are respectively the k_1-th, k_2-th, and k_3-th largest primes of $ap^{(i)}q^{(j)}r^{(k)}$, for all $i, j, k \in \{1, 2\}$, $\#Y_1 = \#Y_2 = M$, and Z is the largest possible set such that all the above conditions are satisfied. Let $Y = Y_1 \times Y_2$ in this case.

4.2.3 Relative governing fields

Recall the definition of $\mathcal{F}_{a,b}$ in Section 2.1. For any nonzero integers a, b satisfying (2.1), fix a choice of $\beta \in \mathcal{F}_{a,b}$, and write $L_{a,b} = \mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{\beta})$.

We define the relative governing fields we need. If we are in (V1), or (V3) with $c_{j,j} = 0$ and $c_{j,n+1} = 1$, take

$$L \coloneqq \prod_{(p_1,p_2)\in Y\times Y} L_{p_1p_2,-1}.$$

If we are in (V3) with $c_{j,j} = 1$, take

$$L \coloneqq \prod_{(p_1,p_2)\in Y\times Y} L_{p_1p_2,(-1)^{c_{j,n+1}}p_1p_2}$$

If we are in (V2), take

$$L \coloneqq \prod_{((p_1,q_1),(p_2,q_2))\in Y\times Y} L_{p_1p_2,q_1q_2}.$$

Let K is the maximal multiquadratic extension of $\mathbb{Q}$ contained in L. By construction any prime in Z splits completely in $K/\mathbb{Q}$.

We have an isomorphism

$$\Psi : \mathrm{Gal}(L/K) \xrightarrow{\cong} \mathcal{A}(Y) \qquad\qquad \sigma \mapsto \left((p_1,p_2) \mapsto \sigma \restriction_{L_{p_1p_2,-1}}\right).$$

Surjectivity of Ψ follows from a dimension calculation in [19, Lemma 3.1].

For any $\sigma \in \mathrm{Gal}(L/K)$, the proportion of primes $r \in Z$ such that $\left(\frac{L/\mathbb{Q}}{r}\right) = \sigma$ is $1/\#\,\mathrm{Gal}(L/K) = 1/2^{M-1}$ up to a small error (see [19, (6.11)]) by a delicate analytic argument, which amounts to careful applications of Chebotarev density theorem for relatively small primes and large sieve for larger primes. This requires the existence of a large gap between primes factors for almost all $D \in \mathcal{P}$ [19, Theorem 4.1(iii)].

Take $g \in \mathcal{A}(Y\times\{1,\dots,M\})$ such that g is not ϵ-bad, i.e. (4.10) does not hold for any $\tilde{F}$ such that $d\tilde{F} = g$, with ϵ taken as $(\log\log\log N)^3$. Then $g(\cdot,\cdot,i,j) \in \mathcal{A}(Y)$. By the equidistribution of $\left(\frac{L/\mathbb{Q}}{r}\right)$ for $r \in Z$, take any r_1 in Z, then find $r_2, r_3, \dots, r_M$ such that $\Psi(\left(\frac{L/\mathbb{Q}}{r_1r_j}\right)) = g(\cdot,\cdot,1,j)$.

Repeating this process of taking $r_1,\dots,r_M$ in Z, by equidistribution of $\left(\frac{L/\mathbb{Q}}{r}\right)$ for $r \in Z$ in $\mathrm{Gal}(L/K)$, we can put almost all elements in Z into disjoint subsets of primes with size M such that $\Psi(\left(\frac{L/\mathbb{Q}}{r_ir_j}\right)) = g(\cdot,\cdot,i,j)$.

It remains to show that the sum in (4.9) restricted to each constructed subset of $\mathcal{P}_A(N)$ of the form $\{a\}\times Y\times\{r_1,\dots,r_M\}$ is small. This follows from the fact that g is not ϵ-bad, provided that we can verify $d\tilde{F} = g$ for some suitable $\tilde{F}$.

Let $X = Y\times\{1,\dots,M\}$. If we are in (V1), or (V3), define $\tilde{F} : X \to \{\pm1\}$ by $\tilde{F}(p,j) = F(R_{2,S,T}(apr_j))$ and $\tilde{F}_{i,j} : X \to \{\pm1\}$ by $\tilde{F}_{i,j}(p,j) = F_{i,j}(R_{2,S,T}(apr_j))$. If we are in (V2), define $\tilde{F} : X \to \{\pm1\}$ by $\tilde{F}((p,q),j) = F(R_{2,S,T}(apqr_j))$ and

$\tilde{F}_{i,j} : X \to \{\pm 1\}$ by $\tilde{F}_{i,j}((p,q),j) = F_{i,j}(R_{2,S,T}(apqr_j))$.

We now check that $d\tilde{F} = g$. For (V1), we apply Theorem 4.7 and Theorem 4.8. Since $c_{j_1,j_2} = c_{j_2,j_1} = 1$, Theorem 4.8 gives $d\tilde{F}_{j_1,j_2} = g$. Now consider any $(j_3, j_4) \neq (j_1, j_2)$, with $c_{j_3,j_4} = 1$. Then $j_4 \leq n$ and $c_{j_4,j_3} = 1$. Hence Theorem 4.7 implies $d\widetilde{F}_{j_3,j_4} = 1$. Altogether we conclude that $d\widetilde{F} = g$.

For (V2), applying Theorem 4.4(ii) twice shows that $d\widetilde{\widetilde{F}}_{j_1,j_2} = g$. Two applications of Theorem 4.5 show that for all $1 \leq j_2 \leq n_2$, we have $d\widetilde{F}_{j_2,j_2} = 1$, while two applications of Theorem 4.4(i) imply $d\widetilde{F}_{j_3,j_4} = 1$ for all (j_3, j_4) such that $(j_1, j_2) \notin \{(j_3, j_4), (j_4, j_3)\}$ and $j_3 \neq j_4$. This shows that $d\widetilde{F} = g$.

The case (V3) follows from an application of Theorem 4.4 and Theorem 4.5.

Notice that Rédei reciprocity played a key role in Section 4.1 in allowing us to separate the primes that end up defining the relative governing field L and the primes in Z which we ask for the splitting behaviour. Without this, the field L would vary with the prime in Z in some cases, which makes it impossible to control in the current framework.

Chapter 5

Kuroda's formula and arithmetic statistics

This chapter is based on joint work with Djordjo Milovic [21].

We are interested in real biquadratic fields, i.e. normal totally real extensions K of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong V_4$. Let k_1, k_2, k_3 be the quadratic subfields of K. and ϵ_i be the generating units for k_i. Kuroda [50] proved that if K is real, the unit group of K has a set of generators of one of seven types

$$\{\epsilon_1, \epsilon_2, \epsilon_3\},\ \{\sqrt{\epsilon_1}, \epsilon_2, \epsilon_3\},\ \{\sqrt{\epsilon_1}, \sqrt{\epsilon_2}, \epsilon_3\},\ \{\sqrt{\epsilon_1\epsilon_2}, \epsilon_2, \epsilon_3\},$$
$$\{\sqrt{\epsilon_1\epsilon_2}, \sqrt{\epsilon_3}, \epsilon_2\},\ \{\sqrt{\epsilon_1\epsilon_2}, \sqrt{\epsilon_2\epsilon_3}, \sqrt{\epsilon_3\epsilon_1}\},\ \{\sqrt{\epsilon_1\epsilon_2\epsilon_3}, \epsilon_2, \epsilon_3\}. \quad (5.1)$$

This shows that the unit group index, defined as

$$Q(K) = [\mathcal{O}_K^\times : \mathcal{O}_{k_1}^\times \mathcal{O}_{k_2}^\times \mathcal{O}_{k_3}^\times],$$

can be 1, 2, or 4.

Let $\hbar(K)$ denote the largest power of 2 dividing the class number of K. Kuroda's class number formula [51, 48, 49] states that

$$\hbar(K) = \frac{1}{4} Q(K) \hbar(k_1) \hbar(k_2) \hbar(k_3). \quad (5.2)$$

A particular choice of K that is natural from the standpoint of Gauss's genus theory

and that appears in the literature [78, 79, 3, 6, 89, 90, 62] is

$$K = \mathbb{Q}(\sqrt{p}, \sqrt{d}),$$

where p is a prime number and d is a positive squarefree integer coprime to p. With this choice of K, we can now ask more precise statistical questions pertaining to the arithmetic objects appearing in (5.2). For instance, if we fix a positive squarefree integer d and $i \in \{1, 2, 4\}$, then we may wish to determine the natural density, if it exists, of prime numbers p such that $Q(K) = i$.

In analogy with numerous works on 2-parts of class groups we discussed in Section 3.2, for instance [23, 24, 85], we may further inquire if there exists a governing field $\mathcal{M}(d)/\mathbb{Q}$, not depending on p, such that $Q(K)$ is determined by the Frobenius conjugacy class of p in the Galois group $\mathrm{Gal}(\mathcal{M}(d)/\mathbb{Q})$.

We first establish our notation for this chapter. Given integers $d_1, \ldots, d_k$, let $\mathcal{K}_{d_1,\ldots,d_k} \coloneqq \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k})$. Let $\mathbf{Cl}_{d_1,\ldots,d_k}$ and $\mathbf{C}_{d_1,\ldots,d_k}$ denote the ordinary and the narrow class group of $\mathcal{K}_{d_1,\ldots,d_k}$ respectively. Let $\mathcal{H}_{d_1,\ldots,d_k}$ (resp. $\mathcal{H}^+_{d_1,\ldots,d_k}$) denote the 2-Hilbert class field (resp. the narrow 2-Hilbert class field) of $\mathcal{K}_{d_1,\ldots,d_k}$, i.e. the maximal abelian at all places (resp. at finite places) unramified 2-power extension of K. Let $\hbar(d_1, \ldots, d_k)$ and $\hbar^+(d_1, \ldots, d_k)$ denote the size of the 2-parts of $\mathbf{Cl}_{d_1,\ldots,d_k}$ and $\mathbf{C}_{d_1,\ldots,d_k}$ respectively. This implies $\hbar(d_1, \ldots, d_k) = [\mathcal{H}_{d_1,\ldots,d_k} : \mathcal{K}_{d_1,\ldots,d_k}]$ and $\hbar^+(d_1, \ldots, d_k) = [\mathcal{H}^+_{d_1,\ldots,d_k} : \mathcal{K}_{d_1,\ldots,d_k}]$. Also let $m_{d,p}$ denote the number of primes dividing d that split completely in $\mathcal{K}_p/\mathbb{Q}$.

We aim to study the natural density of the fibres of the map $\phi_d : p \mapsto Q(\mathcal{K}_{d,p})$. We will describe a case where we can prove that the map ϕ_d is indeed Frobenian and compute the density of the fibres of ϕ_d.

If $\mathrm{Norm}_{k_i/\mathbb{Q}}(\epsilon_i) = -1$ for all $i = 1, 2, 3$, then from (5.1) the only possible cases are

$$\{\epsilon_1, \epsilon_2, \epsilon_3\}, \text{ and } \{\sqrt{\epsilon_1\epsilon_2\epsilon_3}, \epsilon_2, \epsilon_3\}, \tag{5.3}$$

since we can see that all other cases would contradict to K being real by taking the norm from K to one of k_1, k_2, k_3. In (5.3), the first case gives $Q(K) = 1$ and the

second case gives $Q(K) = 2$. The second case happens if and only if

$$x^2 - dy^2 = 4\epsilon_p,$$

where ϵ_d is the fundamental unit of $\mathbb{Q}(\sqrt{p})$, has a solution $x, y \in \mathcal{O}_{\mathbb{Q}(\sqrt{p})}$. Therefore we may ask how often $Q(\mathfrak{K}_{d,p}) = 2$ holds.

We consider this question in some restricted sets of d and p. Define

$$\mathcal{R} \coloneqq \{d \in \mathbb{Z}_{>0} \text{ squarefree} : \operatorname{rk}_2 \mathbf{Cl}_d = \operatorname{rk}_2 \mathbf{C}_d,\ \operatorname{rk}_4 \mathbf{C}_d = 0\}.$$

The condition $\operatorname{rk}_2 \mathbf{Cl}_d = \operatorname{rk}_2 \mathbf{C}_d$ occurs if and only if d has no prime factors congruent to 3 modulo 4, which happens precisely when the *genus field* of $\mathfrak{K}_d$ is totally real. Further take

$$\mathcal{P}_d \coloneqq \{p \equiv 1 \bmod 4 \text{ prime} : p \nmid d,\ \operatorname{rk}_4 \mathbf{C}_{dp} = 0\}.$$

Then for $d \in \mathcal{R}$ and $p \in \mathcal{P}_d$, let $t = \omega(d)$, then we have

$$\hbar(d) = \hbar^+(d) = 2^{t-1}, \quad \hbar(p) = \hbar^+(p) = 1, \quad \text{and} \quad \hbar(dp) = \hbar^+(dp) = 2^t,$$

so that the formula (5.2) becomes

$$\hbar(d,p) = Q(\mathfrak{K}_{d,p}) \cdot 2^{2t-3}. \tag{5.4}$$

We will first prove that $\hbar^+(d,p) = 2^{2t-2}$, so that $Q(\mathfrak{K}_{d,p}) = 2$ or $Q(\mathfrak{K}_{d,p}) = 1$ depending on whether or not $\mathfrak{H}^+_{d,p}$ is totally real.

Theorem 5.1. *Suppose $d \in \mathcal{R}$ and $p \in \mathcal{P}_d$. Let $t = \omega(d)$. Then $\operatorname{rk}_2 \mathbf{C}_{d,p} = t + m_{d,p} - 1$ and $\operatorname{rk}_4 \mathbf{C}_{d,p} = t - m_{d,p} - 1$. In particular, $\hbar^+(d,p) = 2^{2t-2}$, $Q(\mathfrak{K}_{d,p}) \in \{1,2\}$, and $Q(\mathfrak{K}_{d,p}) = 2$ if and only if $\mathfrak{H}^+_{d,p}$ is totally real.*

Furthermore, after proving Theorem 5.1, we will explicitly construct $\mathfrak{H}^+_{d,p}$ as the compositum of $t-1$ disjoint quadratic extensions of the totally real field $\mathfrak{H}_{dp}$, so that $\mathfrak{H}^+_{d,p}$ is totally real if and only if each of the $t-1$ aforementioned quadratic extensions is totally real. Roughly speaking, we can prove that $m_{d,p}$ of those extensions are totally real with probability $1/2$, and we expect the remaining $t - m_{d,p} - 1$ to behave similarly. Hence we make the following conjecture.

Further define $\mathcal{P}_{d,m} \coloneqq \{p \in \mathcal{P}_d : m_{d,p} = m\}$, and $\mathcal{P}_{d,m}(N) \coloneqq \{p \in \mathcal{P}_{d,m} : p < N\}$.

Conjecture 5.2. *For $d \in \mathcal{R}$, we have*

$$\lim_{N\to\infty} \frac{\#\{p \in \mathcal{P}_{d,m}(N) : \ Q(\mathcal{K}_{d,p}) = 2\}}{\#\mathcal{P}_{d,m}(N)} = \frac{1}{2^{t-1}},$$

where $t = \omega(d)$.

Our main "statistical" result about $Q(\mathcal{K}_{d,p})$ is the following theorem.

Theorem 5.3. *Suppose $d \in \mathcal{R}$ and let $t = \omega(d)$. Then the map*

$$\mathcal{P}_{d,m} \to \{1, 2\}, \qquad p \mapsto Q(\mathcal{K}_{d,p})$$

is Frobenian for $m = t - 1$ and $m = t - 2$. Moreover, Conjecture 5.2 holds for $m = t - 1$ and $m = t - 2$, and, for all $m \in \{0, 1, \ldots, t - 3\}$, we have

$$\lim_{N\to\infty} \frac{\#\{p \in \mathcal{P}_{d,m}(N) : \ Q(\mathcal{K}_{d,p}) = 2\}}{\#\mathcal{P}_{d,m}(N)} \leq \frac{1}{2^m}.$$

5.1 The 2-rank of $\mathbf{C}_{d,p}$

Let $d \in \mathcal{R}$ and $t = \omega(d)$ as in the introduction and let $p \in \mathcal{P}_{d,m}$. We begin by constructing an unramified at all finite primes C_2^{t+m-1}-extension of $\mathcal{K}_{p,d}$ and stating a criterion for this extension to be totally positive.

Let $q_1, \ldots, q_t$ be the prime divisors of d. We may reorder the q_i so that $\left(\frac{q_i}{p}\right) = 1$ for $1 \leq i \leq m$ and $\left(\frac{q_i}{p}\right) = -1$ for $m + 1 \leq i \leq t$. First, as we described in Section 1.3, genus theory for the quadratic number field $\mathcal{K}_d$ implies that $\mathcal{K}_{p,q_1,\ldots,q_t}$ is an unramified at *all* primes C_2^{t-1}-extension of $\mathcal{K}_{d,p}$. Now suppose that $1 \leq i \leq m$, so that $\left(\frac{q_i}{p}\right) = 1$. Applying [31, Lemma 19, p.2059] (or more generally our (2.5)) with $D_1 = q_i$ (or $4q_i$ if $q_i = 2$) and $D_2 = p$, we can choose $x_i, y_i, z_i \in \mathbb{Z}$ satisfying the ternary quadratic equation

$$x_i^2 - py_i^2 - q_i z_i^2 = 0$$

such that (i) x_i^2, py_i^2, and $q_iz_i^2$ are pairwise coprime, $y_i, z_i \geq 0$ (ii) x_i odd, and one of y_i and z_i is even, and (iii) $x_i - y_i \equiv 1 \bmod 4$ if y_i is even and $x_i - z_i \equiv 1 \bmod 4$ if z_i is even. We define

$$\alpha_i = \begin{cases} x_i + y_i\sqrt{p} & \text{if } z_i \text{ is odd,} \\ \frac{1}{2}(x_i + y_i\sqrt{p}) & \text{if } z_i \text{ is even;} \end{cases} \tag{5.5}$$

then [31, Lemma 20, p.2060], or more generally Theorem 2.2, implies that $\mathcal{K}_{p,q_i}(\sqrt{\alpha_i})/\mathbb{Q}$ is a D_8-extension, unramified at all finite primes over $\mathcal{K}_{pq_i}$ and a fortiori over $\mathcal{K}_{p,q_i}$. The extension $\mathcal{K}_{p,q_i}(\sqrt{\alpha_i})/\mathcal{K}_p$ is a V_4-extension, and so, upon taking the compositum over all $1 \leq i \leq m$ and also with $\mathcal{K}_{p,q_1,\ldots,q_t}$, we find that

$$\mathcal{C}_{d,p} = \mathcal{K}_{p,q_1,\ldots,q_t}(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m}) \tag{5.6}$$

is normal over $\mathcal{K}_p$ with Galois group isomorphic to C_2^{t+m}. We hence conclude that $\mathcal{C}_{d,p}/\mathcal{K}_{d,p}$ is a normal, unramified at all finite primes extension with Galois group isomorphic to C_2^{t+m-1}. Since $\mathcal{K}_p$ has odd class number, we can apply Lemma 5.4 to over $\mathcal{K}_p$, we see that $\mathrm{rk}_2\,\mathbf{C}_{d,p} \leq t + m - 1$, since the number of primes of $\mathcal{K}_p$ that ramify in $\mathcal{K}_{d,p}$ is $t + m$. This also follows from results in genus theory over $\mathcal{K}_p$ [90, Lemma 2.3]. Hence we have proved

Lemma 5.4. *Define $\mathcal{C}_{d,p}$ as in* (5.6). *Then $\mathcal{C}_{d,p}/\mathcal{K}_{d,p}$ is the maximal unramified at all finite primes abelian extension of K of exponent* 2. *In particular,* $\mathrm{rk}_2\,\mathbf{C}_{d,p} = t + m - 1$.

Now [31, Proposition 5, p.2061] implies that $\mathcal{K}_{p,q_i}(\sqrt{\alpha_i})$ is totally real if and only if

$$\left[\frac{p}{q_i}\right]_4 \left[\frac{q_i}{p}\right]_4 = 1. \tag{5.7}$$

Here, as in [31, p.2061], for a prime ℓ and a rational integer a, we define

$$\left[\frac{a}{\ell}\right]_4 = \begin{cases} 1 & \text{if } a \text{ is a fourth power modulo } \ell \\ -1 & \text{otherwise} \end{cases}$$

whenever ℓ is an odd prime such that $\left(\frac{a}{\ell}\right) = 1$ and

$$\left[\frac{a}{2}\right]_4 = \begin{cases} 1 & \text{if } a \equiv 1 \bmod 16 \\ -1 & \text{if } a \equiv 9 \bmod 16 \end{cases}$$

whenever $a \equiv 1 \bmod 8$. Thus $\mathscr{C}_{d,p}$ is totally real if and only if (5.7) holds for all $i \in \{1, \dots, m\}$. We will now rewrite the condition (5.7) in terms of genuine fourth power residue symbols $\left(\frac{\cdot}{\cdot}\right)_4$ over $\mathcal{K}_{-1}$, a field containing a primitive fourth root of unity. Suppose that p and q_i split into primary primes as $p = \pi\overline{\pi}$ and $q_i = \rho_i\overline{\rho_i}$ in the ring of Gaussian integers $\mathcal{O}_{\mathcal{K}_{-1}}$ (assume for the moment that $q_i \neq 2$). Then, since $\pi\mathcal{O}_{\mathcal{K}_{-1}}$ and $\rho_i\mathcal{O}_{\mathcal{K}_{-1}}$ are primes of degree 1, we have

$$\left[\frac{p}{q_i}\right]_4 \left[\frac{q_i}{p}\right]_4 = \left(\frac{p}{\rho_i}\right)_4 \left(\frac{q_i}{\pi}\right)_4 = \left(\frac{\pi}{\rho_i}\right)_4 \left(\frac{\overline{\pi}}{\rho_i}\right)_4 \left(\frac{\rho_i}{\pi}\right)_4 \left(\frac{\overline{\rho_i}}{\pi}\right)_4.$$

Quartic reciprocity law [42, Theorem 2, p. 123] implies that

$$\left(\frac{\pi}{\rho_i}\right)_4 = \left(\frac{\rho_i}{\pi}\right)_4 \cdot (-1)^{\frac{p-1}{4}\frac{q_i-1}{4}} \quad \text{and} \quad \left(\frac{\overline{\pi}}{\rho_i}\right)_4 = \left(\frac{\rho_i}{\overline{\pi}}\right)_4 \cdot (-1)^{\frac{p-1}{4}\frac{q_i-1}{4}}.$$

Hence

$$\left[\frac{p}{q_i}\right]_4 \left[\frac{q_i}{p}\right]_4 = \left(\frac{\rho_i}{\pi}\right)_4 \overline{\left(\frac{\overline{\rho_i}}{\pi}\right)_4} \left(\frac{\rho_i}{\pi}\right)_4 \left(\frac{\overline{\rho_i}}{\pi}\right)_4 = \left(\frac{\rho_i}{\pi}\right)_2.$$

Hence we have proved that when $2 \nmid q_1 \dots q_m$, $\mathscr{C}_{d,p}$ is totally real if and only if p splits completely in the number field

$$\mathscr{M}_2(d) = \mathcal{K}_{-1,q_1,\dots,q_m}(\sqrt{\rho_1}, \dots, \sqrt{\rho_m}). \tag{5.8}$$

Now suppose $q_1 = 2$, so that $p \equiv 1 \bmod 8$. By definition, $\left[\frac{p}{2}\right]_4 = 1$ if and only if $p \equiv 1 \bmod 16$, i.e., if and only if p splits completely in $\mathcal{K}_{-1,-2}(\sqrt{2+\sqrt{2}})$, while $\left[\frac{2}{p}\right]_4 = 1$ if and only if p splits completely in $\mathcal{K}_{-1,2}(\sqrt[4]{2})$. Hence $\left[\frac{p}{2}\right]_4 \left[\frac{2}{p}\right]_4 = 1$ if and only if p splits completely in $\mathcal{K}_{-1,2}(\sqrt[4]{2}\sqrt{2+\sqrt{2}}) = \mathcal{K}_{-1,2}(\sqrt{1+\sqrt{-1}})$. Thus, if $q_1 \cdots q_m$ is even with $q_1 = 2$, say, then again $\mathscr{C}_{d,p}$ is totally real if and only if p splits completely in $\mathscr{M}_2(d)$, where now $\rho_1 = 1 + \sqrt{-1} \in \mathcal{K}_{-1}$.

Suppose $p \in \mathcal{P}_{d,m}$. It follows from Rédei's classical work [64] on the 4-rank of class groups of quadratic fields, as we discussed in Section 1.4 and Proposition 3.8,

that the condition $\mathrm{rk}_4\,\mathbf{C}_{dp} = 0$ can be detected by the Frobenius conjugacy class of p in the abelian Galois group $\mathrm{Gal}(\mathcal{K}_{q_1,\ldots,q_t}/\mathbb{Q})$; furthermore, since p splits completely in $\mathcal{K}_{q_1,\ldots,q_m}/\mathbb{Q}$, the condition $\mathrm{rk}_4\,\mathbf{C}_{dp} = 0$ is in fact equivalent to $\left(\frac{\mathcal{K}_{q_{m+1},\ldots,q_t}/\mathbb{Q}}{p}\right)$ belonging to some fixed subset $\Sigma \subset \mathrm{Gal}(\mathcal{K}_{q_{m+1},\ldots,q_t}/\mathbb{Q})$. For each element $\sigma \in \Sigma$, let $\mathcal{P}_{d,m,\sigma}$ be the set of p in $\mathcal{P}_{d,m}$ such that $\left(\frac{\mathcal{K}_{q_{m+1},\ldots,q_t}/\mathbb{Q}}{p}\right) = \sigma$. Since $p \in \mathcal{P}_{d,m}$ splits completely in $\mathcal{K}_{-1,q_1,\ldots,q_m}/\mathbb{Q}$, since $\mathcal{K}_{q_{m+1},\ldots,q_t}$ is disjoint from $\mathcal{M}_2(d)$, and since $[\mathcal{M}_2(d) : \mathcal{K}_{-1,q_1,\ldots,q_m}] = 2^m$, the Chebotarev Density Theorem implies that, for each $\sigma \in \Sigma$, the natural density of primes p in $\mathcal{P}_{d,m,\sigma}$ such that $\mathcal{C}_{d,p}$ is totally real is equal to 2^{-m}. Taking the union over all $\sigma \in \Sigma$, we deduce also that the natural density of primes p in $\mathcal{P}_{d,m}$ such that $\mathcal{C}_{d,p}$ is totally real is equal to 2^{-m}. In conjunction with Theorem 5.1, since $\mathcal{H}^+_{d,p}$ cannot be totally real unless $\mathcal{C}_{d,p}$ is totally real, this proves the case $m_0 = t-1$ (with $\mathcal{M}_2(d)$ as the governing field) as well as the upper bound in the second part of Theorem 5.3.

5.2 The 4-rank of $\mathbf{C}_{d,p}$

Define α_i as in (5.5). Let $\widetilde{\alpha_i}$ be the conjugate of α_i in $\mathcal{K}_p$. Let $\mathfrak{q}_i$ be a prime above q_i in $\mathcal{K}_p$ and $\widetilde{\mathfrak{q}_i}$ be its conjugate if $i \le m$, so that $\alpha_i\mathcal{O}_{\mathcal{K}_p}$ factorizes into $\mathfrak{q}_i$ times a square ideal.

Call $a \in \mathcal{K}_p^\times/(\mathcal{K}_p^\times)^2$ a *decomposition of second type for* $\mathcal{K}_{d,p}$ if

(i) $a \equiv \prod_{i=1}^m \alpha_i^{e_i} \prod_{i=1}^m \widetilde{\alpha_i}^{e'_i} \prod_{i=m+1}^t q_i^{f_i} \mod (\mathcal{K}_p^\times)^2$, where $e_i, e'_i, f_i \in \{0,1\}$; and

(ii) $(a, d/a)_{\mathfrak{r}} = 1$ for all finite and infinite primes $\mathfrak{r}$ in $\mathcal{O}_{\mathcal{K}_p}$.

Lemma 5.5. *Let $a \in \mathcal{K}_p^\times/(\mathcal{K}_p^\times)^2$. Suppose that $L/\mathcal{K}_{d,p}$ is a C_4-extension unramified at all finite primes and containing $\mathcal{K}_{d,p}(\sqrt{a}) \subseteq \mathcal{C}_{d,p}$. Then*

(i) $\mathrm{Gal}(L/\mathcal{K}_p) \cong D_8$*; and*

(ii) $(a, d/a)_{\mathfrak{r}} = 1$ *for all* $\mathfrak{r} \in \mathcal{M}_{\mathcal{K}_p}$.

Proof. The first part follows from Lemma 1.13.

For the second part of the lemma we follow the proof [31, Lemma 17] with $\mathbb{Q}$ replaced by $\mathcal{K}_p$. The extension $L/\mathcal{K}_{d,p}$ is the unique central C_4-subextension in $L/\mathcal{K}_p$. Suppose $\mathfrak{q}$ is a prime ideal in $\mathcal{O}_{\mathcal{K}_p}$ that ramifies in $\mathcal{K}_p(\sqrt{a})/\mathcal{K}_p$, the inertia field of $\mathfrak{q}$ in $L/\mathcal{K}_p$ have degree 4 since $L/\mathcal{K}_{d,p}$ is unramified. The inertia field of

$\mathfrak{q}$ therefore must contain $\mathcal{K}_p(\sqrt{d/a})$ and is not $\mathcal{K}_{d,p}$. Since the inertia field is not normal in $L/\mathcal{K}_p$, there must be at least two prime ideal in $\mathcal{O}_L$ above $\mathfrak{q}$. Therefore $\mathfrak{q}$ must split in $\mathcal{K}_p(\sqrt{a})$. Switching the role in of a and d/a proves the lemma. □

The set of decompositions of second type form a multiplicative group in $\mathcal{K}_p^\times / \left(\mathcal{K}_p^\times\right)^2$ of size $2^{1+\mathrm{rk}_4 \mathbf{C}_{d,p}}$.

5.2.1 Generalised Rédei matrix

Similar to [31, Lemma 13], the condition $(a, d/a)_{\mathfrak{r}} = 1$ for all finite and infinite primes $\mathfrak{r}$ in $\mathcal{O}_{\mathcal{K}_p}$ is equivalent to the following conditions

(i) $a > 0$;

(ii) $\left(\frac{\mathcal{K}_{p,a}/\mathcal{K}_p}{\mathfrak{q}}\right) = 1$ if $\mathrm{ord}_{\mathfrak{q}}(da)$ is odd; and

(iii) $\left(\frac{\mathcal{K}_{p,d/a}/\mathcal{K}_p}{\mathfrak{q}}\right) = 1$ if $\mathrm{ord}_{\mathfrak{q}}(a)$ is odd.

5.2.1.1 Rational decompositions of second type

Consider the subset of decompositions of second type where $a \in \mathbb{Q}$, $a > 0$. Studying the splitting of primes in the V_4-extension $\mathcal{K}_{a,p}/\mathbb{Q}$, we see that the condition $(a, d/a)_{\mathfrak{r}} = 1$ for any prime ideal $\mathfrak{r}$ in $\mathcal{K}_p$ is equivalent to asking for each prime $q \mid d$ with $\left(\frac{q}{p}\right) = 1$ to satisfy

$$\left(\frac{a}{q}\right) = 1 \quad \text{if } q \,\Big|\, \frac{d}{a}, \qquad\qquad \left(\frac{d/a}{q}\right) = 1 \quad \text{if } q \mid a.$$

Writing a as a product of q_i, the conditions can be packaged in a matrix over $\mathbb{F}_2$. Take $S = \{q_1, \ldots, q_t\}$ and $T = \{q_1, \ldots, q_m\}$, and let B_0 be the matrix $R_{1,S,T}(d)$ as defined at the end of Section 1.3, i.e.

$$B_0 \coloneqq \begin{pmatrix} \left(\frac{d/q_1}{q_1}\right) & \left(\frac{q_2}{q_1}\right) & \cdots & \left(\frac{q_m}{q_1}\right) & \left(\frac{q_{m+1}}{q_1}\right) & \cdots & \left(\frac{q_t}{q_1}\right) \\ \left(\frac{q_1}{q_2}\right) & \left(\frac{d/q_2}{q_2}\right) & \cdots & \left(\frac{q_m}{q_2}\right) & \left(\frac{q_{m+1}}{q_2}\right) & \cdots & \left(\frac{q_t}{q_2}\right) \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ \left(\frac{q_1}{q_m}\right) & \left(\frac{q_2}{q_m}\right) & \cdots & \left(\frac{d/q_m}{q_m}\right) & \left(\frac{q_{m+1}}{q_m}\right) & \cdots & \left(\frac{q_t}{q_m}\right) \end{pmatrix}_+,$$

where the subscript + denotes the conversion of each entry from $\{\pm 1\}$ to $\{0, 1\}$. Then $\ker B_0$ corresponds to the set of decompositions of the second type. The size of the matrix implies that $\dim \ker B_0 \geq t - m$. Therefore $\mathrm{rk}_4 \mathbf{C}_{d,p} \geq t - m - 1$.

Combining with the fact that $\mathrm{rk}_2\,\mathbf{C}_{d,p} = t + m - 1$, the 2-part of $\mathbf{C}_{d,p}$ has size at least 2^{2t-2}.

5.2.1.2 General decompositions of second type

Now consider all decompositions of second type for $\mathcal{K}_{d,p}$. The set of decompositions of the second type a is given by the kernel of the matrix

$$A \coloneqq \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix},$$

where

$$A_{11} = \left(\begin{pmatrix} \frac{d/\alpha_1}{\mathfrak{q}_1} \end{pmatrix} \cdots \begin{pmatrix} \frac{\alpha_m}{\mathfrak{q}_1} \end{pmatrix} \right)_+, \; A_{12} = \left(\begin{pmatrix} \frac{\widetilde{\alpha_1}}{\mathfrak{q}_1} \end{pmatrix} \cdots \begin{pmatrix} \frac{\widetilde{\alpha_m}}{\mathfrak{q}_1} \end{pmatrix} \right)_+, \; A_{13} = \left(\begin{pmatrix} \frac{q_{m+1}}{\mathfrak{q}_1} \end{pmatrix} \cdots \begin{pmatrix} \frac{q_t}{\mathfrak{q}_1} \end{pmatrix} \right)_+,$$

$$A_{21} = \left(\begin{pmatrix} \frac{\alpha_1}{\widetilde{\mathfrak{q}_1}} \end{pmatrix} \cdots \begin{pmatrix} \frac{\alpha_m}{\widetilde{\mathfrak{q}_1}} \end{pmatrix} \right)_+, \; A_{22} = \left(\begin{pmatrix} \frac{d/\widetilde{\alpha_1}}{\widetilde{\mathfrak{q}_1}} \end{pmatrix} \cdots \begin{pmatrix} \frac{\widetilde{\alpha_m}}{\widetilde{\mathfrak{q}_1}} \end{pmatrix} \right)_+, \; A_{23} = \left(\begin{pmatrix} \frac{q_{m+1}}{\widetilde{\mathfrak{q}_1}} \end{pmatrix} \cdots \begin{pmatrix} \frac{q_t}{\widetilde{\mathfrak{q}_1}} \end{pmatrix} \right)_+,$$

$$A_{31} = \left(\begin{pmatrix} \frac{\alpha_1}{\mathfrak{q}_{m+1}} \end{pmatrix} \cdots \begin{pmatrix} \frac{\alpha_m}{\mathfrak{q}_{m+1}} \end{pmatrix} \right)_+, \; A_{32} = \left(\begin{pmatrix} \frac{\widetilde{\alpha_1}}{\mathfrak{q}_{m+1}} \end{pmatrix} \cdots \begin{pmatrix} \frac{\widetilde{\alpha_m}}{\mathfrak{q}_{m+1}} \end{pmatrix} \right)_+, \; A_{33} = \left(\begin{pmatrix} \frac{d/q_{m+1}}{\mathfrak{q}_{m+1}} \end{pmatrix} \cdots \begin{pmatrix} \frac{q_t}{\mathfrak{q}_{m+1}} \end{pmatrix} \right)_+.$$

The matrix A has the same rank as

$$B \coloneqq \begin{pmatrix} A_{11} & A_{11} + A_{12} & A_{13} \\ A_{11} + A_{21} & A_{11} + A_{12} + A_{21} + A_{22} & A_{13} + A_{23} \\ A_{31} & A_{31} + A_{32} & A_{33} \end{pmatrix} = \begin{pmatrix} A_{11} & B_0 \\ B_0^T & 0 \end{pmatrix}.$$

In particular, when B_0 has maximal rank m and $m < t$, $\operatorname{rank} B = 2 \operatorname{rank} B_0$, then the dimension of $\ker B = (t+m) - 2m = t - m$, and so $\mathrm{rk}_4\,\mathbf{C}_{d,p} \leq t - m - 1$.

5.2.2 The vanishing of the 8-rank of $\mathbf{C}_{d,p}$

Lemma 5.6. *Let K be a biquadratic number field with quadratic subfields k_1, k_2, k_3. Let $n \geq 1$ be an integer. If $\mathrm{rk}_{2^n}\,\mathbf{C}_{k_i}$ is 0 for $i = 1, 2, 3$, then the 2^{n+1}-rank of $\mathbf{C}_K$ is 0.*

Proof. Take a prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ above prime p. It suffices to show that the

order of $[\mathfrak{P}]^2 \in \mathbf{C}_K$ divides the order of some ideal class in $\mathbf{C}_{k_i}$. We split into three possible cases according to the splitting of p in K.

Suppose p is inert in k_1, k_2 and splits in k_3. Let $\mathfrak{p}$ be an ideal below $\mathfrak{P}$ in k_3. Since $\mathfrak{P} = \mathfrak{p}\mathcal{O}_K$, if $\mathfrak{p}^l$ is principal in k_3, then $\mathfrak{P}^l$ must also be principal in K. Therefore the order of $[\mathfrak{P}] \in \mathbf{C}_K$ divides the order of $[\mathfrak{p}] \in \mathbf{C}_{k_3}$.

Now suppose p ramifies in k_1 and k_2. Let $\mathfrak{p}$ be an ideal below $\mathfrak{P}$ in k_3. Since $\mathfrak{P}^2 = \mathfrak{p}\mathcal{O}_K$, the order of $[\mathfrak{P}]^2 \in \mathbf{C}_K$ divides the order of $[\mathfrak{p}] \in \mathbf{C}_{k_3}$.

Suppose instead p splits completely in K. Let $\mathfrak{p}_i$ be the prime ideal below $\mathfrak{P}$ in k_i for $i = 1, 2, 3$. Then $\mathfrak{p}_i\mathcal{O}_K = \mathfrak{P}\mathfrak{P}_i$, where $\mathfrak{P}_i$ is a conjugate prime ideal of $\mathfrak{P}$ under the non-trivial map in $\mathrm{Gal}(K/k_i)$. Then $(p)\mathcal{O}_K = \mathfrak{P}\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$, so $[\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathcal{O}_K] = [\mathfrak{P}]^2$ in $\mathbf{C}_K$. Therefore the order of $[\mathfrak{P}]^2 \in \mathbf{C}_K$ divides the lcm of orders of $[\mathfrak{p}_i] \in \mathbf{C}_{k_i}$. □

Lemma 5.7. *Suppose $d \in \mathcal{R}$ and $p \in \mathcal{P}_{d,m}$. Then* $\mathrm{rk}_8\, \mathbf{C}_{d,p} = 0$.

Proof. The quadratic subfields of the biquadratic field $\mathcal{K}_{d,p}$ are $\mathcal{K}_d$, $\mathcal{K}_p$, and $\mathcal{K}_{dp}$. By assumption on d, we have $\mathrm{rk}_4\, \mathbf{C}_d = 0$. We have $\mathrm{rk}_2\, \mathbf{C}_p = 0$ and so also $\mathrm{rk}_4\, \mathbf{C}_p = 0$. By definition of $\mathcal{P}_{d,p}$, we have $\mathrm{rk}_4\, \mathbf{C}_{dp} = 0$. The result now follows from Lemma 5.6. □

5.2.3 Proof of Theorem 5.1

The lower and upper bounds from Sections 5.2.1.1 and 5.2.1.2, respectively, yield

$$\mathrm{rk}_4\, \mathbf{C}_{d,p} = t - m - 1.$$

In conjunction with Lemma 5.7, we conclude that the 2-part of $\mathbf{C}_{d,p}$ is congruent to

$$C_2^{2m} \times C_4^{t-m-1}.$$

Now equation (5.4) implies that $2^{2t-2} = \hbar^+(d,p) \geq \hbar(d,p) = Q(\mathcal{K}_{d,p}) \cdot 2^{2t-3}$, so that $Q(\mathcal{K}_{d,p}) \leq 2$ with equality if and only if $\hbar^+(d,p) = \hbar(d,p)$, i.e., if and only if $\mathscr{H}^+_{d,p}$ is totally real.

5.3 Construction of $\mathscr{H}^+_{d,p}$

In this section, we will give an explicit construction the narrow 2-Hilbert class field $\mathscr{H}^+_{d,p}$ of $\mathcal{K}_{d,p}$. We have

$$\mathscr{H}^+_{d,p} = \mathscr{C}_{d,p} \quad \text{if} \quad m = t - 1,$$

where $\mathscr{C}_{d,p}$ is defined in (5.6). This follows from the upper bound on the 4-rank of $\mathbf{C}_{d,p}$ given in Section 5.2.1.2.

When $m \leq t-2$, we will construct certain unramified at finite primes C_4-extensions of $\mathscr{K}_{d,p}$ by working over $\mathscr{K}_p$. In general, this does not lead to simple criteria for $\mathscr{H}_{d,p}^{+}$ to be totally real. When $m = t-2$, then we can construct the unramified at finite primes C_4-extension of $\mathscr{K}_{d,p}$ by working over $\mathbb{Q}$, and in this case we can find a criterion for $\mathscr{H}_{d,p}^{+}$ to be totally real that is amenable to density computations.

5.3.1 Constructing unramified C_4-extensions

Lemma 5.8. *Suppose that $a \mid d$ and that a is even if d is even. Let $p \equiv 1 \bmod 4$ be a prime. Suppose that*

$$X^2 - aY^2 = \frac{d}{a}Z^2 \tag{5.9}$$

is solvable for some $X, Y, Z \in \mathscr{K}_p$. Then there exists a solution such that $\beta := X + Y\sqrt{a}$ gives an extension $\mathscr{K}_{d,p,a}(\sqrt{\beta})/\mathscr{K}_{d,p,a}$ that is unramified at all finite primes.

More specifically, β can be taken such that

(i) $X, Y, Z \in \mathcal{O}_{\mathscr{K}_p}$,

(ii) $\gcd((X),(Y),(Z))$ *is a square ideal,*

(iii) X, Z *are coprime with* 2 *and* $2 \mid Y$,

(iv)
$$\left\{ \begin{array}{ll} X - Y & \text{if } a \equiv 1 \bmod 4, \\ X - \frac{Y^2}{2} & \text{if } a \equiv 2 \bmod 4 \end{array} \right\} \equiv \left\{ \begin{array}{ll} 1 \bmod 4 & \text{if } p \equiv 1 \bmod 8, \\ 1 \text{ or } \frac{\frac{1+p}{2} \pm \sqrt{p}}{2} \bmod 4 & \text{if } p \equiv 5 \bmod 8. \end{array} \right.$$

Proof. Our goal is to find a suitable $\beta = X + Y\sqrt{a}$ that satisfies the requirement in Proposition 1.2. Let σ be the generator of $\mathrm{Gal}(\mathscr{K}_p/\mathbb{Q})$. Clearing denominators we can assume $X, Y, Z \in \mathcal{O}_{\mathscr{K}_p}$. Since the fundamental unit in $\mathscr{K}_p$ has norm -1, we can take $x, y \in \mathbb{Z}$ satisfying $x^2 - py^2 = -1$ and set $u = x + y\sqrt{p}$. Looking at $x^2 - py^2 \equiv -1 \bmod 4$ we see that x is even and y is odd, so $u = x + y\sqrt{p} \equiv \pm\sqrt{p} \bmod 4$ in $\mathcal{O}_{\mathscr{K}_p}$.

Choosing β to be coprime to 2. Removing factors of 2 we can assume 2 divides at most one of X, Y, Z. If $p \equiv 5 \bmod 8$, then 2 is inert in $\mathscr{K}_p$ so at most one of X, Y, Z is even.

If $p \equiv 1 \bmod 8$, then 2 splits in $\mathcal{K}_p$. Then

$$\text{Norm}\left(\frac{1+\sqrt{p}}{2}\right) = \frac{1-p}{4}, \text{ and } \text{Norm}\left(\frac{3+\sqrt{p}}{2}\right) = \frac{9-p}{4}$$

are both even but differ by 2, so one must be congruent to 2 mod 4. Say γ is the element from above with norm 2 mod 4. Then exactly one of the primes above 2 divides γ with order 1, call this prime $\mathfrak{t}$. Suppose $\max\{\text{ord}_{\mathfrak{t}} X, \text{ord}_{\mathfrak{t}} Y, \text{ord}_{\mathfrak{t}} Z\} = k$, then take $X(\gamma^\sigma/2)^k, Y(\gamma^\sigma/2)^k, Z(\gamma^\sigma/2)^k$. Repeat the same for the ideal $\mathfrak{t}^\sigma$. Then we can assume that no prime above 2 divides $\gcd((X),(Y),(Z))$. Therefore at least one of X, Y, Z is coprime with 2.

The squares modulo 4 in $\mathcal{O}_{\mathcal{K}_p}$ are 0, 1, $\omega := ((1+p)/2 + \sqrt{p})/2$ and $\omega' := ((1+p)/2 - \sqrt{p})/2$. We have $X^2 = 2Y^2 + Z^2 \bmod 4$ when a is even, and $X^2 = Y^2 + Z^2 \bmod 4$ when a is odd, we see that the possible combinations are

$$(X^2, \{Y^2, Z^2\}) \equiv \begin{cases} (1, \{0,1\}) \bmod 4, & (5.10) \\ (\omega, \{0,\omega\}) \bmod 4, & (5.11) \\ (\omega', \{0,\omega'\}) \bmod 4, & (5.12) \\ (1, \{\omega,\omega'\}) \bmod 4 \quad \text{if } p \equiv 1 \bmod 8. & (5.13) \end{cases}$$

The cases (5.11) and (5.12) are only possible when $p \equiv 5 \bmod 8$. For if $p \equiv 1 \bmod 8$, the norms of ω and ω' are $(1-p)^2/16$, which is even, contradicting with the assumption that at least one of X, Y, Z is coprime with 2.

For case (5.13), one can obtain another solution to (5.9) that satisfies one of (5.10), (5.11), (5.12). Without loss of generality assume $Z^2 \equiv \omega \bmod 4$. Since $X^2 \equiv 1 \bmod 4$ implies $X \equiv \pm 1$ or $\pm\sqrt{p} \bmod 4$, multiplying X, Y, Z by a suitable $\delta \in \{\pm 1, \pm u\}$, we can also assume $X \equiv 1 \bmod 4$. Let $\mathfrak{t}$ denote the prime above 2 such that $\mathfrak{t} \mid Y$, then $t^\sigma \mid Z$ and $\mathfrak{t}, \mathfrak{t}^\sigma \nmid X$. Take

$$\begin{aligned}(X', Y', Z') &:= \left(\frac{1+d/a}{2}X \pm \frac{d}{a}Z\ , \frac{1-d/a}{2}Y,\ \frac{1+d/a}{2}Z \pm X\right) \qquad (5.14)\\ &\equiv \begin{cases} (X \pm Z,\ 0,\ Z \pm X) \bmod 4 & \text{if } \frac{d}{a} \equiv 1 \bmod 8, \\ (-X \pm Z,\ 2,\ -Z \pm X) \bmod 4 & \text{if } \frac{d}{a} \equiv 5 \bmod 8. \end{cases}\end{aligned}$$

Then

$$\mathrm{Norm}(X') \equiv \mathrm{Norm}(Z') \equiv 1 \pm (Z + Z^{\sigma}) + ZZ^{\sigma} \bmod 4.$$

$Z^2 \equiv \omega \bmod 4$ implies $Z \equiv \pm(1+\sqrt{p})/2$ or $\pm(5+\sqrt{p})/2 \bmod 4$. Therefore $Z + Z^{\sigma} \equiv 1 \bmod 4$ and $ZZ^{\sigma} \equiv 0$ or $2 \bmod 4$. Pick the sign such that $\mathrm{Norm}(X') \equiv \mathrm{Norm}(Z') \equiv 2 \bmod 4$. Then $\mathrm{ord}_{\mathfrak{t}} X' = \mathrm{ord}_{\mathfrak{t}} Z' = 1$ and $\mathfrak{t}^{\sigma} \nmid X'Z'$. Carry out the reduction as before we can obtain new X' and Z' that are both coprime to 2. Therefore we can assume X is always coprime with 2 and exactly one of Y, Z is coprime with 2.

If X, Y are coprime with 2 and $2 \mid Z$, the transformation (5.14) gives X', Z' that are coprime to 2 and $2 \mid Y'$. Therefore we can always take X, Z coprime to 2 and $2 \mid Y$. In particular $\beta\mathcal{O}_{\mathcal{K}_{d,p,a}}$ is coprime to 2 since its norm is odd.

Choosing β to be a square ideal. Let h be the class number of $\mathcal{K}_p$, which is odd. If $\mathrm{ord}_{\mathfrak{p}}(\gcd((X),(Y),(Z))$ is odd for some prime ideal $\mathfrak{p}$, we can multiply X, Y, Z by some γ, where γ satisfies $\mathfrak{p}^h = (\gamma)$. Remove any rational prime p dividing $\gcd((X),(Y),(Z))$. Therefore we can assume $\gcd((X),(Y),(Z))$ is a square ideal involving only prime ideals above odd primes that splits in $\mathcal{K}_p/\mathbb{Q}$. For each odd prime p that splits in $\mathcal{K}_p/\mathbb{Q}$ at most one of the primes above p can divide $\gcd((X),(Y),(Z))$.

Suppose there exists an odd prime dividing $\beta\mathcal{O}_{\mathcal{K}_{d,p,a}}$, then there must be a prime $\mathfrak{P}$ below in $\mathcal{O}_{\mathcal{K}_{p,a}}$ dividing $\beta\mathcal{O}_{\mathcal{K}_{p,a}}$. Without loss of generality assume $\mathfrak{P} \nmid d/a$, otherwise consider the prime in $\mathcal{O}_{\mathcal{K}_{p,d/a}}$ and interchange the roles of a and d/a in the following. Let $\mathfrak{p}$ be a prime in $\mathcal{K}_p$ below $\mathfrak{P}$. Taking norms to $\mathcal{K}_p$ we have $\mathfrak{p} \mid Z^2 d/a$, so $\mathfrak{p} \mid Z$. But $\mathfrak{p}$ cannot divide both X and Y with an odd power, otherwise $\mathfrak{p}$ divides $\gcd((X),(Y),(Z))$ with an odd power, so $\mathfrak{p}\mathcal{O}_{\mathcal{K}_{p,a}}$ cannot divide β with an odd power. Let τ be the generator of $\mathrm{Gal}(\mathcal{K}_{p,a}/\mathcal{K}_p)$. Then $\mathrm{ord}_{\mathfrak{P}} \beta + \mathrm{ord}_{\mathfrak{P}^{\tau}} \beta = \mathrm{ord}_{\mathfrak{P}}(X + Y\sqrt{a}) + \mathrm{ord}_{\mathfrak{P}}(X - Y\sqrt{a}) = \mathrm{ord}_{\mathfrak{P}} Z^2 = 2\,\mathrm{ord}_{\mathfrak{p}} Z$ being even implies that $\mathrm{ord}_{\mathfrak{P}} \beta$ is even. Therefore $\beta\mathcal{O}_{\mathcal{K}_{d,p,a}}$ has even valuation at odd primes.

Choosing β to be a square modulo 4. We now handle the ramification at 2 in cases (5.10), (5.11) and (5.12). First suppose a is odd so $a \equiv 1 \bmod 4$. We assumed $2 \mid Y$ so

$$X + Y\sqrt{a} \equiv X - Y + 2Y\left(\frac{1+\sqrt{a}}{2}\right) \equiv X - Y \bmod 4.$$

Also $(X-Y)^2 = X^2 + 2XY + Y^2 \equiv X^2 \bmod 4$.

In case (5.10), $X - Y \equiv \pm 1$ or $\pm\sqrt{p} \equiv \delta \bmod 4$ for some $\delta \in \{\pm 1, \pm u\}$. In case (5.10), multiplying each of X, Y, Z by δ satisfies the requirement since this forces $X - Y \equiv 1 \bmod 4$, which a square modulo 4.

The cases (5.11) and (5.12) are only possible when $p \equiv 5 \bmod 8$. Suppose we are in case (5.11), then $(X-Y)^2 \equiv \omega \bmod 4$. Then $X - Y \equiv \pm(1+\sqrt{p})/2$ or $\pm(5+\sqrt{p})/2 \bmod 4$. One of $\{\pm(1+\sqrt{p})/2$ or $\pm(5+\sqrt{p})/2\}$ is a square modulo 4, and $u(1+\sqrt{p})/2 \equiv (5+\sqrt{p})/2 \bmod 4$. Therefore there exist $\delta \in \{\pm 1, \pm u\}$ such that $\delta(X-Y)$ is a square modulo 4. Replace X, Y, Z by $\delta X, \delta Y, \delta Z$ then β is a square modulo 4. Case (5.12) is similar.

Now suppose a is even so $a \equiv 2 \bmod 4$. In cases (5.10), (5.11) and (5.12), similar to above there exists $\delta \in \{\pm 1, \pm u\}$ such that $\delta X \equiv X^2 + Y^2/2 \equiv X^2 + aY^2/4$. Then $\delta X + \delta Y\sqrt{a} \equiv (X + Y\sqrt{a}/2)^2 \bmod 4$. □

Recall from Sections 5.2.1.1 and 5.2.1.2 that the space of decompositions of the second type has dimension equal to $t-m$ inside the $\mathbb{F}_2$-vector space $\mathfrak{K}_p^\times/(\mathfrak{K}_p^\times)^2$. Let $a_1, \ldots, a_{t-m-1}, d$ denote a basis for this space, with $a_i \mid d$, and let $\beta_1, \ldots, \beta_{t-m-1}$ denote the corresponding solutions constructed in Lemma 5.8. Then we can realize $\mathscr{H}_{d,p}^+$ as the field

$$\mathscr{H}_{d,p}^+ = \mathscr{C}_{d,p}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_{t-m-1}}),$$

where $\mathscr{C}_{d,p}$ is defined in (5.6).

5.3.2 The case $m = t-2$

Throughout this section, we take $m = t-2$, so that $q_1, \ldots, q_t$ satisfies $\left(\frac{p}{q_1}\right) = \cdots = \left(\frac{p}{q_{t-2}}\right) = 1$ and $\left(\frac{p}{q_{t-1}}\right) = \left(\frac{p}{q_t}\right) = -1$.

Lemma 5.9. *There exists a positive integer $a \mid d$, $a \neq 1$ or d, such that*

$$px^2 - ay^2 = \frac{d}{a}z^2 \tag{5.15}$$

is solvable for $x, y, z \in \mathbb{Q}$. Also

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

Proof. Since $\operatorname{rank} B_0 = t-2$, $\dim\ker B_0 = t-(t-2) = 2$. We can pick $(e_1, \ldots, e_t) \in$

$\ker B_0 \setminus \{\{0,\dots,0\},\{1,\dots,1\}\}$. Take $a = q_1^{e_1}\dots q_t^{e_t}$ and $b = d/a$. Then for each $1 \le i \le t-2$,

$$(a,b)_{q_i} = 1.$$

If d is odd, $a \equiv b \equiv 1 \bmod 4$, so $(a,b)_2 = 1$. Hilbert reciprocity implies

$$(a,b)_{q_{t-1}}(a,b)_{q_t} = \prod_{r\in\mathcal{M}_{\mathbb{Q}}} (a,b)_r = 1. \tag{5.16}$$

When d is even, 2 is one of $q_1,\dots,q_{t-2}$ if $p \equiv 1 \bmod 8$, and one of q_{t-1}, q_t if $p \equiv 5 \bmod 8$, so (5.16) still holds.

Without loss of generality assume $q_{t-1} \mid b$, otherwise interchange a and d/a. Since $\mathrm{rk}_4\,\mathbf{C}_d = 0$ and $\mathrm{rk}_4\,\mathbf{C}_{dp} = 0$, there are no decompositions of second type for $\mathfrak{K}_d$ or $\mathfrak{K}_{dp}$, so

$$(a,b)_{q_{t-1}} = (a,b)_{q_t} = -1 \text{ and } \left((pa,b)_{q_{t-1}} = (pa,b)_{q_t} = -1 \text{ or } (pa,b)_p = -1\right).$$

If $q_t \mid b$, then $(pa,b)_p = \left(\frac{b}{p}\right) = \prod_{q\mid b}\left(\frac{q}{p}\right) = 1$, so we must have $(pa,b)_{q_{t-1}} = (pa,b)_{q_t} = -1$, but this contradicts with

$$(p,b)_{q_{t-1}} = (p,b)_{q_t} = \left(\frac{q_{t-1}}{p}\right) = \left(\frac{q_t}{p}\right) = -1.$$

Therefore $q_t \mid a$. Again a cannot give a decomposition of second type for $\mathfrak{K}_d$, so $(a,b)_{q_{t-1}} = (a,b)_{q_t} = -1$, and hence $(pa,b)_{q_{t-1}} = (pa,b)_{q_t} = 1$. We also have

$$\left(\frac{a}{p}\right) = \prod_{q_i\mid a}\left(\frac{q_i}{p}\right) = -1 \qquad \text{and} \qquad (pa,pb)_p = \left(\frac{ab}{p}\right) = \prod_{q_i\mid d}\left(\frac{q_i}{p}\right) = 1.$$

Therefore $(pa,pb)_r = 1$ for any prime $r \in \mathcal{M}_{\mathbb{Q}}$. □

Since the 2-part of the class group and narrow class group of $\mathfrak{K}_p$ are both trivial, the fundamental unit in $\mathfrak{K}_p$ has norm -1, we can take $u, v \in \mathbb{Z}$ satisfying

$$u^2 - pv^2 = -1. \tag{5.17}$$

Looking at $u^2 - pv^2 \equiv -1 \bmod 4$ we see that u is even and v is odd, so $u + v\sqrt{p} \equiv \pm\sqrt{p} \bmod 4\mathcal{O}_{\mathfrak{K}_p}$. Replacing v with $-v$ if necessary we can assume $v - u \equiv 1 \bmod 4$,

so that $u + v\sqrt{p} \equiv \sqrt{p} \bmod 4\mathcal{O}_{\mathcal{K}_p}$. From $u^2 - pv^2 \equiv -1 \bmod 8$, we see that this choice implies

$$(u, v) \equiv \begin{cases} (0,1) \bmod 4 & \text{if } p \equiv 1 \bmod 8, \\ (2,3) \bmod 4 & \text{if } p \equiv 5 \bmod 8. \end{cases} \tag{5.18}$$

If we take some $\beta = (x\sqrt{p} + y\sqrt{a})(u + v\sqrt{p})$, where x, y satisfy (5.15), then $\mathcal{K}_{d,p,a}(\sqrt{\beta})/\mathcal{K}_{d,p}$ is a C_4-extension by Lemma 1.8.

We claim that when β is chosen appropriately, the $\mathcal{K}_{d,p,a}(\sqrt{\beta})/\mathcal{K}_{d,p}$ is unramified at all finite primes. Note that $\mathcal{K}_{d,p,a}$ is contained in $\mathcal{H}_{d,p}^{+}$ so $\mathcal{K}_{d,p,a}/\mathcal{K}_{d,p}$ is unramified.

Lemma 5.10. *Let $d \in \mathbb{Z}$ be a squarefree and has no prime factors congruent to* $3 \bmod 4$. *Suppose $a \mid d$ and a is even if d is even. Let $p \equiv 1 \bmod 4$ be a prime. Suppose* (5.15) *is solvable for some $x, y, z \in \mathbb{Q}$. There exists $x, y, z \in \mathbb{Z}$ satisfying* (5.15) *such that*

(i) $\gcd(x, y, z) = 1$,

(ii) *x, z are odd and y is even, and*

(iii) $x - y \equiv 1 \bmod 4$.

Setting $\beta = (x\sqrt{p} + y\sqrt{a})(u + v\sqrt{p})$ gives an extension $\mathcal{K}_{d,p,a}(\sqrt{\beta})/\mathcal{K}_{d,p,a}$ that is unramified at all finite primes.

Proof. Our goal is to find a suitable $\beta = X + Y\sqrt{a}$ that satisfies the requirement in Proposition 1.2. Let σ be the generator of $\mathrm{Gal}(\mathcal{K}_p/\mathbb{Q})$. Clearing denominators we can assume $x, y, z \in \mathbb{Z}$.

Choosing β to be coprime to 2. Removing factors of 2 we can assume 2 divides at most one of x, y, z. Taking $px^2 - ay^2 = \frac{d}{a}z^2 \bmod 4$, we see that x must be odd and one of y, z is even. If d is even, $a \equiv 2 \bmod 8$ so y must be even. Now suppose d is odd. If x, y are odd and z is even, then we can take instead

$$\left(\frac{a + d/a}{2}px^2,\ \frac{a - d/a}{2}y + \frac{d}{a}z,\ \frac{a - d/a}{2}z - ay\right) \equiv (1, 0, 1) \bmod 2$$

as another set of solution to (5.15). Therefore we can always take x, z odd and y

even. In particular $\beta\mathcal{O}_{\mathcal{K}_{d,p,a}}$ is coprime to 2 since its norm

$$\operatorname{Norm}_{K/\mathcal{K}_p}\beta = (u+v\sqrt{p})^2\frac{d}{a}z^2$$

is odd.

Choosing β to be a square ideal. We can assume $\gcd(x,y,z)=1$ by removing any common divisors.

Suppose there exists an odd prime dividing $\beta\mathcal{O}_{\mathcal{K}_{d,p,a}}$, then there must be a prime $\mathfrak{P}$ below in $\mathcal{O}_{\mathcal{K}_{p,a}}$ dividing $\beta\mathcal{O}_{\mathcal{K}_{p,a}}$. Without loss of generality assume $\mathfrak{P}\nmid d/a$, otherwise consider the prime in $\mathcal{O}_{\mathcal{K}_{p,d/a}}$ and interchange the roles of a and d/a in the following. Let $\mathfrak{p}$ is a prime in $\mathcal{K}_p$ below $\mathfrak{P}$. Taking norms to $\mathcal{K}_p$ we have $\mathfrak{p}\mid z^2 d/a$, so $\mathfrak{p}\mid z$. But $\mathfrak{p}$ cannot divide both x and y, so $\mathfrak{p}\mathcal{O}_{\mathcal{K}_{p,a}}$ cannot divide β. Then $\operatorname{ord}_{\mathfrak{P}}\beta = \operatorname{ord}_{\mathfrak{P}} z^2 = 2\operatorname{ord}_{\mathfrak{p}} z$ is even. Therefore $\beta\mathcal{O}_{\mathcal{K}_{d,p,a}}$ has even valuation at odd primes.

Choosing β to be a square modulo 4. First suppose a is odd so $a\equiv 1 \bmod 4$. We assumed y is even so

$$\begin{aligned}\beta = (x\sqrt{p}+y\sqrt{a})(u+v\sqrt{p}) &\equiv (x\sqrt{p}+y\sqrt{a})\sqrt{p} \equiv x+y\sqrt{ap}\\ &\equiv x-y+2y\left(\frac{1+\sqrt{ap}}{2}\right) \equiv x-y \bmod 4\mathcal{O}_{\mathcal{K}_{d,p}}.\end{aligned}$$

Since x is odd and y is even, taking $-x$ instead if necessary, we can assume $x-y\equiv 1 \bmod 4$. Then β is a square modulo 4 in $\mathcal{O}_{\mathcal{K}_{d,p}}$.

Now suppose a is even so $a\equiv 2 \bmod 4$. Taking $-x$ instead if necessary, we can assume $x-y^2/2\equiv 1 \bmod 4$. Then

$$\begin{aligned}\beta = (x\sqrt{p}+y\sqrt{a})(u+v\sqrt{p}) &\equiv x+y\sqrt{ap}\\ &\equiv x-y\sqrt{a}+2y\sqrt{a}\left(\frac{1+\sqrt{p}}{2}\right) \equiv \left(1-\frac{y}{2}\sqrt{a}\right)^2 \bmod 4.\end{aligned}$$

Since y is even, $\frac{1}{2}y^2\equiv y \bmod 4$. □

Take (5.15) modulo 8, if d is odd, the choice in Lemma 5.10 implies

$$(x,y)\equiv\begin{cases}(1,0) \bmod 4 & \text{if } bp\equiv 1 \bmod 8,\\ (3,2) \bmod 4 & \text{if } bp\equiv 5 \bmod 8.\end{cases} \tag{5.19}$$

5.3.3 Criterion for $\mathscr{H}_{d,p}^{+}$ to be totally real when $m = t-2$

Lemma 5.11. *The field $\mathcal{K}_{d,p,a}(\sqrt{\beta})$ is totally real if and only if $xv > 0$.*

Proof. Let $\beta_1 = (x\sqrt{p}+y\sqrt{a})(u+v\sqrt{p})$, $\beta_2 = (x\sqrt{p}-y\sqrt{a})(u+v\sqrt{p})$, $\beta_3 = (-x\sqrt{p}+y\sqrt{a})(u-v\sqrt{p})$, and $\beta_4 = (-x\sqrt{p}-y\sqrt{a})(u-v\sqrt{p})$. Then $\beta_1\beta_2 = bz^2(u+v\sqrt{p})^2 > 0$, $\beta_1\beta_3 = bz^2 > 0$, and $\beta_3\beta_4 = bz^2(u-v\sqrt{p})^2 > 0$, so $\beta_1, \beta_2, \beta_3, \beta_4$ are always of the same sign. Since $\beta_1+\beta_2+\beta_3+\beta_4 = 4xvp$, we have $\beta_1, \beta_2, \beta_3, \beta_4 > 0$ if and only if $xv > 0$. □

If d is odd, (5.18) and (5.19) implies

$$xv \equiv \begin{cases} 1 \bmod 4 & \text{if } b \equiv 1 \bmod 8, \\ 3 \bmod 4 & \text{if } b \equiv 5 \bmod 8. \end{cases} \tag{5.20}$$

Lemma 5.12. *The field $\mathcal{K}_{d,p,a}(\sqrt{\beta})$ is totally real if and only if*

$$\left[\frac{ab}{p}\right]_4 \left[\frac{ap}{b}\right]_4 \left[\frac{bp}{a}\right]_4 = -1,$$

where $b = d/a$.

Proof. By Lemma 5.11, it suffices to show that

$$\left[\frac{ab}{p}\right]_4 \left[\frac{ap}{b}\right]_4 \left[\frac{bp}{a}\right]_4 = \begin{cases} -1 & \text{if } xv > 0, \\ 1 & \text{if } xv < 0. \end{cases} \tag{5.21}$$

Without loss of generality, assume b is odd. Take $a = 2^j a_0$, where $j = 0$ if d is odd and $j = 1$ if d is even. Take (5.15) modulo p and modulo each odd $q \mid d$, we get

$$\begin{aligned} \left[\frac{-ab}{p}\right]_4 \left(\frac{y}{p}\right) &= \left(\frac{bz}{p}\right) = -\left(\frac{z}{p}\right), \\ \left[\frac{ap}{b}\right]_4 \left(\frac{y}{b}\right) &= \left(\frac{px}{b}\right) = -\left(\frac{x}{b}\right), \\ \left[\frac{bp}{a_0}\right]_4 \left(\frac{z}{a_0}\right) &= \left(\frac{px}{a_0}\right) = -\left(\frac{x}{a_0}\right). \end{aligned}$$

Multiply these equations together

$$-\left[\frac{-ab}{p}\right]_4 \left[\frac{ap}{b}\right]_4 \left[\frac{bp}{a_0}\right]_4 = \left(\frac{x}{a_0 b}\right)\left(\frac{y}{bp}\right)\left(\frac{z}{a_0 p}\right). \tag{5.22}$$

Write $y = 2^i y_0$, where y_0 is odd. Since $a_0 \equiv b \equiv p \equiv 1 \bmod 4$, we can rewrite (5.22) as

$$-\left[\frac{-ab}{p}\right]_4\left[\frac{ap}{b}\right]_4\left[\frac{bp}{a}\right]_4 = \left(\frac{a_0 b}{|x|}\right)\left(\frac{2}{bp}\right)^i\left(\frac{bp}{y_0}\right)\left(\frac{a_0 p}{z}\right). \tag{5.23}$$

Take (5.15) modulo each prime $r \mid x$, $r \mid y_0$, $r \mid z$, we get

$$\left(\frac{a}{|x|}\right) = \left(\frac{-b}{|x|}\right) = \left(\frac{-1}{|x|}\right)\left(\frac{b}{|x|}\right), \qquad \left(\frac{p}{y_0}\right) = \left(\frac{b}{y_0}\right) \qquad \text{and} \qquad \left(\frac{p}{z}\right) = \left(\frac{a}{z}\right).$$

By (5.19), $i = 1$ and $\left(\frac{2}{bp}\right) = -1$ if $bp \equiv 5 \bmod 8$ and $\left(\frac{2}{bp}\right) = 1$ if $bp \equiv 1 \bmod 8$. Simplifying (5.23) gives

$$-\left[\frac{-ab}{p}\right]_4\left[\frac{ap}{b}\right]_4\left[\frac{bp}{a_0}\right]_4 = \left(\frac{-1}{|x|}\right)\left(\frac{2}{bp}\right)^i\left(\frac{2}{xz}\right)^j$$
$$= (-1)^{\frac{|x|-1}{2}}(-1)^{\frac{p-1}{4}+\frac{b-1}{4}}\left(\frac{2}{xz}\right)^j.$$

Take (5.17) modulo each prime $r \mid v$, we have $\left(\frac{-1}{|v|}\right) = 1$, so $|v| \equiv 1 \bmod 4$. Since

$$\left[\frac{-1}{p}\right]_4 = (-1)^{\frac{p-1}{4}},$$

we have

$$\left[\frac{ab}{p}\right]_4\left[\frac{ap}{b}\right]_4\left[\frac{bp}{a_0}\right]_4 = -(-1)^{\frac{|xv|-1}{2}}(-1)^{\frac{b-1}{4}}\left(\frac{2}{xz}\right)^j. \tag{5.24}$$

When d is odd, $j = 0$, so we get (5.21) by (5.20). When d is even, $j = 1$ and a is even. Take (5.15) modulo 16 gives $px^2 \equiv bz^2 \bmod 16$ if $y \equiv 0 \bmod 4$, and $px^2 \equiv 8 + bz^2 \bmod 16$ if $y \equiv 2 \bmod 4$. Then

$$\left(\frac{2}{xz}\right) = (-1)^{\frac{(xz)^2-1}{8}} = \begin{cases} 1 & \text{if } x^2 \equiv z^2 \bmod 16, \\ -1 & \text{if } x^2 \equiv 9z^2 \bmod 16 \end{cases} = (-1)^{\frac{y}{2}}\left[\frac{pb}{2}\right]_4.$$

From (5.24) and since $p \equiv b \bmod 8$ here, we have

$$\left[\frac{ab}{p}\right]_4\left[\frac{ap}{b}\right]_4\left[\frac{bp}{a}\right]_4 = -(-1)^{\frac{|xv|+y-1}{2}}(-1)^{\frac{p-1}{4}}.$$

The choice $x - y \equiv 1 \bmod 4$ in Lemma 5.10, together with (5.18), implies $(-1)^{\frac{xv+y-1}{2}} = (-1)^{\frac{p-1}{4}}$. Therefore (5.21) holds. □

5.4 Computing densities from a governing field

Recall that we proved the cases $m = t - 1$ and the upper bound in the second half of Theorem 5.3 at the end of Section 5.1. It remains to prove the case $m = t - 2$ of Theorem 5.3.

5.4.1 Construction of a governing field

We start by converting the criterion in Lemma 5.12 to a splitting condition in a suitable governing field. If p is a prime number congruent to 1 modulo 4, then we can write $p = \pi\overline{\pi}$ for some $\pi \equiv 1 \bmod (1+\sqrt{-1})^3$ in $\mathbb{Z}[\sqrt{-1}]$; in this case, the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$ induces an isomorphism $\mathbb{Z}/(p) \cong \mathcal{O}_{\mathbb{Q}(\sqrt{-1})}/(\pi)$, so that an integer n is a fourth power modulo p exactly when it is a fourth power modulo π. For each $1 \leq i \leq t$, fix ρ_i such that $q_i = \rho_i\overline{\rho_i}$ with $\rho_i \equiv 1 \bmod (1+i)^3$ if $q_i \equiv 1 \bmod 4$, and take $\rho_i = 1 + \sqrt{-1}$ if $q_i = 2$.

Assuming $d = ab$ is odd for now, we have

$$\begin{aligned}\left[\frac{d}{p}\right]_4\left[\frac{bp}{a}\right]_4\left[\frac{ap}{b}\right]_4 &= \left[\frac{d}{p}\right]_4 \cdot \prod_{q_i|a}\left[\frac{bp}{q_i}\right]_4 \cdot \prod_{q_j|b}\left[\frac{ap}{q_j}\right]_4 \\ &= \left(\frac{d}{\pi}\right)_4 \prod_{\rho_i|a}\left(\frac{bp}{\rho_i}\right)_4 \cdot \prod_{\rho_j|b}\left(\frac{ap}{\rho_j}\right)_4 = \delta(a,b) \cdot \left(\frac{d}{\pi}\right)_4 \cdot \prod_{\rho_k|d}\left(\frac{p}{\rho_k}\right)_4,\end{aligned}$$

where

$$\delta(a,b) \coloneqq \prod_{\rho_i|a}\left(\frac{b}{\rho_i}\right)_4 \cdot \prod_{\rho_j|b}\left(\frac{a}{\rho_j}\right)_4.$$

Using quartic reciprocity as well as the fact that

$$\left(\frac{\rho_k}{\overline{\pi}}\right)_4 = \overline{\left(\frac{\overline{\rho_k}}{\pi}\right)_4} = \left(\frac{\overline{\rho_k}}{\pi}\right)_4^3,$$

we have

$$\left(\frac{d}{\pi}\right)_4 \prod_{\rho_k|d}\left(\frac{p}{\rho_k}\right)_4 = \left(\frac{d}{\pi}\right)_4 \prod_{\rho_k|d}\left(\frac{\rho_k}{\pi}\right)_4\left(\frac{\overline{\rho_k}}{\pi}\right)_4^3 = \left(\frac{d}{\pi}\right)_2 \prod_{\rho_k|d}\left(\frac{\overline{\rho_k}}{\pi}\right)_2 = \prod_{\rho_k|d}\left(\frac{\rho_k}{\pi}\right)_2.$$

Now suppose a is even, write $a = 2a_0$. Define

$$\delta(a,b) = \delta(a_0,b) \cdot (-1)^{\frac{1-b}{8}} \cdot \prod_{\rho_j|b}\left(\frac{2}{\rho_j}\right)_4.$$

Since $2 = -\rho_i^2\sqrt{-1}$, we have

$$\left[\frac{d}{p}\right]_4\left[\frac{bp}{a}\right]_4\left[\frac{ap}{b}\right]_4 = \left(\frac{2}{\pi}\right)_4\left[\frac{bp}{2}\right]_4\left(\frac{a_0 b}{\pi}\right)_4\prod_{\rho_k|a_0 b}\left(\frac{p}{\rho_k}\right)_4\cdot\prod_{\rho_i|a_0}\left(\frac{b}{\rho_i}\right)_4\cdot\prod_{\rho_j|b}\left(\frac{2a_0}{\rho_j}\right)_4$$
$$= \delta(a,b)\cdot(-1)^{\frac{b-1}{8}}\left(\frac{-\sqrt{-1}}{\pi}\right)_4\left[\frac{bp}{2}\right]_4\cdot\prod_{\rho_k|d}\left(\frac{\rho_k}{\pi}\right)_2$$

Note that the assumption that a is even and $(ap, bp)_2 = 1$ implies $p \equiv b \bmod 8$. Consider the possible classes of π in $\mathbb{Z}[\sqrt{-1}]/8\mathbb{Z}[\sqrt{-1}]$ as in the proof of [31, Proposition 7], which are

$$\begin{cases} 1,\ 1+4i & \text{if } p \equiv 1 \bmod 16, \\ 7+6i,\ 7+2i & \text{if } p \equiv 5 \bmod 16, \\ 5,\ 5+4i & \text{if } p \equiv 9 \bmod 16, \\ 3+6i,\ 3+2i & \text{if } p \equiv 13 \bmod 16. \end{cases}$$

Then

$$\left(\frac{-\sqrt{-1}}{\pi}\right)_4 = (-1)^{\frac{1-p}{8}} \qquad \text{and} \qquad \left[\frac{bp}{2}\right]_4 = (-1)^{\frac{p-b}{8}}$$

Therefore $(-1)^{\frac{b-1}{8}}\left(\frac{-\sqrt{-1}}{\pi}\right)_4\left[\frac{bp}{2}\right]_4 = 1$.

In either case we have

$$\left[\frac{d}{p}\right]_4\left[\frac{bp}{a}\right]_4\left[\frac{ap}{b}\right]_4 = \delta(a,b)\cdot\prod_{\rho_k|d}\left(\frac{\rho_k}{\pi}\right)_2.$$

We let

$$\mathcal{M}_4(d) = \mathcal{K}_{-1,d}(\sqrt{\rho_1\cdots\rho_t}). \tag{5.25}$$

Then

$$\left[\frac{d}{p}\right]_4\left[\frac{bp}{a}\right]_4\left[\frac{ap}{b}\right]_4 = \delta(a,b)$$

if and only if π splits in $\mathcal{M}_4(d)/\mathcal{K}_{-1}$, if and only if p splits completely in $\mathcal{M}_4(d)/\mathbb{Q}$.

5.4.2 Computation of densities

Recall that $d = q_1\cdots q_t$ with $q_i \not\equiv 3 \bmod 4$ distinct primes, that $\mathrm{rk}_2\,\mathbf{Cl}_d = \mathrm{rk}_2\,\mathbf{C}_d$, that $\mathrm{rk}_4\,\mathbf{C}_d = 0$, and that $\mathcal{P}_{d,t-2}$ is the set of prime numbers p such that

(i) $p \equiv 1 \bmod 4$,

(ii) $p \nmid d$,

(iii) $\mathrm{rk}_4\, \mathbf{C}_{dp} = 0$, and

(iv) there are exactly $t-2$ indices $i \in \{1, \dots, t\}$ such that $\left(\frac{q_i}{p}\right) = 1$.

For each subset $\Omega \subset \{1, \dots, t\}$ of cardinality $t-2$, let $\mathcal{P}_{d,t-2,\Omega}$ denote the set of $p \in \mathcal{P}_{d,t-2}$ such that $\left(\frac{q_i}{p}\right) = 1$ if and only if $i \in \Omega$. Hence

$$\mathcal{P}_{d,t-2} = \bigcup_{\substack{\Omega \subset \{1,\dots,t\} \\ |\Omega| = t-2}} \mathcal{P}_{d,t-2,\Omega}.$$

If Ω_1 and Ω_2 are two distinct subsets of $\{1, \dots, t\}$ of cardinality $t-2$, then there exists $i \in \Omega_1 \setminus \Omega_2$, and so every prime $p \in \Omega_2$ satisfies $\left(\frac{q_i}{p}\right) = -1$, which means that $p \notin \Omega_1$. Hence the union above is disjoint, and so, to prove Theorem 5.3, it suffices to prove for each Ω that the map

$$\mathcal{P}_{d,t-2,\Omega} \to \{1, 2\}, \qquad p \mapsto Q(\mathfrak{K}_{d,p})$$

is Frobenian, with governing field $\mathcal{M}_\Omega$, say, and that

$$\lim_{N \to \infty} \frac{\#\{p \in \mathcal{P}_{d,m,\Omega} :\ p \le N,\ Q(\mathfrak{K}_{d,p}) = 2\}}{\#\{p \in \mathcal{P}_{d,m,\Omega} :\ p \le N\}} = \frac{1}{2^{t-1}},$$

whenever $\mathcal{P}_{d,t-2,\Omega}$ is non-empty. Then one can take the compositum $\mathcal{M} = \prod_\Omega \mathcal{M}_\Omega$ as a governing field for the map $\mathcal{P}_{d,t-2} \to \{1, 2\}$ given by $p \mapsto Q(\mathfrak{K}_{d,p})$. If $\mathcal{P}_{d,t-2,\Omega}$ is the empty set, then we may take $\mathcal{M}_\Omega = \mathbb{Q}$. Otherwise, by re-numbering the indices, we may assume without loss of generality that $\Omega = \{1, \dots, t-2\}$.

First, if $p \in \mathcal{P}_{d,t-2,\Omega}$, then $\left(\frac{q_{t-1}}{p}\right) = \left(\frac{q_t}{p}\right) = -1$, so p splits completely in

$$\mathfrak{C} = \mathfrak{K}_{-1,q_1,\dots,q_{t-2},q_{t-1}q_t}.$$

Conversely, any prime p that splits completely in $\mathfrak{C}$ but not in

$$\mathfrak{L} = \mathfrak{C}\mathfrak{K}_{q_t} = \mathfrak{K}_{-1,q_1,\dots,q_t}$$

belongs to $\mathcal{P}_{d,t-2,\Omega}$. Hence, letting σ denote the element in $\mathrm{Gal}(L/\mathbb{Q})$ that fixes $\sqrt{-1}$ and $\sqrt{q_i}$ for $1 \le i \le t-2$ and that sends $\sqrt{q_i}$ to $-\sqrt{q_i}$ for $i = t-1,\ t$ (i.e., σ is the

$$\begin{array}{c} \mathscr{M} = \mathfrak{K}_{-1,q_1,\ldots,q_t}(\sqrt{\rho_1},\ldots,\sqrt{\rho_{t-2}},\sqrt{\rho_1\cdots\rho_t}) \\ | \\ \mathscr{L} = \mathfrak{K}_{-1,q_1,\ldots,q_t} \\ | \\ \mathscr{E} = \mathfrak{K}_{-1,q_1,\ldots,q_{t-2},q_{t-1}q_t} \\ | \\ \mathbb{Q} \end{array}$$

Figure 5.1: Field diagram of the fields $\mathscr{E} \subset \mathscr{L} \subset \mathscr{M}$.

non-trivial element of $\mathrm{Gal}(\mathscr{L}/\mathscr{E})$), we see that $p \in \mathcal{P}_{d,t-2,\Omega}$ if and only if $\left(\frac{\mathscr{L}/\mathbb{Q}}{p}\right) = \sigma$.

Next, note that Lemma 5.9 yields the same decomposition a, $b = d/a$ for $\mathfrak{K}_{d,p_1}$ and $\mathfrak{K}_{d,p_2}$ for any two primes $p_1, p_2 \in \mathcal{P}_{d,t-2,\Omega}$. Also note that $\mathfrak{K}_{-1,d} \subset \mathscr{E}$, so, for primes p that split completely in $\mathscr{E}$, the final result of the previous section can be restated as

$$\left[\frac{d}{p}\right]_4 \left[\frac{bp}{a}\right]_4 \left[\frac{ap}{b}\right]_4 = \delta(a,b) \iff p \text{ splits completely in } \mathscr{E}\mathscr{M}_4(d)/\mathbb{Q}, \tag{5.26}$$

where $\mathscr{M}_4(d)$ is as in (5.25). Hence, by Lemma 5.12 and the result of the previous section, a prime p is in $\mathcal{P}_{d,t-2,\Omega}$ and $\mathscr{H}^+_{d,p}$ is totally real if and only if

(i) $\left(\frac{\mathscr{L}/\mathbb{Q}}{p}\right) = \sigma$,

(ii) p splits completely in $\mathscr{E}\mathscr{M}_2(d)/\mathbb{Q}$, where $\mathscr{M}_2(d)$ is as in (5.8), and

(iii) identifying $\mathrm{Gal}(\mathscr{E}\mathscr{M}_4(d)/\mathscr{E})$ with the group $\{\pm 1\}$, and viewing $\mathrm{Gal}(\mathscr{E}\mathscr{M}_4(d)/\mathscr{E})$ as a subgroup of $\mathrm{Gal}(\mathscr{E}\mathscr{M}_4(d)/\mathbb{Q})$ in the canonical way, $\left(\frac{\mathscr{E}\mathscr{M}_4(d)/\mathbb{Q}}{p}\right) = -\delta(a,b)$.

Define $\mathscr{M}$ to be the compositum

$$\mathscr{M} = \mathscr{L}\mathscr{M}_2(d)\mathscr{M}_4(d) = \mathfrak{K}_{-1,q_1,\ldots,q_t}(\sqrt{\rho_1},\ldots,\sqrt{\rho_{t-2}},\sqrt{\rho_1\cdots\rho_t}),$$

and observe that there is a unique element $\tau(a,b) \in \mathrm{Gal}(\mathscr{M}/\mathscr{E}) \subset \mathrm{Gal}(\mathscr{M}/\mathbb{Q})$ depending on a and b such that for every prime p, the three conditions listed above are equivalent to the condition that $\left(\frac{\mathscr{M}/\mathscr{E}}{\mathfrak{p}}\right) = \tau(a,b)$, where $\mathfrak{p}$ is any prime of $\mathscr{E}$ lying above p. Note also that $\mathrm{Gal}(\mathscr{M}/\mathscr{E}) \cong C_2^t$. Applying the Chebotarev Density

Theorem to $\mathscr{M}/\mathscr{E}$ and $\mathscr{L}/\mathscr{E}$, we get

$$\begin{aligned}
&\lim_{N\to\infty} \frac{\#\{p \in \mathcal{P}_{d,t-2,\Omega} :\ p \le N,\ Q(\mathfrak{K}_{d,p}) = 2\}}{\#\{p \in \mathcal{P}_{d,t-2,\Omega} :\ p \le N\}} \\
&\quad = \lim_{N\to\infty} \frac{\#\{p \in \mathcal{P}_{d,t-2,\Omega} :\ p \le N,\ \mathfrak{K}^+_{d,p} \text{ is totally real}\}}{\#\{p \in \mathcal{P}_{d,t-2,\Omega} :\ p \le N\}} \\
&\quad = \lim_{N\to\infty} \frac{\#\{\mathfrak{p} \text{ prime in } \mathcal{O}_{\mathscr{E}} :\ \mathrm{Norm}(\mathfrak{p}) \le N,\ \left(\frac{\mathscr{M}/\mathscr{E}}{\mathfrak{p}}\right) = \tau(a,b)\}}{\#\{\mathfrak{p} \text{ prime in } \mathcal{O}_{\mathscr{E}} :\ \mathrm{Norm}(\mathfrak{p}) \le N,\ \left(\frac{\mathscr{L}/\mathscr{E}}{\mathfrak{p}}\right) = \sigma\}} \\
&\quad = \frac{2^{-t}}{2^{-1}} = 2^{-t+1},
\end{aligned}$$

as desired.

Chapter 6

A density of ramified primes

This chapter is based on joint work with Christine McMeekin and Djordjo Milovic in [20].

Given a number field K, let $\mathbf{Cl}$, and $\mathbf{C}$ denote its class group, and its narrow class group, respectively. We will prove certain density theorems for number fields K satisfying the following five properties:

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, and $\mathbf{C} = \mathbf{Cl}$;

(P2) the class number $h \coloneqq \#\,\mathbf{Cl}$ of K is odd;

(P3) $n \coloneqq [K : \mathbb{Q}]$ is odd;

(P4) $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic; and

(P5) the prime 2 is inert in $K/\mathbb{Q}$.

If K is totally real, then $\mathbf{C} = \mathbf{Cl}$ if and only if every totally positive unit in $\mathcal{O}_K$ is a square; see [20, Lemma 2.1]. Let $\mathcal{O}_{K,+}^{\times} \coloneqq \{u \in \mathcal{O}_K^{\times} : u \text{ totally positive}\}$. Then property (P1) can be restated as

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, and $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$.

Number fields satisfying properties (P1) and (P4) were studied by Friedlander, Iwaniec, Mazur, and Rubin [33]. They studied the behaviour of a quadratic residue symbol defined on odd principal prime ideals

$$\mathrm{spin}(\pi\mathcal{O}_K, \sigma) \coloneqq \left(\frac{\pi}{\pi^{\sigma}\mathcal{O}_K}\right),$$

where π is totally positive. When π and π^σ are not coprime, the symbol is 0 by convention. They proved that if σ is a fixed generator of $\mathrm{Gal}(K/\mathbb{Q})$, the density of principal prime ideals $\pi\mathcal{O}_K$ such that $\mathrm{spin}(\pi\mathcal{O}_K, \sigma) = 1$ is equal to $1/2$, conditional to the following conjecture.

Conjecture C_η ([33, Conjecture C_n, p. 738-739])**.** *Let η be a real number satisfying $0 < \eta \leq 1$. Then there exists a real number $\delta = \delta(\eta) > 0$ such that for all $\epsilon > 0$ there exists a real number $C = C(\eta, \epsilon) > 0$ such that for all integers $Q \geq 3$, all real non-principal characters χ of conductor $q \leq Q$, all integers $N \leq Q^\eta$, and all integers M, we have*

$$\left| \sum_{M < a \leq M+N} \chi(a) \right| \leq CQ^{\eta(1-\delta)+\epsilon}.$$

We note that Conjecture C_η is known for $\eta > 1/4$, as a consequence of the classical Burgess's inequality [14], and remains open for $\eta \leq 1/4$. Moreover, for sums as above starting at $M = 0$, Conjecture C_η (for any η) is a consequence of the Generalised Riemann Hypothesis for the L-function $L(s, \chi)$.

More precisely, the main result in [33] can be stated as follows.

Theorem 6.1 ([33, Theorem 1.1])**.** *Suppose K is a number field satisfying properties (P1) and (P4). Suppose $n = [K : \mathbb{Q}] \geq 3$. Assume Conjecture C_η holds for $\eta = 1/n$ with $\delta = \delta(\eta) > 0$. Let σ be a generator of the Galois group* $\mathrm{Gal}(K/\mathbb{Q})$*. Then for all $x > 3$, we have*

$$\left| \sum_{\substack{\mathfrak{p} \text{ principal} \\ \mathrm{Norm}(\mathfrak{p}) \leq x}} \mathrm{spin}(\mathfrak{p}, \sigma) \right| \ll_{\epsilon, K} x^{1-\theta+\epsilon}$$

where $\theta = \theta(n) = \frac{\delta}{2n(12n+1)}$.

An analogous result when the summation is further restricted those $\mathfrak{p}$ satisfying a suitable congruence condition was also proved in [33]. Also, by Burgess's inequality, Conjecture C_η holds for $\eta = 1/3$ with $\delta = \frac{1}{48}$, so Theorem 6.1 holds unconditionally for $[K : \mathbb{Q}] = 3$ where $\theta = \frac{1}{10656}$.

In [33, Section 11], Friedlander et al. pose some questions about the joint distribution of $\mathrm{spin}(\mathfrak{p}, \sigma)$ and $\mathrm{spin}(\mathfrak{p}, \tau)$ as $\mathfrak{p}$ varies over prime ideals, where σ and τ are two distinct generators of the cyclic group $\mathrm{Gal}(K/\mathbb{Q})$. In [47], Koymans and Milovic

prove that such spins are distributed independently if $n \geq 5$, i.e., that the product $\text{spin}(\mathfrak{p}, \sigma)\,\text{spin}(\mathfrak{p}, \tau)$ oscillates similarly as in Theorem 6.1. In fact, they prove that the product of spins

$$\prod_{\sigma \in H} \text{spin}(\mathfrak{p}, \sigma)$$

oscillates as long as the fixed non-empty subset H of $\text{Gal}(K/\mathbb{Q})$ satisfies the property that $\sigma \notin H$ whenever $\sigma^{-1} \in H$. Moreover, their result holds for number fields K satisfying property (P1) and having arbitrary Galois groups, i.e., not necessarily satisfying property (P4).

The assumption in [47] that $\sigma \notin H$ whenever $\sigma^{-1} \in H$ is made because $\text{spin}(\mathfrak{p}, \sigma)$ and $\text{spin}(\mathfrak{p}, \sigma^{-1})$ are not independent in the following sense.

Proposition 6.2 ([33, Lemma 11.1])**.** *Suppose K is a number field satisfying properties (P1) and (P4). Suppose $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal and $\sigma \in \text{Gal}(K/\mathbb{Q})$ is an automorphism such that $\mathfrak{p}$ and $\mathfrak{p}^\sigma$ are coprime. Then*

$$\text{spin}(\mathfrak{p}, \sigma)\,\text{spin}(\mathfrak{p}, \sigma^{-1}) = \prod_{v|2} (\alpha, \alpha^\sigma)_v,$$

where α is a totally positive generator of $\mathfrak{p}^h$ and the product is taken over places v dividing 2.

Proof. Since α and α^σ are relatively prime, $(\alpha, \alpha^\sigma)_\mathfrak{p} = \text{spin}(\mathfrak{p}, \sigma^{-1})$ and $(\alpha, \alpha^\sigma)_{\mathfrak{p}^\sigma} = \text{spin}(\mathfrak{p}, \sigma)$. By Hilbert reciprocity $\prod_v (\alpha, \alpha^\sigma)_v = 1$. Since α is totally positive, $(\alpha, \alpha^\sigma)_v = 1$ for all infinite places v. For any odd prime $v \neq \mathfrak{p}$ or $\mathfrak{p}^\sigma$, we have $(\alpha, \alpha^\sigma)_v = 1$ by Lemma 1.4. □

In this chapter, we study the joint distribution of multiple spins $\text{spin}(\mathfrak{p}, \sigma)$, $\sigma \in H$, in a setting where $H = \text{Gal}(K/\mathbb{Q}) \setminus \{1\}$, so there are in fact many $\sigma \in H$ such that $\sigma^{-1} \in H$ as well.

By assuming property (P2), we are now also able to study the spin of *all* odd prime ideals, and not only those that are principal. We give the following definition of *spin*, which extends the definition of spin from [33] in a natural way.

Definition 6.3. *Suppose K is a number field satisfying properties (P1) and (P2). Let $\sigma \in \text{Gal}(K/\mathbb{Q})$ be non-trivial. Given an odd ideal $\mathfrak{a}$, we define the spin of $\mathfrak{a}$ (with*

respect to σ) to be

$$\operatorname{spin}(\mathfrak{a}, \sigma) \coloneqq \left(\frac{\alpha}{\mathfrak{a}^\sigma}\right),$$

where α is any totally positive generator of the principal ideal $\mathfrak{a}^h$, and where $\left(\frac{\cdot}{\cdot}\right)$ denotes the quadratic residue symbol in K.

The assumption $\mathcal{O}_{K,+}^\times = \left(\mathcal{O}_K^\times\right)^2$ is important for two reasons. First, $\mathbf{Cl} = \mathbf{C}$ ensures that the principal ideal $\mathfrak{a}^h$ has a generator α that is totally positive. Second, any two totally positive generators of $\mathfrak{a}^h$ differ by a square, so the value of the quadratic residue symbol defining the spin does not depend on the choice of totally positive generator α.

Suppose $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ and α is any totally positive generator of the principal ideal $\mathfrak{p}^h$. It is immediate from the definition of spin, that $\mathfrak{p}$ splits in $K(\sqrt{\alpha^{\sigma^{-1}}})/K$ if and only if $\operatorname{spin}(\mathfrak{p}, \sigma) = 1$. Therefore, for any prime $\mathfrak{p}$ in K coprime to 2, the following are equivalent:

(i) $\operatorname{spin}(\mathfrak{p}, \sigma) = 1$ for all non-trivial $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$, and

(ii) $\mathfrak{p}$ splits completely in $K(\sqrt{\alpha^\sigma} : \sigma \in H)/K$, where $H = \operatorname{Gal}(K/\mathbb{Q}) \setminus \{1\}$.

Let $\mathcal{P}_{\mathbb{Q}}^2$ denote the set of rational primes coprime to 2. For a fixed sign, $\pm$, we define the following sets of rational primes.

$$\begin{aligned} S &\coloneqq \{p \in \mathcal{P}_{\mathbb{Q}}^2 : p \text{ splits completely in } K/\mathbb{Q}\}, \\ S_\pm &\coloneqq \{p \in S : p \equiv \pm 1 \bmod 4\mathbb{Z}\}, \\ F &\coloneqq \{p \in S : \operatorname{spin}(\mathfrak{p}, \sigma) = 1 \text{ for all } \sigma \in \operatorname{Gal}(K/\mathbb{Q}) \setminus \{1\}\}, \\ F_\pm &\coloneqq S_\pm \cap F, \end{aligned}$$

where $\mathfrak{p}$ denotes a prime ideal in K lying above p.

For sets of primes $A \subseteq B$, we define the restricted density of A (restricted to B) to be

$$d(A|B) \coloneqq \lim_{N\to\infty} \frac{\#\{p \in A : \operatorname{Norm}(p) < N\}}{\#\{p \in B : \operatorname{Norm}(p) < N\}}.$$

When Π consists of all but finitely many primes, then $d(A) \coloneqq d(A|\Pi)$ is the usual natural density of A.

Our main result is as follows.

Theorem 6.4. *Let K be a cyclic totally real number field of odd degree n over $\mathbb{Q}$ with odd class number, such that every totally positive unit is the square of a unit, and such that 2 is inert in $K/\mathbb{Q}$. Assume Conjecture C_η holds for $\eta = \frac{2}{n(n-1)}$. For $k \neq 1$ dividing n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Then for a fixed sign $\pm$,*

$$d(F_\pm|S_\pm) = \frac{s_\pm}{2^{3(n-1)/2}}, \quad \text{and} \quad d(F|S) = \frac{s_+ + s_-}{2^{(3n-1)/2}}$$

where

$$s_+ \coloneqq 1 + \prod_{\substack{k|n,\ k\neq 1 \\ d_k\, odd}} 2^{\frac{\phi(k)}{2d_k}} \left(\prod_{\substack{k|n,\ k\neq 1 \\ d_k\, odd}} 2^{\frac{\phi(k)}{2}} - 1 \right),$$

and

$$s_- \coloneqq \prod_{\substack{k|n,\ k\neq 1 \\ d_k\, even}} (2^{\frac{d_k}{2}} + 1)^{\frac{\phi(k)}{d_k}} \prod_{\substack{k|n,\ k\neq 1 \\ d_k\, odd}} (2^{d_k} - 1)^{\frac{\phi(k)}{2d_k}},$$

where ϕ denotes the Euler's totient function.

Unlike in [47], we have assumed here that $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic.

In particular, when n is prime, writing $d = d_n$, we have

$$(s_+, s_-) = \begin{cases} \left(1 + 2^{\frac{n-1}{2d}}(2^{\frac{n-1}{2}} - 1),\ (2^d - 1)^{\frac{n-1}{2d}}\right) & \text{if } d \text{ is odd,} \\ \left(1,\ (2^{\frac{d}{2}} + 1)^{\frac{n-1}{d}}\right) & \text{if } d \text{ is even.} \end{cases}$$

Table 6.1: Densities from Theorem 6.4, computed for K of degree n satisfying the necessary hypotheses.

n	$d(F_+\|S_+)$	$d(F_-\|S_-)$	$d(F\|S)$
3	1/8	3/8	1/4
5	1/64	5/64	3/64
7	15/512	7/512	11/512
9	1/4096	27/4096	7/2048
11	1/32768	33/32768	17/32768
13	1/262144	65/262144	33/262144
15	1/2097152	375/2097152	47/262144

In the cubic case, we have the following unconditional theorem.

Theorem 6.5. *Let $K/\mathbb{Q}$ be a cubic cyclic number field and odd class number in which 2 is inert. Then*

$$d(F|S) = \frac{1}{4},$$

$$d(F_+|S_+) = \frac{1}{8}, \quad \textit{and} \quad d(F_-|S_-) = \frac{3}{8}.$$

If the spins of a fixed prime ideal $\mathrm{spin}(\mathfrak{p}, \sigma)$ and $\mathrm{spin}(\mathfrak{p}, \tau)$ were independent for all non-trivial $\sigma \neq \tau \in \mathrm{Gal}(K/\mathbb{Q})$, then one might expect the density of F restricted to S to be $2^{-(n-1)}$. However, Proposition 6.2 gives a relation between the spins of a prime ideal, which poses new challenges in our setting compared to that in [33] or [47].

Define

$$R \coloneqq \{p \in S : \mathrm{spin}(\mathfrak{p}, \sigma)\,\mathrm{spin}(\mathfrak{p}, \sigma^{-1}) = 1 \text{ for all } \sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})\},$$

where $\mathfrak{p}$ is a fixed prime of K above p. Observe that $F \subseteq R \subseteq S$, so if the limits exist then

$$d(F|S) = d(F|R)d(R|S).$$

It follows from (6.2), that R is the set of primes satisfying a certain Hilbert symbol condition. The densities appearing in our main theorems are of greater complexity than those appearing in [33] or [47] because of the necessary consideration of the density $d(R|S)$. Toward computing the density $d(R|S)$, the terms $s_\pm$ arise from counting the number of solutions to this Hilbert symbol condition over $(\mathcal{O}_K/4\mathcal{O}_K)^\times/((\mathcal{O}_K/4\mathcal{O}_K)^\times)^2$, through a combinatorial argument given in Section 6.2. The argument relies on properties (P4) and (P5), and allows us to obtain explicit density formulas.

Another issue that we had to resolve arises from our generalisation of "spin" to non-principal ideals. This extended definition means that techniques in the study of oscillation of spins in [33] and [47] do not easily carry over. We describe some of the new ideas in Section 6.3 in order to evaluate $d(F|R)$ using results from [47].

Property (P3) ensures that $\mathrm{Gal}(K/\mathbb{Q})$ contains no involutions. While methods to deal with involutions do exist (see [33, Section 12, p. 745]), incorporating them into our arguments is non-trivial and may pose interesting new challenges in our

analytic arguments.

6.1 A consequence of Chebotarev density theorem

In this section, we use Chebotarev density theorem to prove that the primes of K are equidistributed in

$$\mathbf{M}_4 \coloneqq (\mathcal{O}_K/4\mathcal{O}_K)^\times / \left((\mathcal{O}_K/4\mathcal{O}_K)^\times\right)^2,$$

under the map

$$\mathbf{r}_4 : \mathcal{P}_K^2 \to \mathbf{M}_4 \qquad \mathfrak{p} \mapsto [\alpha],$$

where $\alpha \in \mathcal{O}_K$ is a totally positive generator of the principal ideal $\mathfrak{p}^h$. Since squares are trivial in $\mathbf{M}_4$ by definition and $\mathcal{O}_{K,+}^\times = \left(\mathcal{O}_K^\times\right)^2$, the map $\mathbf{r}_q$ is well-defined. Note that $\mathbf{M}_4$ is a group with a natural action from $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathbf{r}_4$ commutes with the Galois action, i.e. $\mathbf{r}_4(\mathfrak{p}^\sigma) = \mathbf{r}_4(\mathfrak{p})^\sigma$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Proposition 6.6. *Suppose K satisfies properties (P3),(P4) and (P5). Then*

(i) $\mathbf{M}_4 \cong \mathbb{F}_2^n$ *as a* $\mathbb{F}_2$*-vector space,*

(ii) the invariants of the action of $\mathrm{Gal}(K/\mathbb{Q})$ *on* $\mathbf{M}_4$ *are exactly* ± 1.

Proof. Let $U_m \coloneqq (\mathcal{O}_K/m)^\times$.

(i) Fix a set of representatives $\mathcal{R}$ for $\mathcal{O}_K/2$ in $\mathcal{O}_K$. Let $\mathcal{R}^\times$ be a subset of $\mathcal{R}$ containing representatives for $(\mathcal{O}_K/2)^\times$. Observe that $\{x+2y : x \in \mathcal{R}^\times, y \in \mathcal{R}\}$ is a set of representatives for U_4 and $\#U_4 = 2^n(2^n-1)$. Therefore elements of U_4^2 are of the form $(x+2y)^2 \equiv x^2 \bmod 4\mathcal{O}_K$ for $x \in \mathcal{R}^\times$ and $y \in \mathcal{R}$. Since $\#(\mathcal{O}_K/2)^\times = 2^n - 1$ is odd, the squaring map on $U_2 = (\mathcal{O}_K/2)^\times$ is surjective and so $\#U_4^2 = 2^n - 1$. Therefore $\#\mathbf{M}_4 = \#U_4/\#U_4^2 = 2^n$. Since $\mathbf{M}_4$ is formed by taking the quotient of U_4 modulo squares, $\mathbf{M}_4$ is a direct product of cyclic groups of order 2.

For any $\alpha \in \mathcal{O}_K$ coprime to 2, write $[\alpha]$ as the projection of $\alpha\mathcal{O}_K$ in $\mathbf{M}_4$. Since every $x \in \mathcal{R}^\times$ is a square in U_2, we can write down the isomorphism explicitly as

$$\mathbf{M}_4 \to \mathcal{O}_K/2 \cong \mathbb{F}_2^n \qquad [x+2y] = [1+2x^{-1}y] \mapsto x^{-1}y. \tag{6.1}$$

We see that $\mathbf{M}_4 = \{[1+2y] : y \in \mathcal{O}_K/2\}$.

(ii) Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. The action of σ on $[1+2y] \in \mathbf{M}_4$, simply maps y to y^σ. Then we see that $y \equiv y^\sigma \bmod \mathcal{O}_K/2$ if and only if $y \equiv 0$ or $1 \bmod \mathcal{O}_K/2$. These correspond to ± 1 in $\mathbf{M}_4$. □

6.1.1 Primes are equidistributed on $\mathbf{M}_4$

Lemma 6.7. *Assume K satisfies (P1), (P2), and (P5). Let $[\alpha] \in \mathbf{M}_4$. Let $\mathfrak{p}$ be an odd prime of K such that $\mathbf{r}_4(\mathfrak{p}) = \alpha$. The map*

$$\begin{aligned} \mathbf{M}_4 &\to (\mathbb{Z}/4\mathbb{Z})^\times \\ [\alpha] &\mapsto \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) \equiv \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \bmod 4\mathbb{Z} \end{aligned}$$

is well-defined.

Proof. By Lemma 6.8, for any $\alpha \in \mathbf{M}_4$, there exists a prime $\mathfrak{p} \in \mathcal{P}_K^2$ such that $\mathbf{r}_4(\mathfrak{p}) = \alpha$.

Let $\mathfrak{p}$ and $\mathfrak{q}$ be (odd) primes of K such that $\mathbf{r}_4(\mathfrak{p}) = \mathbf{r}_4(\mathfrak{q})$. Let α be a totally positive generator of $\mathfrak{p}^h$ and let β be a totally positive generator of $\mathfrak{q}^h$, where h is the (odd) class number of K. Since $\mathbf{r}_4(\mathfrak{p}) = \mathbf{r}_4(\mathfrak{q})$, $\alpha \equiv \beta$ in $\mathbf{M}_4$. Then $\alpha \equiv \beta\gamma^2 \bmod 4\mathcal{O}_K$ for some $\gamma \in \mathcal{O}_K$. Since 2 is inert, $\alpha^\sigma \equiv \beta^\sigma(\gamma^\sigma)^2 \bmod 4\mathcal{O}_K$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Therefore $\mathrm{Norm}(\alpha) \equiv \mathrm{Norm}(\beta)\,\mathrm{Norm}(\gamma)^2 \bmod 4\mathcal{O}_K$. Since the norms are in $\mathbb{Z}$, $\mathrm{Norm}(\alpha) \equiv \mathrm{Norm}(\beta) \bmod 4\mathbb{Z}$. □

For $\mathfrak{m}$ an ideal of $\mathcal{O}_K$, let $J_K^{\mathfrak{m}}$ denote the group of fractional ideals of K prime to $\mathfrak{m}$. Also let $\mathbf{C}_{\mathfrak{m}}$ denote the narrow ray class group of conductor $\mathfrak{m}$, that is, the quotient of $J_K^{\mathfrak{m}}$ by the set of principal fractional ideals generated by totally positive $a \in K$ with $a \equiv 1 \bmod \mathfrak{m}$.

Lemma 6.8 ([58, Lemma 3.5], [20, Lemma 4.6])**.** *For K satisfying property (P1) and (P2), the homomorphism $J_K^2 \to \mathbf{M}_4$ induced by $\mathbf{r}_4$ induces a canonical surjective homomorphism $\varphi_4 : \mathbf{C}_4 \to \mathbf{M}_4$.*

For a fixed sign $\pm$, let $S'_\pm$ denote the set of primes of K lying above some $p \in S$ such that $p \equiv \pm 1 \bmod 4\mathbb{Z}$. We now state a lemma that handles the densities restricted to primes of a fixed congruence class modulo $4\mathbb{Z}$.

Under the Artin map, φ_4 induces a canonical isomorphism

$$\mathrm{Gal}(L/K) \cong \mathbf{M}_4,$$

where L is contained in the narrow ray class field over K of conductor 4. Then applying the Chebotarev density theorem over the extension $L/K \cdot \mathbb{Q}(\sqrt{-1})$ gives the following lemma.

Lemma 6.9 ([20, Lemma 4.8])**.** *Assume K satisfies conditions (P1)-(P3) and (P5). For any $[\alpha] \in \mathbf{M}_4$, the density of $\mathfrak{p} \in S'_{\pm}$ such that $\varphi_4(\mathfrak{p}) = \alpha$ is given by*

$$d(\mathbf{r}_4^{-1}(\alpha) \cap S'_{\pm} | S'_{\pm}) = \frac{1}{2^{n-1}}.$$

6.1.2 The Hilbert symbol on $\mathbf{M}_4$

Lemma 6.10. *The Hilbert symbol $(\cdot, \cdot)_2$ is well-defined on $\mathbf{M}_4$.*

Proof. We show that $(\alpha, \beta)_2 = (\alpha + 4B, \beta)_2$ for any $B \in \mathcal{O}_K$ coprime to 2, which implies that $(\cdot, \cdot)_2$ is well-defined on $(\mathcal{O}_K/4\mathcal{O}_K)^\times \times (\mathcal{O}_K/4\mathcal{O}_K)^\times$. Suppose $B \in \mathcal{O}_K$ is coprime to 2. It suffices to show that $(\alpha, \beta)_2 = 1$ implies $(\alpha + 4B, \beta)_2 = 1$. Take $x, y, z \in \mathcal{O}_K$ not all divisible by 2 satisfying $x^2 - \alpha y^2 = \beta z^2 \bmod 8$. Since $(\mathcal{O}_K/2\mathcal{O}_K)^\times$ contains all its squares, there exists $C, D \in \mathcal{O}_K$ such that $C^2 \equiv \alpha^{-1}\beta B \bmod 2$ and $D^2 \equiv \alpha^{-1}\beta^{-1}B \bmod 2$. Take $X = x + 2Cz$, $y = Y$ and $Z = z + 2Dx$, then one can check that $X^2 - (\alpha + 4B)Y^2 \equiv \beta Z^2 \bmod 8$. □

Lemma 6.11. *The Hilbert symbol $(\cdot, \cdot)_2$ is non-degenerate on $\mathbf{M}_4$.*

Proof. Fix some $\alpha \in \mathcal{O}_K$ coprime to 2. We claim that $(\alpha + 4B, 2)_2 = 1$ for some $B \in \mathcal{O}_K$. Since $(\mathcal{O}_K/2\mathcal{O}_K)^\times$ contains all its squareroots, there exist some $\gamma, z \in \mathcal{O}_K$ such that $\alpha \equiv \gamma^2 - 2z^2 \bmod 4$. Write $x = \gamma + 2x'$ for some $x' \in \mathcal{O}_K$, set $B = x'\gamma + x'^2$ and $y = 1$. Then $x^2 - (\alpha + 4B)y^2 \equiv 2z^2 \bmod 8$. This proves our claim.

Now suppose $(\alpha, \beta)_2 = 1$ for all $\beta \in \mathcal{O}_K$ coprime to 2. Then taking B from the above claim, $(\alpha + 4B, \beta)_2 = 1$ holds for all $\beta \in \mathcal{O}_K$ coprime to 2 by Lemma 6.10, and for all $\beta \in \mathcal{O}_K$ divisible by 2, by the above claim. Since the Hilbert symbol is non-degenerate on $K_2/K_2^\times$ [68, Chapter XIV, Proposition 7], this implies that $\alpha + 4B \in \mathcal{O}_K^2$. Hence $[\alpha] = [\alpha + 4B]$ is trivial in $\mathbf{M}_4$. □

Proposition 6.2 and (P5) shows that for $\mathfrak{p}$ a prime of K with totally positive generator $\alpha \in \mathcal{O}_K$, and for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ a generator,

$$\mathrm{spin}(\mathfrak{p}, \sigma)\,\mathrm{spin}(\mathfrak{p}, \sigma^{-1}) = (\alpha, \alpha^\sigma)_2,$$

which motivates the following definition.

Definition 6.12 ([58])**.** *Assume K satisfies (P1), (P2), and (P5) with abelian Galois group. Let $\alpha \in \mathcal{O}_K$ denote a representative of $[\alpha] \in \mathbf{M}_4$. Define the map*

$$\star : \mathbf{M}_4 \to \{\pm 1\}$$
$$[\alpha] \mapsto \begin{cases} 1 & \text{if } (\alpha, \alpha^\sigma)_2 = 1 \text{ for all non-trivial } \sigma \in \mathrm{Gal}(K/\mathbb{Q}), \\ -1 & \text{otherwise.} \end{cases}$$

Observe that $\star$ is a well-defined map by Lemma 6.10. If (6.2) holds for some $\alpha \in \mathcal{O}_K$, then it holds for α^σ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Therefore $\star(\alpha) = \star(\alpha^\sigma)$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Let $\star_+$ denote the restriction of $\star$ to

$$\mathbf{M}_4^+ \coloneqq \{[\alpha] \in \mathbf{M}_4 : \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \equiv 1 \bmod 4\}$$

and let $\star_-$ denote the restriction of $\star$ to

$$\mathbf{M}_4^- \coloneqq \{[\alpha] \in \mathbf{M}_4 : \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \equiv -1 \bmod 4\}.$$

For a fixed sign $\pm$, define $R_\pm \coloneqq R \cap S_\pm$.

By Proposition 6.2, fixing any prime $\mathfrak{p}$ of K above p, the following are equivalent

(i) $\mathrm{spin}(\mathfrak{p}, \sigma)\,\mathrm{spin}(\mathfrak{p}, \sigma^{-1}) = 1$ for all $\sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})$, and

(ii) $\star \circ \mathbf{r}_4(\mathfrak{p}) = 1$.

Therefore, for each fixed sign $\pm$,

$$R_\pm = \{p \in S_\pm : \star \circ \mathbf{r}_4(\mathfrak{p}) = 1 \text{ for } \mathfrak{p} \text{ a prime of } K \text{ above } p\}.$$

Summing up the densities in Lemma 6.9 over classes $[\alpha] \in \mathbf{M}_4^+$ and $[\alpha] \in \mathbf{M}_4^-$, we get

$$d(R_\pm | S_\pm) = \frac{\#\ker(\star_\pm)}{\#\mathbf{M}_4^\pm}.$$

Applying Proposition 6.6 we get $\#\mathbf{M}_4 = 2^n$. Since half the elements of $\mathbf{M}_4$ are in $\mathbf{M}_4^+$ and half in $\mathbf{M}_4^-$, $\#\mathbf{M}_4^+ = \#\mathbf{M}_4^- = 2^{n-1}$.

Theorem 6.13. *Assume K satisfies properties (P1)-(P5). Then*

$$d(R|S) = \frac{\#\ker(\star)}{2^n},$$

$$d(R_+|S_+) = \frac{\#\ker(\star_+)}{2^{n-1}} \quad \textit{and} \quad d(R_-|S_-) = \frac{\#\ker(\star_-)}{2^{n-1}}.$$

6.2 Counting solutions to a Hilbert symbol condition

In this section, we will prove the formulae for $\#\ker(\star_\pm)$.

Fix τ to be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. For any $\alpha \in K$, write $\alpha_{(k)} \coloneqq \alpha^{\tau^k}$ for $k \in \mathbb{Z}$.

Lemma 6.14. $(-1,-1)_2 = -1$.

Proof. Assume for contradiction that $(-1,1)_2 = 1$. Consider a homomorphism $\psi : \mathbf{M}_4 \to \{\pm 1\}$ given by $[\alpha] \mapsto (\alpha,-1)_2$. Since the Hilbert symbol is non-degenerate, and -1 is not a square modulo 4 in K, ψ is not identically 1. Therefore $\#\ker\psi = \#\mathbf{M}_4/\#\operatorname{im}\psi = 2^{n-1}$.

For any $[\alpha] \in \mathbf{M}_4 \setminus \{\pm 1\}$, we have $(\alpha_{(k)},-1)_2 = (\alpha,-1)_2$ for any k. Therefore ψ is stable under the Galois action. The size of each Galois orbit is n except the orbit of ± 1. But then n divides both $\#\{[\alpha] \in \mathbf{M}_4 \setminus \{\pm 1\} : \psi(\alpha) = 1\} = \#\{[\alpha] \in \mathbf{M}_4 : \psi(\alpha) = 1\} - 2 = 2^{n-1} - 2$ and $\#\{[\alpha] \in \mathbf{M}_4 : \psi(\alpha) = -1\} = 2^{n-1}$, which is a contradiction. □

Our aim is to count the number of elements in $\mathbf{M}_4$ with a representative $\alpha \in \mathcal{O}_K$ satisfying the spin relation

$$(\alpha, \alpha^\sigma)_2 = 1 \text{ for all non-trivial } \sigma \in \mathrm{Gal}(K/\mathbb{Q}). \tag{6.2}$$

By Lemma 6.11, the property (6.2) only depends on the class of $[\alpha] \in \mathbf{M}_4$.

6.2.1 The Hilbert symbol as a bilinear form on $\mathbf{M}_4$

By the Kronecker–Weber theorem, K is contained in the cyclotomic field $\mathbb{Q}(\zeta_\mathfrak{f})$, where $\mathfrak{f}$ is the conductor of K. The conductor $\mathfrak{f}$ is odd since we assumed that 2 is unramified in K. By [29, Theorem 4.5], there exists a normal 2-integral basis of $\mathbb{Q}(\zeta_\mathfrak{f})$, i.e. we can find some $a \in \mathcal{O}_{\mathbb{Q}(\zeta_\mathfrak{f})}$ such that the localization of $\mathcal{O}_{\mathbb{Q}(\zeta_\mathfrak{f})}$ at 2 can be written as $\mathcal{O}_{\mathbb{Q}(\zeta_\mathfrak{f}),2} = \oplus_{g \in \mathrm{Gal}(\mathbb{Q}(\zeta_\mathfrak{f})/\mathbb{Q})} \mathbb{Z}_{(2)} a^g$. Similar to the classic result for integral bases [59,

Proposition 4.31(i)], taking $y = \mathrm{Tr}_{\mathbb{Q}(\zeta_\mathfrak{f})/K}(a)$, then $\{y, y^\tau, \ldots, y^{\tau^{n-1}}\}$ gives a normal 2-integral basis of K. Since $\mathbb{Z}_{(2)}/2\mathbb{Z}_{(2)} \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathcal{O}_{K,2}/2\mathcal{O}_{K,2} \cong \mathcal{O}_K/2\mathcal{O}_K$, we know that $y, y^\tau, \ldots, y^{\tau^{n-1}}$ also form a normal $\mathbb{F}_2$-basis of $\mathcal{O}_K/2\mathcal{O}_K$.

Set $\alpha = 1 + 2y$. It follows from the isomorphism in (6.1) that

$$\mathbf{M}_4 = \left\{ \prod_{i=0}^{n-1} [\alpha_{(i)}]^{u_i} : (u_0, \ldots, u_{n-1}) \in \mathbb{F}_2^n \right\}.$$

Write $(\alpha, \alpha_{(i)})_2 = (-1)^{c_i}$, $c_i \in \{0, 1\}$. Note that $(\alpha_{(i)}, \alpha_{(j)})_2 = (\alpha, \alpha_{(j-i)})_2$. The Hilbert symbol is multiplicatively bilinear, so we can represent $(\,\cdot\,, \cdot\,)_2$ by the matrix

$$A \coloneqq \begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \ldots & c_1 \\ c_1 & c_0 & c_{n-1} & \ldots & c_2 \\ c_2 & c_1 & c_0 & \ldots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \ldots & c_0 \end{pmatrix} \tag{6.3}$$

with respect to the basis $[\alpha_{(i)}]$, $0 \le i \le n-1$.

Define the $n \times n$ $\mathbb{F}_2$-matrix

$$T_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix},$$

$T_k = T_1^k$ and $T_0 = I$.

Lemma 6.15. *Let A be the matrix representation of $(\,\cdot\,, \cdot\,)_2$ on $\mathbf{M}_4$ with respect to a normal basis, as given in* (6.3)*. Define a map*

$$\begin{aligned} &\Psi : \mathbb{F}_2^n \to \mathbb{F}_2[x]/(x^n - 1) \\ &\quad \mathbf{u} = (u_0, \ldots, u_{n-1}) \mapsto F_\mathbf{u}(x) \coloneqq u_0 + u_1 x + u_2 x^2 + \cdots + u_{n-1} x^{n-1}. \end{aligned}$$

Also define

$$\Phi : \mathbb{F}_2^n \to \mathbb{F}_2^n \qquad \mathbf{u} \mapsto (\mathbf{u}^T T_0 \mathbf{u},\ \mathbf{u}^T T_1 \mathbf{u},\ \ldots,\ \mathbf{u}^T T_{n-1} \mathbf{u}).$$

Let $B \coloneqq \Psi \circ \Phi$, *so*

$$B : \mathbb{F}_2^n \to \mathbb{F}_2[x]/(x^n - 1) \qquad \mathbf{u} \mapsto x^n \cdot F_{\mathbf{u}}(x) F_{\mathbf{u}}(1/x) \bmod (x^n - 1).$$

Then $\#\ker(\star_+) = \#B^{-1}(0)$ *and* $\#\ker(\star_-) = \#B^{-1}(h(x))$, *where* $h(x) = \Psi(A^{-1}(1, 0, \ldots, 0))$. *Furthermore*

$$h(x) \equiv x^n h(1/x) \bmod (x^n - 1). \tag{6.4}$$

Proof. For any $\mathbf{u} = (u_0, \ldots, u_{n-1}), \mathbf{v} = (v_0, \ldots, v_{n-1}) \in \mathbb{F}_2^n$, we have

$$\left(\prod_i \alpha_{(i)}^{u_i}, \prod_j \alpha_{(j)}^{v_j} \right)_2 = (-1)^{\mathbf{u}^T A \mathbf{v}}.$$

Since $(\cdot, \cdot)_2$ is non-degenerate on $\mathbf{M}_4$ by Lemma 6.11, the matrix A has rank n and is invertible. Note also that A is symmetric.

Now $\prod_i \alpha_{(i)}^{u_i}$, $\mathbf{u} = (u_0, \ldots, u_{n-1}) \in \mathbb{F}_2^n$ satisfies (6.2) if and only if

$$\mathbf{u}^T A T_1 \mathbf{u} = \mathbf{u}^T A T_2 \mathbf{u} = \cdots = \mathbf{u}^T A T_{n-1} \mathbf{u} = 0. \tag{6.5}$$

Since $\{T_0, T_1, \ldots, T_{n-1}\}$ is a basis of $\mathrm{GL}_n(\mathbb{F}_2)$, we can write

$$A = \sum_{i=0}^{n-1} c_i T_i, \qquad c_i \in \mathbb{F}_2.$$

Then (6.5) becomes

$$A \circ \Phi(\mathbf{u}) = A \begin{pmatrix} \mathbf{u}^T T_0 \mathbf{u} \\ \mathbf{u}^T T_1 \mathbf{u} \\ \vdots \\ \mathbf{u}^T T_{n-1} \mathbf{u} \end{pmatrix} \in \left\{ \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\}. \tag{6.6}$$

Since A is invertible, we can set $h(x) = \Psi(A^{-1}(1, 0, \ldots, 0))$. Notice that Ψ is a one-to-one correspondence. Then (6.6) can be rewritten as $B(\mathbf{u}) = \Psi \circ \Phi(\mathbf{u}) \in \{0, h(x)\}$. Since A is symmetric, A^{-1} is also symmetric, so (6.4) holds. Also $(\alpha, \alpha)_2 = (\alpha, -1)_2 = (\alpha, -1)_2^n = \prod_i (\alpha_{(i)}, -1)_2 = (\mathrm{Norm}_{K/\mathbb{Q}}(\alpha), -1)_2$, which is 1 if $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \equiv 1 \bmod 4$ and -1 if $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \equiv -1 \bmod 4$ by Lemma 6.14. Therefore $\#\ker(\star_+) = \#B^{-1}(0)$ and $\#\ker(\star_-) = \#B^{-1}(h(x))$. □

6.2.2 The counting problem

Our aim is to obtain the size of the preimage of 0 and $h(x)$ under B. For any polynomial f, let f^* denote its reciprocal, i.e. $f^*(x) = x^{\deg f} \cdot f(1/x)$.

Lemma 6.16. *For any factor $k \neq 1$ of n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Also set $d_1 = 1$. Consider the following factorisation in $\mathbb{F}_2[x]$,*

$$x^n - 1 = f_1(x) \ldots f_r(x) f_{m+1}^*(x) \ldots f_r^*(x),$$

where f_i are irreducible and $f_i = f_i^*$ for $i = 1, \ldots, m$. Then $\sum_{i=1}^r \deg f_i = \sum_{k|n} r_k d_k$ and $r = \sum_{k|n} r_k$ and $m = \sum_{k|n} m_k$, where $r_1 = m_1 = 1$, and

$$(r_k, m_k) = \begin{cases} \left(\frac{\phi(k)}{2d_k},\ 0\right) & \text{if } d_k \text{ is odd,} \\ \left(\frac{\phi(k)}{d_k},\ \frac{\phi(k)}{d_k}\right) & \text{if } d_k \text{ is even,} \end{cases}$$

for $k \neq 1$.

Proof. Take f to be an irreducible factor of $x^n - 1$ in $\mathbb{F}_2[x]$. Let γ be a root of f in an extension of $\mathbb{F}_2$. Then γ is a primitive k-th root of unity, where k is some integer dividing n. Galois theory on finite fields shows that $\mathrm{Gal}(\mathbb{F}_2(\gamma)/\mathbb{F}_2)$ is generated by the Frobenius $\varphi : x \mapsto x^2$. Since $\varphi^i : x \mapsto x^{2^i}$ for any $i \in \mathbb{Z}$, we see that the order of φ must be d_k, the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Therefore $\deg f = d_k$. The set of roots of f is $\{\gamma, \varphi(\gamma), \varphi^2(\gamma), \ldots, \varphi^{d_k - 1}(\gamma)\}$, which is closed under inversion precisely when d_k is even. Therefore f is self-reciprocal if and only if d_k is even. There are $\phi(k)$ roots of $x^n - 1$ which are primitive k-th root of unity, so $(2r_k - m_k)d_k = \phi(k)$. □

We are now ready to prove the formulae for $\#\ker(\star_+)$ and $\#\ker(\star_-)$.

Proposition 6.17. *For each $k \neq 1$ dividing n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Then*

$$\#\ker(\star_+) = 1 + \prod_{k|n,\ d_k\, odd,\ k\neq 1} 2^{\frac{\phi(k)}{2d_k}} \left(\prod_{k|n,\ d_k\, odd,\ k\neq 1} 2^{\frac{\phi(k)}{2}} - 1 \right),$$

and

$$\#\ker(\star_-) = \prod_{k|n,\ d_k\, even,\ k\neq 1} (2^{d_k/2}+1)^{\frac{\phi(k)}{d_k}} \prod_{k|n,\ d_k\, odd,\ k\neq 1} (2^{d_k}-1)^{\frac{\phi(k)}{2d_k}},$$

where ϕ denotes the Euler's totient function. If n is a prime, then writing $d = d_n$,

$$(\#\ker(\star_+), \#\ker(\star_-)) = \begin{cases} \left(1 + 2^{\frac{n-1}{2d}}(2^{\frac{n-1}{2}} - 1),\ (2^d-1)^{\frac{n-1}{2d}}\right) & \text{if } d \text{ is odd,} \\ \left(1,\ (2^{\frac{d}{2}}+1)^{\frac{n-1}{d}}\right) & \text{if } d \text{ is even.} \end{cases}$$

In particular, when $n = 3$, $\#\ker(\star_+) = 1$ and $\#\ker(\star_-) = 3$.

Proof. The first case $B(\mathbf{u}) = 0$ implies $(x^n - 1) \mid F_{\mathbf{u}}(x)F^*_{\mathbf{u}}(x)$. Obtain the following factorisation in $\mathbb{F}_2[x]$ as described in Lemma 6.16,

$$x^n - 1 = f_1(x) \dots f_r(x) f^*_{m+1}(x) \dots f^*_r(x), \tag{6.7}$$

where $f_1(x) = x+1$, f_i are irreducible and $f_i = f_i^*$ for $i = 1, \dots, m$. Write $F_{\mathbf{u}} = G \cdot H$, where $G = \gcd(F_{\mathbf{u}}, x^n - 1)$. Then for each $k = 0, \dots, r$, we have $f_k \mid F_{\mathbf{u}}$ or $f_i^* \mid F_{\mathbf{u}}$. This leaves us with 2^{r-m} choices for G. Since

$$\deg\left((x^n-1)/G\right) = n - \sum_{i=1}^{r} \deg f_i = \sum_{k|n} (r_k - m_k) d_k,$$

There are $2^{\sum_{k|n}(r_k - m_k)d_k} - 1$ choices for $H \not\equiv 0 \bmod (x^n-1)/G$, so

$$\#\ker(\star_+) = 1 + \#|B^{-1}(0) \setminus \{0\}| = 1 + 2^{r-m}\left(2^{\sum_{k|n}(r_k-m_k)d_k} - 1\right). \tag{6.8}$$

The second case $B(\mathbf{u}) = h(x)$. We count the number of $\mathbf{u} \in \mathbb{F}_2^n$ such that

$$x^n \cdot F_{\mathbf{u}}(x) F_{\mathbf{u}}(1/x) \equiv h(x) \bmod (x^n - 1). \tag{6.9}$$

Fix a primitive complex n-th root of unity ζ_n. Consider the isomorphism

$$(\mathbb{F}_2[x]/(x^n-1))^\times \to (\mathbb{Z}[\zeta_n]/2\mathbb{Z}[\zeta_n])^\times \qquad F_{\mathbf{u}}(x) \mapsto F_{\mathbf{u}}(\zeta_n) \bmod 2.$$

Now (6.9) becomes

$$F_{\mathbf{u}}(\zeta_n)\overline{F_{\mathbf{u}}(\zeta_n)} \equiv h(\zeta_n) \bmod 2.$$

Notice from (6.4) that $h(\zeta_n) = h(\zeta_n^{-1}) = \overline{h(\zeta_n)}$ is real. We compute from (6.7),

$$\begin{aligned}\#(\mathbb{Z}[\zeta_n]/2\mathbb{Z}[\zeta_n])^\times &= \#(\mathbb{F}_2[x]/(x^n-1))^\times \\ &= \prod_{i=1}^{r} \#\left(\mathbb{F}_2[x]/(f_i)\right)^\times \prod_{j=m+1}^{r} \#\left(\mathbb{F}_2[x]/(f_j^*)\right)^\times \\ &= \prod_{k|n} (2^{d_k}-1)^{2r_k-m_k}.\end{aligned}$$

Take $g \in \mathbb{F}_2[x]$ such that

$$\frac{x^n-1}{x-1} \equiv x^{n-1}+x^{n-2}+\cdots+x+1 = x^{\frac{n-1}{2}} g(x+x^{-1}).$$

We can factorise $g(x) = g_2(x)\dots g_r(x)$, where $x^{\deg g_k}\cdot g_k(x+x^{-1}) = f_k(x)$ for $2 \le k \le m$ and $x^{\deg g_k}\cdot g_k(x+x^{-1}) = f_k(x)f_k^*(x)$ for $m+1 \le k \le r$. Then since $(\mathbb{Z}[\zeta_n+\zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times \cong (\mathbb{F}_2[x]/(g))^\times$, we compute

$$\begin{aligned}\#\left(\mathbb{Z}[\zeta_n+\zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}]\right)^\times &= \#(\mathbb{F}_2[x]/(g))^\times \\ &= \prod_{i=2}^{r} \#\left(\mathbb{F}_2[x]/(g_i)\right)^\times \\ &= \prod_{k|n,\ k\neq 1} (2^{d_k/2}-1)^{m_k}(2^{d_k}-1)^{r_k-m_k}.\end{aligned}$$

Our goal is to compute the size of the kernel of the homomorphism

$$\psi : (\mathbb{Z}[\zeta_n]/2\mathbb{Z}[\zeta_n])^\times \to (\mathbb{Z}[\zeta_n+\zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times \qquad \beta \mapsto \beta\overline{\beta}.$$

We claim that ψ is surjective. Since $(\mathbb{Z}[\zeta_n+\zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times$ has odd order, every element is a square, so suppose $\beta^2 \in (\mathbb{Z}[\zeta_n+\zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times$, then $\psi(\hat{\beta}) = \beta^2$

for any lift $\hat{\beta} \in \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ of β. Therefore

$$\#\ker(\star_-) = \#B^{-1}(h(x)) = \#\ker\psi = \frac{\#(\mathbb{Z}[\zeta_n]/2\mathbb{Z}[\zeta_n])^\times}{\#\operatorname{im}\psi} = \prod_{k|n,\ k\neq 1} (2^{d_k/2}+1)^{m_k}(2^{d_k}-1)^{r_k-m_k}. \quad (6.10)$$

Putting in (6.8) and (6.10) the values of r and m in terms of n and d as in Lemma 6.16 proves the proposition. □

6.3 Joint spins

Fix a sign $\mu \in \{\pm\}$. The following formula for the relative density of F_μ in R_μ was proved in [20, Section 6].

Theorem 6.18 ([20, Theorem 6.1])**.** *Assume Conjecture C_η for $\eta = \frac{2}{n(n-1)}$. Then*

$$d(F_\mu|R_\mu) = 2^{-\frac{n-1}{2}}.$$

Since each $p \in S_\mu$ splits into exactly the same number of prime ideals in $\mathcal{O}_K$, and since R_μ is a set of primes of positive natural density, it suffices to show that

$$\sum_{\substack{\mathrm{Norm}(\mathfrak{p})\leq X \\ \mathfrak{p}\in F'_\mu}} 1 = 2^{-\frac{n-1}{2}} \sum_{\substack{\mathrm{Norm}(\mathfrak{p})\leq X \\ \mathfrak{p}\in R'_\mu}} 1 + o\left(\frac{X}{\log X}\right), \quad (6.11)$$

where F'_μ is the set of prime ideals lying above primes in F_μ, and R'_μ is defined similarly. Let τ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$, a cyclic group of order n. Then, by definition of the set R_μ, a prime $p \in R_\mu$ belongs to the set F_μ if and only if $\mathrm{spin}(\mathfrak{p}, \tau^k) = 1$ for all $k \in \{1, 2, \ldots, \frac{n-1}{2}\}$. The product

$$\prod_{k=1}^{\frac{n-1}{2}} \frac{1+\mathrm{spin}(\mathfrak{p},\tau^k)}{2}$$

is the indicator function of the property that $\mathrm{spin}(\mathfrak{p}, \tau^k) = 1$ for all $k \in \{1, 2, \ldots, \frac{n-1}{2}\}$. Expanding this product gives

$$2^{-\frac{n-1}{2}} \sum_{H\subset\{\tau,\ldots,\tau^{\frac{n-1}{2}}\}} \prod_{\sigma\in H} \mathrm{spin}(\mathfrak{p},\sigma), \quad (6.12)$$

where the sum is over all subsets H of $\{\tau, \tau^2, \dots, \tau^{\frac{n-1}{2}}\}$. When $H = \varnothing$, the product is 1 by convention.

Let $\mathcal{A}$ denote the set of disjoint G-orbits of elements of $\mathbf{M}_4^\mu$, so that we can write

$$\mathbf{M}_4^\mu = \bigsqcup_{A \in \mathcal{A}} A.$$

Each G-orbit A is then a collection of invertible congruence classes modulo $4\mathcal{O}_K$ that are distinct modulo squares. Let $\mathcal{A}_0 \subset \mathcal{A}$ be the set of G-orbits A such that $\mathrm{spin}(\mathfrak{p}, \sigma) = \mathrm{spin}(\mathfrak{p}, \sigma^{-1})$ for all non-trivial $\sigma \in G$ and for all prime ideals $\mathfrak{p}$ such that $\mathbf{r}_4(\mathfrak{p}) \in A$. Note that a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ lies over a prime $p \in R_\mu$ if and only if $\mathbf{r}_4(\mathfrak{p}) \in A$ for some $A \in \mathcal{A}_0$.

Summing (6.12) over all prime ideals $\mathfrak{p}$ of norm $\mathrm{Norm}(\mathfrak{p}) \leq X$, we get that

$$\sum_{\substack{\mathrm{Norm}(\mathfrak{p}) \leq X \\ \mathfrak{p} \in F'_\mu}} 1 = 2^{-\frac{n-1}{2}} \sum_{\substack{H \subset \{\tau, \dots, \tau^{\frac{n-1}{2}}\} \\ A \in \mathcal{A}_0}} \Sigma(X; H, A),$$

where

$$\Sigma(X; H, A) = \sum_{\substack{\mathrm{Norm}(\mathfrak{p}) \leq X \\ \mathbf{r}_4(\mathfrak{p}) \in A}} \prod_{\sigma \in H} \mathrm{spin}(\mathfrak{p}, \sigma). \tag{6.13}$$

The sums $\Sigma(X; \varnothing, A)$ feature no cancellation and provide the main term in (6.11). It then remains to show that

$$\Sigma(X; H, A) = o\left(\frac{X}{\log X}\right)$$

for each non-empty subset H of $\{\tau, \dots, \tau^{\frac{n-1}{2}}\}$ and each $A \in \mathcal{A}_0$. To this end, we need a slight generalization of Theorem 1 of [47].

One of the main reasons we cannot apply [47] directly, is due to our extended definition of spin. If we attempt to modify the arguments in [47] using our previous association of $\mathfrak{a}$ to a totally positive generator α of $\mathfrak{a}^h$, then since $\mathrm{Norm}(\alpha) = \mathrm{Norm}(\mathfrak{a})^h$, we will find that the set of α arising from the ideals $\mathfrak{a}$ with $\mathrm{Norm}(\mathfrak{a}) < X$ is too "sparsely" distributed in the set of totally positive elements with norm less than X^h in a way that we are unable to control.

To circumvent this issue, we introduce another relation between prime ideals $\mathfrak{p}$

and some totally positive $\alpha_0 \in \mathcal{O}_K$. Fix a set $\mathcal{C}$ consisting of h unramified degree-one prime ideals in $\mathcal{O}_K$ that is a complete set of representatives of ideal classes in the class group of K; its existence is guaranteed by an application of the Chebotarev Density Theorem to the Hilbert class field of K.

Now suppose that $\mathfrak{a}$ is a nonzero ideal in $\mathcal{O}_K$ coprime to $\prod_{\mathfrak{p}\in\mathcal{C}} \mathrm{Norm}(\mathfrak{p})$, and let α denote a totally positive generator of $\mathfrak{a}^h$. As h is odd, the set $\{\mathfrak{p}^2 : \mathfrak{p} \in \mathcal{C}\}$ is also a complete set of representatives. Hence there exists a unique $\mathfrak{p} \in \mathcal{C}$ such that $\mathfrak{a}\mathfrak{p}^2$ is a principal ideal. Let π denote a totally positive generator of the ideal $\mathfrak{p}^h$. Let α_0 denote a totally positive generator of $\mathfrak{a}\mathfrak{p}^2$. Then α_0^h and $\alpha\pi^2$ are both totally positive generators of the ideal $(\mathfrak{a}\mathfrak{p}^2)^h$, so we have

$$\mathrm{spin}(\mathfrak{a},\sigma) = \left(\frac{\alpha}{\sigma(\mathfrak{a})}\right) = \left(\frac{\alpha\pi^2}{\sigma(\mathfrak{a}\mathfrak{p}^2)}\right) = \mathrm{spin}(\mathfrak{a}\mathfrak{p}^2,\sigma) = \left(\frac{\alpha_0^h}{\sigma(\mathfrak{a}\mathfrak{p}^2)}\right) = \left(\frac{\alpha_0}{\sigma(\alpha_0)}\right),$$

since h is odd. Note that for each $\mathfrak{p} \in \mathcal{C}$ there is a bijection given by $\mathfrak{a} \mapsto \alpha_0$ as above, between

$$\{\mathfrak{a} \subset \mathcal{O}_K : \mathrm{Norm}(\mathfrak{a}) \le X, \mathfrak{a}\mathfrak{p}^2 \text{ is principal}\}$$
$$\simeq \{\alpha_0 \in \mathcal{D} : \mathrm{Norm}(\alpha_0) \le X \cdot \mathrm{Norm}(\mathfrak{p})^2,\ \alpha_0 \equiv 0 \bmod \mathfrak{p}^2\},$$

where $\mathcal{D}$ is a set of totally positive elements in $\mathcal{O}_K$ defined in [33, (4.2), p.713]. Moreover, $\mathbf{r}_4(\mathfrak{a})$ is the class in $\mathbf{M}_4$ of a totally positive generator of $\mathfrak{a}^h$, i.e., the class of α in $\mathbf{M}_4$. Since squares vanish in $\mathbf{M}_4$, the classes of α and $\alpha\pi^2$, and so also of α_0^h, coincide in $\mathbf{M}_4$. Hence, if A is a G-orbit, then

$$\mathbf{r}_4(\mathfrak{a}) \in A \quad \text{if and only if} \quad [\alpha_0^h] \in A.$$

We now state the adaptation of [47, Theorem 1] proved in [20].

Theorem 6.19 ([20, Theorem 6.2])**.** *Take $\Sigma(X; H, A)$ as defined in* (6.13)*. Assume Conjecture C_η holds true for $\eta = 1/(|H|n)$ with $\delta = \delta(\eta) > 0$ (see [47, p. 7]). Let $\epsilon > 0$. Then for all $X \ge 2$, we have*

$$\Sigma(X; H, A) \ll_{\epsilon,K} X^{1-\frac{\delta}{54|H|^2 n(12n+1)}+\epsilon}.$$

6.4 Proof of main results

Proof of Theorem 6.4. By Theorem 6.13 and Proposition 6.17, $d(R_\pm|S_\pm) = s_\pm/2^{n-1}$. By Theorem 6.18, $d(F_\pm|R_\pm) = 2^{-(n-1)/2}$. Therefore

$$d(F_\pm|S_\pm) = d(F_\pm|R_\pm)d(R_\pm|S_\pm) = \frac{s_\pm}{2^{3(n-1)/2}}.$$

Since $d(F|S) = d(F_+|S_+)d(S_+|S) + d(F_-|S_-)d(S_-|S)$, and $d(S_\pm|S) = 1/2$,

$$d(F|S) = \frac{s_+ + s_-}{2^{(3n-1)/2}}.$$

□

Theorem 6.4 settles a generalised version of Conjecture 1.1 in [58]

Proof of Theorem 6.5. For K a cyclic cubic number field with odd class number, by [2, Theorem V] or [58, Theorem 1.4], K satisfies property (P1). It is a consequence of the classical Burgess's inequality [14] that Conjecture C_η is true for $m = 3$, as is shown in Section 9 of [33]. Therefore the result follows from Theorem 6.4. □

Chapter 7

Integral points on the congruent number curve

This chapter contains results presented in [18].

For squarefree positive integer D, we consider the elliptic curve

$$\mathcal{E}_D : y^2 = x^3 - D^2 x.$$

We are interested in the set of integral points on the curve, defined as

$$\mathcal{E}_D(\mathbb{Z}) \coloneqq \left\{(x, y) \in \mathbb{Z}^2 : y^2 = x^3 - D^2 x\right\}.$$

Given an elliptic curve with Weierstrass equation $y^2 = x^3 + Ax + B$, Siegel [72] proved that there are only finitely many integral points, using techniques from the theory of Diophantine approximation. Baker [5, page 45] gave the first effective bound on the height of integral points: if an integral point (x, y) exists, then

$$|x| \leq \exp\left((10^6 \max\{A, B\})^{10^6}\right).$$

Lang [53, page 140] conjectured that the number of integral points on an elliptic curve should be bounded only in terms of its rank. This was proven for elliptic curves with integral j-invariant [75, Theorem A] and for elliptic curves with bounded Szpiro ratio [41, Theorem 0.7]. The curves $\mathcal{E}_D$ satisfy both of these properties, and more specifically the theorems show that there exists some constant C, such that

$$\mathcal{E}_D(\mathbb{Z}) \leq C^{\operatorname{rank} \mathcal{E}_D(\mathbb{Q})}. \tag{7.1}$$

From a more general theorem by Helfgott and Venkatesh [40, Corollary 3.11], we can deduce that

$$\#\mathcal{E}_D(\mathbb{Z}) \ll C^{\omega(D)}(\log D)^2(1.33)^{\operatorname{rank}\mathcal{E}_D(\mathbb{Q})},$$

where C is some absolute constant and $\omega(D)$ denotes the number of distinct prime factors of the integer D. We obtain an upper bound with a smaller and explicit base, specifically for the curves $\mathcal{E}_D$.

Theorem 7.1. *We have*

$$\#\mathcal{E}_D(\mathbb{Z}) \ll (3.8)^{\operatorname{rank}\mathcal{E}_D(\mathbb{Q})}.$$

Therefore if we expect the rank to be uniformly bounded for all $\mathcal{E}_D(\mathbb{Q})$ (as has been recently conjectured by various authors), then there would be a squarefree positive integer D such that $\#\mathcal{E}_D(\mathbb{Z})$ attains its maximum.

We proceed by partitioning $\mathcal{E}_D(\mathbb{Z})$ into cosets of $2\mathcal{E}_D(\mathbb{Q})$. For any $R \in \mathcal{E}_D(\mathbb{Q})$, define

$$\mathcal{Z}_D(R) \coloneqq \mathcal{E}_D(\mathbb{Z}) \cap (R + 2\mathcal{E}_D(\mathbb{Q})).$$

We obtain an upper bound on the size of each $\mathcal{Z}_D(R)$ in terms of the rank of $\mathcal{E}_D(\mathbb{Q})$:

Theorem 7.2. *If D is sufficiently large and $R \in \mathcal{E}_D(\mathbb{Q})$ then*

$$\#\mathcal{Z}_D(R) < 30 + (1.89)^{r+19r^{1/3}},$$

where $r \coloneqq \operatorname{rank}\mathcal{E}_D(\mathbb{Q})$.

Since $\#\mathcal{E}_D(\mathbb{Q})/2\mathcal{E}_D(\mathbb{Q}) = 2^{2+\operatorname{rank}\mathcal{E}_D(\mathbb{Q})}$, Theorem 7.1 is immediate from Theorem 7.2.

Fix $\epsilon > 0$. We partition $\mathcal{Z}_D(R)$ into the points with "small" x-coordinates,

$$\mathcal{S}_D(R) \coloneqq \left\{P \in \mathcal{Z}_D(R) : x(P) \le D^{2(1+\epsilon)}\right\}$$

and the points with "large" x-coordinates,

$$\mathcal{L}_D(R) \coloneqq \left\{P \in \mathcal{Z}_D(R) : x(P) > D^{2(1+\epsilon)}\right\},$$

which we will bound by very different techniques.

Theorem 7.3 (Points with large x-coordinates)**.** *There exists some $\epsilon > 0$ such that the following holds for any sufficiently large D and $R \in \mathcal{E}_D(\mathbb{Q})$.*

(i) $\#\mathcal{L}_D(R) \leq 30$*;*

(ii) If the abc conjecture holds, then $\mathcal{L}_D(R) = \varnothing$*.*

We will complete the proof of Theorem 7.2 by showing that $\#\mathcal{S}_D(R) < (1.89)^{r+19r^{1/3}}$.

If $x(R) \leq D$ then we can improve the bound to $\#\mathcal{Z}_D(R) \leq 4$.

Theorem 7.4 (Cosets with respect to points with very small x-coordinates)**.**

(i) $\mathcal{Z}_D(\mathcal{O}) = \varnothing$*;*

(ii) $\mathcal{Z}_D((-D, 0)) = \{(-D, 0)\}$ *and* $\mathcal{Z}_D((0, 0)) = \{(0, 0)\}$*;*

(iii) $\mathcal{Z}_D((D, 0))$ *contains* $(D, 0)$ *and no more than one other pair* $P, -P \in \mathcal{E}_D(\mathbb{Z})$*, given by* $x(P) = (2v^2 - 1)D$*, where* $v + u\sqrt{D}$ *is the fundamental solution of the equation* $v^2 - Du^2 = 1$*;*

(iv) If $R \in \mathcal{E}_D(\mathbb{Q})$ *and* $-D < x(R) < 0$*, then* $\mathcal{Z}_D(R)$ *contains at most one pair* $P, -P \in \mathcal{E}_D(\mathbb{Z})$*, except for the sets*

$$\{(-98, \pm 12376),\ (-1058, \pm 21896)\} \text{ when } D = 1254,$$
$$\text{and } \{(-5184, \pm 398664),\ (-7056, \pm 233772)\} \text{ when } D = 7585.$$

The sets considered in Theorem 7.4 ((i)), ((ii)) contains no non-trivial integral points, and the upper bounds obtained in ((iii)), ((iv)) are sharp. Indeed, on the curve $\mathcal{E}_6(\mathbb{Q})$ of rank 1, the distinct cosets $\mathcal{Z}_6(R)$ of integral points are $\{(-6, 0)\}$, $\{(0, 0)\}$, as well as

$$\{(-3, \pm 9)\},\ \{(-2, \pm 8)\},\ \{(6, 0),\ (294, \pm 5040)\},\ \{(12, \pm 36)\},\ \{(18, \pm 72)\}.$$

Ordering the curves $\mathcal{E}_D$ with increasing D, Heath-Brown [36, Theorem 1] showed that the moments of the 2-Selmer of $\mathcal{E}_D$ are bounded. Together with (7.1) or Theorem 7.1, this implies that the average size of $\mathcal{E}_D(\mathbb{Z})$ is bounded. The boundedness

of the average of $\#\mathcal{E}_D(\mathbb{Z})$ was first proved by Alpoge [1], but the upper bound was not explicitly evaluated.

Let $\mathcal{D}(N)$ be the set of positive squarefree integers less than N. Define $\mathcal{T}_D$ to be the set of torsion points on $\mathcal{E}_D(\mathbb{Q})$. It is standard that $\mathcal{T}_D = \{\mathcal{O},\ (0,0),\ (\pm D, 0)\}$ (see for example [46, Chapter I, Proposition 17]). Let $s_{2^\infty}(D)$ denote the $\mathbb{Z}_2$-corank of the 2-power Selmer group of $\mathcal{E}_D(\mathbb{Q})$, and $s_{2^k}(D)$ denote the $\mathbb{F}_2$-rank of the 2^k-Selmer rank of $\mathcal{E}_D(\mathbb{Q})$. Then $s_{2^\infty}(D) = \lim_{k\to\infty} s_{2^k}(D)$. Each $s_{2^k}(D)$ and hence also $s_{2^\infty}(D)$ provides an upper bound on the rank of $\mathcal{E}_D(\mathbb{Q})$. Heath-Brown [36] notes that it can be derived from results of Cassels [16] and Birch and Stephens [10], that $s_2(D)$ is even for $D \equiv 1$, 2 or 3 mod 8, and odd for $D \equiv 5$, 6 or 7 mod 8. An elementary proof of this parity condition was given by Monsky [36, Appendix]. Furthermore, the 2^{k+1}-Selmer group is computed from the kernel of the Cassels-Tate pairing on the 2^k-Selmer group. Since the Cassels-Tate pairing is always skew-symmetric [15], we have $s_{2^k}(D) \equiv s_{2^{k+1}}(D) \bmod 2$ for all k, so $s_{2^\infty}(D)$ and $s_2(D)$ are of the same parity. Smith [81, Corollary 1.2] recently claimed that

$$\{D \in \mathcal{D}(N) : s_{2^\infty}(D) \geq 2\} = o(N).$$

It then follows that for $s \in \{0, 1\}$, we have

$$\lim_{N\to\infty} \frac{1}{\#\mathcal{D}(N)} \#\{D \in \mathcal{D}(N) : s_{2^\infty}(D) = s\} = \frac{1}{2}. \tag{7.2}$$

Since $\operatorname{rank} \mathcal{E}_D(\mathbb{Q}) \leq s_{2^\infty}(D)$, asymptotically at most half of the curves are of rank 1, and density 0 of curves are of rank 2 or above. This allows us to focus on curves with rank 0 and 1, hence we can find a better upper bound on the average.

Theorem 7.5. *We have*

$$\limsup_{N\to\infty} \frac{1}{\#\mathcal{D}(N)} \sum_{D\in\mathcal{D}(N)} \#(\mathcal{E}_D(\mathbb{Z}) \setminus \mathcal{T}_D) \leq 2.$$

If we further assume the abc conjecture, the upper bound can be improved to 1.

Note that non-torsion integral points come in pairs of $(x, \pm y)$. The upper bound from Theorem 7.5 comes from the possible existence of a pair of small points in the range $D^2/(\log D)^{12+\epsilon} < x < D^{2+\epsilon}$, and a pair of large points of size $x >$

$\exp(\exp(\frac{23}{12}\sqrt{\log D}))$ left from an application of Roth's Theorem, which we are unable to eliminate on most curves of rank 1.

We expect the order of $\sum_{D\in\mathcal{D}(N)} \#(\mathcal{E}_D(\mathbb{Z}) \setminus \mathcal{T}_D)$ to be roughly $N^{1/2}$. To obtain a lower bound, we attempt by counting a subset of integral points. Suppose $u > v$ are squarefree positive coprime integers. Let w be the squarefree part of $u^2 - v^2$, so u, v, w are pairwise coprime. If $D = uvw$, then $(u^2w, u^2w^{3/2}\sqrt{u^2 - v^2}) \in \mathcal{E}_D(\mathbb{Z})$, since $w(u^2 - v^2)$ is a square by the definition of w. If $uv(u^2 - v^2) < N$, then $D \in \mathcal{D}(N)$, so counting the number of squarefree coprime positive integers u, v in the range $v < u < N^{1/4}$, gives a lower bound of $\gg N^{1/2}$.

Now we give a heuristic on the maximum size of $\sum_{D\in\mathcal{D}(N)} \#(\mathcal{E}_D(\mathbb{Z}) \setminus \mathcal{T}_D)$. The larger points $(x, y) \in \mathcal{E}_D(\mathbb{Z})$ with $x > D^{2+\epsilon}$ can be removed by assuming the *abc* conjecture as in Theorem 7.3, so let's look at $D \in \mathcal{D}(N)$ and $|x| < D^{2+\epsilon}$. If $x = -j$, $j - D$, or $D + j$ for $1 \le j \le D/2$ then $x^3 - D^2x \approx jD^2$. If $\frac{3}{2}D < x < N^3$ then $x^3 - D^2x \approx x^3$. Then we expect the number of pairs (D, x) such that $x^3 - D^2x$ is a square to be approximately

$$\sum_{\frac{1}{2}N\le D<N} \left(\sum_{1\le j\le D/2} \left(\frac{1}{jD^2}\right)^{1/2} + \sum_{\frac{3}{2}D<x<D^3} \left(\frac{1}{x^3}\right)^{1/2} \right) \ll N^{1/2}.$$

To prove Theorem 7.2, we bound $\#\mathcal{S}_D(R)$ and $\#\mathcal{L}_D(R)$ separately. We prove that $\#\mathcal{S}_D(R)$ is bounded above by

$$\#\left\{ P \in R + 2\mathcal{E}_D(\mathbb{Q}) : \hat{h}(P) \le 2(1+\epsilon)\log D + o(1) \right\},$$

where $\hat{h}$ denotes the canonical height. Then viewing $\mathcal{E}_D(\mathbb{Q})$ as an r-dimensional Euclidean space, we apply sphere packing bounds to get an upper bound of $(1.89)^{r+19r^{1/3}}$ after fixing some appropriate ϵ.

On the other hand, we show that $\#\mathcal{L}_D(R)$ is bounded by some constant depending only on ϵ. Assume $x(R) > D$ and $R \notin \mathcal{T}_D + 2\mathcal{E}_D(\mathbb{Q})$, otherwise the result follows from Theorem 7.4. We first prove that points in $\mathcal{L}_D(R)$ obey a gap principle. Then, for points with larger heights in $\mathcal{L}_D(R)$, we apply Roth's theorem in a way that is similar to a classical argument of Siegel's Theorem, which also appeared in Alpoge's work [1]. Suppose $P = 2Q + R \in \mathcal{Z}_D(R)$ and $x(P)$ is large, P is close to the

point at infinity. Let K be the minimal number field containing the x-coordinates of all points in $\frac{1}{2}\mathcal{E}_D(\mathbb{Q})$. If $4S = R$ and $2\tilde{Q} = Q$, where $\tilde{Q}, S \in \mathcal{E}_D(\overline{\mathbb{Q}})$, then S and $\tilde{Q}$ are close together. Making this precise, we can show that $x(\tilde{Q})$ gives a K-approximation to $x(S)$ with exponent close to 8. Roth's theorem show that there are finitely many such $\tilde{Q}$. In [1], large integral points of the form $P = 3Q + R$ were considered, where Q, R are rational points on a general elliptic curve. The main difference of our approach is that we apply Roth's theorem over K instead of $\mathbb{Q}$. Given a class in $\mathcal{E}_D(\mathbb{Q})/n\mathcal{E}_D(\mathbb{Q})$, the exponents of the $\mathbb{Q}$-approximations obtained from the argument in [1] are close to $\frac{1}{2}n^2$. If we had taken $n = 2$, the exponent would be just under 2 which would not be large enough to apply Roth's theorem. Applying the argument over K instead gives a large enough exponent.

7.1 Applications to other Diophantine equations

Given positive integers a, b and c, Bennett [8, Theorem 1.2] proved that there exists at most one set of three consecutive integers of the form cZ^2, bY^2, aX^2. In other words, the simultaneous equations

$$aX^2 - bY^2 = 1, \qquad bY^2 - cZ^2 = 1, \qquad (X, Y, Z) \in \mathbb{Z}^3_{>0}$$

possess at most one solution. We can ask a more general question replacing the 1 in the equations with an integer d.

Theorem 7.6. *Let a, b, c, d be pairwise coprime positive integers and set $D = abcd$. Then for any sufficiently large D, the system of equations*

$$aX^2 - bY^2 = d, \qquad bY^2 - cZ^2 = d \tag{7.3}$$

has at most $15+(1.89)^{r+19r^{1/3}} \leq 15+(3.58)^{\omega(D)+12\omega(D)^{1/3}}$ solutions $(X, Y, Z) \in \mathbb{Z}^3_{>0}$, where $r \coloneqq \operatorname{rank} \mathcal{E}_D(\mathbb{Q})$.

We prove Theorem 7.6 by relating the problem to our result in Theorem 7.2. If we take $D = abcd$ and $x = ac(bY)^2$, then $x - D = ab(cZ)^2$ and $x + D = bc(aX)^2$. Therefore $(ac(bY)^2, (abc)^2XYZ) \in \mathcal{E}_D(\mathbb{Z})$. The image of such a point under the

injective homomorphism

$$\theta : \mathcal{E}_D(\mathbb{Q})/2\mathcal{E}_D(\mathbb{Q}) \to \mathbb{Q}/(\mathbb{Q}^*)^2 \times \mathbb{Q}/(\mathbb{Q}^*)^2 \times \mathbb{Q}/(\mathbb{Q}^*)^2$$

given at non-torsion points by

$$(x, y) \mapsto (x - D,\ x,\ x + D),$$

is (ab, ac, bc). If P and R are both integral points on $\mathcal{E}_D$ that correspond to solutions to (7.3), then $P - R \in 2\mathcal{E}_D(\mathbb{Q})$. Moreover, $x(P) > 0$ and $b^2 \mid x(P)$. Theorem 7.6 is a corollary of Theorem 7.2 as $\pm P$ corresponds to the same solution for (7.3).

More general forms of simultaneous Pell equations have been studied previously. For nonzero integers a_1, a_2, b_1, b_2, u, v, let $\mathcal{N}(a_1, a_2, b_1, b_2, u, v)$ denote the number of solutions to the system of equations

$$a_1X^2 - b_1Y^2 = u, \qquad b_2Y^2 - a_2Z^2 = v$$

in positive integers X, Y, Z such that $\gcd(X, Y, Z, u, v) = 1$. Theorem 7.6 provides an upper bound to $\mathcal{N}(a, c, b, b, d, -d)$, where a, b, c, d are pairwise coprime positive integers. Transforming the equations (7.3) by $X \mapsto aX$ and $Z \mapsto cZ$, we get $\mathcal{N}(a, c, b, b, d, -d) = \mathcal{N}(1, 1, ab, bc, ad, -cd)$. Assuming a, b are distinct positive integers and $-av \neq bu$, Bennett [7, Theorem 2.1] showed that

$$\mathcal{N}(1, 1, a, b, u, v) \ll 2^{\min\{\omega(u),\omega(v)\}} \log(|u| + |v|).$$

This implies $\mathcal{N}(a, c, b, b, d, -d) \ll 2^{\omega(d)\min\{\omega(a),\omega(c)\}} \log((a+c)d)$. Bugeaud, Levesque and Waldschmidt [13, Théorème 2.2] gave the bound

$$\mathcal{N}(a_1, a_2, b_1, b_2, u, v) \leq 2 + 2^{3996(\omega(a_1a_2uv)+1)}.$$

Translating to our case, this gives an upper bound $\mathcal{N}(a, c, b, b, d, -d) \leq 2 + 2^{3996(\omega(acd^2)+1)}$.

Theorem 7.6 can also provide an upper bound to a different Diophantine equa-

tion. In 1942, Ljunggren [56] showed that for a fixed integer d, the equation

$$X^4 - dY^2 = 1, \qquad (X, Y) \in \mathbb{Z}^2_{>0},$$

has at most two solutions, through a study of units in certain quadratic and biquadratic fields. More recently, Bennett and Walsh [9] used the theory of linear forms in logarithms of algebraic numbers, to show that for squarefree positive integers $b, d \geq 2$, the equation

$$b^2X^4 - dY^2 = 1, \qquad (X, Y) \in \mathbb{Z}^2_{>0},$$

has at most one solution. We prove the following as a corollary to Theorem 7.6.

Theorem 7.7. *Let A, B, C be pairwise coprime positive squarefree integers. Then there are $\ll 2^{\omega(AB^2C^2)}$ integral solutions (X, Y) to*

$$A^2X^4 - BY^2 = C^2.$$

Proof. Let $g \coloneqq \gcd(X, C)$. Observe that

$$\left(Ag\left(\frac{X}{g}\right)^2 - \frac{C}{g}\right)\left(Ag\left(\frac{X}{g}\right)^2 + \frac{C}{g}\right) = B\left(\frac{Y}{g}\right)^2.$$

The factors on the left hand side have common factor 1 or 2. Therefore we can write

$$Ag\left(\frac{X}{g}\right)^2 - \frac{C}{g} = B_1Y_1^2 \text{ and } Ag\left(\frac{X}{g}\right)^2 + \frac{C}{g} = B_2Y_2^2, \tag{7.4}$$

where B_1 and B_2 are positive integers such that $B_1B_2 = B$ or $4B$, and $Y_1Y_2g = Y$. Now applying Theorem 7.6, the system of equations (7.4) has $\ll 2^{\omega(ABC)}$ solutions. There are $2^{\omega(C)}$ choices of $g \mid C$ and $\ll 2^{\omega(B)}$ choices of pairs (B_1, B_2). This proves Theorem 7.7. □

7.1.1 The *abc* conjecture

In Theorem 7.3, if we are allowed to assume the *abc* conjecture, we can show that there exists some ϵ (determined by the conjecture) such that the set $\mathcal{L}_D(R)$ is empty when D is sufficiently large. The *abc* conjecture states that for every $\epsilon > 0$, for any

pairwise coprime positive integers a, b, c, with $a+b=c$, we have

$$c \ll_\epsilon \prod_{p|abc} p^{1+\epsilon}.$$

Suppose that $(x,y) \in \mathcal{E}_D(\mathbb{Z})$ and $x>0$. Let $g=\gcd(x,D)$. Dividing $y^2=x^3-D^2x$ by xg^2 and rearranging, we have

$$\left(\frac{D}{g}\right)^2 + \frac{y^2}{xg^2} = \left(\frac{x}{g}\right)^2.$$

Assuming the *abc* conjecture,

$$\left(\frac{x}{g}\right)^2 \ll_\epsilon \prod_{p|\left(\frac{D}{g}\right)^2\left(\frac{x}{g}\right)^2\frac{y^2}{xg^2}} p^{1+\epsilon}. \tag{7.5}$$

If $p \mid (\frac{D}{g})^2(\frac{x}{g})^2\frac{y^2}{xg^2}$, then $p \mid (\frac{D}{g})(\frac{x}{g})\frac{y^2}{xg^2} = \frac{Dy^2}{g^4}$. By construction $g \mid D$ and $g^3 \mid y^2$. Since g is squarefree, so $g^2 \mid y$. Therefore $p \mid \frac{Dy}{g^2}$. Putting this back to (7.5),

$$\left(\frac{x}{g}\right)^2 \ll_\epsilon \left(\frac{Dy}{g^2}\right)^{1+\epsilon} < \left(\frac{Dx^{3/2}}{g^2}\right)^{1+\epsilon}.$$

Then for $\epsilon < \frac{1}{15}$, since $g \le D$,

$$x \ll_\epsilon \left(\frac{D^{2(1+\epsilon)}}{g^{4\epsilon}}\right)^{1-3\epsilon} \le D^{2\left(\frac{1+\epsilon}{1-3\epsilon}\right)} < D^{2(1+5\epsilon)}.$$

This proves the last assertion in Theorem 7.3.

7.2 Height estimates

Notice that if $(x,y) \in \mathcal{E}_D(\mathbb{Q})$, then either $x \ge D$ or $-D \le x \le 0$. For $\alpha \in \overline{\mathbb{Q}}$, define height functions $H(\alpha) \coloneqq \prod_v \max\{1, |\alpha|_v\}$ and $h(\alpha) = \log H(\alpha) = \sum_v \log^+ |\alpha|_v$, where v is taken over the set of places of $\mathbb{Q}(\alpha)$ and $\log^+$ is a function on the positive real numbers, defined as $\log^+ t = \max\{0, \log t\}$. For any point $P \in \mathcal{E}_D(\overline{\mathbb{Q}})$, define $H(P) = H(x(P))$, denote the (Weil) height by $h(P) \coloneqq h(x(P))$ and the canonical

height by

$$\hat{h}(P) \coloneqq \lim_{n\to\infty} \frac{h(nP)}{n^2}.^{1}$$

Lemma 7.8. *Let $P \in \mathcal{E}_D(\mathbb{Q})$ be a non-torsion point. Write $x(2P) = \frac{r}{s}$, where r and s are coprime integers and $s > 0$. Then* $\gcd(r, D) = 1$.

Proof. Suppose $P \in \mathcal{E}_D(\mathbb{Q})$, then $\theta(2P) = (1, 1, 1)$, so write

$$x(2P) = \frac{r^2}{s^2}, \qquad x(2P) - D = \frac{u^2}{v^2},$$

where $r, s, u, v \in \mathbb{Z}$ and $\gcd(r, s) = \gcd(u, v) = 1$. Combining gives

$$r^2v^2 - u^2s^2 = Dv^2s^2.$$

We see that $v = s$, since $\gcd(r, s) = \gcd(u, v) = 1$. Rewriting

$$r^2 - u^2 = Ds^2.$$

Since $\gcd(r, s) = \gcd(u, s) = 1$ and D is squarefree, $\gcd(r, D) = 1$. □

We prove for points on $\mathcal{E}_D(\mathbb{Q})$ that the Weil height and the canonical height are close together.

Lemma 7.9. *Let $P = (x, y) \in \mathcal{E}_D(\mathbb{Q}) \setminus \{\mathcal{O}, (0, 0)\}$. Write $x = \frac{r}{s}$, where r and s are coprime integers and $s > 0$. If $x \geq D$, then*

$$-\log|\gcd(r, D)| - 2\log 2 \leq \hat{h}(P) - h(P) \leq -\log|\gcd(r, D)| + \frac{2}{3}\log 2. \tag{7.6}$$

If $-D \leq x < 0$, then

$$\log\left|\frac{D}{\gcd(r, D)}\right| - \log^+|x| - 2\log 2 \leq \hat{h}(P) - h(P) \leq \log\left|\frac{D}{\gcd(r, D)}\right| - \log^+|x| + \frac{2}{3}\log 2. \tag{7.7}$$

In particular,

$$-2\log 2 \leq 4\hat{h}(P) - h(2P) = \hat{h}(2P) - h(2P) \leq \frac{2}{3}\log 2. \tag{7.8}$$

[1] This is sometimes defined with an extra factor of $\frac{1}{2}$ in literature.

Proof. Focusing on the $h(2^nP)$ terms in the limit defining $\hat{h}(P)$, we can express the canonical height as a telescoping series

$$\hat{h}(P) = h(P) - \sum_{n=0}^{\infty} \frac{1}{4^n}\left(h(2^nP) - \frac{1}{4}h(2^{n+1}P)\right). \tag{7.9}$$

Consider a point $P \in \mathcal{E}_D(\mathbb{Q}) \setminus \{\mathcal{O}, (0,0)\}$. Write $x(P) = \frac{r}{s}$, where r, s are coprime integers and $s > 0$. Then

$$x(2P) = \frac{(r^2 + D^2s^2)^2}{4rs(r - Ds)(r + Ds)}.$$

If an odd prime p divides both $(r^2 + D^2s^2)^2$ and $4rs(r - Ds)(r + Ds)$, then since $\gcd(r, s) = 1$, p divides both r and D. If $r^2 + D^2s^2$ is even, either r, D, s are all odd, or r, D are even and s is odd. The first case implies that $r^2 + D^2s^2 \equiv 2 \bmod 8$, so $4 \parallel (r^2 + D^2s^2)^2$. The second case note that D is squarefree so $2 \parallel D$. If $2 \parallel r$ we have $4 \cdot 2^4 \parallel (r^2 + D^2s^2)^2$, otherwise the $2^4 \parallel (r^2 + D^2s^2)^2$.

Therefore

$$\gcd\left((r^2 + D^2s^2)^2, 4rs(r - Ds)(r + Ds)\right) = (\gcd(r, D))^4 \text{ or } 4(\gcd(r, D))^4.$$

Since $x(2P) > D$, we have

$$\begin{aligned} h(2P) &= \log(r^2 + D^2s^2)^2 - \log\gcd\left((r^2 + D^2s^2)^2, 4rs(r - Ds)(r + Ds)\right) \\ &= 2\log(r^2 + D^2s^2) - 4\log\gcd(r, D) - \mathbb{1}_{\{s \text{ odd}\}}\mathbb{1}_{\{\operatorname{ord}_2 r = \operatorname{ord}_2 D\}}2\log 2. \end{aligned} \tag{7.10}$$

We first prove (7.6). Suppose $x(P) \geq D$. Then

$$h(P) - \frac{1}{4}h(2P) = -\frac{1}{2}\log\left(1 + \frac{D^2s^2}{r^2}\right) + \log\gcd(r, D) + \mathbb{1}_{\{s \text{ odd}\}}\mathbb{1}_{\{\operatorname{ord}_2 r = \operatorname{ord}_2 D\}}2\log 2. \tag{7.11}$$

Apply (7.11) to (7.9). Then

$$0 < \log\left(1 + \frac{D^2s^2}{r^2}\right) < \log 2.$$

We know from Lemma 7.8 that $\gcd(r, D) = 1$ for double points. The conditions $2 \nmid s$ and $\operatorname{ord}_2 r = \operatorname{ord}_2 D$ can only hold simultaneously at most once in the sequence

$2^n P$. For if s, r, D are all odd, then subsequent terms would have even s. On the other hand, since the x-coordinates of double points must be squares, $2 \parallel r$ can only happen in the first term. Noting that $\sum_{n=0}^{\infty} \frac{1}{4^n} = \frac{4}{3}$, we get (7.6).

For (7.7), suppose instead $-D < x(P) < 0$. Then from (7.10)

$$\begin{aligned} & h(P) - \frac{1}{4} h(2P) \\ &= \mathbb{1}_{\{r>s\}} \log|x| - \frac{1}{2} \log\left(1 + \frac{r^2}{D^2 s^2}\right) - \log\left|\frac{D}{\gcd(r, D)}\right| + \mathbb{1}_{\{s \text{ odd}\}} \mathbb{1}_{\{\mathrm{ord}_2 r = \mathrm{ord}_2 D\}} 2 \log 2. \end{aligned}$$

Apply this to (7.9). Similar to the argument for (7.6), but here instead

$$0 < \log\left(1 + \frac{r^2}{D^2 s^2}\right) < \log 2,$$

we get (7.7).

Finally (7.8) follows from (7.6) and Lemma 7.8. □

Estimates equivalent to (7.8) were obtained in Section 2 of [12] by analysing the local height functions specifically for $\mathcal{E}_D$. The inequalities (7.6),(7.7) with larger constant terms can be obtained via a study of local heights by applying theorems for general elliptic curves [77, Theorem 4.1, Theorem 5.4], and [76, Theorem 5.2].

For general algebraic points on $\mathcal{E}_D$, we obtain the following estimate by applying [77, Equation(3)], noting that the discriminant of $\mathcal{E}_D$ is $\Delta_D = (2D)^6$ and j-invariant is 1728.

Lemma 7.10. *Any $P \in \mathcal{E}_D(\overline{\mathbb{Q}})$ satisfies*

$$|\hat{h}(P) - h(P)| < \log D + 4.6. \tag{7.12}$$

Since $\hat{h}(2P) = h(2P) + O(1)$ by (7.8), we have

$$\hat{h}(2P) = h(2P) - 2\log 2 \geq \log D - 2\log 2. \tag{7.13}$$

Therefore for any $P \in \mathcal{E}_D(\mathbb{Q}) \setminus \mathcal{T}_D$,

$$\hat{h}(P) \geq \frac{1}{4} \log D - \frac{1}{2} \log 2. \tag{7.14}$$

The equation (7.14) is a version of Lang's conjecture, which says that the canonical height of a non-torsion point on an elliptic curve should satisfy

$$\hat{h}(P) \gg \log|\Delta|,$$

where Δ is the discriminant of the elliptic curve. This conjecture was proven for elliptic curves with integral j-invariant [73], for elliptic curves which are twists [74], and for elliptic curves with bounded Szpiro ratio [41]. The curves $\mathcal{E}_D$ are in all three of these categories, as remarked in [12]. The bound (7.14) for curves $\mathcal{E}_D$ with the explicit constant factor $\frac{1}{4}$ was first given in [12, (11)].

7.3 Bounding small points via spherical codes

In this section we prove the following lemma, which gives the upper bound of $\#\mathcal{S}_D(R)$ for Theorem 7.2.

Lemma 7.11. *Suppose $R \in \mathcal{E}_D(\mathbb{Q})$ with $x(R) > D$. Let $\epsilon < \frac{1}{650}$. Then for any sufficiently large D we have*

$$\#\{P \in R + 2\mathcal{E}_D(\mathbb{Q}) : \hat{h}(P) \leq 2(1+\epsilon)\log D\} < (1.89)^{r+19r^{1/3}}.$$

We know that the the canonical height of the difference between any two distinct points in $R + 2\mathcal{E}_D(\mathbb{Q})$ is at least $\log D + O(1)$ from equation (7.13). Viewing $R + 2\mathcal{E}_D(\mathbb{Q})$ as a Euclidean space $\mathbb{R}^r$ of dimension r, we can bound the number of points by the maximum number of spheres of radius $\frac{1}{2}\sqrt{\log D} + O(1)$ with centres lying inside a sphere S_R^{r-1} of radius $R = \sqrt{2(1+\epsilon)\log D}$.

A *spherical code* in dimension r with minimum angle θ is a set of points on the unit sphere S_1^{r-1} in $\mathbb{R}^r$ with the property that no two points subtend an angle less than θ at the origin. Let $A(r,\theta)$ denote the greatest size of such a spherical code.

We can obtain an upper bound in terms of the function A via a classical argument (see for example the proof of (2.1) in [25]). Project the sphere centres in S_R^{r-1} onto the upper hemisphere of S_R^r orthogonally to the hyperplane. The projections of the sphere centres are still at least distance $\sqrt{\log D} + O(1)$ apart, and thus separated by angles of at least θ, where $\sin\frac{\theta}{2} = \frac{1}{2\sqrt{2(1+\epsilon)}} - o(1)$. Therefore the number of small points is bounded above by $\leq A(r+1,\theta)$.

7.3.1 For large dimensions

Kabatiansky and Levenshtein proved the following upper bound on $A(r,\theta)$.

Theorem 7.12 ([44, (52)]). *Let $r \geq 3$ and $\alpha = \frac{r-3}{2}$, and let t_k^α be the largest root of*

$$P_k^\alpha(t) = \frac{1}{2^k}\sum_{i=0}^{k}\binom{k+\alpha}{i}\binom{k+\alpha}{k-i}(t+1)^i(t-1)^{k-i}.$$

Take any k such that $\cos\theta \leq t_k^\alpha$. Then

$$A(r,\theta) \leq \frac{4}{1-t_{k+1}^\alpha}\binom{k+r-2}{r}.$$

From the proof of [44, Lemma 4], we know that

$$\tau_k - \frac{2\pi^{2/3}}{((k+\alpha)(k+\alpha+1)\tau_k)^{1/3}} \leq t_k^\alpha \leq \tau_k,$$

where

$$\tau_k = \sqrt{1-\frac{\alpha^2-1}{(k+\alpha)(k+\alpha+1)}}.$$

Therefore if we take k such that

$$\cos\theta \leq \tau_k - \frac{2\pi^{2/3}}{((k+\alpha)(k+\alpha+1)\tau_k)^{1/3}}, \tag{7.15}$$

and since $t_{k+1}^\alpha \leq \tau_{k+1}$, we have

$$A(r,\theta) \leq \frac{4}{1-\tau_{k+1}}\binom{k+r-2}{r}.$$

Take θ such that $\sin\frac{\theta}{2} = \frac{1}{2\sqrt{2(1+\epsilon)}} - o(1)$. Let

$$N = \frac{1-\sin\theta}{2\sin\theta} = \frac{2(1-\epsilon)}{\sqrt{7-8\epsilon}} - \frac{1}{2} + o(1),$$

so that

$$\tau_k \to \sqrt{1-\frac{1}{(2N+1)^2}}$$

as $k\to\infty$ and $\frac{k}{r}\to N$.

Fix some

$$C^3 > 16\pi^2 N(N+1)(2N+1)^5 \tag{7.16}$$

Take $k-2=\lfloor rN+Cr^{1/3}\rfloor$, so (7.15) is satisfied for large enough r. By Stirling's formula, we have

$$\binom{k+r-2}{r}\le\frac{e}{2\pi}\frac{(k+r-2)^{k+r-\frac{3}{2}}}{r^{r+\frac{1}{2}}(k-2)^{k-2+\frac{1}{2}}}\le\frac{e}{2\pi\sqrt{r}}\left(1+\frac{1}{N}\right)^{Cr^{1/3}+\frac{1}{2}}\left(\frac{(1+N)^{1+N}}{N^N}\right)^r$$

for large enough r. Therefore for large enough r, we have the upper bound

$$A(r,\theta)<\left(\frac{(1+N)^{1+N}}{N^N}\right)^{r+\frac{\log(1+N)-\log N}{(1+N)\log(1+N)-N\log N}Cr^{1/3}},\tag{7.17}$$

taking some small C in the range (7.16).

We can now prove Lemma 7.11 for $r\ge 2000$. Take $\epsilon<\frac{1}{650}$ and $C=\frac{189}{25}$, so (7.16) is satisfied. Then we can rewrite the bound in (7.17) as $A(r,\theta)<(1.89)^{r+19r^{1/3}}$.

7.3.2 For small dimensions

To prove Lemma 7.11, it remains to check the same bound holds for $r<2000$. The two following bounds, obtained respectively by Rankin and Shannon, are weaker asymptotically when $r\to\infty$ but are better bounds for small r.

Theorem 7.13 ([63, Theorem 2])**.** *If $0<\theta<\frac{\pi}{4}$ and $\sin\beta=\sqrt{2}\sin\theta$, then*

$$\begin{aligned}A(r,\theta)&\le\frac{\sqrt{\pi}\Gamma(\frac{r-1}{2})\sin\beta\tan\beta}{2\Gamma(\frac{r}{2})\int_0^\beta\sin^{r-2}x(\cos x-\cos\beta)dx}\\&\le\frac{2\sqrt{\pi}\Gamma(\frac{r+3}{2})\cos\beta}{\Gamma(\frac{r}{2})\sin^{r-1}\beta(1-\frac{3}{r+3}\tan^2\beta)}\sim\frac{\sqrt{\frac{1}{2}\pi r^3\cos 2\theta}}{(\sqrt{2}\sin\theta)^{r-1}}.\end{aligned}$$

Theorem 7.14 ([71, (21),(27)])**.** *Suppose $0<\theta<\frac{\pi}{2}$. Then*

$$A(r,\theta)\le\frac{\sqrt{\pi}\Gamma(\frac{r-1}{2})}{\Gamma(\frac{r}{2})\int_0^\theta\sin^{r-2}x\,dx}\le\frac{2\sqrt{\pi}\Gamma(\frac{r+1}{2})\cos\theta}{\Gamma(\frac{r}{2})\sin^{r-1}\theta(1-\frac{1}{r}\tan^2\theta)}\sim\frac{\sqrt{2\pi r}\cos\theta}{\sin^{r-1}\theta}.$$

Evaluating the bounds in Theorems 7.13 and 7.14 for $r<2000$ proves Lemma 7.11 in those cases.

7.4 Repulsion between medium points

Suppose $P=(X,Y)$ and $R=(x,y)$ are integral points in the same coset of $2\mathcal{E}_D(\mathbb{Q})$. Assume $D^{2(1+\epsilon)}<x<X$ and $Yy>0$. Suppose $P=2Q+R$ for some $Q\in\mathcal{E}_D(\mathbb{Q})$.

Replacing Q with one of $Q+(0,0)$, $Q+(D,0)$, $Q+(-D,0)$ if necessary, we can assume $x(Q) > (1+\sqrt{2})D$.

Lemma 7.15. *Suppose $P=(X,Y)$, $R=(x,y)\in\mathcal{E}_D(\mathbb{Q})$ and $D<x\le X$. Let $B=\frac{X}{x}>1$ and $\mu=\frac{D^2}{x^2}$. Then*

$$x(P+R)\ge\left(\frac{B+\mu}{\sqrt{B^2-\mu}+\sqrt{B(1-\mu)}}\right)^2 x. \tag{7.18}$$

Also this lower bound is always greater than $\frac{1}{4}x$.

Proof. First suppose $Yy>0$. Without loss of generality assume $y,Y>0$. Then

$$x(P+R)=\left(\frac{\sqrt{B^2-\mu}-\sqrt{B(1-\mu)}}{B-1}\right)^2 x=\left(\frac{B+\mu}{\sqrt{B^2-\mu}+\sqrt{B(1-\mu)}}\right)^2 x>\frac{1}{4}x.$$

If instead $Yy<0$, the lemma follows from the fact that $x(P+R)>x(P-R)$. □

We now show that $x(Q+R)$ is properly bounded away from D. If $(1+\sqrt{2})D<x(Q)<4(1+\sqrt{2})D$, since we assumed $x(R)>D^{2(1+\epsilon)}$, by (7.18) we have $x(Q+R)>\frac{3}{4}(1+\sqrt{2})D$ for large enough D. If $x(Q)\ge 4(1+\sqrt{2})D$, then $x(Q+R)\ge(1+\sqrt{2})D$ by Lemma 7.15.

Lemma 7.16. *Suppose $Q\in\mathcal{E}_D(\mathbb{Q})$. Assume $x(Q)>\frac{1}{\delta}D$, where $\delta>1$. Then*

$$\frac{1}{4}x(Q)\le x(2Q)\ll_\delta x(Q).$$

Proof. This follows immediately from the formula

$$x(2Q)=\frac{\left(1+(\frac{D}{x(Q)})^2\right)^2}{4\left(1-(\frac{D}{x(Q)})^2\right)}x(Q).$$ □

Trivially $h(Q)\ge\log x(Q)$ and $h(Q+R)\ge\log x(Q+R)$. By Lemma 7.16 and the lower bounds on $x(Q)$ and $x(Q+R)$, we have $x(Q)\gg x(2Q)=x(P-R)$ and $x(Q+R)\gg x(2Q+2R)=x(P+R)$. Also $x(P\pm R)\gg x$ by Lemma 7.15. Putting together we have $h(Q),h(Q+R)\ge\log x+O(1)$. Now apply (7.6) to P and $P-R$, then to Q and $Q+R$, it follows that

$$\log X+\log x+O(1)\ge\hat{h}(P)+\hat{h}(R)=2\hat{h}(Q)+2\hat{h}(Q+R)\ge 4\log x-4\log D+O(1).$$

Rearranging gives

$$\log X \geq 3\log x - 4\log D + O(1). \tag{7.19}$$

7.5 Large integral points giving Diophantine approximations

In this section we will prove the following lemma.

Lemma 7.17. *Suppose $P \in \mathcal{E}_D(\mathbb{Z})$ such that $P = 4\tilde{Q} + R$, for some $\tilde{Q} \in \mathcal{E}_D(\overline{\mathbb{Q}})$ and $R \in \mathcal{E}_D(\mathbb{Q}) \setminus 2\mathcal{E}_D(\mathbb{Q})$. Assume $h(P) > \max\{\frac{1}{\lambda}h(R), \frac{1}{\delta}\log D\}$ and $x(R) > D$. Take $S \in \{\tilde{S} \in \mathcal{E}_D(\overline{\mathbb{Q}}) : 4\tilde{S} = R\}$ such that $|x(\tilde{Q}) - x(S)|$ is minimum. Then*

$$\frac{\log|x(\tilde{Q}) - x(S)|}{h(\tilde{Q})} \leq -8 \cdot \frac{1 - 63\lambda - 418\delta}{(1+\sqrt{\lambda})^2(1+\delta) + 16\delta} + o(1).$$

Suppose $P \in \mathcal{E}_D(\mathbb{Z})$ such that $P = 4\tilde{Q} + R$, for some $\tilde{Q} \in \mathcal{E}_D(\overline{\mathbb{Q}})$ and $R \in \mathcal{E}_D(\mathbb{Q})$. Assume $h(R) < \lambda h(P)$, $x(P) > D^{1/\delta}$ and $x(R) > D$. Then $x(\tilde{Q}) \ll x(2Q) = x(P - R) \ll_\lambda x(R)$.

7.5.1 Height estimates

Applying estimates (7.12) to

$$4\sqrt{\hat{h}(\tilde{Q})} - \sqrt{\hat{h}(R)} \leq \sqrt{\hat{h}(P)} \leq 4\sqrt{\hat{h}(\tilde{Q})} + \sqrt{\hat{h}(R)},$$

also using $h(R) < \lambda h(P)$ and squaring, we have

$$(1-\sqrt{\lambda})^2(1-\delta) - 16\delta - o(1) \leq \frac{16h(\tilde{Q})}{h(P)} \leq (1+\sqrt{\lambda})^2(1+\delta) + 16\delta + o(1). \tag{7.20}$$

7.5.2 Approximation of algebraic numbers

If $S \in \mathcal{E}_D(\overline{\mathbb{Q}})$ such that $4S = R$, write

$$x(R) = x(4S) = \frac{\phi_4(S)}{\psi_4(S)^2},$$

where ψ_n is the nth-division polynomial of $\mathcal{E}_D$ and $\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$. Define

$$f_R(T) \coloneqq \prod_{S:4S=R} (T - x(S)) = \phi_4(T) - x(R)\psi_4(T)^2.$$

The two expressions are equivalent as they are both are monic polynomials of degree 16 with roots $\{x(S) \in \mathcal{E}_D(\overline{\mathbb{Q}}) : 4S = R\}$. Put $T = x(\tilde{Q})$, then

$$\prod_{4S=R} (x(\tilde{Q}) - x(S)) = \phi_4(\tilde{Q}) - x(R)\psi_4(\tilde{Q})^2.$$

Substitute $\phi_4(\tilde{Q}) = \psi_4(\tilde{Q})^2 x(4\tilde{Q})$, we get

$$\prod_{4S=R} (x(\tilde{Q}) - x(S)) = \psi_4(\tilde{Q})^2 (x(4\tilde{Q}) - x(R)). \tag{7.21}$$

Now

$$\begin{aligned} x(P) = x(4\tilde{Q} + R) &= \left(\frac{y(4\tilde{Q}) - y(R)}{x(4\tilde{Q}) - x(R)} \right)^2 - x(4\tilde{Q}) - x(R) \\ &= \frac{-y(4\tilde{Q})y(R) + x(4\tilde{Q})^2 x(R) + x(4\tilde{Q})x(R)^2 - D^2(x(4\tilde{Q}) + x(R))}{(x(4\tilde{Q}) - x(R))^2}. \end{aligned}$$

Using (7.21), we have

$$\begin{aligned} & x(P) \left(\prod_{4S=R} (x(\tilde{Q}) - x(S)) \right)^2 \\ &\quad = \psi_4(\tilde{Q})^4 \left(-y(4\tilde{Q})y(R) + x(4\tilde{Q})^2 x(R) + x(4\tilde{Q})x(R)^2 - D^2(x(4\tilde{Q}) + x(R)) \right) \\ &\quad \ll x(4\tilde{Q})x(R)^2 \max\{x(\tilde{Q}), D\}^{2(4^2-1)} \ll x(R)^{33} \ll x(P)^{33\lambda}. \end{aligned}$$

Taking logs,

$$\frac{\log \prod_{4S=R} |x(\tilde{Q}) - x(S)|}{h(P)} \leq -\frac{1}{2} + \frac{33}{2}\lambda + O\left(\frac{\delta}{\log D} \right). \tag{7.22}$$

Let $\alpha = x(S)$ be a root of f_R. Apply [57, p.262 last line],

$$|f_R'(\alpha)| \gg |\Delta(f_R)|^{1/2} \|f_R\|_1^{-14},$$

where $\Delta(\cdot)$ denotes the discriminant and $\|\cdot\|_1$ denotes the ℓ_1-norm. Write $x(R) = \frac{r}{s}$, where $\gcd(r, s) = 1$. Since $s f_R(T) \in \mathbb{Z}[T]$, so $|\Delta(f_R)| \geq s^{-30}$. Also we can check

that $\|f_R\|_1 \ll D^{14}\max\{x(R), D^2\}$. Therefore noting that $H(R) = r \geq Ds$,

$$\prod_{\tilde{S}\neq S:4\tilde{S}=R} |x(\tilde{S})-x(S)| = |f_R'(\alpha)| \gg |s|^{-15}(D^{14}\max\{x(R), D^2\})^{-14} \geq H(R)^{-15}D^{-209}.$$

Take $S \in \{\tilde{S} \in \mathcal{E}_D(\overline{\mathbb{Q}}) : 4\tilde{S} = R\}$ such that $|x(\tilde{Q}) - x(S)|$ is minimum. By the triangle inequality

$$|x(S) - x(\tilde{S})| \leq |x(\tilde{Q}) - x(S)| + |x(\tilde{Q}) - x(\tilde{S})| \leq 2|x(\tilde{Q}) - x(\tilde{S})|.$$

Taking products

$$\prod_{\tilde{S}\neq S:4\tilde{S}=R} |x(\tilde{Q}) - x(\tilde{S})| \gg \prod_{\tilde{S}\neq S:4\tilde{S}=R} |x(S) - x(\tilde{S})| \gg H(R)^{-15}D^{-209}.$$

Take logs

$$\log \prod_{\tilde{S}\neq S:4\tilde{S}=R} |x(\tilde{Q}) - x(\tilde{S})| \geq -15h(R) - 209\log D + O(1).$$

Put this back to (7.22),

$$\frac{\log|x(\tilde{Q}) - x(S)|}{h(P)} \leq -\frac{1}{2} + \frac{63}{2}\lambda + 209\delta + o(1).$$

Applying the upper bound in (7.20) proves Lemma 7.17.

7.6 Roth's Theorem

In this section we follow the proof of Roth's Theorem in Chapter 6 of [11], specialising in the bivariate case.

Let $K \subseteq E$ be number fields such that $m \coloneqq [E : K]$. Suppose $\alpha \in E$. Let $|\cdot|$ be the ordinary absolute value on $\mathbb{C}$. Let $\mathcal{S}$ be a set containing exactly one infinite place of K, i.e. an embedding $K \hookrightarrow \mathbb{C}$. We call $\beta \in K$ a *K-approximation to α with exponent κ*, if

$$|\beta - \alpha| < H(\beta)^{-\kappa}.$$

Approximations obey the following strong gap principle.

Theorem 7.18 (strong gap principle [11, Theorem 6.5.4])**.** *Let $\beta, \beta' \in K$ be distinct*

elements such that $|\alpha-\beta|<H(\beta)^{-\kappa}$, $|\alpha-\beta'|<H(\beta')^{-\kappa}$ *and* $h(\beta')\geq h(\beta)$. *Then*

$$h(\beta')\geq -2\log 2+(\kappa-1)h(\beta).$$

Proof. We have

$$\begin{aligned}\log|\beta-\beta'|=\log|(\alpha-\beta')-(\alpha-\beta)|&\leq \max\big(\log|\alpha-\beta'|,\log|\alpha-\beta|\big)+\log 2\\&\leq -\kappa\min\big(h(\beta'),h(\beta)\big)+\log 2=-\kappa h(\beta)+\log 2.\end{aligned}$$

Also

$$\log|\beta-\beta'|\geq -h(\beta-\beta')\geq -h(\beta)-h(\beta')-\log 2. \qquad \square$$

Theorem 7.19. *Let* $c<1$, $M\geq 72$ *and* $L=(\frac{h(\alpha)+\log 2}{c^{-2}-1}+4)M$. *Assume*

$$\kappa>\left(c-4\sqrt{\frac{m}{M}}\right)^{-1}\left(1+\frac{c^{-2}+1}{M}\right)\sqrt{2m}. \tag{7.23}$$

Suppose $\beta_1,\beta_2\in K$ *are both approximations to* $\alpha\in E$ *with exponent* κ. *If* $h(\beta_1)\geq L$, *then* $h(\beta_2)<Mh(\beta_1)$.

We prove Theorem 7.19 by contradiction. Suppose we can find β_1,β_2 under the assumptions in Theorem 7.19, and such that $h(\beta_1)\geq L$ and $h(\beta_2)\geq Mh(\beta_1)$. Let $\sigma\coloneqq\sqrt{\frac{2}{M}}$ and $t\coloneqq c\sqrt{\frac{2}{m}}$.

7.6.1 The auxiliary polynomial

Take N large. Choose

$$d_j=\left\lfloor\frac{N}{h(\beta_j)}\right\rfloor \text{ for } j=1,2.$$

Let $t<1$, $\boldsymbol{\alpha}=(\alpha,\alpha)\in E^2$ and $\boldsymbol{\beta}=(\beta_1,\beta_2)\in K^2$. Let

$$V_2(t)\coloneqq \mathrm{vol}\left(\{(x_1,x_2):x_1+x_2\leq t,\ 0\leq x_j\leq 1\}\right)=\frac{1}{2}t^2.$$

For a polynomial $F(x_1,x_2)=\sum_{\mathbf{j}}a_{\mathbf{j}}\mathbf{x}^{\mathbf{j}}\in\overline{\mathbb{Q}}[x_1,x_2]$, define $|F|_v=\max_{\mathbf{j}}|a_{\mathbf{j}}|_v$, $H(F)\coloneqq\prod_v|F|_v$ and $h(F)=\log H(F)$.

We apply the following lemma to construct an auxiliary polynomial.

Lemma 7.20 ([11, Lemma 6.3.4])**.** *Suppose* $mV_2(t)<1$. *Then for all sufficiently large* $d_1,d_2\in\mathbb{Z}$, *there exist* $F\in K[x_1,x_2]$, $F\not\equiv 0$, *with partial degrees at most* d_1,d_2

such that

$$\operatorname{ind}(F;\mathbf{d},\boldsymbol{\alpha}) \coloneqq \min_{\boldsymbol{\mu}} \left\{ \frac{\mu_1}{d_1} + \frac{\mu_2}{d_2} : \partial_\mu F(\boldsymbol{\alpha}) \neq 0 \right\} \geq t;$$

and

$$h(F) \leq \frac{mV_2(t)}{1-mV_2(t)} \sum_{j=1}^{2} (h(\alpha_j) + \log 2 + o(1)) d_j,$$

as $d_j \to \infty$.

Since $\frac{1}{2}mt^2 < 1$, we have

$$\frac{mV_2(t)}{1-mV_2(t)} \leq \frac{mt^2}{2-mt^2} = \frac{1}{2m^{-1}t^{-2}-1}.$$

Take $C_1 \coloneqq \frac{h(\alpha)+\log 2}{c^{-2}-1}$, so $L = (C_1+4)M$. Then we can obtain a non-trivial polynomial $F \in K[x_1, x_2]$ with partial degrees at most d_1, d_2 such that

$$\operatorname{ind}(F;\mathbf{d},\boldsymbol{\alpha}) \geq t \quad \text{and} \quad h(F) < \frac{2C_1N}{L}. \tag{7.24}$$

7.6.2 Non-vanishing at the rational point

Next we apply Roth's lemma to construct a suitable derivative of F that does not vanish at β.

Lemma 7.21 (Roth's lemma [11, Lemma 6.3.7])**.** *Let* $F \in \overline{\mathbb{Q}}[x_1, x_2]$ *with partial degrees at most* d_1, d_2 *and* $F \not\equiv 0$. *Let* $(\xi_1, \xi_2) \in \overline{\mathbb{Q}}^2$ *and* $0 < \sigma^2 \leq \frac{1}{2}$. *Suppose that* $d_2 \leq \sigma^2 d_1$ *and* $\min_j d_j h(\xi_j) \geq \sigma^{-2}(h(F) + 8d_1)$. *Then* $\operatorname{ind}(F;\mathbf{d},\boldsymbol{\xi}) \leq 4\sigma$.

Since $L \geq 2\sigma^{-2}(C_1+4)$ and $M \geq 2\sigma^{-2}$, we can apply the lemma to get $\operatorname{ind}(F;\mathbf{d},\boldsymbol{\beta}) \leq 4\sigma$. Now we can take $\boldsymbol{\mu}$ such that $\partial_{\boldsymbol{\mu}} F(\boldsymbol{\beta}) \neq 0$ and $\frac{\mu_1}{d_1} + \frac{\mu_2}{d_2} = \operatorname{ind}(F;\mathbf{d},\boldsymbol{\beta})$. Let $G = \partial_{\boldsymbol{\mu}} F$. Since $\operatorname{ind}(G;\mathbf{d},\boldsymbol{\alpha}) \geq \operatorname{ind}(F;\mathbf{d},\boldsymbol{\alpha}) - \frac{\mu_1}{d_1} - \frac{\mu_2}{d_2}$ by [11, 6.3.2(c)], we deduce from (7.24) that

$$\operatorname{ind}(G;\mathbf{d},\boldsymbol{\alpha}) \geq t - 4\sigma, \qquad G(\beta) \neq 0, \quad \text{and} \quad h(G) \leq \frac{4C_1N}{L}. \tag{7.25}$$

7.6.3 The upper bound

For places $v \notin \mathcal{S}$, we have

$$\log |G(\boldsymbol{\beta})|_v \leq \log |G|_v + \sum_{j=1}^{2} d_j (\log^+ |\beta_j|_v + \varepsilon_v o(1)), \tag{7.26}$$

where $o(1) \to 0$ as $d_j \to \infty$, and

$$\varepsilon_v = \begin{cases} \frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} & \text{if } v \text{ is archimedean} \\ 0 & \text{if } v \text{ is non-archimedean.} \end{cases}$$

For $v \in \mathcal{S}$, expand G in Taylor series with center $\boldsymbol{\alpha}$

$$G(\boldsymbol{\beta}) = \sum_{\mathbf{k}} \partial_{\mathbf{k}} G(\boldsymbol{\alpha})(\beta_1 - \alpha)^{k_1}(\beta_2 - \alpha)^{k_2}. \tag{7.27}$$

We have from (7.25), that

$$\partial_{\mathbf{k}} G(\boldsymbol{\alpha}) = 0 \quad \text{if} \quad \frac{k_1}{d_1} + \frac{k_2}{d_2} < t - 4\sigma,$$

and

$$\log |\partial_{\mathbf{k}} G(\boldsymbol{\alpha})| \le \log |G|_v + \sum_{j=1}^{2} (d_j - k_j) \log^+ |\alpha| + \varepsilon_v (\log 2 + o(1)) d_j,$$

so putting back to (7.27) and taking absolute values and logs,

$$\begin{aligned} \log |G(\boldsymbol{\beta})| &\le \max_{\mathbf{k}} \log \left| \partial_{\mathbf{k}} G(\boldsymbol{\alpha}) \prod_{j=1}^{2} (\beta_j - \alpha)^{k_j} \right| + \varepsilon_v \sum_{j=1}^{2} \log(d_j + 1) \\ &\le - \min_{\frac{k_1}{d_1} + \frac{k_2}{d_2} \ge t - 4\sigma} \left(\sum_{j=1}^{2} k_j \log^+ \frac{1}{|\beta_j - \alpha|} \right) + \log |G|_v \\ &\qquad + \sum_{j=1}^{2} \left(\log^+ |\beta_j| + \log^+ |\alpha| + \varepsilon_v (\log 2 + o(1)) \right) d_j. \end{aligned} \tag{7.28}$$

Adding up the bounds (7.26) and (7.28) for all places $v \in \mathcal{M}_{\mathbb{Q}}$, and noting that $\sum_v \varepsilon_v = 1$, we have

$$\begin{aligned} \sum_{v \in \mathcal{M}_{\mathbb{Q}}} \log |G(\boldsymbol{\beta})|_v &\le - \min_{\frac{k_1}{d_1} + \frac{k_2}{d_2} \ge t - 4\sigma} \left(\sum_{j=1}^{2} k_j \log^+ \frac{1}{|\beta_j - \alpha|} \right) + h(G) \\ &\qquad + \sum_{j=1}^{2} \left(h(\beta_j) + \log^+ |\alpha| + 2 \log 2 + o(1) \right) d_j \\ &\le - \min_{\frac{k_1}{d_1} + \frac{k_2}{d_2} \ge t - 4\sigma} \left(\sum_{j=1}^{2} k_j \log^+ \frac{1}{|\beta_j - \alpha|} \right) + \left(2 + \frac{C_2}{L} \right) N + o(N), \end{aligned}$$

where $C_2 = 4C_1 + 4\log 2 + 2\log^+ |\alpha|$.

Since

$$\kappa h(\beta_j) \le \log^+ \frac{1}{|\beta_j - \alpha|},$$

we have

$$\sum_{j=1}^{2} k_j \log^+ \frac{1}{|\beta_j - \alpha|} \ge \kappa \sum_{j=1}^{2} (h(\beta_j) d_j) \frac{k_j}{d_j} \sim N\kappa \left(\frac{k_1}{d_1} + \frac{k_2}{d_2} \right).$$

This gives us the upper bound

$$\sum_{v \in \mathcal{M}_{\mathbb{Q}}} \log |G(\boldsymbol{\beta})|_v \le -\kappa (t - 4\sigma) N + \left(2 + \frac{C_2}{L} \right) N + o(N). \tag{7.29}$$

7.6.4 Obtaining the bound

Since $G(\boldsymbol{\beta}) \neq 0$, we have $\sum_v \log |G(\boldsymbol{\beta})|_v = 0$. Put this into (7.29) and let $N \to \infty$, we get

$$-\kappa \left(\frac{t}{2} - 2\sigma \right) + 1 + \frac{C_2}{2L} \ge 0.$$

Since by assumption $\sigma < \frac{1}{6}$, we have

$$\kappa \le \left(\frac{t}{2} - 2\sigma \right)^{-1} \left(1 + \frac{C_2}{2L} \right),$$

which contradicts (7.23). The completes the proof of Theorem 7.19.

7.7 Bounding the number of points

In this section we prove the explicit upper bound of $\#\mathcal{L}_D(R)$ given in Theorem 7.3, when $x(R) > D$ and $R \notin \mathcal{T}_D + 2\mathcal{E}_D(\mathbb{Q})$. Take R to be the point with minimum canonical height in the coset $R + 2\mathcal{E}_D(\mathbb{Q})$. Let $\epsilon = 0.00153$, which satisfies the assumption in Lemma 7.11.

For each $\tilde{Q} \in \frac{1}{2}\mathcal{E}_D(\mathbb{Q})$, define $L_{\tilde{Q}} \coloneqq (\frac{h(S)+\log 2}{c^{-2}-1} + 4)M$ as in Theorem 7.19, where S is chosen in $\frac{1}{4}R$ such that $|x(S) - x(\tilde{Q})|$ is minimum, with absolute constants M and c to be specified later. We bound the number of medium points

$$\mathcal{A}_1 \coloneqq \left\{ P \in \mathcal{L}_D(R) : h(\tilde{Q}) < L_{\tilde{Q}} \text{ for some } \tilde{Q} \in \frac{1}{4}(P - R) \right\}$$

and large points

$$\mathcal{A}_2 \coloneqq \Big\{P \in \mathcal{L}_D(R) : h(\tilde{Q}) \geq L_{\tilde{Q}} \text{ for all } \tilde{Q} \in \frac{1}{4}(P-R)\Big\}.$$

For each $S \in \frac{1}{4}R$, define

$$\mathcal{B}_2(S) \coloneqq \Big\{\tilde{Q} \in \frac{1}{2}\mathcal{E}_D(\mathbb{Q}) : 4\tilde{Q}+R \in \mathcal{A}_2,\ |x(S)-x(\tilde{Q})| \text{ minimum over } S \in \frac{1}{4}R\Big\}.$$

7.7.1 Medium points

Let $P_1, P_2, \ldots, P_s$ be points in $\mathcal{A}_1$ with strictly increasing height. Applying (7.19) repeatedly,

$$\hat{h}(P_s) > \left(1 - \frac{2\log D + O(1)}{\hat{h}(P_1)}\right) 3^{s-1}\hat{h}(P_1) = \left(\frac{\epsilon}{1+\epsilon} - o(1)\right) 3^{s-1}\hat{h}(P_1). \tag{7.30}$$

Take $\lambda > \frac{1+\epsilon}{3^{s-1}\epsilon}$ and $\delta > \frac{1}{2\cdot 3^{s-1}\epsilon}$, so that $\lambda h(P_s) > h(P_1) > h(R)$ and $\delta h(P_s) > \frac{1}{2(1+\epsilon)}h(P_1) > \log D$.

For each $S \in \frac{1}{4}R$, since $16\hat{h}(S) = \hat{h}(R) \leq \hat{h}(P_1)$, we have by (7.12)

$$h(S) < \frac{1}{16}h(P_1) + \log D - o(1).$$

Writing $P_s = 4\tilde{Q}_s + R$ and using the lower bound in (7.20),

$$\begin{aligned}\frac{1}{16}h(P_s)\left((1-\sqrt{\lambda})^2(1-\delta) - 16\delta - o(1)\right) &\leq h(\tilde{Q}_s) \\ &< L_{\tilde{Q}_s} < \left(\frac{\frac{1}{16}h(P_1) + \log D + \log 2 + o(1)}{c^{-2}-1} + 5\right) M.\end{aligned}$$

Now apply (7.30) and divide both sides by $\frac{1}{16}h(P_1)$,

$$\left(\frac{\epsilon}{1+\epsilon} - o(1)\right) 3^{s-1}\left((1-\sqrt{\lambda})^2(1-\delta) - 16\delta + o(1)\right) < \left(1 + \frac{8}{1+\epsilon} + o(1)\right)\frac{M}{c^{-2}-1}.$$

Simplifying we have

$$3^{s-1} < \left(1+\frac{9}{\epsilon}\right)\frac{M}{(c^{-2}-1)\left((1-\sqrt{\lambda})^2(1-\delta) - 16\delta\right)} + o(1). \tag{7.31}$$

Therefore taking s to be the maximum integer satisfying (7.31), then $\#\mathcal{A}_1 \leq 2s$, where the factor of 2 comes from the possible existence of $-P_1, \ldots, -P_s$.

7.7.2 Large points

Now fix some $S \in \frac{1}{4}R$ and consider the set $\mathcal{B}_2(S)$. Let K be the minimal number field containing the x-coordinates of all points in $\frac{1}{2}\mathcal{E}_D(\mathbb{Q})$, and let E be the field $K(x(S))$.

Suppose $\tilde{Q} \in \mathcal{B}_2(S)$. Fix $\lambda = 0.000137$, $\delta = 0.0000684$, and take $\kappa = 7.516$, which satisfies

$$\kappa < 8 \cdot \frac{1 - 63\lambda - 418\delta}{(1+\sqrt{\lambda})^2(1+\delta) + 16\delta} + o(1),$$

then Lemma 7.17 implies that $x(\tilde{Q})$ is a K-approximation to $x(S)$ with exponent κ. Now we can apply Theorem 7.19 with $m = [E : K] \leq 4$, $M = 276.1$ and $c = 0.861$, noting that (7.23) is satisfied. Take $\beta_1 = x(\tilde{Q})$ such that $h(\tilde{Q})$ is minimum over all $\tilde{Q} \in \mathcal{B}_2(S)$. Then Theorem 7.19 shows that all points in $\mathcal{B}_2(S)$ must have height in the interval $[h(\beta_1), Mh(\beta_1)]$. By Theorem 7.18, if t is the smallest integer such that

$$(\kappa - 1)^t > M,$$

then $\#\mathcal{B}_2(S) \leq t$. This is achieved by $t = 3$. There are 16 choices of S, but since $\mathcal{E}_D(\overline{\mathbb{Q}})[4] \subseteq \frac{1}{2}\mathcal{E}_D(\mathbb{Q})$, if $x(\mathbb{Q})$ is a K-approximation to $x(S)$, then $x(\mathbb{Q}+T)$ is also a K-approximation to $x(S+T)$ for any $T \in \mathcal{E}_D(\overline{\mathbb{Q}})[4]$. Therefore $\#\mathcal{A}_2 \leq 3$.

Returning to the medium points with our choice of constants, we have $\#\mathcal{A}_1 \leq 28$. If $P \in \mathcal{E}_D(\mathbb{Z})$ then $-P \in \mathcal{E}_D(\mathbb{Z})$, so $\#(\mathcal{A}_1 \cup \mathcal{A}_2) \leq 30$.

7.8 Integral points in other cosets of $2\mathcal{E}_D(\mathbb{Q})$

We now prove the upper bounds in Theorem 7.4.

7.8.1 Cosets with respect to a non-torsion point

Here we will treat the case in Theorem 7.4 ((iv)), assuming $R \notin \mathcal{T}_D + 2\mathcal{E}_D(\mathbb{Q})$. Suppose $x(R) < 0$. If $P \in \mathcal{Z}_D(R)$, then $-D < x(P) < 0$ and so $\hat{h}(P) < \log D + \frac{2}{3}\log 2$ by (7.7). Following the argument in Section 7.3, we obtain an upper bound of $A(r+1, \theta)$ where $\sin\frac{\theta}{2} = \frac{1}{2}\sqrt{\frac{\log D - 2\log 2}{\log D + \frac{2}{3}\log 2}} = \frac{1}{2} - o(1)$. For $D \geq 97353$, applying the following estimate by Rankin gives us an upper bound of 3. Since non-torsion integral points in comes in pairs of $\pm P$, we can reduce the upper bound to 2 if

$R \notin \mathcal{T}_D + 2\mathcal{E}_D(\mathbb{Q})$.

Theorem 7.22 ([63, Lemma 2])**.** *If $\frac{\pi}{4} < \theta < \frac{\pi}{2}$, then*

$$A(r,\theta) \leq \frac{2\sin^2\theta}{2\sin^2\theta - 1}.$$

Checking all the integral points in the range $-D < x(P) < 0$ on $\mathcal{E}_D$ for each $D < 97353$, we see that the only exceptions are those listed in Theorem 7.4 ((iv)).

7.8.2 Integral points in $2\mathcal{E}_D(\mathbb{Q}) + \mathcal{T}_D$

We now prove cases ((i)), ((ii)) and ((iii)) in Theorem 7.4. We first show that if a rational point has a multiple which is an integral point, then the original point must also be integral.

Lemma 7.23. *Suppose $P \in \mathcal{E}_D(\mathbb{Q})$. If $mP \in \mathcal{E}_D(\mathbb{Z})$ for some integer $m \geq 2$, then $P \in \mathcal{E}_D(\mathbb{Z})$.*

Proof. Suppose $P = mQ$, where $Q \in \mathcal{E}_D(\mathbb{Q})$. We have

$$x(P) = \frac{\phi_m(Q)}{\psi_m(Q)^2},$$

where ψ_m is the mth division polynomial, and $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$ as usual. The polynomials $\phi_m(x)$ and $\psi_m(x)^2$ have leading terms x^{m^2} and $m^2x^{m^2-1}$ respectively. Putting $x(Q) = \frac{u}{v}$ with $\gcd(u,v) = 1$, and clearing denominators we have

$$x(Q) = \frac{u^{m^2} + vF(u,v)}{v(m^2u^{m^2-1} + vG(u,v))},$$

for some polynomials $F, G \in \mathbb{Z}[x,y]$. Therefore $x(P) \in \mathbb{Z}$ implies $v \mid u$, so $v = 1$ and Q is also integral. □

We show that $2\mathcal{E}_D(\mathbb{Q})$ contains no integral points.

Lemma 7.24. *Suppose $P \in \mathcal{E}_D(\mathbb{Q})$ is non-torsion. Then $2P \notin \mathcal{E}_D(\mathbb{Z})$.*

Proof. Suppose $P \in \mathcal{E}_D(\mathbb{Q})$ and $2P \in \mathcal{E}_D(\mathbb{Z})$, then P must be an integral point by Lemma 7.23. Write $P = (x,y)$, so

$$x(2P) = \left(\frac{x^2 + D^2}{2y}\right)^2.$$

Suppose $2P \in \mathcal{E}_D(\mathbb{Z})$. Then $4y^2 = 4x(x+D)(x-D) \mid (x^2+D^2)^2$. Therefore $x \mid D$ and so x is squarefree. Write $d = -\frac{D}{x}$, and we have $4(d-1)(d+1) \mid x(d^2+1)^2$. Since we assumed that P is not a torsion point, $x \neq D$ and $-D < x < 0$. Suppose d is odd, then $(d^2+1)^2 \equiv 4 \bmod 8$ and $8 \mid (d-1)(d+1)$, so $8 \mid x$, but this contradicts with x being squarefree. Now suppose d is even, then $(d^2+1)^2$ is odd, so $4 \mid x$, which is also a contradiction. □

We now look at points of the form $2P + (-D, 0)$ or $2P + (0, 0)$.

Lemma 7.25. *Suppose $P \in \mathcal{E}_D(\mathbb{Q})$. For each $T \in \{(-D,0),\ (0,0)\}$, we have $2P + T \in \mathcal{E}_D(\mathbb{Z})$ if and only if P is a torsion point.*

Proof. Notice that $\theta(2P + (0,0)) = (-D, -1, D)$ and $\theta(2P + (-D,0)) = (-2D, -D, 2)$. If $2P + (-D,0) \in \mathcal{E}_D(\mathbb{Z})$, taking $x(2P + (0,0)) = -s^2$, we see that the equation

$$s^2 + Dt^2 = D$$

is solvable for $s, t \in \mathbb{Z}$. Similarly if $2P + (0,0) \in \mathcal{E}_D(\mathbb{Z})$, taking $x(2P + (-D,0)) = -Du^2$, then

$$Du^2 + 2v^2 = D$$

is solvable for $u, v \in \mathbb{Z}$. The only solutions to each of these equations over the integers are given by $s = 0$ and $u^2 = 1$. This implies that in both cases P is a torsion point. □

The only possible non-torsion integral points in $2\mathcal{E}_D(\mathbb{Q}) + \mathcal{T}_D$ are in $(D,0) + 2\mathcal{E}_D(\mathbb{Q})$ and satisfies the property in the following theorem.

Lemma 7.26. *Then there exists some $P \in \mathcal{E}_D(\mathbb{Q})$ such that $2P + (D,0) \in \mathcal{E}_D(\mathbb{Z})$ if and only if the system*

$$s^2 - 1 = 2Du^2, \qquad s^2 + 1 = 2v^2 \tag{7.32}$$

is solvable for some $s, u, v \in \mathbb{Z}_{>0}$. Furthermore, (7.32) has at most one solution for each D. If a solution (s, u, v) exists, then $x(2P + (D,0)) = Ds^2$,

$$s^2 + 2uv\sqrt{D} = (v + u\sqrt{D})^2, \tag{7.33}$$

and $v + u\sqrt{D}$ is the fundamental solution to $v^2 - Du^2 = 1$.

Proof. Note that $\theta(2P + (D, 0)) = (2, D, 2D)$. If $2P + (D, 0) \in \mathcal{E}_D(\mathbb{Z})$, then writing $x(2P + (D, 0)) = Ds^2$ finds us a solution (s, u, v) to the system (7.32). Conversely if (7.32) is solvable, it is easy to check that Ds^2 is the x-coordinate of an integral point on $\mathcal{E}_D$, and this point must be in the same coset of $2\mathcal{E}_D(\mathbb{Q})$ as $(D, 0)$ since θ is injective.

If (7.32) is solvable, taking the difference of the two equations in (7.32), we get $v^2 - Du^2 = 1$. From (7.32), we see that (7.33) holds, and also $s^4 - D(2uv)^2 = 1$. Cohn showed that such equation has at most one solution unless $D = 1785$. More precisely, the main theorem in [26] implies that $s^2 + 2uv\sqrt{D}$ is either $a + b\sqrt{D}$ or $(a + b\sqrt{D})^2$ if $a + b\sqrt{D}$ is the fundamental solution to $v^2 - Du^2 = 1$. This proves the final claim. □

7.9 Average number of integral points

In this section we prove Theorem 7.5. From Theorem 7.1

$$\#\mathcal{E}_D(\mathbb{Z}) \ll 4^{\operatorname{rank} \mathcal{E}_D(\mathbb{Q})}.$$

Heath-Brown [36, Theorem 1] proved that[2]

$$\lim_{N\to\infty} \frac{1}{\#\mathcal{D}(N)} \sum_{D\in\mathcal{D}(N)} 2^{k\cdot \operatorname{rank} \mathcal{E}_D(\mathbb{Q})} \ll_k 1.$$

Therefore

$$\limsup_{N\to\infty} \frac{1}{\#\mathcal{D}(N)} \sum_{D\in\mathcal{D}(N)} (\#\mathcal{E}_D(\mathbb{Z}))^2 \ll 1.$$

Suppose $\mathcal{G}_N \subseteq \mathcal{D}_N$. By Cauchy–Schwarz inequality,

$$\sum_{D\in\mathcal{G}_N} \#\mathcal{E}_D(\mathbb{Z}) \le \Big(\sum_{D\in\mathcal{D}(N)} (\#\mathcal{E}_D(\mathbb{Z}))^2 \Big)^{1/2} (\#\mathcal{G}_N)^{1/2} \ll (\#\mathcal{D}(N))^{1/2} (\#\mathcal{G}_N)^{1/2}.$$

Therefore the contribution from any subset $\mathcal{G}_N$ of $\mathcal{D}(N)$ of size $o(N)$ to the average of $\#\mathcal{E}_D(\mathbb{Z})$ over $\mathcal{D}(N)$ tends to 0 as $N \to \infty$.

[2]To be precise, the theorem was only stated for odd D, but it is possible to extend the proof to even D.

Assuming (7.2) implies that we only need to consider the contribution from the curves $\mathcal{E}_D$ with rank 0 or 1. A theorem by Le Boudec [55, Proposition 1] shows that

$$\sum_{D\geq 1} \# \left\{ P \in \mathcal{E}_D(\mathbb{Z}) : x(P) < \frac{N^2}{(\log N)^\kappa} \right\} \ll \frac{N}{(\log N)^{\kappa/2-6}},$$

where we take $\kappa > 12$. Therefore we can also exclude all $\mathcal{E}_D$ with any integral point $H(P) < \frac{N^2}{(\log N)^\kappa}$ since there are $o(N)$ of them.

If $\operatorname{rank} \mathcal{E}_D(\mathbb{Q}) = 0$, then there are automatically no non-torsion integral points. In the following we consider $\mathcal{E}_D$ such that $\operatorname{rank} \mathcal{E}_D(\mathbb{Q}) = 1$ and any $P \in \mathcal{E}_D(\mathbb{Z}) \setminus \mathcal{T}_D$ satisfy $H(P) > \frac{D^2}{(\log D)^\kappa}$. This removes the need to consider the points arising from cases ((i)), ((ii)), ((iv)) in Theorem 7.4.

Our aim is to prove the following.

Theorem 7.27. *Assume that* $\operatorname{rank} \mathcal{E}_D(\mathbb{Q}) = 1$ *and that any* $P \in \mathcal{E}_D(\mathbb{Z}) \setminus \mathcal{T}_D$ *satisfy* $H(P) > \frac{D^2}{(\log D)^\kappa}$. *Then*

$$\#(\mathcal{E}_D(\mathbb{Z}) \setminus \mathcal{T}_D) \leq 4.$$

We now demonstrate that the integral points that appear in Theorem 7.4 ((iii)) are rare for $D \in \mathcal{D}(N)$ and do not contribute to the average average in Theorem 7.5. Recall that these points are classified in Lemma 7.26. Dirichlet class number formula for real quadratic number fields states that the class number of $\mathbb{Q}(\sqrt{D})$ equals

$$\frac{\sqrt{D} L(1, \chi_D)}{\log \epsilon_D},$$

where χ_D is the Kronecker symbol $\left(\frac{D}{\cdot}\right)$ and ϵ_D is the fundamental unit of $\mathbb{Q}(\sqrt{D})$. Since the class number is at least 1, this gives an inequality

$$\log \epsilon_D \leq \sqrt{D} L(1, \chi_D).$$

It is well-known that $L(1, \chi_D) \ll \log D$. Therefore together with (7.33), we have

$$\log s < 2 \log \epsilon_D \ll \sqrt{D} \log D. \tag{7.34}$$

On the other hand, since $s^2 - 2v^2 = -1$ and $1 + \sqrt{2}$ is the fundamental unit of

$\mathbb{Q}(\sqrt{2})$, we the possible values of s is given by

$$s = \frac{1}{2}\left((1+\sqrt{2})^k + (1-\sqrt{2})^k)\right),$$

where k is any positive odd integer. For large values of k, $|(1-\sqrt{2})^k|$ is bounded, so

$$s \gg (1+\sqrt{2})^k. \tag{7.35}$$

Putting together the inequalities (7.34) and (7.35), we get

$$k \ll \sqrt{D}\log D.$$

Therefore for $D \in \mathcal{D}(N)$, there are $\ll \sqrt{N}\log N$ integral points of the form $2P + (D,0)$, which does not contribute to the average in Theorem 7.5.

7.9.1 Odd multiples of a generator

It now remains to treat the points not covered by Theorem 7.4. Notice that if m is odd, $mP + T = m(P+T)$ for any $P \in \mathcal{E}_D(\mathbb{Q})$ and $T \in \mathcal{T}_D$, so any integral points not in $2\mathcal{E}_D(\mathbb{Q}) + \mathcal{T}_D$ are odd multiples of a generator of the free part of $\mathcal{E}_D(\mathbb{Q})$. By Lemma 7.23, if $mP \in \mathcal{E}_D(\mathbb{Z})$ then $P \in \mathcal{E}_D(\mathbb{Z})$.

If $P \in \mathcal{E}_D(\mathbb{Z})$ and $H(P) > \frac{N^2}{(\log N)^\kappa}$, then $x(P+(0,0))$, $x(P+(-D,0))$, $x(P+(D,0)) \ll D$, therefore by assumption $P+(0,0)$, $P+(-D,0)$, $P+(D,0) \notin \mathcal{E}_D(\mathbb{Z})$. Therefore it is enough to consider odd multiples of one integral point that is also generator.

We show that small multiples of a reasonably sized rational point, as assumed in Theorem 7.27 which we wish to prove, cannot be integral.

Theorem 7.28. *Let $\kappa > 0$ and $C_1 < \sqrt{\frac{4}{3}\log 2}$. Suppose D is some sufficiently large squarefree integer, $P \in \mathcal{E}_D(\mathbb{Q})$ and assume $x(P) > \frac{D^2}{(\log D)^\kappa}$, then $mP \notin \mathcal{E}_D(\mathbb{Z})$ for all $1 < m \le \exp(C_1\sqrt{\log D})$.*

We have shown that $2P$ cannot be integral, so assume $m \ge 3$. With the formulae

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \tag{7.36}$$

$$\psi_{2m} = \frac{\psi_m}{2y}\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right), \tag{7.37}$$

we prove the following by induction.

Lemma 7.29. *Fix some $C_2 > \frac{3}{2\log 2}$. Let $x > D$ such that $(x, y) \in \mathcal{E}_D(\mathbb{Q})$. Then for any positive integer m satisfying $C_2(\log m)^2 < 2(\log x - \log D)$, we have*

$$\psi_m(x) > \left(1 - \exp\left(C_2(\log m)^2\right)\left(\frac{D}{x}\right)^2\right) m x^{\frac{m^2-1}{2}}.$$

Proof. Write $\psi_m(x) = (1 - E_m(\frac{D}{x})^2)mx^{\frac{m^2-1}{2}}$. Assuming $E_m\left(\frac{D}{x}\right)^2 < 1$, we obtain from (7.36)

$$E_{2m+1} < E_{m-1} + 3E_{m+1} + \frac{m^3(m+2)}{2m+1}(E_{m+1} + 3E_m), \tag{7.38}$$

from (7.37)

$$E_{m+2} < \frac{1}{2} + E_m + \frac{(m-1)^2(m+2)}{4}(E_{m-1} + 2E_{m+2}) + \frac{1}{2}(E_{m-2} + 2E_{m+1}). \tag{7.39}$$

Assuming $E_m < \exp\left(C_2(\log m)^2\right)$ for all $m < N$, we obtain an upper bound for $E_N < \exp\left(C_2(\log N)^2\right)$ from (7.38) and (7.39). Checking the base cases $\psi_2 = 2x^{3/2}(1 - (\frac{D}{x})^2)^{1/2}$ and $\psi_3 = 3x^4(1 - 2(\frac{D}{x})^2 - \frac{1}{3}(\frac{D}{x})^4)$ completes the induction. □

Write uniquely $x(mP) = \frac{u}{v_m^2}$, where $\gcd(u, v_m) = 1$ and $v_m > 0$. By [82, Lemma 11.4]

$$\log v_m \le \log|\psi_m(x)| \le \log v_m + \frac{1}{8}m^2 \log|\Delta_D|, \tag{7.40}$$

where $\Delta_D = (2D)^6$ is the discriminant of $\mathcal{E}_D$.

Proof of Theorem 7.28. Let $x := x(P) > \frac{D^2}{(\log D)^\kappa}$. Suppose $mP \in \mathcal{E}_D(\mathbb{Z})$, then (7.40) reduces to

$$\psi_m(x) \le (2D)^{\frac{3}{4}m^2}. \tag{7.41}$$

Fix $\epsilon > 0$ such that

$$\log m < \sqrt{\frac{1}{C_2}\left(\log(1-\epsilon) + 2\log D - 2\kappa \log\log D\right)},$$

then by Lemma 7.29,

$$\psi_m(x) > \epsilon m x^{\frac{m^2-1}{2}} > \epsilon m \left(\frac{D}{(\log D)^{\kappa/2}} \right)^{m^2-1},$$

which contradicts (7.41) for sufficiently large D. □

Now following Section 7.7, we have $\#\mathcal{A}_1 = 0$ for the medium points using Theorem 7.28, and $\#\mathcal{A}_2 \leq 3$ for the large points. Since non-torsion integral points come in pairs $\pm P$, $\#(\mathcal{A}_1 \cup \mathcal{A}_2) \leq 2$. Therefore the possible points contributing to the upper bound in Theorem 7.27 comes from the generator and its corresponding negative point, together with the pair of large points in $\#\mathcal{A}_2$.

Bibliography

[1] L. Alpoge. The average number of integral points on elliptic curves is bounded. `arXiv:1412.1047v3 [math.NT]`, 2014.

[2] J. V. Armitage and A. Fröhlich. Classnumbers and unit signatures. *Mathematika*, 14:94–98, 1967.

[3] A. Azizi and A. Mouhib. Sur le rang du 2-groupe de classes de $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ où $m = 2$ ou un premier $p \equiv 1 \pmod 4$. *Trans. Amer. Math. Soc.*, 353(7):2741–2752, 2001.

[4] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[5] A. Baker. *Transcendental number theory*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 1990.

[6] E. Benjamin, F. Lemmermeyer, and C. Snyder. On the unit group of some multiquadratic number fields. *Pacific J. Math.*, 230(1):27–40, 2007.

[7] M. A. Bennett. On the number of solutions of simultaneous Pell equations. *J. Reine Angew. Math.*, 498:173–199, 1998.

[8] M. A. Bennett. On consecutive integers of the form ax^2, by^2 and cz^2. *Acta Arith.*, 88(4):363–370, 1999.

[9] M. A. Bennett and G. Walsh. The Diophantine equation $b^2X^4 - dY^2 = 1$. *Proc. Amer. Math. Soc.*, 127(12):3481–3491, 1999.

[10] B. J. Birch and N. M. Stephens. The parity of the rank of the Mordell-Weil group. *Topology*, 5:295–299, 1966.

[11] E. Bombieri and W. Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[12] A. Bremner, J. H. Silverman, and N. Tzanakis. Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$. *J. Number Theory*, 80(2):187–208, 2000.

[13] Y. Bugeaud, C. Levesque, and M. Waldschmidt. Équations de Fermat–Pell–Mahler simultanées. *Publ. Math. Debrecen*, 79(3-4):357–366, 2011.

[14] D. A. Burgess. On character sums and L-series. *Proc. London Math. Soc. (3)*, 12:193–206, 1962.

[15] J. W. S. Cassels. Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups. *Proc. London Math. Soc. (3)*, 12:259–296, 1962.

[16] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[17] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*. London Mathematical Society, London, 2010. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata.

[18] S. Chan. Integral points on the congruent number curve. `arXiv:2004.03331 [math.NT]`, 2020.

[19] S. Chan, P. Koymans, D. Milovic, and C. Pagano. On the negative pell equation. `arXiv:1908.01752 [math.NT]`, 2019.

[20] S. Chan, C. McMeekin, and D. Milovic. A density of ramified primes. `arXiv:2005.10188 [math.NT]`, 2020.

[21] S. Chan and D. Milovic. Kuroda's formula and arithmetic statistics. `arXiv:1905.09745 [math.NT]`, 2019.

[22] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[23] H. Cohn and J. C. Lagarias. On the existence of fields governing the 2-invariants of the classgroup of $\mathbf{Q}(\sqrt{dp})$ as p varies. *Math. Comp.*, 41(164):711–730, 1983.

[24] H. Cohn and J. C. Lagarias. Is there a density for the set of primes p such that the class number of $\mathbf{Q}(\sqrt{-p})$ is divisible by 16? In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, volume 34 of *Colloq. Math. Soc. János Bolyai*, pages 257–280. North-Holland, Amsterdam, 1984.

[25] H. Cohn and Y. Zhao. Sphere packing bounds via spherical codes. *Duke Math. J.*, 163(10):1965–2002, 2014.

[26] J. H. E. Cohn. The Diophantine equation $x^4 - Dy^2 = 1$. II. *Acta Arith.*, 78(4):401–403, 1997.

[27] J. Corsman. *Rédei symbols and governing fields*. PhD thesis, McMaster University, September 2007.

[28] D. A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[29] S. Feisel, J. von zur Gathen, and M. A. Shokrollahi. Normal bases via general Gauss periods. *Math. Comp.*, 68(225):271–290, 1999.

[30] E. Fouvry and J. Klüners. On the 4-rank of class groups of quadratic number fields. *Invent. Math.*, 167(3):455–513, 2007.

[31] E. Fouvry and J. Klüners. On the negative Pell equation. *Ann. of Math. (2)*, 172(3):2035–2104, 2010.

[32] E. Fouvry and J. Klüners. The parity of the period of the continued fraction of $\sqrt{d}$. *Proc. Lond. Math. Soc. (3)*, 101(2):337–391, 2010.

[33] J. B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin. The spin of prime ideals. *Invent. Math.*, 193(3):697–749, 2013.

[34] C. F. Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[35] F. Gerth, III. The 4-class ranks of quadratic fields. *Invent. Math.*, 77(3):489–515, 1984.

[36] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[37] E. Hecke. *Lectures on the theory of algebraic numbers*, volume 77 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

[38] K. Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253, 1952.

[39] H. Heilbronn. On the class-number in imaginary quadratic fields. *The Quarterly Journal of Mathematics*, os-5(1):150–160, 01 1934.

[40] H. A. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.*, 19(3):527–550, 2006.

[41] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988.

[42] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[43] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[44] G. A. Kabatjanskiĭ and V. I. Levenšteĭn. Bounds for packings on the sphere and in space. *Problemy Peredači Informacii*, 14(1):3–25, 1978.

[45] D. Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Algebra Number Theory*, 7(5):1253–1279, 2013.

[46] N. Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1984.

[47] P. Koymans and D. Milovic. Joint distribution of spins. `arXiv:1809.09597 [math.NT]`, 2018.

[48] T. Kubota. Über die Beziehung der Klassenzahlen der Unterkörper des bizyklischen biquadratischen Zahlkörpers. *Nagoya Math. J.*, 6:119–127, 1953.

[49] T. Kubota. Über den bizyklischen biquadratischen Zahlkörper. *Nagoya Math. J.*, 10:65–85, 1956.

[50] S. Kuroda. Über den Dirichletschen Körper. *J. Fac. Sci. Imp. Univ. Tokyo Sect. I.*, 4:383–406, 1943.

[51] S. Kuroda. Über die Klassenzahlen algebraischer Zahlkörper. *Nagoya Math. J.*, 1:1–10, 1950.

[52] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464, 1977.

[53] S. Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1978.

[54] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[55] P. Le Boudec. Linear growth for certain elliptic fibrations. *Int. Math. Res. Not. IMRN*, 2015(21):10859–10871, 2015.

[56] W. Ljunggren. Über die Gleichung $x^4 - Dy^2 = 1$. *Arch. Math. Naturvid.*, 45(5):61–70, 1942.

[57] K. Mahler. An inequality for the discriminant of a polynomial. *Michigan Math. J.*, 11:257–262, 1964.

[58] C. McMeekin. On the asymptotics of a prime spin relation. *J. Number Theory*, 200:407–426, 2019.

[59] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[60] J. Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1986.

[61] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[62] Y. Ouyang and Z. Zhang. Hilbert genus fields of real biquadratic fields. *Ramanujan J.*, 37(2):345–363, 2015.

[63] R. A. Rankin. The closest packing of spherical caps in n dimensions. *Proc. Glasgow Math. Assoc.*, 2:139–144, 1955.

[64] L. Rédei. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 171:55–60, 1934.

[65] L. Rédei. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I. *J. Reine Angew. Math.*, 180:1–43, 1939.

[66] L. Rédei and H. Reichardt. Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *J. Reine Angew. Math.*, 170:69–74, 1934.

[67] A. Selberg. Note on a paper by L. G. Sathe. *J. Indian Math. Soc. (N.S.)*, 18:83–87, 1954.

[68] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[69] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[70] J.-P. Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[71] C. E. Shannon. Probability of error for optimal codes in a Gaussian channel. *Bell System Tech. J.*, 38:611–656, 1959.

[72] C. L. Siegel. Über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1]. In *On some applications of Diophantine approximations*, volume 2 of *Quad./Monogr.*, pages 81–138. Ed. Norm., Pisa, 2014.

[73] J. H. Silverman. Lower bound for the canonical height on elliptic curves. *Duke Math. J.*, 48(3):633–648, 1981.

[74] J. H. Silverman. Lower bounds for height functions. *Duke Math. J.*, 51(2):395–403, 1984.

[75] J. H. Silverman. A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves. *J. Reine Angew. Math.*, 378:60–100, 1987.

[76] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.

[77] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[78] P. J. Sime. Hilbert class fields of real biquadratic fields. *J. Number Theory*, 50(1):154–166, 1995.

[79] P. J. Sime. On the ideal class group of real biquadratic fields. *Trans. Amer. Math. Soc.*, 347(12):4855–4876, 1995.

[80] A. Smith. Governing fields and statistics for 4-Selmer groups and 8-class groups. `arXiv:1607.07860 [math.NT]`, 2016.

[81] A. Smith. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. `arXiv:1702.02325 [math.NT]`, 2017.

[82] K. E. Stange. Integral points on elliptic curves and explicit valuations of division polynomials. *Canad. J. Math.*, 68(5):1120–1158, 2016.

[83] R. P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.

[84] H. M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[85] P. Stevenhagen. Ray class groups and governing fields. In *Théorie des nombres, Année 1988/89, Fasc. 1*, Publ. Math. Fac. Sci. Besançon, page 93. Univ. Franche-Comté, Besançon, 1989.

[86] P. Stevenhagen. The number of real quadratic fields having units of negative norm. *Experiment. Math.*, 2(2):121–136, 1993.

[87] P. Stevenhagen. Redei reciprocity, governing fields, and negative pell. `arXiv:1806.06250 [math.NT]`, 2018.

[88] G. Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

[89] Q. Yue. The generalized Rédei-matrix. *Math. Z.*, 261(1):23–37, 2009.

[90] Q. Yue. Genus fields of real biquadratic fields. *Ramanujan J.*, 21(1):17–25, 2010.