On the 16-rank of class groups of quadratic number fields

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op maandag 4 juli 2016
klokke 11:15 uur

door

Djordjo Zeljko Milovic
geboren te Belgrado, Servië in 1989

Promotor: Prof. dr. Peter Stevenhagen

Promotor: Prof. dr. Étienne Fouvry (Université Paris-Sud)

Samenstelling van de promotiecommissie:

Prof. dr. Hendrik Lenstra

Prof. dr. Lillian Pierce (Duke University)

Prof. dr. Peter Sarnak (Princeton University)

Prof. dr. Bart de Smit

Dr. Marco Streng

Prof. dr. Aad van der Vaart

This work was funded by Algant-Doc Erasmus-Mundus and was carried out at Universiteit Leiden and Université Paris-Sud.

THÈSE DE DOCTORAT

Présentée pour obtenir

LE GRADE DE DOCTEUR EN SCIENCES
DE L'UNIVERSITÉ PARIS-SUD

Préparée à l'École Doctorale de Mathématiques
de la région Paris-Sud (ED 142)

Cotutelle par Mathematisch Instituut,
Université de Leiden (Pays-Bas)

Spécialité : Mathématiques

par

Djordjo Zeljko Milovic

On the 16-rank of class groups of quadratic number fields

Soutenue le 4 Juillet 2016 devant la Commission d'examen :

M. Aad van der Vaart	Professeur	Universiteit Leiden	Président du Jury
Mme Lillian Pierce	Professeur	Duke University	Rapporteur (excusé)
M. Peter Sarnak	Professeur	Princeton University	Rapporteur (excusé)
M. Frits Beukers	Professeur	Universiteit Utrecht	Examinateur
M. Jan-Hendrik Evertse	Professeur	Universiteit Leiden	Examinateur
Mme Damaris Schindler	Professeur	Universiteit Utrecht	Examinateur
M. Bart de Smit	Professeur	Universiteit Leiden	Examinateur
M. Marco Streng	Professeur	Universiteit Leiden	Examinateur
M. Étienne Fouvry	Professeur	Université Paris Saclay	Directeur de thèse
M. Peter Stevenhagen	Professeur	Universiteit Leiden	Directeur de thèse

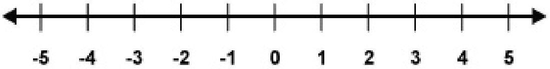
Thèse préparée au
Département de Mathématiques d'Orsay
Laboratoire de Mathématiques (UMR 8628), Bât. 425
Université Paris-Sud, CNRS
Université Paris Saclay
91405 Orsay CEDEX

Contents

Chapter 1

Introduction

The main object of study in *number theory* is the ring of rational integers $\mathbb{Z}$.



The ring $\mathbb{Z}$ can be studied from several different perspectives. One of them is to study the distribution of prime numbers, the building blocks of its multiplicative structure, and functions theoreof. More precisely, given a sufficiently well-behaved sequence of complex numbers $\{a_n\}_n$ indexed by natural numbers $n \in \mathbb{N}$, one might ask for an estimate of the sum

$$\sum_{p \text{ prime}} a_p. \tag{1.1}$$

For instance, if the sequence $\{a_n\}_n$ is defined by

$$a_n = \begin{cases} 1 & \text{if } n \leq X \\ 0 & \text{otherwise,} \end{cases}$$

then the statement that

$$\left| \sum_{p \text{ prime}} a_p - \int_2^X \frac{dt}{\log t} \right| \leq \frac{X^{\frac{1}{2}} \log X}{8\pi}$$

for all sufficiently large real numbers X is equivalent to the famous Riemann Hypothesis [37, Corollary 1, p. 339].

Another way to study arithmetic of the ring $\mathbb{Z}$ is to study solutions of polynomial equations over the integers. One such equation is the *negative Pell equation*: given a positive integer d, one might ask when the equation

$$x^2 - dy^2 = -1 \tag{P$^-$}$$

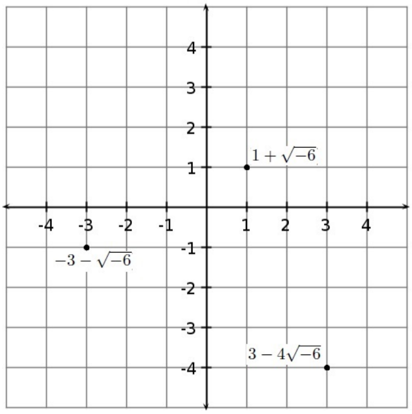
has solutions $x, y \in \mathbb{Z}$. For example, if $d = 2016$, then (P$^-$) has no solutions, while if $d = 2017$, then (P$^-$) has infinitely many solutions, the smallest of which is

$$(x, y) = (10651529913260318450384444, 23716961153808075597914481).$$

An area of number theory that naturally combines the above two perspectives of studying the integers is the study of *arithmetic statistics* of 2-parts of class groups of quadratic number fields.

1.1 Quadratic rings and arithmetic statistics

When solving polynomial equations over $\mathbb{Z}$, it is often useful to view these equations inside rings that are slightly larger than $\mathbb{Z}$. One natural generalization of $\mathbb{Z}$ that is particularly conducive to studying the negative Pell equation is a *quadratic ring*, i.e., a commutative ring with unity that is a free $\mathbb{Z}$-module of rank 2. An example of a quadratic ring is $\mathbb{Z}[\sqrt{-6}] = \mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{-6}$.



$$(1+\sqrt{-6}) \cdot (-3-\sqrt{-6}) = 3 - 4\sqrt{-6}$$

There are many quadratic rings. In fact, their isomorphism classes are in one-to-one correspondence with the set of integers congruent to 0 or 1 modulo 4, where a quadratic ring corresponds to its *discriminant* (see for instance [2, Theorem 8, p. 231]). In light of this, instead of studying a particular quadratic ring, one might study the *average* behavior of certain arithmetic invariants attached to quadratic rings in families parametrized by special types of discriminants. The subject dealing with these types of problems is called *arithmetic statistics.*

A quadratic ring whose discriminant is not a square is an integral domain and in fact an *order* in the quadratic number field that is its field of fractions. We will call such a ring a *quadratic domain.* If R is a quadratic domain of discriminant D, then there exists an isomorphism of rings

$$R \cong \mathbb{Z}[(D+\sqrt{D})/2].$$

Among quadratic domains, a special role is played by those that are maximal orders in quadratic number fields. The discriminant of a quadratic number field is defined to be the discriminant of the maximal order in the quadratic number field. Such a discriminant is called a *fundamental discriminant.* Fundamental discriminants are exactly the integers of the form

$$\begin{cases} d, & \text{where } d \neq 1 \text{ is squarefree and } d \equiv 1 \bmod 4, \text{ and} \\ 4d, & \text{where } d \text{ is squarefree and } d \equiv 2 \text{ or } 3 \bmod 4. \end{cases}$$

We now introduce two arithmetic invariants of quadratic domains that are relevant to the negative Pell equation.

1.2 Class groups

The arithmetic of quadratic domains can be more complicated than that of the ring $\mathbb{Z}$. The *fundamental theorem of arithmetic* states that $\mathbb{Z}$ is a *unique factorization domain*, that is, a domain in which every non-zero element has a factorization into irreducible elements that is *unique* up to reordering and multiplication by units. In a quadratic domain, this need not be the case. For example, in $\mathbb{Z}[\sqrt{-6}]$,

$$2 \cdot 5 \quad \text{and} \quad (2+\sqrt{-6}) \cdot (2-\sqrt{-6})$$

are two distinct factorizations of the element 10 into irreducible elements. An integral domain which is not a unique factorization domain cannot be a principal ideal domain. Hence one obstruction to unique factorization in a quadratic domain is the failure of ideals to be principal. One way to measure this obstruction is via an algebraic invariant called the *class group.*

Let R be a quadratic domain, and let D and K denote its discriminant and its field of fractions, respectively. Then the (ordinary) class group Cl of R is defined as the quotient

$$\mathrm{Cl} = \mathcal{I}/\mathcal{P},$$

where $\mathcal{I}$ is the group of invertible fractional ideals of R and $\mathcal{P}$ is the subgroup of $\mathcal{I}$ consisting of principal invertible fractional ideals. Since a discriminant determines a quadratic ring up to isomorphism, we will sometimes denote the class group of R by $\mathrm{Cl}(D)$. A closely related group is the *narrow class group* Cl^+, defined as the quotient

$$\mathrm{Cl}^+ = \mathcal{I}/\mathcal{P}^+,$$

where now $\mathcal{P}^+$ is the subgroup of $\mathcal{I}$ consisting of principal invertible fractional ideals that can be generated by a totally positive element (i.e., an element $\alpha \in K$ such that $\sigma(\alpha) > 0$ for all real embeddings $\sigma : K \hookrightarrow \mathbb{R}$). The study of the narrow class group precedes that of the ordinary class group – the narrow class group was introduced by Gauss [21], albeit in the language of binary quadratic forms.

We recall that Cl is a finite abelian group. We also note that if a quadratic domain is the maximal order in a quadratic number field, then it is a unique factorization domain if and only if it is a principal ideal domain, and so the class group is in fact the *only* obstruction to unique factorization. For example, the ring $\mathbb{Z}[\sqrt{-6}]$ from above is the maximal order in the quadratic number field $\mathbb{Q}(\sqrt{-6})$, its class group $\mathrm{Cl}(-24)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and the ideal generated by 2 and $\sqrt{-6}$ is not principal. A standard reference for these definitions and facts is [25].

As a fairly simple algebraic object that nonetheless carries very important information about the arithmetic of the corresponding quadratic domain, the class group is one of the most important and widely studied invariants in number theory.

1.3 What do class groups look like?

We already mentioned above that class groups are finite abelian groups. Given a finite abelian group G, a prime number ℓ, and a positive integer k, we define the ℓ^k-rank of G to be

$$\mathrm{rk}_{\ell^k} G = \dim_{\mathbb{F}_\ell} \left(\ell^{k-1}G/\ell^k G\right).$$

In other words, $\mathrm{rk}_\ell G$ is the number of cyclic ℓ-groups appearing in the decomposition of G as a direct sum of cyclic subgroups of prime-power order, and $\mathrm{rk}_{\ell^k} G$ is the number of these cyclic ℓ-groups that have an element of order ℓ^k. Hence the ℓ-rank measures the "width" of the ℓ-part, while the ℓ^k-rank as k increases measures the "depth" of the ℓ-part.

Knowing the ℓ^k-rank of G for every prime power ℓ^k is equivalent to knowing the isomorphism class of G. Therefore, as $\mathrm{Cl}(D)$ is a finite abelian group, we can study the average behavior of $\mathrm{Cl}(D)$ as D ranges over some family of discriminants by studying the distribution of $\mathrm{rk}_{\ell^k}\mathrm{Cl}(D)$ for various prime powers ℓ^k.

Let D be a fundamental discriminant. The "width" of the 2-part of $\mathrm{Cl}(D)$ is given by *Gauss's genus theory* [21]. More precisely, we have

$$\mathrm{rk}_2\mathrm{Cl}(D)^+ = \omega(D) - 1, \tag{1.2}$$

where $\omega(D)$ denotes the number of distinct primes dividing D.

Cohen and Lenstra [4] developed a heuristic model to predict the behavior of the *odd* parts of class groups of maximal orders in quadratic number fields. Roughly, *Cohen-Lenstra heuristics* stipulate that an odd abelian group G occurs as the odd part of a class group with probability proportional to the inverse of the size of the automorphism group of G. These heuristics can be used to make many precise conjectures about the distribution of ℓ^k-ranks for $\ell \neq 2$. Gerth [22] noticed that after accounting for Gauss's genus theory, the Cohen-Lenstra heuristics can be extended to the 2-parts of class groups, leading to precise conjectures about the distribution of 2^k-ranks for $k \geq 2$. Proving these conjectures is a principal goal of arithmetic statistics.

After more than 30 years, very few such conjectures have been proved. In fact, the only result for $\ell \neq 2$ giving a precise asymptotic formula is that of Davenport and Heilbronn [11], for the average value of $3^{\mathrm{rk}_3\mathrm{Cl}(D)}$ as D ranges over all positive (or negative) fundamental discriminants (their result actually predates the Cohen-Lenstra heuristics by more than 10 years; see also [3] and [43] for subsequent refinements). Their methods and results are still insufficient to produce a positive proportion of D with $\mathrm{rk}_3\mathrm{Cl}(D) = 1$.

Much more is known in the case that $\ell = 2$. Rédei [34] gave formulas for the 4-rank in terms of the individual primes dividing the discriminant (see also [28, Theorem 1.2.3, p. 20]), and his work was sufficient to deduce distribution results over discriminants with a fixed 2-rank (see [22]). Extending these distribution results to all discriminants was a much harder problem, resolved by Fouvry and Klüners [14]. They succeeded in proving that, for each integer $k \geq 0$, the set of fundamental discriminants D such that $\mathrm{rk}_4\mathrm{Cl}(D) = k$ has the positive density predicted by Cohen and Lenstra (see [14] and also [13]).

Fouvry and Klüners [16] proved certain distribution results about the 8-rank in a special family of positive discriminants, but under the constraint that the 4-rank is equal to 1. Perhaps the most general result concerning the 8-rank is due to Stevenhagen [40]. He proved that if $d \neq 0$ and $k \geq 0$ are integers, then the set of primes p such that $\mathrm{rk}_8\mathrm{Cl}(dp) = k$ and such that dp is a fundamental discriminant has a density which is a rational number.

Density results appear to be far more difficult to obtain for the 16-rank than for the lower 2-power ranks (see [41, p. 16-18]). Our main goal is to prove density results about the 16-rank, albeit in certain particularly simple families of quadratic number fields. Before we state our results, we first give further motivation coming from the study of the negative Pell equation.

1.4 Fundamental units and the negative Pell equation

Let R, D, K, $\mathcal{I}$, $\mathcal{P}$, and $\mathcal{P}^+$ be defined as in Section 1.2. We say that R is *imaginary* if there are no real embeddings $K \hookrightarrow \mathbb{R}$, or, equivalently, if its discriminant D is negative. In this case, the narrow class group clearly coincides with the ordinary class group. Otherwise, if $D > 0$, we say that R is *real.* In this case, the relationship between the ordinary and the narrow class groups is more interesting.

Let R be a real quadratic domain. The group $\mathcal{P}^+$ is an index-1 or -2 subgroup of $\mathcal{P}$, depending on whether or not R has a unit of norm -1. Indeed, the norm of a totally positive element is clearly positive, while the norm of

$\sqrt{D} \in R$ is negative, and so the principal ideal generated by $\sqrt{D}$ can be generated by a totally positive element if and only if R has a unit of norm -1.

The unit group of R is of the form

$$R^\times \cong \langle -1 \rangle \times \langle \varepsilon \rangle ,$$

where ε is a unit of infinite order (see for instance [25, Theorem 11.19, p. 61]). We say that ε is a *fundamental unit*. The norm $\mathrm{Norm}(\varepsilon)$ does not depend on the choice of ε, and is thus an invariant of a real quadratic domain.

As the norm function is multiplicative, the real quadratic domain R has a unit of norm -1 if and only if $\mathrm{Norm}(\varepsilon) = -1$. Hence the invariant $\mathrm{Norm}(\varepsilon)$ simply detects if the ordinary and the narrow class groups differ.

We now link the invariant $\mathrm{Norm}(\varepsilon)$ to a negative Pell equation. Let

$$d = \begin{cases} D & \text{if } D \equiv 1 \bmod 4 \\ D/4 & \text{if } D \equiv 0 \bmod 4. \end{cases}$$

One can check that the unit group $\mathbb{Z}[\sqrt{d}]^\times$ is a subgroup of index 1 or 3 of the unit group $R^\times$. Hence $\mathrm{Norm}(\varepsilon) = -1$ if and only if $\mathbb{Z}[\sqrt{d}]$ has a unit of norm -1, and this happens if and only if (P^-) is solvable. Hence

$$x^2 - dy^2 = -1 \text{ is solvable over } \mathbb{Z} \Longleftrightarrow \mathrm{Cl}(D) = \mathrm{Cl}(D)^+. \tag{1.3}$$

The odd parts of Cl and Cl^+ coincide, so the study of the 2-parts of the ordinary and the narrow class groups is closely related to the study of solutions of the negative Pell equation. In fact, the equation $x^2 - dy^2 = -1$ is solvable over $\mathbb{Z}$ if and only if

$$\mathrm{rk}_{2^k} \mathrm{Cl}(D) = \mathrm{rk}_{2^k} \mathrm{Cl}(D)^+ \tag{1.4}$$

for all integers $k \geq 1$.

It follows from (1.3) that comparing the ordinary and the narrow class groups of *quadratic number fields* corresponds exactly to solving (P^-) for *squarefree* integers d. If d is divisible by a prime number $p \equiv 3 \bmod 4$, then (P^-) clearly has no solutions. Let $\mathbb{D}$ be the set of positive squarefree integers not divisible by a prime $p \equiv 3 \bmod 4$. Stevenhagen [42] made the remarkable conjecture that the set of squarefree d for which (P^-) is solvable has a positive density inside the set $\mathbb{D}$, given in terms of an explicit infinite product (see [42, Conjecture 1.2, p. 122]). Using the criterion (1.4), Fouvry and Klüners made significant progress on Stevenhagen's conjecture; they proved strong upper and lower bounds for the proportion of squarefree d in $\mathbb{D}$ for which (P^-) is solvable (see [15] and [16]).

1.5 The equation $x^2 - 2py^2 = -1$

To demonstrate the difficulty of improving the upper and lower bounds of Fouvry and Klüners, we now restrict our attention to a certain subset of $\mathbb{D}$, namely the set of integers of the form $2p$, where p is a prime number congruent to 1 mod 4. The associated quadratic number fields are the fields $\mathbb{Q}(\sqrt{2p})$ of discriminant $8p$. The reason this family is relatively simple is given by Gauss's genus theory.

From (1.2), we see that the 2-part of $\mathrm{Cl}(D)^+$ (and so also $\mathrm{Cl}(D)$) is relatively simpler to study when D has fewer prime divisors. If D has only one prime divisor, however, then the 2-part of the narrow class group is trivial and there is nothing to be done. Therefore, if we wish to study how the 2-part of the class group varies in some family of quadratic number fields, the simplest non-trivial types of families to consider are those parametrized by fundamental discriminants of the form qp, where $\pm q$ is an odd prime, 4, or 8, and where p varies over the set of prime numbers in some fixed congruence classes modulo 4. For instance, if we take $q = 8$ and allow p to vary over the set of prime numbers congruent to 1 modulo 4, we recover the family $\{\mathbb{Q}(\sqrt{2p})\}_{p\equiv 1 \bmod 4}$ that we mentioned above.

For details of the following discussion, see [42]. Given a real number $X > 5$, let $\rho(X)$ denote the proportion of primes $p \equiv 1 \bmod 4$ less than X for which the negative Pell equation $x^2 - 2py^2 = -1$ is solvable. Stevenhagen's conjectural framework predicts that $\rho(X) \to \frac{2}{3}$ as $X \to \infty$. However, the best known bounds are

$$\frac{5}{8} \leq \liminf_{X\to\infty} \rho(X) \leq \limsup_{X\to\infty} \rho(X) \leq \frac{3}{4}. \tag{1.5}$$

These bounds are obtained in the following way. Gauss's genus theory implies that the 2-part of $\mathrm{Cl}(8p)^+$ is cyclic, so that the 2-part of $\mathrm{Cl}(8p)^+$ is completely determined by the largest integer k such that $\mathrm{rk}_{2^k}\mathrm{Cl}(8p)^+ = 1$. As $\mathrm{Cl}(8p)$ is a quotient of $\mathrm{Cl}(8p)^+$ by a subgroup of order 1 or 2, we deduce that

$$\mathrm{rk}_{2^k}\mathrm{Cl}(8p)^+ - 1 \leq \mathrm{rk}_{2^k}\mathrm{Cl}(8p) \leq \mathrm{rk}_{2^k}\mathrm{Cl}(8p)^+ \tag{1.6}$$

for all integers $k \geq 1$. The condition $p \equiv 1 \bmod 4$ ensures that

$$\mathrm{rk}_2\mathrm{Cl}(8p) = \mathrm{rk}_2\mathrm{Cl}(8p)^+ = 1.$$

By (1.6) and (1.3), we have the implications

$$\mathrm{rk}_4\mathrm{Cl}(8p)^+ = 0 \Longrightarrow \mathrm{Cl}(8p) = \mathrm{Cl}(8p)^+ \Longrightarrow x^2 - 2py^2 = -1 \text{ is solvable.}$$

It turns out that for a prime $p \equiv 1 \bmod 4$,

$$\mathrm{rk}_4\mathrm{Cl}(8p)^+ = 1 \Longleftrightarrow p \equiv 1 \bmod 8,$$

which gives a lower bound of

$$\frac{1}{2} \leq \liminf_{X \to \infty} \rho(X). \tag{1.7}$$

Now, again by (1.6) and (1.3), we have the implication

$$\mathrm{rk}_4\mathrm{Cl}(8p)^+ = 1 \text{ and } \mathrm{rk}_4\mathrm{Cl}(8p) = 0 \Longrightarrow x^2 - 2py^2 = -1 \text{ is not solvable.}$$

The 4-rank of the ordinary class group and the 8-rank of the narrow class group are determined by variants of fourth-power residue symbols. More precisely, for a prime $p \equiv 1 \bmod 8$, let $[2,p]_4 = 1$ if 2 is a fourth power modulo p and let $[2,p]_4 = -1$ otherwise. Similarly, for a prime $p \equiv 1 \bmod 8$, let $[p,2]_4 = 1$ if $p \equiv 1 \bmod 16$ and let $[p,2]_4 = -1$ otherwise. Then, for a prime $p \equiv 1 \bmod 8$,

$$\mathrm{rk}_4\mathrm{Cl}(8p) = 1 \Longleftrightarrow [2,p]_4 = [p,2]_4. \tag{1.8}$$

Passing to Gaussian integers and using the Čebotarev Density Theorem, it is not too hard to see that the condition above is satisfied for one-half of primes $p \equiv 1 \bmod 8$. This gives the upper bound in (1.5). Next, to improve the lower bound in (1.7), we use the implication

$$\mathrm{rk}_4\mathrm{Cl}(8p)^+ = \mathrm{rk}_4\mathrm{Cl}(8p) = 1 \text{ and } \mathrm{rk}_8\mathrm{Cl}(8p)^+ = 0 \Longrightarrow x^2 - 2py^2 = -1 \text{ is solvable}$$ [redacted]

and the criterion, valid for primes $p \equiv 1 \bmod 8$,

$$\mathrm{rk}_8\mathrm{Cl}(8p)^+ = 1 \Longleftrightarrow [2,p]_4 = [p,2]_4 = 1. \tag{1.9}$$

Again, one can show that this holds for one-fourth of primes $p \equiv 1 \bmod 8$, which gives the lower bound in (1.5).

At this point, we emphasize the the best known bounds (1.5), although first explicitly stated in [42, p. 127], can be readily deduced from algebraic criteria (1.8) and (1.9) that were already known to Rédei [35] and Scholz [38] in the 1930's. In other words, there has been no tangible progress on the bounds (1.5) in over 80 years.

If we wish to improve the bounds in (1.5) using the same general strategy that we employed above, we would have to be able to compute the density of primes $p \equiv 1 \bmod 4$ satisfying either (for an improvement of the upper bound)

$$\mathrm{rk}_8\mathrm{Cl}(8p)^+ = 1 \text{ and } \mathrm{rk}_8\mathrm{Cl}(8p) = 0$$

or (for an improvement of the lower bound)

$$\mathrm{rk}_8\mathrm{Cl}(8p)^+ = \mathrm{rk}_8\mathrm{Cl}(8p) = 1 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(8p) = 0.$$

As we will soon see, these two problems are of a similar difficulty. We focus on the second problem, namely the 16-rank of $\mathrm{Cl}(8p)^+$.

The fields $\mathbb{Q}(\sqrt{2p})$ are real quadratic fields, so at first sight there seems to be no relation to studying imaginary quadratic fields. Generally, studying class groups of real quadratic fields is much more difficult than studying class groups of imaginary quadratic fields, primarily because real quadratic domains have units of infinite order. However, in this particular case, Stevenhagen established a connection between the 16-rank of $\mathrm{Cl}(8p)$ and the 16-ranks of $\mathrm{Cl}(-4p)$ and $\mathrm{Cl}(-8p)$ for primes $p \equiv 1 \bmod 4$ (see [41, Theorem 3, p. 3]). One consequence of Stevenhagen's result (already known to Oriat [33]) that can be stated simply is

$$\mathrm{rk}_{16}\mathrm{Cl}(8p)^{+} = 1 \Longrightarrow \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1.$$

Hence we could improve the lower bound in (1.5) by showing that

$$\mathrm{rk}_{8}\mathrm{Cl}(8p)^{+} = \mathrm{rk}_{8}\mathrm{Cl}(-8p) = 1 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 0$$

occurs for a positive density of primes $p \equiv 1 \bmod 4$. Similar improvements on the lower bound in (1.5) could be achieved by proving density results about the 16-rank of $\mathrm{Cl}(-4p)$ for primes $p \equiv 1 \bmod 4$.

Limitations in certain analytic tools prevented us from proving density results about the 16-rank for either of the families $\{\mathbb{Q}(\sqrt{-p})\}_{p\equiv 1 \bmod 4}$ and $\{\mathbb{Q}(\sqrt{-2p})\}_{p\equiv 1 \bmod 4}$. Instead, we proved results about the 16-rank for a subfamily of $\{\mathbb{Q}(\sqrt{-p})\}_{p\equiv 1 \bmod 4}$ and for the family $\{\mathbb{Q}(\sqrt{-2p})\}_{p\equiv -1 \bmod 4}$.

1.6 Statements of main results

The two main results of this thesis come from the articles [32] and [31], which will comprise Chapter 2 and Chapter 3, respectively. In the following, p always denotes a prime number. The first result concerns a subfamily of $\{\mathbb{Q}(\sqrt{-p})\}_{p\equiv 1 \bmod 4}$.

Theorem A. *We have*

$$\lim_{X\to\infty} \frac{\#\{p \leq X : p = a^2 + c^4 \textit{ with } c \textit{ even and } \mathrm{rk}_{16}\mathrm{Cl}(-4p) = 1\}}{\#\{p \leq X : p = a^2 + c^4 \textit{ with } c \textit{ even}\}} = \frac{1}{4}.$$

The second result concerns the family $\{\mathbb{Q}(\sqrt{-2p})\}_{p\equiv -1 \bmod 4}$.

Theorem B. *We have*

$$\lim_{X\to\infty} \frac{\#\{p \leq X : p \equiv -1 \bmod 4 \textit{ and } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1\}}{\#\{p \leq X : p \equiv -1 \bmod 4\}} = \frac{1}{8}.$$

Theorem A and Theorem B are the first non-trivial density results about the 16-rank in families of quadratic number fields. Both of these theorems follow from new criteria for the 16-rank and estimates of sums of type (1.1), namely the sums

$$\sum_{p\leq X} a_p \tag{1.10}$$

where $\{a_n\}_n$ is a reasonably nice sequence of complex numbers indexed by natural numbers n and X is a positive real number tending to infinity. For Theorem A, the relevant sequence is given by

$$a_n = \begin{cases} 1 & \text{if } n = a^2 + c^2 \text{ with } a \equiv \alpha \bmod 16 \text{ and } c \equiv \gamma \bmod 4 \\ 0 & \text{otherwise,} \end{cases}$$

where α and γ are specified congruence classes modulo 16 and modulo 4, respectively. Proving an asymptotic formula for the sum (1.10) with a_n defined as above is a very difficult problem, and its solution by Friedlander and Iwaniec [19] in the 1990's is still considered a major achievement in analytic number theory.

For Theorem B, the relevant sequence $\{a_n\}_n$ is much more difficult to define for general n. At prime indices p, the sequence is given by

$$a_p = \begin{cases} 1 & \text{if } p \equiv -1 \bmod 4 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1 \\ -1 & \text{if } p \equiv -1 \bmod 4 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = \mathrm{rk}_8\mathrm{Cl}(-8p) - 1 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

As such, proving Theorem B consists of proving a density result for the 8-rank, which is classical, and proving that a_p oscillates as p varies. In fact, with a_p defined as above, we prove that there exists $\delta > 0$ such that

$$\sum_{p\leq X} a_p \ll X^{1-\delta}$$

as X tends to infinity. The power-saving in X in the estimate above has additional implications about the 16-rank which we discuss in the introduction to Chapter 3. The method we use to prove that a_p oscillates can be traced back to the work of Vinogradov [44] from the 1930's, but our application of this method is reminiscent of its use by Friedlander and Iwaniec, coincidentally again in [19].

1.7 Strategies for the 16-rank

We now describe one reason that density results about the 16-rank are difficult to prove, and we present our strategies to circumvent these difficulties in case of the families from Theorem A and Theorem B. Before we can do so, we have to introduce some algebraic objects that allow us to interpret class groups as Galois groups.

1.7.1 Class groups as Galois groups

The following definitions and facts can be found in [25]. Let E/F be a finite abelian extension of number fields. Let $\mathcal{I}_F$ denote the free abelian group generated by prime ideals of F that are unramified in E. The *Artin map* is the group homomorphism

$$\left(\frac{\cdot}{E/F}\right) : \mathcal{I}_F \to \operatorname{Gal}(E/F)$$

defined as follows. Let $\mathfrak{p}$ be a prime ideal of F which is unramified in E and let $\mathfrak{P}$ be any prime ideal of E lying above $\mathfrak{p}$. Let $\operatorname{Norm}(\mathfrak{p})$ be the cardinality of the residue field at $\mathfrak{p}$. Then the *Artin symbol*

$$\left(\frac{\mathfrak{p}}{E/F}\right)$$

is the unique element of $\operatorname{Gal}(E/F)$ such that

$$\left(\frac{\mathfrak{p}}{E/F}\right)(\alpha) \equiv \alpha^{\operatorname{Norm}(\mathfrak{p})} \bmod \mathfrak{P}$$

for all α in the maximal order of E. We then extend $\left(\frac{\cdot}{E/F}\right)$ multiplicatively to $\mathcal{I}_F$.

The *Hilbert class field* H of F is the maximal unramified abelian extension of F. The Artin symbol induces a canonical isomorphism of groups

$$\left(\frac{\cdot}{H/F}\right) : \mathrm{Cl} \xrightarrow{\sim} \operatorname{Gal}(H/F), \tag{1.11}$$

where Cl is the ordinary class group of F. Similarly, the Artin symbol induces a canonical isomorphism between the narrow class group Cl^+ and the Galois group $\operatorname{Gal}(H^+/F)$, where H^+ denotes the *narrow Hilbert class field* of F, i.e., the maximal unramified at all finite primes abelian extension of F.

The isomorphism (1.11) shows that information about the class group of F is encoded in the Galois theory of unramified abelian extensions of F. Whenever we can construct such an extension E/F, it must hold true that $E \subset H$, and so $\operatorname{Gal}(E/F)$ is canonically isomorphic to a quotient of Cl.

1.7.2 2^n-Hilbert class fields

Let qp be a fundamental discriminant divisible by exactly two primes, as in the beginning of Section 1.5. Then Gauss's genus theory (see (1.2)) implies that the 2-part of the narrow class group $\mathrm{Cl}(qp)^+$ is cyclic. Let K denote the quadratic field $\mathbb{Q}(\sqrt{qp})$, and let $\mathrm{Cl}^+ = \mathrm{Cl}(qp)^+$. Suppose for the moment that $\mathrm{rk}_{2^n}\mathrm{Cl}^+ = 1$. Then $(\mathrm{Cl}^+)^{2^n}$ is a subgroup of Cl^+ of index 2^n. We define the 2^n-*Hilbert class field* H_{2^n} to be the subfield of H fixed by the the image of $(\mathrm{Cl}^+)^{2^n}$ under the isomorphism (1.11). Since the 2-primary part of Cl is cyclic, it follows immediately that H_{2^n} is the *unique* unramified at all finite primes, cyclic, degree-2^n extension of K. Moreover, (1.11) induces a canonical isomorphism of cyclic groups of order 2^n

$$\left(\frac{\cdot}{H_{2^n}/K}\right) : \mathrm{Cl}^+/(\mathrm{Cl}^+)^{2^n} \longrightarrow \mathrm{Gal}(H_{2^n}/K). \tag{1.12}$$

1.7.3 General strategy

The general strategy to prove density statements about 2^n-ranks of class groups $\mathrm{Cl}(qp)$ with q fixed and p varying is to find a criterion, in terms of p, for the existence of the 2^n-Hilbert class field of $K = \mathbb{Q}(\sqrt{qp})$. We then use the criterion to encode some information about the 2^n-rank of $\mathrm{Cl}(dp)$ via a complex number a_p and study the sum

$$\sum_{p\leq X} a_p.$$

To prove something interesting about the sum above, our criterion must be sufficiently conducive to the available analytic techniques. In practice, we often have to extend the definition of a_n to all natural numbers n in some structured way. If the function $n \mapsto a_n$ is multiplicative, we can usually apply the classical theory of L-functions to deduce interesting results about the sum over primes. Otherwise, if the function $n \mapsto a_n$ is *not* multiplicative, in special cases we may be able to apply more advanced sieving techniques.

If we have an ideal of K, explicitly defined in terms of p, that generates the class of order 2 in $\mathrm{Cl}(qp)^+$, then we might be able to deduce a criterion for $\mathrm{rk}_{2^n}\mathrm{Cl}(qp)^+$ once we have found the 2^{n-1}-Hilbert class field of K, again explicitly in terms of p. Indeed, we see from (1.12) and the definition of the Artin symbol that $\mathrm{rk}_{2^n}\mathrm{Cl}(qp)^+ = 1$ if and only if the ideal generating the class of order 2 splits in the 2^{n-1}-Hilbert class field.

The main difficulty in proving density results about 16-ranks of the narrow class groups $\mathrm{Cl}(qp)^+$ with q fixed and p varying is that there is *no known* way to generate the 8-Hilbert class field H_8 explicitly enough in terms of p so that one could apply analytic techniques. This is also the reason that density results about 8-ranks of the ordinary class groups $\mathrm{Cl}(8p)$ and 16-ranks of the narrow class groups $\mathrm{Cl}(8p)^+$ are both difficult – if $\mathrm{rk}_8\mathrm{Cl}(8p)^+ = 1$, then $\mathrm{rk}_8\mathrm{Cl}(8p) = 1$ if and only if H_8 is totally real.

In the two cases $q = -4$ and $q = -8$, we manage to overcome the difficulty of explicitly generating the 8-Hilbert class field as follows. In the case $q = -4$, instead of finding H_8 for *all* prime numbers $p \equiv 1 \bmod 4$, we are able to write down H_8 explicitly when p is a prime of the form $a^2 + c^4$ with c even. Thus, we trade the generality of working with the full family $\{\mathbb{Q}(\sqrt{-p})\}_{p \equiv 1 \bmod 4}$ in exchange for an explicit understanding of the 8-Hilbert class field of $\mathbb{Q}(\sqrt{-p})$.

If $p \equiv -1 \bmod 4$, then $\mathrm{rk}_4\mathrm{Cl}(-8p) = 1$ if and only if $p \equiv -1 \bmod 8$. In the case $q = -8$, the idea is to write down, for $p \equiv -1 \bmod 8$, *both*

- the 4-Hilbert class field H_4 of $\mathbb{Q}(\sqrt{-2p})$, *and*
- an ideal $\mathfrak{u}$ generating a class of order 4 in $\mathrm{Cl}(-8p)$

in terms of integers u and v satisfying $p = u^2 - 2v^2$, and then to characterize those p such that

$$\left(\frac{\mathfrak{u}}{H_4/\mathbb{Q}(\sqrt{-2p})}\right) = 1. \tag{1.13}$$

The isomorphism (1.12) for $n = 2$ and the equality (1.13) then imply that the class of order 4 in Cl in fact belongs to Cl^4, which proves that Cl has an element of order 16.

Without further ado, we now move to the main body of this thesis, which consists of two chapters. Chapter 2 is based on [32] and deals with Theorem A and related results. Since we deal with a family of quadratic number fields whose class groups have cyclic 2-parts, the 16-rank is 1 or 0 according to whether or not 16 divides the *class number*, i.e., the order of the class group. We adopt this terminology in Chapter 2.

Chapter 3, dedicated to Theorem B and related results, is based on [31].

Chapter 2

Infinitude of $\mathbb{Q}(\sqrt{-4p})$ with class number divisible by 16

Let p be a prime number, and let Cl and h be the class group and the class number of $\mathbb{Q}(\sqrt{-4p})$, respectively. Since the discriminant of this field is either $-p$ or $-4p$, Gauss's genus theory implies that the 2-part of Cl is cyclic, and so the structure of the 2-part of the class group is entirely determined by the highest power of 2 dividing h. More precisely, Gauss's genus theory implies that

$$2|h \Longleftrightarrow p \equiv 1 \bmod 4.$$

The criterion

$$4|h \Longleftrightarrow p \equiv 1 \bmod 8$$

can be deduced easily from Rédei's work on the 4-rank of quadratic number fields [34]. In [1], Barrucand and Cohn gave an explicit criterion for divisibility by 8 by successively extracting square roots of the class of order two. It states that

$$8|h \Longleftrightarrow p = x^2 + 32y^2 \text{ for some integers } x \text{ and } y.$$

This can be restated as

$$8|h \Longleftrightarrow p \equiv 1 \bmod 8 \text{ and } 1+i \text{ is a square modulo } p \tag{2.1}$$

where i is a square root of -1 modulo p (see [1, (10), p.68]). In [40], Stevenhagen also obtained the criterion (2.1), albeit by a more abstract argument using class field theory over the field $\mathbb{Q}(i)$.

Given a subset S of the prime numbers, and a real number $X \geq 2$, define

$$R(S, X) := \frac{\#\{p \leq X \text{ prime } : p \in S\}}{\#\{p \leq X \text{ prime }\}}.$$

If the limit $\lim_{X\to\infty} R(S, X)$ exists, we denote it by $\rho(S)$ and call it the *natural density of* S. Let

$$S(n) = \{p \text{ prime } : n|h(-4p)\};$$

here we write $h(-4p)$ for the class number of $\mathbb{Q}(\sqrt{-4p})$ to emphasize its dependence on p. From the above, classical results about primes in arithmetic progressions imply that $\rho(S(2)) = 1/2$ and $\rho(S(4)) = 1/4$. From (2.1), we see that 8 divides h if and only if p splits completely in $\mathbb{Q}(\zeta_8, \sqrt{1+i})$, where ζ_8 is a primitive 8th root of unity. Since this is a degree 8 extension of $\mathbb{Q}$, Čebotarev's density theorem implies that $\rho(S(8)) = 1/8$. For a discussion of these and similar density results, see [41, p.16-19].

The Cohen-Lenstra heuristics [4] can be adapted to this situation to predict the density of primes p such that 2^k divides h for $k \geq 1$. Cohen and Lenstra stipulate that an abelian group G occurs as the class group of an imaginary quadratic field with probability proportional to the inverse of the size of the automorphism group of G. Under this assumption, the cyclic group of order 2^{k-1} would occur as the 2-part of the class group of an imaginary quadratic number field twice as often as the cyclic group of order 2^k. As we just saw above, $\rho(S(2^k)) = \frac{1}{2}\rho(S(2^{k-1}))$ for $k \leq 3$, so we are led to conjecture

Conjecture 2.1. *For all $k \geq 1$, the limit $\lim_{X\to\infty} R(S(2^k), X)$ exists and is equal to 2^{-k}.*

While Conjecture 2.1 is true for $k \leq 3$, it has not been proven for any $k \geq 4$. In fact, proving the conjecture for $k \geq 4$ would likely require significant new ideas because a proof along the lines of the arguments for $k \leq 3$ seems far out of reach (see [41, p. 16]). Although several criteria for divisibility by 16 have been found already (see [26], [45], and [30]), none of them appear to be sufficient to produce even infinitely many primes p for which the class number of $\mathbb{Q}(\sqrt{-4p})$ is divisible by 16. This is precisely our aim in this chapter – we will show that there is an infinite number of primes p for which $16|h$ and also an infinite number of primes p for which $8|h$ but $16 \nmid h$. We also derive some consequences for the fundamental unit ϵ_p of the real quadratic number field $\mathbb{Q}(\sqrt{p})$.

We tackle the question of infinitude not by developing a new criterion for divisibility by 16 which handles all primes, but by focusing on a very special subset of primes. These are the primes of the form

$$p = a^2 + c^4, \qquad c \text{ even}. \tag{2.2}$$

The main theorem that we prove gives a new and very explicit criterion for divisibility by 16 of class numbers of $\mathbb{Q}(\sqrt{-4p})$ for p of the form (2.2).

Theorem 2.1. *Suppose p is a prime of the form $a^2 + c^4$, where a and c are integers. Let $h(-4p)$ denote the class number of $\mathbb{Q}(\sqrt{-4p})$.*

(i) If $a \equiv \pm 1 \bmod 16$ and $c \equiv 0 \bmod 4$, then $h(-4p) \equiv 0 \bmod 16$.

(ii) If $a \equiv \pm 3 \bmod 16$ and $c \equiv 2 \bmod 4$, then $h(-4p) \equiv 0 \bmod 16$.

(iii) If $a \equiv \pm 7 \bmod 16$ and $c \equiv 0 \bmod 4$, then $h(-4p) \equiv 8 \bmod 16$.

(iv) If $a \equiv \pm 5 \bmod 16$ and $c \equiv 2 \bmod 4$, then $h(-4p) \equiv 8 \bmod 16$.

Once we prove Theorem 2.1, Theorem A follows from the following generalization of a powerful theorem of Friedlander and Iwaniec (see [19, Theorem 1]):

Proposition 2.1. *Let $a_0 \in \{1,3,5,7,9,11,13,15\}$ and $c_0 \in \{0,2\}$. Then, uniformly for $X \geq 3$, we have the equality*

$$\sum_{\substack{a^2+c^4 \leq X \\ a \equiv a_0 \bmod 16 \\ c \equiv c_0 \bmod 4 \\ a^2+c^4 \text{ prime}}} \sum 1 = \frac{\kappa}{2\pi} \frac{X^{3/4}}{\log X} \left(1 + O\left(\frac{\log\log X}{\log X}\right)\right), \tag{2.3}$$

where a and c run over $\mathbb{Z}$ and

$$\kappa = \int_0^1 (1-t^4)^{\frac{1}{2}} dt \approx 0.874\ldots.$$

In particular, there exist infinitely many primes of the form $a^2 + c^4$ with $a \equiv a_0 \bmod 16$ and $c \equiv c_0 \bmod 4$.

Proposition 2.1 also implies the infinitude of primes p of the form as in the statements $(i) - (iv)$ Theorem 2.1. We have the following quantitative result:

Corollary 2.1. *For a prime p, let $h(-4p)$ denote the class number of $\mathbb{Q}(\sqrt{-4p})$.* [redacted] *Then, for sufficiently large X, we have*

$$\#\{p \leq X : h(-4p) \equiv 0 \bmod 16\} \geq \frac{X^{3/4}}{8\log X}$$

and

$$\#\{p \leq X : h(-4p) \equiv 8 \bmod 16\} \geq \frac{X^{3/4}}{8\log X}.$$

The proof of Proposition 2.1 will take a significant portion of this chapter. Although the ideas required to generalize [19, Theorem 1] in this way are not particularly deep, implementing them turns out to be quite complicated simply because the proof of [19, Theorem 1] itself is very difficult. One can thus view Sections 2.4-2.6 as a summary of the proof of [19, Theorem 1] in a slightly more general context.

Since primes of the form $a^2 + c^4$ with c even have density 0 in the set of all primes, our methods cannot be used to tackle Conjecture 2.1. Nonetheless, each of the cases $(i) - (iv)$ in Theorem 2.1 occurs with the same density among all primes this form, so the analogous conjecture for $k = 4$ deduced from the Cohen-Lenstra heuristics above holds within the thin family of imaginary quadratic number fields $\mathbb{Q}(\sqrt{-4p})$ where p is a prime of the form $a^2 + c^4$ with c even. This is yet another piece of evidence suggesting that Conjecture 2.1 is true for $k = 4$. However, we also note that Conjecture 2.1 for $k = 4$ does not imply Corollary 2.1, as knowledge of the behavior of the class numbers of $\mathbb{Q}(\sqrt{-4p})$ over the set of all primes p does not necessarily give information about their behavior over a thin subset of all primes.

We now give a consequence of our results and a criterion for divisibility by 16 due to Williams [45]. Let $p \equiv 1 \bmod 8$, and let ϵ_p be a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$, written in the form $\epsilon_p = T + U\sqrt{p}$, where T and U are integers. The criterion states that if $8|h$, then

$$h \equiv T + p - 1 \bmod 16, \tag{2.4}$$

so that $16|h$ if and only if $T \equiv 1 - p \bmod 16$. An immediate byproduct of Theorem 2.1 and criterion (2.4) is the following corollary.

Corollary 2.2. *Suppose p is a prime of the form $a^2 + c^4$, where a is odd and c is even. Let $\epsilon_p = T + U\sqrt{p}$ denote a fundamental unit of $\mathbb{Q}(\sqrt{p})$.*

(i) If $a \equiv \pm 1 \bmod 16$ and $c \equiv 0 \bmod 4$, then $T \equiv 0 \bmod 16$ and $U \equiv \pm 1 \bmod 8$.

(ii) If $a \equiv \pm 3 \bmod 16$ and $c \equiv 2 \bmod 4$, then $T \equiv 8 \bmod 16$ and $U \equiv \pm 5 \bmod 8$.

(iii) If $a \equiv \pm 7 \bmod 16$ and $c \equiv 0 \bmod 4$, then $T \equiv 8 \bmod 16$ and $U \equiv \pm 1 \bmod 8$.

(iv) If $a \equiv \pm 5 \bmod 16$ and $c \equiv 2 \bmod 4$, then $T \equiv 0 \bmod 16$ and $U \equiv \pm 5 \bmod 8$.

This can be viewed as an extension of [27, Corollary 1.2(i), p.115-116] to primes of the form $p = a^2 + c^4$. Now Proposition 2.1 gives

Corollary 2.3. *For a prime $p \equiv 1 \bmod 8$, let $\epsilon_p = T + U\sqrt{p}$ denote the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Then, for sufficiently large X, we have*

$$\#\{p \leq X : p \equiv 1 \bmod 8,\ T \equiv 0 \bmod 16\} \geq \frac{X^{3/4}}{8 \log X}$$

and

$$\#\{p \leq X : p \equiv 1 \bmod 8,\ T \equiv 8 \bmod 16\} \geq \frac{X^{3/4}}{8 \log X}.$$

The existence of infinitely many $p \equiv 1 \bmod 8$ such that $T \equiv T_0 \bmod 16$ for a fixed $T_0 \in \{0, 8\}$ is not at all trivial. Hence Corollary 2.2 sheds some new light on the fundamental unit ϵ_p of $\mathbb{Q}(\sqrt{p})$, one of the most mysterious quantities in number theory.

2.1 Hilbert class fields

Suppose $p \equiv 1 \pmod 4$. Then there are two finite primes of $\mathbb{Q}$ which ramify in $\mathbb{Q}(\sqrt{-4p})$, namely 2 and p. The prime $\mathfrak{p} = (\sqrt{-p})$ of $\mathbb{Q}(\sqrt{-4p})$ lying above

p is principal, and so its ideal class in Cl is the identity. Genus theory then implies that the class of the prime ideal $\mathfrak{t} = (2, 1+\sqrt{-p})$ of $\mathbb{Q}(\sqrt{-4p})$ lying above 2 is the unique element of order two in Cl. Assuming that h is divisible by 2^n for some non-negative integer n, to check that it is divisible by 2^{n+1}, it would suffice to check that the class of $\mathfrak{t}$ belongs to Cl^{2^n}.

2.1.1 2^n-Hilbert class fields

Suppose that $2^n|h$ for some non-negative integer n. Then recall that (1.11) induces a canonical isomorphism of cyclic groups of order 2^n

$$\left(\frac{\cdot}{H_{2^n}/K}\right) : \mathrm{Cl}/\mathrm{Cl}^{2^n} \longrightarrow \mathrm{Gal}(H_{2^n}/K). \tag{2.5}$$

Hence the class $[\mathfrak{t}]$ belongs to Cl^{2^n} if and only if $\mathfrak{t}$ has trivial Artin symbol in $\mathrm{Gal}(H_{2^n}/K)$. By class field theory, this is equivalent to $\mathfrak{t}$ splitting completely in H_{2^n}. Therefore

$$2^{n+1}|h \Longleftrightarrow [\mathfrak{t}] \text{ splits completely in } H_{2^n}. \tag{2.6}$$

The main idea of the proof of Theorem 2.1 is to write down explicitly the 8-Hilbert class field H_8 of $\mathbb{Q}(\sqrt{-4p})$, and then to characterize those p such that $\mathfrak{t}$ splits completely in H_8. We remark here that although Cohn and Cooke [7] have already written down H_8 in terms of the fundamental unit ϵ_p of the real quadratic number field $\mathbb{Q}(\sqrt{p})$ and certain integer solutions u and v to $p = 2u^2 - v^2$, not enough is known about either ϵ_p or u and v to deduce anything about the distribution of primes p such that $\mathfrak{t}$ splits completely in H_8.

2.1.2 Generating 2^n-Hilbert class fields

We first state and prove some lemmas which will prove to be useful in our quest to explicitly generate H_8.

The 2-Hilbert class field, also called the *genus field* of $\mathbb{Q}(\sqrt{-4p})$, is known to be $H_2 = \mathbb{Q}(i, \sqrt{p})$. Hence every 2^n-Hilbert class field of $\mathbb{Q}(\sqrt{-4p})$ contains $\mathbb{Q}(i)$, and so we can study the splitting behavior of $\mathfrak{t}$ in H_{2^n} by working over the quadratic subfield $\mathbb{Q}(i)$ of H_2. With this in mind, we now state some well-known generalities about the completion of $\mathbb{Q}(i)$ with respect to the prime ideal $(1+i)$ lying over 2.

This completion is $\mathbb{Q}_2(i)$, and its ring of integers $\mathbb{Z}_2[i]$ is a discrete valuation ring with uniformizer $m = 1+i$ and maximal ideal $\mathfrak{m} = (m)$. Let $U = (\mathbb{Z}_2[i])^\times$ denote the group of units of $\mathbb{Z}_2[i]$ and for each positive integer k, define $U^{(k)} = 1 + \mathfrak{m}^k$. Then there is a filtration

$$U = U^{(1)} \supset U^{(2)} \supset \cdots \supset U^{(k)} \supset \cdots.$$

For any $k \geq 3$, squaring gives an isomorphism $U^{(k)} \xrightarrow{\sim} U^{(k+2)}$. Indeed, let $1 + m^{k+2}y \in U^{(k+2)}$. Hensel's lemma implies that there exists $x \in \mathfrak{m}^{k-2}$ such that $x^2 + x = -m^{k-2}y$. Then $(1+2x)^2 = 1 + m^{k+2}y$ and $1 + 2x \in U^{(k)}$. It is not hard to see that

$$U = \langle i \rangle \times U^{(3)} = \langle i \rangle \times \langle 2 + i \rangle \times U^{(4)},$$

so that $U^2 = \langle -1 \rangle \times U^{(5)}$. In other words, $u \in U$ is a square in $\mathbb{Q}_2(i)$ if and only if $u \equiv \pm 1 \pmod{\mathfrak{m}^5}$. Moreover, if $\omega \equiv \pm 1 \pmod{\mathfrak{m}^4}$, then $\mathbb{Q}_2(i, \sqrt{\omega})$ is generated over $\mathbb{Q}_2(i)$ by a root of the polynomial $X^2 - X + (1 \mp \omega)/4$, which reduces to $X^2 + X$ or $X^2 + X + 1$ modulo $\mathfrak{m}$. We collect these observations into the following lemma.

Lemma 2.1. *Let ω be a unit in $\mathbb{Z}_2[i]$. Then $\mathbb{Q}_2(i, \sqrt{\omega})$ is unramified over $\mathbb{Q}_2(i)$ if and only if $\omega \equiv \pm 1 \pmod{\mathfrak{m}^4}$. Moreover, $\mathbb{Q}_2(i, \sqrt{\omega}) = \mathbb{Q}_2(i)$, i.e., ω is a square in $\mathbb{Q}_2(i)$ if and only if $\omega \equiv \pm 1 \pmod{\mathfrak{m}^5}$.*

Next, we state two lemmas which we will use to check that the extensions of $\mathbb{Q}(\sqrt{-4p})$ which we construct are normal and cyclic. First, in both Chapter 2 and Chapter 3, we will make extensive use of the following lemma from Galois theory (see [29, Chapter VI, Exercise 4, p.321]).

Lemma 2.2. *Let F be a field of characteristic different from 2, let $E = F(\sqrt{d})$, where $d \in F^\times \setminus (F^\times)^2$, and let $L = E(\sqrt{x})$, where $x \in E^\times \setminus (E^\times)^2$. Let $N = \mathrm{Norm}_{E/F}(x)$. Then we have three cases:*

1. *If $N \notin (E^\times)^2 \cap F^\times = (F^\times)^2 \cup d \cdot (F^\times)^2$, then L/F has normal closure $L(\sqrt{N})$ and $\mathrm{Gal}(L(\sqrt{N})/F)$ is a dihedral group of order 8.*

2. *If $N \in (F^\times)^2$, then L/F is normal and $\mathrm{Gal}(L/F)$ is a Klein four-group.*

3. *If $N \in d \cdot (F^\times)^2$, then L/F is normal and $\mathrm{Gal}(L/F)$ is a cyclic group of order 4.*

Lemma 2.3. *Let K be a field. Suppose M/K is a cyclic extension of degree $2m$ and let σ be a generator of $\mathrm{Gal}(M/K)$. Let L be the subfield of M fixed by σ^m. Suppose N/K is a Galois extension containing M such that N/L is cyclic of degree 4. Then N/K is cyclic of degree $4m$.*

Proof. Let σ_1 denote a lift of σ to $\mathrm{Gal}(N/K)$. The order of σ_1 is at least $2m$ since the order of σ is $2m$. As σ^m fixes L, σ_1^m is an element of $\mathrm{Gal}(N/L)$which is non-trivial on M and hence has order 4. Thus the order of σ_1 is $4m$. □

Finally, we arrive at the main lemma we will use to construct 2^n-Hilbert class fields from 2^{n-1}-Hilbert class fields. This result is inspired by a theorem of Reichardt [36, 3. Satz, p.82]. His theorem proves the existence of generators $\sqrt{\varpi}$ for H_{2^n} over $H_{2^{n-1}}$ with $\varpi \in H_{2^{n-1}}$ of a certain form. We prove sufficient conditions for an element ϖ of a similar form to give rise to a generator, so that we can actually construct H_{2^n}.

Lemma 2.4. *Let h be the class number of $\mathbb{Q}(\sqrt{-4p})$, let $n \geq 2$, and suppose that 2^n divides h. Suppose that we have a sequence of field extensions*

$$\mathbb{Q} = A_1 \subset \mathbb{Q}(i) = A_2 \subset A_4 \subset \cdots \subset A_{2^{n-1}}$$

such that:

- *A_{2^k} is a degree 2^k extension of $\mathbb{Q}$ for $1 \leq k \leq n-1$,*
- *$A_{2^k} \subset H_{2^k}$ for $1 \leq k \leq n-1$,*
- *$A_{2^k} \cap H_{2^{k-1}} = A_{2^{k-1}}$ for $2 \leq k \leq n-1$,*
- *$(1+i)$ is unramified in $A_{2^{n-1}}/\mathbb{Q}(i)$, and*
- *there is a prime element ϖ in the ring of integers of $A_{2^{n-1}}$ such that:*
  - *ϖ lies above p and its ramification and inertia indices over p are equal to 1,*
  - *denoting the conjugate of ϖ over $A_{2^{n-2}}$ by ϖ', we have $H_{2^{n-1}} = H_{2^{n-2}}(\sqrt{\varpi\varpi'}) = A_{2^{n-1}}(\sqrt{\varpi\varpi'})$,*
  - *(U_2): $(1+i)$ remains unramified in $A_{2^n} = A_{2^{n-1}}(\sqrt{\varpi})$, and*
  - *(N): $H_{2^{n-1}}(\sqrt{\varpi})$ is normal over $\mathbb{Q}$.*

Then $H_{2^n} = H_{2^{n-1}}(\sqrt{\varpi})$.

Proof. The ramification index of ϖ over p is 1, so ϖ and ϖ' are coprime in $A_{2^{n-1}}$.

First we check that ϖ is not a square in $H_{2^{n-1}}$. Since $[A_{2^n} : A_{2^{n-1}}] = [H_{2^{n-1}} : A_{2^{n-1}}] = 2$ and $A_{2^n} = A_{2^{n-1}}(\sqrt{\varpi})$, we deduce that ϖ is a square in $H_{2^{n-1}}$ if and only if $A_{2^n} = H_{2^{n-1}}$. But this cannot happen because the ramification index of p in $H_{2^{n-1}}$ is 2, while ϖ' has ramification index 1 over p and, as ϖ and ϖ' are coprime, ϖ' remains unramified in A_{2^n}.

By assumption, $H_{2^{n-1}}(\sqrt{\varpi})$ is normal over $\mathbb{Q}$, and hence also over $\mathbb{Q}(\sqrt{-4p})$ and $H_{2^{n-2}}$. Since ϖ and ϖ' are conjugates over $A_{2^{n-2}}$, they are also conjugates over $H_{2^{n-2}}$. As $H_{2^{n-1}} = H_{2^{n-2}}(\sqrt{\varpi\varpi'})$ and $\varpi\varpi' = \varpi\varpi' \cdot 1^2$, Lemma 2.2 implies that $H_{2^{n-1}}(\sqrt{\varpi})$ is degree 4 cyclic extension of $H_{2^{n-2}}$. Moreover, $H_{2^{n-1}}$ is a degree 2^{n-1} cyclic extension of $\mathbb{Q}(\sqrt{-4p})$, so Lemma 2.3 implies that $H_{2^{n-1}}(\sqrt{\varpi})$ is a degree 2^n cyclic extension of $\mathbb{Q}(\sqrt{-4p})$.

It remains to show that $H_{2^{n-1}}(\sqrt{\varpi})/\mathbb{Q}(\sqrt{-4p})$ is unramified. We will establish this by showing that each of the ramification indices of the primes 2 and p in $H_{2^{n-1}}(\sqrt{\varpi})$ is at most 2.

The prime 2 ramifies in $\mathbb{Q}(i)$, but by assumption $(1+i)$ is unramified in

A_{2^n}. As $H_{2^{n-1}}(\sqrt{\varpi}) = A_{2^n}(\sqrt{\varpi\varpi'})$ and $p \equiv 1 \bmod 4$, Lemma 2.1 ensures that $(1+i)$ is unramified in $H_{2^{n-1}}(\sqrt{\varpi})$. Hence the ramification index of 2 in $H_{2^{n-1}}(\sqrt{\varpi})$ is 2.

Now note that $[H_{2^{n-1}}(\sqrt{\varpi}) : A_{2^n}] = 2$, the ramification index of the prime ϖ' over p is 1, and ϖ' does not ramify in $A_{2^n}/A_{2^{n-1}}$. Hence the ramification index of p in $H_{2^{n-1}}(\sqrt{\varpi})$ is at most 2, and this completes the proof. □

2.1.3 Explicit constructions of H_4 and H_8

Recall from (2.6) that 4 divides h if and only if the prime $\mathfrak{t}$ of $\mathbb{Q}(\sqrt{-4p})$ lying over 2 splits in H_2, which happens if and only if $(1+i)$ splits in $H_2/\mathbb{Q}(i)$. As H_2 is obtained from $\mathbb{Q}(i)$ by adjoining a square root of p, Lemma 2.1 implies that this happens if and only if $p \equiv \pm 1 \pmod{\mathfrak{m}^5}$, which, for $p \equiv 1 \pmod 4$, is true if and only if $p \equiv 1 \pmod 8$. Thus we have recovered the criterion for divisibility by 4.

From now on, assume that 4 divides h, i.e. that $p \equiv 1 \pmod 8$. We will now use Lemma 2.4 to construct the 4-Hilbert class field of $\mathbb{Q}(\sqrt{-4p})$.

A prime $p \equiv 1 \pmod 4$ splits in $\mathbb{Q}(i)$, so that there exists π in $\mathbb{Z}[i]$ such that $p = \pi\overline{\pi}$; here $\overline{\pi}$ denotes the conjugate of π over $A_1 := \mathbb{Q}$. If we write π as $a+bi$ with a and b integers, then we see that $p = a^2 + b^2$. We choose π so that b is even. As $p \equiv 1 \pmod 8$, we see that b is in fact divisible by 4. Hence

$$\pi = a + bi, \quad b \equiv 0 \bmod 4. \tag{2.7}$$

Now fix a square root of π and denote it by $\sqrt{\pi}$. Recall that $H_2 = \mathbb{Q}(i, \sqrt{p})$ is the 2-Hilbert class field of $\mathbb{Q}(\sqrt{-4p})$. We claim that the hypotheses of Lemma 2.4 for $n = 2$ are satisfied with $A_2 := \mathbb{Q}(i)$ and $\varpi = \pi$.

All of the hypotheses other than (U_2) and (N) are easy to check. Note that our choice of π ensures that $\pi \equiv \pm 1 \pmod 4$, so that (U_2) follows from Lemma 2.1. To see that (N) is satisfied, note that $H_2(\sqrt{\pi})$ is the splitting field (over $\mathbb{Q}$) of the polynomial $f_4(X) := (X^2 - \pi)(X^2 - \overline{\pi})$. Indeed, $\pi\overline{\pi}$ is a square in H_2, so both square roots of $\overline{\pi}$ are also contained in $H_2(\sqrt{\pi})$. Hence we conclude by Lemma 2.4 that the 4-Hilbert class field is given by

$$H_4 = H_2(\sqrt{\pi}) = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi}) \tag{2.8}$$

with π as in (2.7).

$$\begin{tikzcd}
& H_4 = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi}) \arrow[dl, dash] \arrow[d, dash] \\
A_4 = \mathbb{Q}(i, \sqrt{\pi}) \arrow[d, dash] & H_2 = \mathbb{Q}(i, \sqrt{p}) \arrow[dl, dash] \arrow[d, dash] \\
A_2 = \mathbb{Q}(i) \arrow[dr, dash] & \mathbb{Q}(\sqrt{-4p}) \arrow[d, dash] \\
& \mathbb{Q}
\end{tikzcd}$$

Next, we find a criterion for divisibility by 8. Recall that h is divisible by 8 if and only if $\mathfrak{t}$ splits completely in H_4, i.e. if and only if π is a square in $\mathbb{Q}_2(i)$. By Lemma 2.1, this happens if and only if $\pi \equiv \pm 1 \pmod{\mathfrak{m}^5}$. In terms of a and b from (2.7), this means that

$$8|h \Longleftrightarrow a + b \equiv \pm 1 \bmod 8.$$

We remark that Fouvry and Klüners developed similar methods in [16], where they constructed an analogue of the 4-Hilbert class field to deduce a criterion for the 8-rank of class groups in a family of real quadratic number fields. From now on, suppose that $8|h$. Replacing π by $-\pi$ if necessary, we assume that

$$\pi \equiv 1 \pmod{\mathfrak{m}^5}. \tag{2.9}$$

This means that $a + b \equiv 1 \pmod 8$. Our choice of $\sqrt{\pi}$ above is only unique up to sign. By Hensel's lemma, we can now fix this sign by imposing that

$$\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^3}. \tag{2.10}$$

In order to explicitly generate H_8 from H_4 using Lemma 2.4, we are led to the problem of finding a prime element in $A_4 = \mathbb{Q}(i, \sqrt{\pi})$ whose norm down to $\mathbb{Q}(i)$ is $\overline{\pi}$, up to units. This is the problem that we cannot solve explicitly enough in general to answer questions about infinitude or density.

However, for a very thin subset of primes, we can write down an element of A_4 of norm $-\overline{\pi}$. These are primes p of the form

$$p = a^2 + c^4, \quad c \text{ even}, \tag{2.11}$$

that is, primes p of the form $a^2 + b^2$ with b a perfect square divisible by 4.

Suppose that p is a prime of the form (2.11). Set

$$\varpi_0 = c(1 + i) + \sqrt{\pi}. \tag{2.12}$$

For $1 \leq m \leq 3$, set $\varpi_m = \sigma^m(\varpi)$, where σ is a generator for $\mathrm{Gal}(H_4/\mathbb{Q}(\sqrt{-4p}))$. [redacted] The restriction of σ to H_2 generates $\mathrm{Gal}(H_2/\mathbb{Q}(\sqrt{-4p}))$, so $\sigma(i) = -i$. Also, looking at the polynomial $f_4(X)$ above, we see that $\sigma(\sqrt{\pi}) = -\sqrt{\pi}$. Hence

$$\varpi_0 \cdot \varpi_2 = (c(1+i) + \sqrt{\pi})(c(1+i) - \sqrt{\pi}) = -\overline{\pi}. \tag{2.13}$$

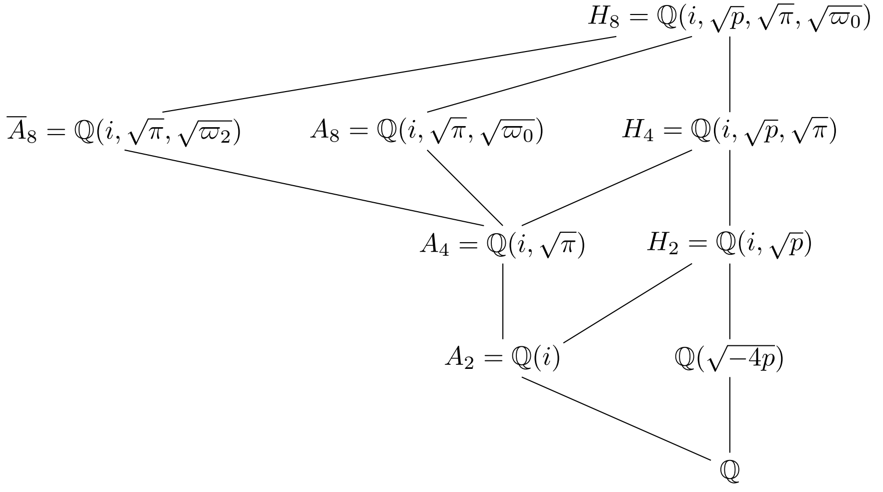
and

$$\varpi_1 \cdot \varpi_3 = (c(1-i) + \sigma(\sqrt{\pi}))(c(1-i) - \sigma(\sqrt{\pi})) = -\pi. \tag{2.14}$$

We can now prove the main result of this section.

Proposition 2.2. *Let p be a prime of the form* (2.11)*, let π be as in* (2.9)*, let $\sqrt{\pi}$ be as in* (2.10)*, and let ϖ_0 be as in* (2.12)*. Let $\sqrt{\varpi_0}$ denote a square root of ϖ_0. Then $H_4(\sqrt{\varpi_0})$ is the 8-Hilbert class field of $\mathbb{Q}(\sqrt{-4p})$.*

Proof. We again use Lemma 2.4, but this time with $n = 3$, $A_4 = \mathbb{Q}(i, \sqrt{\pi})$ and $\varpi = \varpi_0$. All of the hypotheses except for (U_2) and (N) immediately follow from the identity (2.13).


$H_8 = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi}, \sqrt{\varpi_0})$
$\overline{A}_8 = \mathbb{Q}(i, \sqrt{\overline{\pi}}, \sqrt{\varpi_2})$
$A_8 = \mathbb{Q}(i, \sqrt{\pi}, \sqrt{\varpi_0})$
$H_4 = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi})$
$A_4 = \mathbb{Q}(i, \sqrt{\pi})$
$H_2 = \mathbb{Q}(i, \sqrt{p})$
$A_2 = \mathbb{Q}(i)$
$\mathbb{Q}(\sqrt{-4p})$
$\mathbb{Q}$

We now prove hypothesis (N). We claim that $H_4(\sqrt{\varpi_0})$ is the splitting field of the polynomial

$$f_8(X) = (X^2 - \varpi_0)(X^2 - \varpi_1)(X^2 - \varpi_2)(X^2 - \varpi_3).$$

It is easy to see that $\varpi_0\varpi_2 = -\overline{\pi}$ and $\varpi_1\varpi_3 = -\pi$ are squares in H_4. To prove (N), it now suffices to show that $\varpi_0\varpi_1$ is a square in H_4. Let

$$d = \frac{\sqrt{\pi} + \sigma(\sqrt{\pi})}{2} \quad \text{and} \quad e = \frac{\sqrt{\pi} - \sigma(\sqrt{\pi})}{2i} \in H_4.$$

Then

$$\begin{aligned}\varpi_0 \cdot \varpi_1 &= (c(1+i)+\sqrt{\pi})(c(1-i)+\sigma(\sqrt{\pi}))\\ &= 2c^2+\sqrt{\pi}\sigma(\sqrt{\pi})+c\left((1+i)\sigma(\sqrt{\pi})+(1-i)\sqrt{\pi}\right)\\ &= (c^2+2de)+(d^2+e^2)+c(2d+2e)=(c+d+e)^2,\end{aligned}$$

which completes the proof of hypothesis (N).

It remains to prove hypothesis (U_2). The assumption that $\pi \equiv 1 \pmod{\mathfrak{m}^5}$ actually means that π is a square in $\mathbb{Q}_2(i)$, i.e. that $(1+i)$ splits in A_4. Hence it remains to show that $\mathbb{Q}_2(i, \sqrt{\varpi_0})$ is unramified over $\mathbb{Q}_2(i)$, and Lemma 2.1 implies that it is enough to prove that $\varpi_0 \equiv \pm 1 \pmod{\mathfrak{m}^4}$.

Recall from (2.10) that $\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^3}$, so that $\sqrt{\pi} \equiv 1$ or $1+m^3 \pmod{\mathfrak{m}^4}$. Squaring, we find that $\pi \equiv 1$ or $1+m^5 \pmod{\mathfrak{m}^6}$, respectively. Also recall that $a+b \equiv 1 \bmod 8$, i.e., $a+c^2 \equiv 1 \pmod{\mathfrak{m}^6}$. We now split our argument into two cases, the first when $c \equiv 0 \bmod 4$ and the second when $c \equiv 2 \bmod 4$.

If $c \equiv 0 \pmod{\mathfrak{m}^4}$, then $c^2 \in \mathfrak{m}^6$, so $a-1 \in \mathfrak{m}^6$ as well. Then $\pi = a + c^2 i \equiv 1 \pmod{\mathfrak{m}^6}$, which means that $\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^4}$. Then

$$\varpi_0 = c(1+i)+\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^4}.$$

If $c \equiv 2 \pmod{\mathfrak{m}^4}$, then $c^2 \equiv -m^4 \pmod{\mathfrak{m}^6}$. In this case, we have $a-1+m^4 \in \mathfrak{m}^6$, so that $\pi = a+c^2 i \equiv 1-m^4-m^4 i \equiv 1+m^4(-1-i) \equiv 1+m^5 \pmod{\mathfrak{m}^6}$. This means that $\sqrt{\pi} \equiv 1+m^3 \pmod{\mathfrak{m}^4}$, and hence

$$\varpi_0 = \sqrt{\pi}+c(1+i) \equiv 1+m^3+m^3 \equiv \pm 1 \pmod{\mathfrak{m}^4}.$$

This finishes the proof that $\mathbb{Q}_2(i, \sqrt{\varpi_0})$ is unramified over $\mathbb{Q}_2(i)$. □

2.2 Proof of Theorem 2.1

The proof of Theorem 2.1 will proceed in much the same way as the last part of the proof of Proposition 2.2. Now, instead of showing that $\mathbb{Q}_2(i, \sqrt{\varpi_0})$ is unramified over $\mathbb{Q}_2(i)$, we must decide when this extension is trivial (i.e. when $\mathfrak{t}$ splits completely in H_8) and when it is unramified of degree 2 (i.e. when $\mathfrak{t}$ does not split completely in H_8). This is equivalent to determining when ϖ_0 is a square in $\mathbb{Q}_2(i)$.

We will distinguish between two cases as above. The first case is when $c \equiv 0 \pmod 4$, i.e., $c \in \mathfrak{m}^4$. Recall from above that then $a \equiv 1 \pmod 8$ and $\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^4}$.

To check whether or not ϖ_0 is a square in $\mathbb{Q}_2(i)$, we must compute ϖ_0 modulo $\mathfrak{m}^5$. Since $c \equiv 0 \pmod 4$, we deduce that $\varpi_0 \equiv \sqrt{\pi}$ modulo $\mathfrak{m}^5$. Thus, we must determine conditions on a such that $\sqrt{\pi} \equiv \pm 1 \pmod{\mathfrak{m}^5}$, and for this, by Hensel's lemma, it is necessary to determine π modulo $\mathfrak{m}^7$. Hence, assuming $c \equiv 0 \pmod 4$,

$$\begin{aligned} 16|h \quad &\iff \quad \sqrt{\pi} \equiv \pm 1 \pmod{\mathfrak{m}^5} \\ &\iff \quad \pi \equiv 1 \pmod{\mathfrak{m}^7} \\ &\iff \quad a \equiv 1 \pmod{16}. \end{aligned}$$

This proves parts (i) and (iii) of Theorem 2.1.

We handle the second case similarly. Now $c \equiv 2 \pmod 4$, $a \equiv 5 \pmod 8$ and $\sqrt{\pi} \equiv 1 + m^3 \pmod{\mathfrak{m}^4}$. Then $\varpi_0 \equiv 2m + \sqrt{\pi}$ modulo $\mathfrak{m}^5$ and so we must determine conditions on a such that $\sqrt{\pi} \equiv \pm 1 - 2m \pmod{\mathfrak{m}^5}$. Under the current assumptions,

$$\begin{aligned} 16|h \quad &\iff \quad \sqrt{\pi} \equiv \pm 1 - 2m \pmod{\mathfrak{m}^5} \\ &\iff \quad \pi \equiv 1 + m^5 + m^6 \pmod{\mathfrak{m}^7} \\ &\iff \quad a \equiv -3 \pmod{16}. \end{aligned}$$

Note that because of the choice (2.9) we have actually shown the theorem for $a \equiv 1 \pmod 4$. If $p = a^2 + c^4$ with $a \equiv 3 \pmod 4$, then $p = (-a)^2 + c^4$ with $-a \equiv 1 \pmod 4$, so that the other cases can be deduced immediately. This finishes the proof of Theorem 2.1.

2.3 Overview of the proof of Proposition 2.1

In [19], Friedlander and Iwaniec prove an asymptotic formula for the number of primes of the form $a^2 + c^4$, that is, primes of the form $a^2 + b^2$ where b itself is a square. For a summary of their proof, see the exposition in [20, Chapter 21]. They use a new sieve that they developed to detect primes in relatively thin sequences [18]. This sieve has its roots in the work of Fouvry and Iwaniec [12], where they used similar sieve hypotheses to give an asymptotic formula for the number of primes of the form $a^2 + b^2$ where b is a prime.

The purpose of the following three sections is to demonstrate that the method of Friedlander and Iwaniec is robust enough to incorporate congruence conditions on a and c. While we are convinced that the appropriate analogue of Proposition 2.1 is true when a and c satisfy reasonable congruence conditions modulo any positive integers q_1 and q_2, respectively, the technical obstacles necessary to insert the congruence condition for c are cumbersome. Hence we will restrict ourselves to the case $q_2 = 4$.

The proof of Proposition 2.1 involves certain alterations in the way that the sieve [18] is used. For this reason, we first briefly recall the inputs and the output of the sieve.

2.3.1 Asymptotic sieve for primes

Suppose (a_n) $(n \in \mathbb{N})$ is a sequence of non-negative real numbers. Then the asymptotic sieve for primes developed in [18] yields an asymptotic formula for

$$S(x) = \sum_{\substack{p \leq x \\ p \text{ prime}}} a_p \log p,$$

provided that the sequence (a_n) satisfies several hypotheses, all but two of which are not difficult to verify. To state them, we first need to fix some terminology. For $d \geq 1$, let

$$A_d(x) = \sum_{\substack{n \leq x \\ n \equiv 0 \bmod d}} a_n,$$

and let $A(x) = A_1(x)$. Moreover, let g be a multiplicative function, and define the *error term* $r_d(x)$ by the equality

$$A_d(x) = g(d)A(x) + r_d(x). \tag{2.15}$$

The hypotheses which are not difficult to verify are listed in equations (2.1)-(2.8) in [19]. We briefly recall them here. We assume the bounds

$$A(x) \gg A(\sqrt{x})(\log x)^2 \tag{H1}$$

and

$$A(x) \gg x^{\frac{1}{3}} \left(\sum_{n \leq x} a_n^2 \right)^{\frac{1}{2}}. \tag{H2}$$

We assume that the multiplicative function g satisfies

$$0 \leq g(p^2) \leq g(p) \leq 1, \tag{H3}$$

$$g(p) \ll p^{-1}, \tag{H4}$$

and

$$g(p^2) \ll p^{-2}. \tag{H5}$$

We also assume that for all $y \geq 2$,

$$\sum_{p \leq y} g(p) = \log \log y + c + O((\log y)^{-10}), \tag{H6}$$

where c is a constant depending only on g; this is the linear sieve assumption. Finally, we assume the bound

$$A_d(x) \ll d^{-1} \tau(d)^8 A(x) \tag{H7}$$

uniformly in $d \leq x^{\frac{1}{3}}$; here τ is the divisor function.

Now we state the two hypotheses which are more difficult to verify. The first is a classical sieve hypothesis; it is a condition on the average value of the error terms $r_d(x)$. Let $L = (\log x)^{2^{24}}$.

Hypothesis (R). *There exists $x_r > 0$ and $D = D(x)$ in the range*

$$x^{\frac{2}{3}} < D < x \tag{2.16}$$

such that for all $x \geq x_r$, we have

$$\sum_{\substack{d \text{ cubefree} \\ d \leq DL^2}} |r_d(t)| \leq A(x)L^{-2} \tag{R}$$

uniformly in $t \leq x$.

In our applications, D will be $x^{3/4-\varepsilon}$ for a sufficiently small ε. This condition about *remainders* will be called condition (R).

The second is a complicated condition on bilinear forms in the elements of the sequence (a_n) weighed by truncated sums of the Möbius function

$$\beta(n, C) = \mu(n) \sum_{c|n,\ c \leq C} \mu(c). \tag{2.17}$$

It is designed to make sure that the sequence (a_n) is orthogonal to the Möbius function; this is crucial in overcoming the parity problem. We now state this hypothesis, named (B) for *bilinear.*

Hypothesis (B). *Suppose (R) is satisfied for x_r and $D = D(x)$. Then there exists $x_b > x_r$ such that for every $x > x_b$, there exist δ, Δ, and P satisfying*

$$2 \leq \delta \leq \Delta,$$

$$2 \leq P \leq \Delta^{1/2^{35} \log\log x},$$

and such that for every C with

$$1 \leq C \leq xD^{-1},$$

and for every N with

$$\Delta^{-1}\sqrt{D} < N < \delta^{-1}\sqrt{x},$$

we have

$$\sum_m \left| \sum_{\substack{N \leq n \leq 2N \\ mn \leq x \\ (n, m\Pi)=1}} \beta(n, C) a_{mn} \right| \leq A(x)(\log x)^{-2^{26}}, \tag{B}$$

where

$$\Pi = \prod_{p \le P} p. \tag{2.18}$$

Note that establishing condition (R) for a larger D decreases the range of C and N for which we have to verify condition (B).

The main result of [18] is

Theorem 2.2. *Assuming hypotheses (H1)-(H7), (R), and (B), we have*

$$S(x) = HA(x)\left(1 + O\left(\frac{\log \delta}{\log \Delta}\right)\right),$$

where H is the positive constant given by the convergent product

$$H = \prod_p (1 - g(p))\left(1 - \frac{1}{p}\right)^{-1}$$

and the constant implied in the O-symbol depends on the function g and the constants implicit in (H1), (H2), and (H7).

2.3.2 Preparing the sieve for Proposition 2.1

For our application, we will denote by v' the analogue of a quantity v from the proof of Friedlander and Iwaniec in [19]. We take (a'_n) to be the following sequence. Suppose q_1 and q_2 are positive integers and let q denote the least common multiple of q_1 and q_2. We say that a pair of congruence classes

$$a_0 \bmod q_1 \qquad c_0 \bmod q_2$$

is *admissible* if for every pair of congruence classes

$$a_1 \bmod q \qquad c_1 \bmod q$$

such that $a_1 \equiv a_0 \bmod q_1$ and $c_1 \equiv c_0 \bmod q_2$, the congruence class $a_1^2 + c_1^4 \bmod q$ is a unit modulo q.

Example. Suppose that $a_0 \in \{1, 3, 5, 7, 9, 11, 13, 15\}$ and $c_0 \in \{0, 2\}$. Then the pair of congruence classes $a_0 \bmod 16$ and $c_0 \bmod 4$ is admissible.

Example. Suppose that $a_0 = c_0 = 1$. Then the pair of congruence classes $a_0 \bmod 3$ and $c_0 \bmod 2$ is *not* admissible. Indeed, $1 \equiv a_0 \equiv c_0 \bmod 6$ but $2 \equiv 1^2 + 1^4 \bmod 6$ is not invertible modulo 6. This does not mean, however, that there are no primes of the form $a^2 + c^4$ with $a \equiv 1 \bmod 3$ and $c \equiv 1 \bmod 2$; one such prime is $4^2 + 1^4$.

Henceforth, suppose q_1 and q_2 are positive integers, let q be the least common multiple of q_1 and q_2, and suppose $a_0 \bmod q_1$ and $c_0 \bmod q_2$ is an admissible pair of congruence classes. We define

$$a'_n := \sum_{\substack{a,\ b\ \in\ \mathbb{Z} \\ a^2+b^2=n \\ a \equiv a_0 \bmod q_1}} \sum \mathfrak{z}'(b), \tag{2.19}$$

where

$$\mathfrak{z}'(b) := \sum_{\substack{c \in \mathbb{Z} \\ c^2=b \\ c \equiv c_0 \bmod q_2}} 1. \tag{2.20}$$

Let g be the multiplicative function supported on cubefree integers defined in [19, Equation 3.16, p.961] as follows: let χ_4 denote the character of conductor 4; for $p \geq 3$ set

$$g(p)p = 1 + \chi_4(p)\left(1 - \frac{1}{p}\right)$$

and

$$g(p^2)p^2 = 1 + (1 + \chi_4(p))\left(1 - \frac{1}{p}\right);$$

finally, set $g(2) = \frac{1}{2}$ and $g(4) = \frac{1}{4}$. For our extension, we define a multiplicative function g' by setting

$$g'(n) = \begin{cases} g(n) & \text{if } (n,q) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then, provided that (H1)-(H7), (R), and (B) are satisfied with δ a large power of $\log x$ and Δ a small power of x, the asymptotic formula given by the sieve (see Theorem 2.2) is

$$S'(x) := \sum_{\substack{p \leq x \\ p \text{ prime}}} a'_p \log p = c(q_1,q_2)\frac{16\kappa}{\pi}x^{3/4}\left(1 + O\left(\frac{\log\log x}{\log x}\right)\right) \tag{2.21}$$

where

$$c(q_1,q_2) = \frac{1}{q_1 q_2}\prod_{p|q}(1 - g(p))^{-1}$$

and κ is the integral given in the statement of Proposition 2.1. Note that the sieve applied to the original sequence (a_n) from [19], with

$$a_n = \sum_{\substack{a,\ b\ \in\ \mathbb{Z} \\ a^2+b^2=n}} \sum \mathfrak{z}(b), \tag{2.22}$$

where

$$\mathfrak{z}(b) = \sum_{\substack{c \in \mathbb{Z} \\ c^2 = b}} 1, \tag{2.23}$$

yields the asymptotic formula

$$S(x) = \frac{16\kappa}{\pi} x^{3/4} \left(1 + O\left(\frac{\log\log x}{\log x}\right)\right)$$

(see [19, Theorem 1, p.946]). Thus $c(q_1, q_2)$ can be interpreted as the density of primes of the form $a^2 + c^4$ such that $a \equiv a_0 \bmod q_1$ and $c \equiv c_0 \bmod q_2$ within the set of all primes of the form $a^2 + c^4$.

Remark. Throughout the following two sections, we regard q_1 and q_2 as fixed constants, and so the implied constants in every bound we give may depend on q_1 and q_2, even if this dependence is not explicitly stated. Thus, whenever we state "the implied constant is absolute," the implied constant may actually depend on q_1 and q_2. In our application $q_1 = 16$ and $q_2 = 4$, so we are not concerned with uniformity of the above asymptotic formula with respect to q_1 and q_2.

It is obvious that our modified sequence (a'_n) satisfies (H1)-(H7) for the same reasons as the original sequence (a_n). We will prove that (a'_n) above satisfies condition (R) for general q_1 and q_2. The congruence condition on c is more difficult to insert into the proof of condition (B), so we prove condition (B) only for the special case where $q_2 = 4$ and $c_0 \in \{0, 2\}$.

2.4 Proof of condition (R)

Here we closely follow and refer to the arguments laid out in [19, Section 3, p.955-962]. Define

$$A'_d(x) := \sum_{\substack{n \le x \\ n \equiv 0 \bmod d}} a'_n$$

and

$$A'(x) := A'_1(x).$$

The goal is to check that the error terms $r'_d(x)$ defined by

$$r'_d(x) := A'_d(x) - g'(d)A'(x) \tag{2.24}$$

are small on average. To do this, we will prove an analogue of [19, Lemma 3.1, p.956], with $M_d(x)$ (representing the *main term* and defined in [19, p.955]) replaced by

$$M'_d(x) = \frac{1}{dq_1} \sum\sum_{0 < a^2 + b^2 \le x} \mathfrak{z}'(b)\rho(b; d) \qquad \text{if } (d, q) = 1$$

and $M'_d(x) = 0$ otherwise; here $\rho(b; d)$ is defined as in [19, p.955], i.e. it is the number of solutions α mod d to

$$\alpha^2 + b^2 \equiv 0 \bmod d.$$

We separate the case when d is not coprime to q because in this case $A'_d(x) = 0$. This follows because the pair of congruences a_0 mod q_1 and c_0 mod q_2 is admissible and hence a'_n is supported on n coprime to q. The lemma we wish to prove is now identical to [19, Lemma 3.1, p.956].

Lemma 2.5. *For any $D \geq 1$, any $\varepsilon > 0$, and any $x \geq 2$, we have*

$$\sum_{d \leq D} |A'_d(x) - M'_d(x)| \ll D^{\frac{1}{4}} x^{\frac{9}{16}+\varepsilon},$$

where the implied constant depends only on ε.

This result is useful because it is easy to obtain an asymptotic formula for $M'_d(x)$ where the coefficient of the leading term is, up to a constant, a nice multiplicative function of d. In fact, let h be the multiplicative function supported on cubefree integers defined in [19, (3.16), p.961] by

$$\begin{cases} h(p)p = 1 + 2(1 + \chi_4(p)) \\ h(p^2)p^2 = p + 2(1 + \chi_4(p)), \end{cases} \tag{2.25}$$

and define a multiplicative function h' by setting

$$h'(n) = \begin{cases} h(n) & \text{if } (n, q) = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{2.26}$$

Then following the same argument as in the proof of [19, Lemma 3.4, p.961], we get

Lemma 2.6. *For d cubefree we have*

$$M'_d(x) = g'(d) \frac{4\kappa x^{\frac{3}{4}}}{q_1 q_2} + O\left(h'(d) x^{\frac{1}{2}}\right),$$

where κ is the integral given in the statement of Proposition 2.1 and the implied constant is absolute. □

Combining Lemmas 2.5 and 2.6, we get, as in [19, Proposition 3.5, p.362],

Proposition 2.3. *Let*

$$a_0 \bmod q_1 \qquad c_0 \bmod q_2$$

be an admissible pair of congruence classes, let a'_n be defined as in (2.19), and let $r'_d(x)$ be defined as in (2.24). Then for every $\varepsilon > 0$ and every $D \geq 1$, there *exists an* $x_0 = x_0(\varepsilon) > 0$ *and* $C = C(\varepsilon) > 0$ *such that for every* $x \geq x_0$*, we have*

$$\sum_{\substack{d \ cubefree \\ d \leq D}} |r'_d(t)| \leq C D^{\frac{1}{4}} x^{\frac{9}{16}+\varepsilon}$$

uniformly for $t \leq x$*.*

Choosing $D = x^{\frac{3}{4}-8\varepsilon}$, we obtain hypothesis (R).

It remains to prove Lemma 2.5. We may assume that the sum is over $d \leq D$ with $(d,q)=1$. For such d, we first approximate the sum $A'_d(x)$ by a smoothed sum

$$A'_d(f) = \sum_{n \equiv 0 \bmod d} a'_n f(n),$$

where f is a smooth function satisfying:

- f is supported on $[0,x]$,
- $f(u) = 1$ for $0 < u \leq x-y$,
- $f^{(j)}(u) \ll y^{-j}$ for $x - y < u < x$,

where $y = D^{\frac{1}{4}} x^{\frac{13}{16}}$ and the implied constants depend only on j (see [19, p.958]). Since a'_n is supported on integers of the form $a^2 + c^4$, we trivially have

$$\sum_{\substack{d \leq D \\ (d,q)=1}} |A'_d(x) - A'_d(f)| \ll y x^{-\frac{1}{4}+\varepsilon},$$

where the implied constant depends only on ε. With the above choice of y, it remains to prove Lemma 2.5 with $A'_d(x)$ replaced by $A'_d(f)$. Similarly as on [19, p.958], we write

$$A'_d(f) = \sum_b \mathfrak{z}'(b) \sum_{\substack{\alpha \bmod d \\ \alpha^2+b^2 \equiv 0 \bmod d}} \sum_{\substack{a \equiv \alpha \bmod d \\ a \equiv a_0 \bmod q_1}} f(a^2+b^2). \tag{2.27}$$

Since $(d,q)=1$, so also $(d,q_1)=1$, and the two conditions $a \equiv \alpha \bmod d$ and $a \equiv a_0 \bmod q_1$ can be combined into one condition $a \equiv \alpha' \bmod dq_1$. In fact, fixing an integer $\bar{d}$ that is an inverse of d modulo q_1 and an integer $\bar{q}_1$ that is an inverse of q_1 modulo d, we can define α' as

$$\alpha' = \alpha q_1 \bar{q}_1 + a_0 d \bar{d}.$$

We apply Poisson's summation formula to the sum over a to obtain

$$\sum_{a \equiv \alpha' \bmod dq_1} f(a^2+b^2) = \frac{1}{dq_1} \sum_k e\left(\frac{\alpha' k}{dq_1}\right) \int_{-\infty}^{\infty} f(t^2+b^2) e\left(\frac{-tk}{dq_1}\right) dt.$$

Here and henceforth, we use the standard notation

$$e(t) := e^{2\pi i t}.$$

Substituting this into (2.27) we get

$$A'_d(f) = \frac{2}{dq_1} \sum_b \mathfrak{z}'(b) \sum_k \rho'(k, b; d) I(k, b; dq_1) dt,$$

where

$$\rho'(k, b; d) = \sum_{\substack{\alpha \bmod d \\ \alpha^2 + b^2 \equiv 0 \bmod d}} e\left(\frac{\alpha' k}{dq_1}\right),$$

and where

$$I(k, b; dq_1) = \int_0^\infty f(t^2 + b^2) \cos(2\pi t k / dq_1) dt$$

is defined exactly the same as on [19, p.959]. We define $M'_d(f)$ to be the main term in this expansion, i.e. the term corresponding to $k = 0$,

$$M'_d(f) = \frac{2}{dq_1} \sum_b \mathfrak{z}'(b) \rho(b; d) I(0, b; dq_1).$$

Since $I(0, b; dq_1) = I(0, b; q_1)$, the argument on page 959 shows that

$$\sum_{\substack{d \leq D \\ (d,q)=1}} |M'_d(f) - M'_d(x)| \ll y x^{-\frac{1}{4}} (\log x)^2 \ll D^{\frac{1}{4}} x^{\frac{9}{16} + \varepsilon},$$

where the implied constants depend only on ε. It remains to prove Lemma 2.5 with $A'_d(f)$ in place of $A'_d(x)$ and $M'_d(f)$ in place of $M'_d(x)$, i.e. to show that $M'_d(f)$ is indeed (on average) the main term in the above Fourier expansion of $A'_d(f)$.

Following the argument on [19, p.959-960], we see that it suffices to show an analogue of [19, Lemma 3.3, p.957] for $\rho'(k, l; d)$.

Lemma 2.7. *For any D, K, and $L \geq 1$, for any complex numbers $\xi(k, l)$, and for any $\varepsilon > 0$, we have the inequality*

$$\sum_{d \leq D} \left| \sum_{\substack{0 < k \leq K \\ 0 < l \leq L}} \sum \xi(k, l) \rho'(k, l; d) \right| \ll (D + \sqrt{DKL})(DKL)^\varepsilon \|\xi\|$$

where

$$\|\xi\|^2 = \sum_{\substack{0 < k \leq K \\ 0 < l \leq L}} \sum |\xi(k, l)|^2,$$

and the implied constant depends only on ε.

Recall the following inequality from [19, (3.6), p.957]: for any complex numbers α_n and any $D, N \geq 1$, we have

$$\sum_{d \leq D} \sum_{\substack{\nu \bmod d \\ \nu^2+1 \equiv 0 \bmod d}} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu n}{d}\right) \right| \ll D^{\frac{1}{2}} (D+N)^{\frac{1}{2}} \|\alpha\|, \tag{2.28}$$

where

$$\|\alpha\| := \left(\sum_n |\alpha_n|^2 \right)^{\frac{1}{2}},$$

and the implied constant is absolute. Lemma 2.7 can be proved in the same way as [19, Lemma 3.3, p.957] given the following analogue of inequality (2.28).

Lemma 2.8. *Let $D, N \geq 1$ and let α_n be any complex numbers. For integers d such that $(d, q_1) = 1$, let ν' be an integer in the unique residue class modulo dq_1 that reduces to ν modulo d and a_0 modulo q_1. Then there exists an absolute constant $C = C(q_1)$ such that for all D and N sufficiently large, we have*

$$\sum_{\substack{d \leq D \\ (d,q_1)=1}} \sum_{\substack{\nu \bmod d \\ \nu^2+1 \equiv 0 \bmod d}} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu' n}{dq_1}\right) \right| \leq C D^{\frac{1}{2}} (D+N)^{\frac{1}{2}} \|\alpha\|. \tag{2.29}$$

Inequality (2.28) is a consequence of a large sieve inequality applied to the rationals $\nu/d \bmod 1$ with ν ranging over the roots of $\nu^2 + 1 \equiv 0 \bmod d$ for d in a range around D. The large sieve inequality can be applied because these rationals ν/d are well-spaced modulo 1 for d in a certain range around D (i.e. pairwise differences are uniformly bounded from below by about $1/D$ instead of $1/D^2$). This is a key ingredient in the work of [12]. In our analogue, however, it is not clear that ν'/dq_1 are also well-spaced modulo 1 for d in a similar range around D. Nonetheless, we can reduce Lemma 2.8 to inequality (2.28) as follows.

We first split the sum over n into congruence classes modulo q_1 to get

$$\sum_{n_0 \bmod q_1} \sum_{\substack{n \leq N \\ n \equiv n_0 \bmod q_1}} \alpha_n e\left(\frac{\nu' n}{dq_1}\right) = \sum_{n_0 \bmod q_1} \sum_{m \leq (N-n_0)/q_1} \alpha_{m,n_0} e\left(\frac{\nu' m}{d}\right) e\left(\frac{\nu' n_0}{dq_1}\right),$$

where

$$\alpha_{m,n_0} = \alpha_{mq_1+n_0}.$$

Since $e\left(\nu' n_0/dq_1\right)$ does not depends on m, the sum on the left-hand-side of (2.29) is

$$\leq \sum_{n_0 \bmod q_1} \sum_{\substack{d \leq D \\ (d,q_1)=1}} \sum_{\substack{\nu \bmod d \\ \nu^2+1 \equiv 0 \bmod d}} \left| \sum_{m \leq (N-n_0)/q_1} \alpha_{m,n_0} e\left(\frac{\nu' m}{d}\right) \right|.$$

Now $e\left(\frac{\nu' m}{d}\right) = e\left(\frac{\nu m}{d}\right)$ and

$$\sum_m |\alpha_{m,n_0}|^2 \leq \sum_n |\alpha_n|^2,$$

so that by (2.28) we get

$$\sum_{\substack{d \leq D \\ (d,q_1)=1}} \sum_{\substack{\nu \bmod d \\ \nu^2+1 \equiv 0 \bmod d}} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu' n}{dq_1}\right) \right| \ll q_1 D^{1/2} (D + N/q_1)^{1/2} \|\alpha\|.$$

This finishes the proof of (2.8) and thus also the proof of condition (R).

2.5 Proof of condition (B)

Many of the upper bound estimates carried out in sections 4 and 5 of [19] require no changes since $0 \leq a'_n \leq a_n$ (compare (2.19) and (2.22)). In most cases, we now sum over fewer non-negative terms.

Recall that we established condition (R) with $D = x^{\frac{3}{4}-8\varepsilon}$. All of the refinements from [19, Section 4, p.962-966] remain valid for our modified sequence (a'_n). We briefly recall these refinements. First note that it is enough to prove the analogue of [19, Proposition 4.1, p.963]:

Proposition 2.4. *Let $c_0 \in \{0, 2\}$, let $q_2 = 4$, and let*

$$a_0 \bmod q_1 \qquad c_0 \bmod q_2$$

be an admissible pair of congruence classes. Define $\beta(n, C)$ as in (2.17), Π as in (2.18), and a'_n as in (2.19). Let $x \geq 3$, $\eta > 0$, and $A > 0$. Let P be in the range

$$(\log\log x)^2 \leq \log P \leq (\log x)(\log\log x)^{-2}. \tag{2.30}$$

Let

$$B = 4A + 2^{20}. \tag{2.31}$$

Then there exists $x_0 = x_0(\eta, A)$ such that for all $x \geq x_0$, for all N with

$$x^{\frac{1}{4}+\eta} < N < x^{\frac{1}{2}} (\log x)^{-B}, \tag{2.32}$$

and for all C with

$$1 \leq C \leq N^{1-\eta}, \tag{2.33}$$

we have

$$\sum_m \left| \sum_{\substack{N \leq n \leq 2N \\ mn \leq x \\ (n, m\Pi)=1}} \beta(n, C) a_{mn} \right| \leq A'(x)(\log x)^{5-A}. \tag{2.34}$$

2.5.1 From Propositions 2.3 and 2.4 to Proposition 2.1

Before proving Proposition 2.4, we deduce Proposition 2.1 from Propositions 2.3 and 2.4. Let $a_0 \in \{1,3,5,7,9,11,13,15\}$, $q_1 = 16$, $c_0 \in \{0,2\}$, and $q_2 = 4$. Then

$$a_0 \bmod q_1 \qquad c_0 \bmod q_2$$

is an admissible pair of congruences. We apply the asymptotic sieve for primes described in Section 2.3.1 to the sequence (a'_n) defined in (2.19). Hypotheses (H1)-(H7) for (a'_n) are verified in the same way as hypotheses (H1)-(H7) for the sequence (a_n) defined in (2.22) (see comment at the end of Section 2.3.2).

Proposition 2.3 implies that (a'_n) satisfies hypothesis (R) for $\varepsilon = 1/8000$,

$$D = x^{\frac{3}{4}-\frac{1}{1000}}, \tag{2.35}$$

which is indeed in the range (2.16), and $x_r = x_r(\varepsilon)$ large enough.

Applying Proposition 2.4 with the same D as in (2.35), with P any number in the range (2.30), with $A = 5+2^{26}$, and with $\eta = \frac{1}{100}$ establishes hypothesis (B) for the sequence (a'_n) with $\delta = (\log x)^B$, $\Delta = x^\eta$, and $x_b = \max\{x_r, x_0(\eta, A)\}$.

We then obtain the asymptotic formula (2.21) with

$$c(q_1, q_2) = \frac{1}{32},$$

which proves (2.3).

2.5.2 Proof of Proposition 2.4

Suppose that we are in the setting of Proposition 2.4. Now take $A' = 2A+2^{20}$ (see [19, p.1018]) and define

$$\vartheta := (\log x)^{-A}$$

and

$$\theta := (\log x)^{-A'} \tag{2.36}$$

as on [19, p.965]. We split the sum (2.34) by using a smooth partition of unity. Let p be a smooth function supported on an interval

$$N' < n \le (1+\theta)N'$$

with $N < N' < 2N$, and suppose that p is twice differentiable with

$$p^{(j)} \ll (\theta N)^{-j}$$

for $j = 0, 1, 2$ (see [19, (4.14), p.965]). It then suffices to show Proposition 2.4 with $\beta(n, C)$ replaced by a smoothed version

$$\beta(n) = \beta(n, C) = p(n)\mu(n) \sum_{c|n,\ c \leq C} \mu(c) \tag{2.37}$$

and the bound $\leq A'(x)(\log x)^{5-A}$ replaced by $\leq C\vartheta\theta A'(x)(\log x)^5$ (see [19, (4.17), p.965]). Moreover, one can split the sum over m in (2.34) into dyadic segments $M \leq m \leq 2M$ with M satisfying

$$\vartheta x \leq MN \leq x. \tag{2.38}$$

We remark that (2.32) now implies that $N \leq \vartheta\theta(MN)^{\frac{1}{2}}$. Sums over the remaining dyadic segments are bounded trivially at an acceptable cost. Again, for an acceptable cost, one can suppose that $\beta(n, C)$ is supported on n with

$$\tau(n) \leq \tau := (\log x)^{A+2^{20}}. \tag{2.39}$$

(see [19, p.963-966, 1018]). For convenience of notation, we also restrict the support of $\beta(n, C)$ to n satisfying

$$(n, \Pi) = 1, \tag{2.40}$$

where Π is defined in (2.18). Finally, let $\alpha(m)$ be any complex numbers supported on $M < m \leq 2M$ with $|\alpha(m)| \leq 1$, and define

$$\mathcal{B}'^*(M, N) := \sum\sum_{(m,n)=1} \alpha(m)\beta(n)a'_{mn}, \tag{2.41}$$

where $\beta(n) = \beta(n, C)$ is defined as in (2.37) (see [19, (4.20), p.966]). To establish condition (B) it then suffices to prove

Lemma 2.9. *Let $\eta > 0$ and $A > 0$ and take B as in* (2.31). *Then there exists $x_0 = x_0(\eta, A) > 0$ such that for all $x \geq x_0$, for all M and N satisfying* (2.32) *and* (2.38)*, and for all C satisfying* (2.33) *we have*

$$|\mathcal{B}'^*(M, N)| \leq \vartheta\theta(MN)^{\frac{3}{4}}(\log MN)^5. \tag{B'}$$

2.5.3 Proof of Lemma 2.9

In [19, Section 5], one begins to exploit the arithmetic in $\mathbb{Z}[i]$ and the inequality (B') is reduced to another inequality involving sums over Gaussian integers. In our context, where a'_n are defined in (2.19), equation [19, (5.2), p.967] now becomes (for $(m, n) = 1$)

$$a'_{mn} = \sum_{\substack{|w|^2=m \\ \mathrm{Im}\overline{w}z \equiv a_0 \bmod q_1}} \sum_{|z|^2=n} \mathfrak{Z}'(\mathrm{Re}\overline{w}z),$$

where the sum over z is restricted to primary Gaussian integers, i.e. z satisfying

$$z \equiv 1 \bmod 2(1+i).$$

Recall from (2.20) that the congruence condition $c \equiv c_0 \bmod q_2$ is incorporated into the definition of $\mathfrak{Z}'$. We now define $\alpha_w := \alpha(|w|^2)$ and $\beta_z := \beta(|z|^2)$ as on [19, p.967], so that (2.41) becomes

$$\mathcal{B}'^{*}(M,N) = \sum_{\substack{(w\overline{w}, z\overline{z})=1 \\ \mathrm{Im}\overline{w}z \equiv a_0 \bmod q_1}}\sum \alpha_w \beta_z \mathfrak{Z}'(\mathrm{Re}\overline{w}z). \tag{2.42}$$

Similarly as in [19, (5.7), p.967], we split the sum $\mathcal{B}'^{*}(M,N)$ into $O(q_1^4)$ sums by restricting the support of α_w to w in a fixed residue class modulo q_1 and β_z to z in a fixed residue class z_0 modulo $64q_1$, such that $z_0 \equiv 1 \bmod 2(1+i)$. Now the residue class of $\mathrm{Im}\overline{w}z$ modulo q_1 is fixed, and so we can eliminate the condition $\mathrm{Im}\overline{w}z \equiv a_0 \bmod q_1$.

We further modify the support of β_z as in equation [19, (5.13), p.969]. Let $r(\alpha)$ be a smooth periodic function of period 2π supported on $\varphi < \alpha \leq \varphi + 2\pi\theta$ (where θ is as defined in (2.36)) for some $-\pi < \varphi < \pi$ such that $r^{(j)} \ll \theta^{-j}$ for $j = 0, 1, 2$, and let

$$\beta_z = r(\alpha)p(n)\mu(n) \sum_{c|n,\ c \leq C} \mu(c), \tag{2.43}$$

where $\alpha = \arg z$ and $n = |z|^2$. Recall that by (2.39) and (2.40), $\beta_z = 0$ if either $\tau(|z|^2) > \tau$ or if $|z|^2$ is not coprime with Π. We remove the condition $(w\overline{w}, z\overline{z}) = 1$ from (2.42) at an acceptable cost as in [19, (5.10), p.968] to get

$$\mathcal{B}'(M,N) = \mathcal{B}'^{*}(M,N) + O\left(\left(M^{\frac{1}{4}}N^{\frac{5}{4}} + P^{-1}M^{\frac{3}{4}}N^{\frac{3}{4}}\right)(\log N)^3\right)$$

where

$$\mathcal{B}'(M,N) := \sum_{\mathrm{Im}\overline{w}z \equiv a_0 \bmod q_1}\sum \alpha_w \beta_z \mathfrak{Z}'(\mathrm{Re}\overline{w}z). \tag{2.44}$$

We then apply Cauchy-Schwarz as in [19, (5.17), p.970] and introduce a smooth radial majorant f supported on the annulus $\frac{1}{2}\sqrt{M} \leq |w| \leq 2\sqrt{M}$ (see [19, p.970]) to get

$$\mathcal{B}'(M,N) \ll M^{\frac{1}{2}}\mathcal{D}'(M,N)^{\frac{1}{2}},$$

where

$$\mathcal{D}'(M,N) := \sum_w f(w)\left|\sum_z \beta_z \mathfrak{Z}'(\mathrm{Re}\overline{w}z)\right|^2.$$

This eliminates the dependence on α_w, so that the sum over w above is free. After inserting a coprimality condition, we arrive at the sum

$$\mathcal{D}'^{*}(M,N) := \sum_{(z_1,z_2)=1}\sum \beta_{z_1}\overline{\beta}_{z_2}\mathcal{C}'(z_1,z_2) \tag{2.45}$$

where

$$\mathcal{C}'(z_1,z_2) := \sum_w f(w)\mathfrak{Z}'(\mathrm{Re}\overline{w}z_1)\mathfrak{Z}'(\mathrm{Re}\overline{w}z_2)$$

(see [19, (5.26), p.972] and [19, (5.27), p.972]). The coprimality condition was inserted at the cost

$$\mathcal{D}'^*(M,N) = \mathcal{D}'(M,N) + O\left(\tau^2(M^{\frac{3}{4}}N^{\frac{3}{4}} + P^{-1}M^{\frac{1}{2}}N^{\frac{3}{2}})(\log MN)^{516}\right)$$

(see [19, (5.22), p.972]). Recall that the congruence condition $c \equiv c_0 \bmod q_2$ is hidden in the definition of $\mathfrak{Z}'$, while the congruence condition $a \equiv a_0 \bmod q_1$ has been removed by restricting the support of β_z. To prove Lemma 2.9, we now have left to prove

Lemma 2.10. *Let $\eta > 0$ and $A > 0$, and take B as in* (2.31). *Then there exists $x_0 = x_0(\eta, A)$ such that for all $x \geq x_0$, for all M and N satisfying* (2.32) *and* (2.38), *and for all C satisfying* (2.33), *we have*

$$|\mathcal{D}'^*(M,N)| \leq C\vartheta^2\theta^4 M^{\frac{1}{2}}N^{\frac{3}{2}}(\log MN)^{10}. \tag{B”}$$

Note the extra factor of θ coming from the restriction of support of β to a sector of angle θ.

2.5.4 Proof of Lemma 2.10

In order to obtain this upper bound, Friedlander and Iwaniec introduce a quantity they call the “modulus”

$$\Delta = \Delta(z_1,z_2) = \mathrm{Im}(\overline{z}_1 z_2),$$

which is non-zero whenever $(z_1,z_2) = 1$ and z_1 and z_2 are odd and primitive. The sum defining $\mathcal{D}'^*(M,N)$ is split into several different sums depending on the size of the modulus Δ. Different techniques are used to treat each of these sums, but we will manage to avoid going into the details by reducing our sums to those already studied in [19].

The Fourier analysis carried out on [19, p.974] depends on the greatest common divisor of Δ and q_2. Using the Poisson summation formula similarly as on [19, p.974], equation (2.45) can now be written as

$$\mathcal{D}'^*(M,N) = \sum_{\delta|q_2} \sum\sum_{\substack{(z_1,z_2)=1 \\ (q_2,|\Delta|)=\delta}} \beta_{z_1}\overline{\beta}_{z_2}\mathcal{C}'(z_1,z_2),$$

where

$$\begin{aligned}\mathcal{C}'(z_1,z_2) \quad &= \quad (q_2/\delta)^{-2}|z_1z_2|^{-1/2} \\ &\quad \cdot \textstyle\sum_{h_1}\sum_{h_2} F\left(\frac{h_1}{|\Delta z_2|^{1/2}q_2/\delta}, \frac{h_2}{|\Delta z_1|^{1/2}q_2/\delta}\right) G'(h_1,h_2),\end{aligned} \tag{2.46}$$

the Fourier integral

$$F(u_1,u_2)=\int\int f\left(\frac{z_2}{|z_2|}t_1^2-\frac{z_1}{|z_1|}t_2^2\right)e(u_1t_1+u_2t_2)dt_1dt_2$$

is the same as the one defined in [19, (6.8), p.974] and

$$G'(h_1,h_2)=\frac{1}{|\Delta|}\sum\sum_{\substack{\gamma_1,\gamma_2 \bmod |\Delta| \\ \gamma_1^2z_2\equiv\gamma_2^2z_1 \bmod |\Delta| \\ \gamma_1\equiv\gamma_2\equiv c_0 \bmod \delta}} e\left(\frac{\gamma_1'h_1+\gamma_2'h_2}{|\Delta|q_2/\delta}\right)$$

is an arithmetic sum similar to $G(h_1,h_2)$ defined in [19, (6.10), p.974], but now incorporating the congruence condition $c\equiv c_0 \bmod q_2$; here γ_i' is the solution (modulo $\frac{|\Delta|q_2}{\delta}$) to the system of congruences

$$\begin{cases}\gamma_i'\equiv\gamma_i \bmod |\Delta|\\ \gamma_i'\equiv c_0 \bmod q_2.\end{cases}$$

Such a solution is guaranteed to exist because $\gamma_1\equiv\gamma_2\equiv c_0 \bmod \delta$. Note that similarly as in [19], we omit in the notation the dependence of F and G' on z_1 and z_2.

The *main term* in the above expansion for $\mathcal{C}'(z_1,z_2)$ comes, as usual, from the terms with $h_1=h_2=0$ in equation (2.46). Similarly as in the proof of condition (R) above, we don't need to make any changes in the treatment of the Fourier integral; [19, Lemma 7.1, p.976] and [19, Lemma 7.2, p.977] are still valid, with the implied constants now depending on q_2 as well. We recall that [19, Lemma 7.2, p.977] states that for z_1 and z_2 in the support of β_z we have

$$F_0(z_1,z_2):=F(0,0)=2\hat{f}(0)\log 2|z_1z_2/\Delta|+O(\Delta^2M^{\frac{1}{2}}N^{-2}\log N). \quad (2.47)$$

We now have to give an upper bound for $G'(h_1,h_2)$ similar to the bound given in [19, Lemma 8.1, p.978], as well as give an exact formula for

$$G_0'(z_1,z_2):=G'(0,0)$$

similar to the one in [19, Lemma 8.4, p.980]. This is where we now specialize to the case

$$q_2=4 \text{ and } c_0\in\{0,2\}.$$

Recall that we restricted the support of β_z to z in a fixed congruence class modulo $64q_1$. Hence $z_1\equiv z_2 \bmod 64$, so that $\Delta=\mathrm{Im}(\overline{z}_1z_2)\equiv 0 \bmod 64$. This significantly simplifies our arguments since now $\delta=(4,|\Delta|)=4$.

The arithmetic sum $G'(h_1,h_2)$ now simplifies to

$$G'(h_1,h_2)=\frac{1}{|\Delta|}\sum_{\substack{\gamma_1,\gamma_2 \bmod |\Delta| \\ \gamma_1^2 z_2\equiv\gamma_2^2 z_1 \bmod |\Delta| \\ \gamma_1\equiv\gamma_2\equiv c_0 \bmod 4}}\sum e\left(\frac{\gamma_1 h_1+\gamma_2 h_2}{|\Delta|}\right).$$

We first prove a lemma analogous to [19, Lemma 8.1, p.978].

Lemma 2.11. *Fix $\theta\in\{2,4\}$ and let*

$$G''(h_1,h_2;\theta)=\frac{1}{|\Delta|}\sum_{\substack{\gamma_1,\gamma_2 \bmod |\Delta| \\ \gamma_1^2 z_2\equiv\gamma_2^2 z_1 \bmod |\Delta| \\ \gamma_1\equiv\gamma_2\equiv 0 \bmod \theta}}\sum e\left(\frac{\gamma_1 h_1+\gamma_2 h_2}{|\Delta|}\right).$$

Then

$$|G''(h_1,h_2;\theta)|\le 16\tau_3(\Delta)|\Delta|^{-1}(z_1h_1^2-z_2h_2^2,\Delta). \qquad (2.48)$$

Introducing a change of variables $\gamma_1=\theta\omega_1$ and $\gamma_2=\theta\omega_2$, we get

$$G''(h_1,h_2;\theta)=\frac{1}{|\Delta|}\sum_{\substack{\omega_1,\omega_2 \bmod |\Delta|/\theta \\ \omega_1^2 z_2\equiv\omega_2^2 z_1 \bmod |\Delta|/\theta^2}}\sum e\left(\frac{\omega_1 h_1+\omega_2 h_2}{|\Delta|/\theta}\right).$$

Proceeding in a similar fashion as on [19, p.977-978], we write

$$\Delta/\theta=\theta\Delta_1(\Delta_2)^2,$$

with Δ_1 squarefree. The condition $\omega_1^2 z_2\equiv\omega_2^2 z_1 \bmod |\Delta|/\theta^2$ implies that $(\omega_1^2,\Delta/\theta^2)=(\omega_2^2,\Delta/\theta^2)$, so we can write

$$(\omega_1^2,\Delta/\theta^2)=(\omega_2^2,\Delta/\theta^2)=d_1d_2^2$$

with d_1 squarefree. Then $d_1|\Delta_1$, $d_2|\Delta_2$, $(d_1,\Delta_2/d_2)=1$, and we can make a change of variables $\omega_i=d_1d_2\eta_i$, there η_i runs over the residue classes modulo $|\Delta|/\theta d_1d_2$ and coprime with $|\Delta|/\theta^2 d_1d_2^2$. Setting $b_1=\Delta_1/d_1$ and $b_2=\Delta_2/d_2$, the analogue of the equation on top of [19, p.978] becomes

$$G''(h_1,h_2;\theta)=\frac{1}{|\Delta|}\sum_{\substack{b_1d_1=|\Delta_1| \\ b_2d_2=\Delta_2 \\ (d_1,b_2)=1}}\sum\ \sum_{\substack{\eta_1,\eta_2 \bmod \theta b_1b_2^2d_2 \\ (\eta_1\eta_2,b_1b_2)=1 \\ \eta_1^2z_2\equiv\eta_2^2z_1 \bmod b_1b_2^2}}\sum e((\eta_1h_1+\eta_2h_2)/\theta b_1b_2^2d_2)$$

The innermost sum vanishes unless $h_1\equiv h_2\equiv 0 \bmod \theta d_2$, so $G''(h_1,h_2)$ is equal to

$$\frac{1}{|\Delta|}\sum_{\substack{b_1d_1=|\Delta_1| \\ (d_1,b_2)=1}}\ \sum_{\substack{b_2d_2=\Delta_2 \\ \theta d_2|(h_1,h_2)}}\theta^2d_2^2\sum_{\substack{\eta_1,\eta_2 \bmod b_1b_2^2 \\ (\eta_1\eta_2,b_1b_2)=1 \\ \eta_1^2z_2\equiv\eta_2^2z_1 \bmod b_1b_2^2}}\sum e((\eta_1h_1+\eta_2h_2)/\theta b_1b_2^2d_2).$$

Performing the change of variables $\eta_2 = \omega\eta_1$, the analogue of equation [19, (8.3), p.978] becomes

$$\frac{1}{|\Delta|}\sum_{\substack{b_1d_1=|\Delta_1| \\ (d_1,b_2)=1}}\ \sum_{\substack{b_2d_2=\Delta_2 \\ \theta d_2|(h_1,h_2)}} \theta^2 d_2^2 \sum_{\omega\equiv z_2/z_1 \bmod b_1b_2^2} R((h_1+\omega h_2)(\theta d_2)^{-1}; b_1b_2^2),$$

where $R(h;b)$ is the classical Ramanujan sum defined on [19, p.978]. Now the same argument as on [19, p.978] yields the desired upper bound (2.48).□

We now turn our attention back to $G'(h_1,h_2)$. In case $c_0 = 0$, we're in the case of Lemma 2.11 and

$$|G'(h_1,h_2)| = |G''(h_1,h_2;4)| \leq 16\tau_3(\Delta)|\Delta|^{-1}(z_1h_1^2 - z_2h_2^2, \Delta).$$

If, on the other hand, $c_0 = 2$, we note that $G'(h_1,h_2) = G''(h_1,h_2;2) - G''(h_1,h_2;4)$ since $\Delta \equiv 0 \bmod 16$. Hence

$$|G'(h_1,h_2)| \leq 32\tau_3(\Delta)|\Delta|^{-1}(z_1h_1^2 - z_2h_2^2, \Delta).$$

The same arguments as those in Section 9 of [19] now suffice to show that the main term in the Fourier expansion indeed comes from $h_1 = h_2 = 0$. Specifically, if we define

$$\mathcal{D}_0'(M,N) := \sum\sum_{(z_1,z_2)=1} \beta_{z_1}\overline{\beta}_{z_2}\mathcal{C}_0'(z_1,z_2),$$

where

$$\mathcal{C}_0'(z_1,z_2) = |z_1z_2|^{-1/2}F_0(z_1,z_2)G_0'(z_1,z_2), \tag{2.49}$$

then the reader may easily check that the above estimates yield the following analogue of [19, (9.10), p.983].

Lemma 2.12. *Let $\eta > 0$ and $A > 0$, and take B as in* (2.31)*. Then there exists $x_0 = x_0(\eta, A)$ such that for all $x \geq x_0$, for all M and N satisfying* (2.32) *and* (2.38)*, and for all C satisfying* (2.33)*, we have*

$$|\mathcal{D}'^*(M,N) - \mathcal{D}_0'(M,N)| \leq \vartheta^{-1}\tau^2N^2(\log N)^{\eta^{-1/\eta}},$$

where τ is defined in (2.39)*.*

It now remains to estimate $\mathcal{D}_0'(M,N)$. We turn to obtaining an exact formula for $G_0'(z_1,z_2)$. Recall, from top of [19, p.979], that

$$G_0(z_1,z_2) := \frac{1}{|\Delta|}\sum\sum_{\substack{\gamma_1,\gamma_2 \bmod |\Delta| \\ \gamma_1^2z_2\equiv\gamma_2^2z_1 \bmod |\Delta|}} 1 = N(z_2/z_1;|\Delta|)/|\Delta|,$$

where $N(a;r)$ denotes the number of solutions (γ_1, γ_2) modulo r to

$$a\gamma_1^2 \equiv \gamma_2^2 \bmod r.$$

Similarly,

$$G_0'(z_1, z_2) = N'(z_2/z_1; |\Delta|)/|\Delta|,$$

where $N'(a;r)$ is the number of solutions (γ_1, γ_2) modulo r to the congruences

$$\begin{cases} a\gamma_1^2 \equiv \gamma_2^2 \bmod r \\ \gamma_1 \equiv \gamma_2 \equiv c_0 \bmod 4. \end{cases}$$

Since $z_2/z_1 \equiv 1 \bmod 64$ and $\Delta \equiv 0 \bmod 64$, we are only concerned with the case $a \equiv 1 \bmod 64$ and $r \equiv 0 \bmod 64$.

2.5.5 Computation of $N'(a;r)/r$

Case $c_0 = 0$

First let us compute $N'(a;r)/r$ when $c_0 = 0$. Since $\gamma_1 \equiv \gamma_2 \equiv 0 \bmod 4$, we can make a change of variables $\gamma_1 = 4\omega_1$ and $\gamma_2 = 4\omega_2$, where now ω_i are congruence classes modulo $r/4$, to find that $N'(a;r) = 16N(a;r/16)$, i.e.

$$N'(a;r)/r = N(a;r/16)/(r/16).$$

This leads to a formula of type [19, (8.16), p.980]. If $16 \cdot 2^\nu$ with $\nu \geq 1$ is the exact power of 2 dividing Δ, we get

$$G_0'(z_1, z_2) = \nu \sum_{\substack{16d|\Delta \\ d \text{ odd}}} \frac{\varphi(d)}{d} \left(\frac{z_2/z_1}{d}\right).$$

Since $\Delta \equiv 0 \bmod 64$, we are only interested in the case $\nu \geq 2$, where this becomes

$$G_0'(z_1, z_2) = 2 \sum_{64d|\Delta} \frac{\varphi(d)}{d} \left(\frac{z_2/z_1}{d}\right), \tag{2.50}$$

by the same reasoning as in [19, Lemma 8.4, p.980].

Case $c_0 = 2$

When $c_0 = 2$ and $4|r$, we can make a change of variables $\gamma_1 = 2\omega_1$ and $\gamma_2 = 2\omega_2$ so that $N'(a;r)$ is 4 times the number of solutions (ω_1, ω_2) modulo $r/4$ to the system of congruences

$$\begin{cases} \omega_1 \equiv \omega_2 \equiv 1 \bmod 2 \\ a\omega_1^2 \equiv \omega_2^2 \bmod r/4. \end{cases}$$

When $16|r$, we must subtract from $4N(a;r/4)$ those solutions with $\omega_1 \equiv \omega_2 \equiv 0 \bmod 2$. This gives $N'(a;r) = 4N(a;r/4) - 16N(a;r/16)$, i.e.

$$\frac{N'(a;r)}{r} = \frac{N(a;r/4)}{r/4} - \frac{N(a;r/16)}{r/16}.$$

Hence if $16 \cdot 2^{\nu}$ with $\nu \geq 2$ is the exact power of 2 dividing Δ, we get

$$G_0'(z_1, z_2) = 2 \sum_{16d|\Delta} \frac{\varphi(d)}{d} \left(\frac{z_2/z_1}{d}\right) - 2 \sum_{64d|\Delta} \frac{\varphi(d)}{d} \left(\frac{z_2/z_1}{d}\right), \qquad (2.51)$$

which is the analogue of (2.50).

2.5.6 End of proof of of Lemma 2.10

We now turn back to estimating $\mathcal{D}_0'(M,N)$. As in [19, (10.4), p.985], we can use (2.47) to write

$$\mathcal{D}_0'(M,N) = 2\hat{f}(0)N^{\frac{1}{2}}T'(\beta) + O\left((\tau^{-1} + \theta)Y'(\beta)M^{\frac{1}{2}}N^{-\frac{1}{2}}\log N\right)$$

where

$$T'(\beta) := \sum_{(z_1,z_2)=1}\sum \beta_{z_1}\overline{\beta}_{z_2} G_0'(z_1,z_2) \log 2|z_1z_2/\Delta|$$

and

$$Y'(\beta) := \sum_{(z_1,z_2)=1}\sum |\beta_{z_1}\overline{\beta}_{z_2}| \tau(|z_1|^2)\tau(|z_2|^2)\tau_3(\Delta).$$

Similarly as in [19, Lemma 10.1, p.985], we can bound $Y'(\beta)$ by

$$Y'(\beta) \ll \theta^4 N^2 (\log N)^{2^{19}},$$

so that we are left with estimating the sum $T'(\beta)$. In each of the cases $c_0 = 0$ and $c_0 = 2$, we can use the formula for $G_0'(z_1,z_2)$ and $F_0(z_1,z_2)$ to write $T'(\beta)$ as a sum similar to [19, (10.13), p.986]. If we define

$$T'(\beta,\xi) := 2\sum_{d} \frac{\varphi(d)}{d} \sum_{\substack{(z_1,z_2)=1 \\ \Delta(z_1,z_2)\equiv 0 \bmod \xi d}}\sum \beta_{z_1}\overline{\beta}_{z_2} \left(\frac{z_2/z_1}{d}\right) \log 2|z_1z_2/\Delta|,$$

then

$$T'(\beta) = \begin{cases} T'(\beta,64) & \text{if } c_0 = 0 \\ T'(\beta,16) - T'(\beta,64) & \text{if } c_0 = 2 \end{cases}$$

Lemma 2.10 now follows from this analogue of [19, Proposition 10.2, p.986]:

Lemma 2.13. *Fix $\xi \in \{16, 64\}$. Let $\eta > 0$, $A > 0$, and $\sigma > 0$, and take B as in* (2.31)*. Then there exists $x_0 = x_0(\eta, A)$ and $C_0 = C_0(\eta, A, \sigma) > 0$ such that for all $x \geq x_0$, for all N satisfying* (2.32)*, and for all C satisfying* (2.33)*, we have*

$$T'(\beta, \xi) \leq C_0 N^2 (\log N)^{-\sigma} + P^{-1} N^2 \log N,$$

where P is any number in the range (2.30)*.*

We recall that N and P appear as parameters restricting the support of β_z; see (2.43).

2.5.7 Proof of Lemma 2.13: oscillations of characters and symbols

Although complicated, the proof of [19, Proposition 10.2] generalizes directly to the proof of Lemma 2.13. One can check in [19, Sections 15-17] that the same arguments are valid when $\xi = 16$ or 64 instead of $\xi = 4$. For instance, on [19, p. 1005] and [19, p. 1015], one now sums over multiplicative characters of the groups $(\mathbb{Z}[i]/\xi d\mathbb{Z}[i])^\times$ and $(\mathbb{Z}[i]/\xi bd\mathbb{Z}[i])^\times$, respectively. Here b is a variable appearing from the Möbius inversion formula $\varphi(\Delta) = \sum_{b|\Delta} \mu(b) b^{-1}$ (see [19, p. 1013]).

Moreover, the restriction on the support of β_z to z in a fixed primary congruence class modulo $64q_1$ (where q_1 is as in (2.19)) as opposed to modulo 8 is handled in the same way as in [19, Sections 15-17]. For sums over medium-size moduli, the estimation of β_z is trivial and so the restriction on the support is irrelevant (see bottom of [19, p. 1003]). For sums over small moduli, i.e., d of size at most a large power of $\log N$, the key sum to bound from above is the character sum

$$S_\chi^k(\beta) = \sum_z \beta_z \chi(z) \left(\frac{z}{|z|}\right)^k, \tag{2.52}$$

where χ is a multiplicative character of the group $(\mathbb{Z}[i]/\xi d\mathbb{Z}[i])^\times$ (see [19, (16.14), p. 1005]). The restriction on the support of β_z can be detected by multiplicative characters modulo $64q_1$, so that we can simply transform χ into a character for the group $(\mathbb{Z}[i]/64q_1 d\mathbb{Z}[i])^\times$. The sum (2.52) is bounded by studying the Hecke L-functions

$$L(s, \psi) = \sum_{\mathfrak{a}} \psi(\mathfrak{a})(N\mathfrak{a})^{-s},$$

where the sum ranges over the non-zero odd ideals $\mathfrak{a}$ of $\mathbb{Z}[i]$ and

$$\psi(\mathfrak{a}) := \chi(z) \left(\frac{z}{|z|}\right)^k$$

where z is the unique primary Gaussian integer which generates $\mathfrak{a}$. The dependence on χ of the bound given for $S_\chi^k(\beta)$ is only through the modulus of

χ (see [19, Lemma 16.2, p. 1012]) and this modulus is different from $4d$ by a fixed constant. Similarly, for the sums over large moduli, the key sum to bound from above is the character sum

$$S_\chi^k(\beta') = \sum_z \beta'_z \chi(z) \left(\frac{z}{|z|} \right)^k , \tag{2.53}$$

where χ is a multiplicative character of the group $(\mathbb{Z}[i]/\xi bd\mathbb{Z}[i])^\times$ (where b is an integer and d is again bounded by a large power of $\log N$) but β'_z is now

$$\beta'_z = i^{\frac{r-1}{2}} \left(\frac{s}{|r|} \right) \beta_z$$

if $z = r + is$ (see [19, (17.8), p. 1014] and [19, (17.12), p. 1015]). Again, the restriction on the support of β_z (and hence also β'_z) can be detected by multiplicative characters modulo $64q_1$, so that we can transform χ into a character for the group $(\mathbb{Z}[i]/64q_1bd\mathbb{Z}[i])^\times$. Cancellation in the sum (2.53) is now achieved due to the oscillation of the symbol

$$i^{\frac{r-1}{2}} \left(\frac{s}{|r|} \right)$$

as z varies over primary Gaussian integers, but again the dependence on χ of the bound given for (2.53) is only through the modulus of χ (see [19, Proposition 17.2, p. 1016]) and this modulus is again different from $4bd$ by a fixed constant. This shows that Lemma 2.13 follows from [19, Proposition 10.2] and hence Proposition 2.4 is proved.

Chapter 3

On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \bmod 4$

Let D be a fundamental discriminant, i.e., a discriminant of a quadratic number field, and let $\mathrm{Cl}(D)$ denote the (narrow) class group of the quadratic number field $\mathbb{Q}(\sqrt{D})$. Although there are algorithms to compute $\mathrm{Cl}(D)$ for any particular discriminant D, very little has been proved about the average behavior of $\mathrm{Cl}(D)$ as D ranges over families of fundamental discriminants.

Rédei [34], Gerth [22], Fouvry and Klüners [16, 14, 13], and Stevenhagen [40], among others, obtained many density results about 4- and 8-ranks of class groups in various families of quadratic number fields.

Density results appear to be far more difficult to obtain for the 16-rank than for the lower 2-power ranks (see [41, p. 16-18]). Our main goal in this chapter is to prove a density result about the 16-rank, albeit in a particularly simple family of quadratic number fields. This family is indexed by fundamental discriminants of the form $-8p$. Although $-8p$ is a fundamental discriminant for all odd prime numbers p, the 8-rank of $\mathbb{Q}(\sqrt{-8p})$ behaves differently in the cases that $p \equiv 1 \bmod 4$ and $p \equiv -1 \bmod 4$. Hence it is natural to study the families $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv -1(4)}$ and $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 1(4)}$ separately.

Equation (1.2) implies that the 2-part of the class group $\mathrm{Cl}(-8p)$ is nontrivial and cyclic, so the structure of the 2-part is completely determined by its "depth," i.e., the largest integer k such that $\mathrm{rk}_{2^k}\mathrm{Cl}(-8p) = 1$. This motivates the following definition. Given an integer $k \geq 0$, a real number $X \geq 2$, and $\omega \in \{\pm 1\}$, define $\rho(2^k; \omega)$ to be the limit

$$\rho(2^k;\omega) = \lim_{X\to\infty} \frac{\#\{p \leq X \text{ prime} : p \equiv \omega \bmod 4,\ \mathrm{rk}_{2^k}\mathrm{Cl}(-8p) = 1\}}{\#\{p \leq X \text{ prime}\}},$$

if it exists.

We now suppose that $p \equiv -1 \bmod 4$. It follows from the work of Rédei [34] that

$$\mathrm{rk}_4\mathrm{Cl}(-8p) = 1 \Longleftrightarrow p \equiv -1 \bmod 8.$$

Furthermore, Hasse [24] proved that

$$\mathrm{rk}_8\mathrm{Cl}(-8p) = 1 \Longleftrightarrow p \equiv -1 \bmod 16.$$

Both congruence conditions on p in the criteria above can be interpreted as splitting conditions on p in the degree-8 cyclotomic extension $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$. Now the Čhebotarev's Density Theorem implies that $\rho(2^k;-1)=2^{-k}$ for $1\leq k\leq 3$.

A simple splitting condition that determines the value of $\mathrm{rk}_{16}\mathrm{Cl}(D)$ has *not* been found, and in fact *might not even exist.* Nonetheless, numerics and heuristics both suggest that $\rho(2^k;-1)$ exists and is equal to 2^{-k} for all $k\geq 1$. Indeed, Cohen-Lenstra heuristics [4] suggest that the cyclic group of order 2^{k-1} would occur as the 2-part of the class group of an imaginary quadratic number field twice as often as the cyclic group of order 2^k. As we just saw above, $\rho(2^k;-1)=\frac{1}{2}\rho(2^{k-1};-1)$ for $k=2,3$, so we are led to conjecture

Conjecture 3.1. *For all $k\geq 1$, the limit $\rho(2^k,-1)$ exists and is equal to 2^{-k}.*

No progress had been made on Conjecture 3.1 since the case $k=3$ was settled by Hasse in 1969. Our main result of this chapter, Theorem A, now proves that $\rho(16;-1)=\frac{1}{16}$.

Theorem B. *The density of the set of prime numbers $p\equiv -1 \bmod 4$ for which $\mathrm{rk}_{16}\mathrm{Cl}(-8p)=1$ is equal to*

$$\lim_{X\to\infty}\frac{\#\{p\leq X, p\ \mathit{prime}, p\equiv -1 \bmod 4, \mathrm{rk}_{16}\mathrm{Cl}(-8p)=1\}}{\#\{p\leq X, p\ \mathit{prime}\}}=\frac{1}{16}.$$

To the best of the author's knowledge, this is the first density result about the 16-rank of class groups of quadratic number fields.

Prior to this work, the only method for obtaining a density result was to construct certain normal extensions of $\mathbb{Q}$ that govern the 2^k-rank and then to apply the Čebotarev Density Theorem. To be more precise, given a non-zero integer d and an integer $k\geq 1$, we say that a normal extension $M/\mathbb{Q}$ is a *governing field* for the 2^k-rank in the family of quadratic number fields $\{\mathbb{Q}(\sqrt{dp})\}_p$ (parametrized by primes p for which dp is a fundamental discriminant) if the value of $\mathrm{rk}_{2^k}\mathrm{Cl}(dp)$ is determined by the Frobenius class of p in $\mathrm{Gal}(M/\mathbb{Q})$. Knowing explicitly a governing field for the 2^k-rank makes it easy to study the density of primes p for which $\mathrm{rk}_{2^k}\mathrm{Cl}(dp)=k$. Indeed, by the Čebotarev Density Theorem, the mere existence of a governing field already guarantees that this density exists and is equal to a rational number.

Although Cohn and Lagarias [6, 5] conjectured that, for a family $\{\mathbb{Q}(\sqrt{dp})\}_p$ as above, a governing field for the 2^k-rank exists for every integer $k\geq 1$, and although Stevenhagen [40] proved their conjecture for $k\leq 3$, a governing field has *not* been found for the 16- or higher 2-power ranks in *any* family. This is the main reason that Conjecture 3 has remained open for $k\geq 4$ for such a long time.

Theorem B gives a positive answer to Conjecture 3.1 for $k=4$ *without appealing to a governing field.* Instead, we use a criterion for the 16-rank of $\mathrm{Cl}(-8p)$ that is conducive to analytic techniques. In [30, Theorem 3, p.205], Leonard and Williams stated the following criterion. A prime $p \equiv -1 \bmod 16$ can be written as

$$p = u^2 - 2v^2 \tag{3.1}$$

where u and v are integers, $u > 0$, and

$$u \equiv 1 \bmod 16. \tag{3.2}$$

Given such a representation, we have

$$\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1 \Longleftrightarrow \left(\frac{v}{u}\right) = 1. \tag{3.3}$$

Here $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi symbol. The first few primes satisfying the above criterion are 127, 223, 479, 719, $\dots$. Note that integers $u > 0$ and v satisfying (3.1) and (3.2) are *not* unique. Nonetheless, the criterion (3.3) is valid for *any* choice of integers $u > 0$ and v satisfying (3.1) and (3.2). If u and v are such integers, then criterion (3.3) states that

$$\frac{1}{2}\left(1 + \left(\frac{v}{u}\right)\right) = \begin{cases} 1 & \text{if } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1, \\ 0 & \text{if } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 0. \end{cases}$$

Hence Theorem B is a corollary of the following theorem:

Theorem 3.1. *For every $\epsilon > 0$, there is a constant $C_\epsilon > 0$ depending only on ϵ such that for every $X \geq 2$, we have*

$$\left| \sum_{\substack{p \leq X \\ p \equiv -1 \bmod 16}} \left(\frac{v}{u}\right) \right| \leq C_\epsilon X^{\frac{149}{150} + \epsilon},$$

where, for each p in the sum above, u and v are taken to be integers satisfying (3.1) *and* (3.2).

Theorem 3.1 is an equidistribution result reminiscent of [19, Theorem 2, p.948]. In [19], Friedlander and Iwaniec associate a *binary symbol* (i.e., a quantity taking values in $\{\pm 1\}$) to each non-zero ideal in $\mathbb{Z}[i]$ and show that its value is equidistributed over prime ideals in $\mathbb{Z}[i]$ ordered by the norm. Theorem 3.1 is a very similar type of result for the ring $\mathbb{Z}[\sqrt{2}]$, although we encounter substantial new difficulties coming from the more complicated unit group in $\mathbb{Z}[\sqrt{2}]$. In essence, an odd ideal in $\mathbb{Z}[\sqrt{2}]$ does not have a canonical generator, and we resort to averaging over four carefully chosen generators to define an analogous binary symbol. Proving that the resulting symbol is well-defined already requires significant new ideas.

Section 3.1 contains the class field theoretic construction of the *governing symbol* $[p] = \left(\frac{v}{u}\right)\chi(u)$ for the 16-rank in the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p \equiv -1(4)}$ (see

Proposition 3.1). Another aim of Section 3.1 is to prove an invariance result for the Jacobi symbol $\left(\frac{v}{u}\right)$ (see Proposition 3.2). In Section 3.2, we construct binary symbols that both encode behavior of the 16-rank in our family and are conducive to analytic techniques (see Equations (3.29) and (3.30)). We also reduce Theorem 3.1 to a purely analytic statement (see Theorem 3.2) that can be attacked by the machinery of Friedlander, Iwaniec, Mazur, and Rubin (see Proposition 3.4). The goal of Section 3.3 is to construct convenient fundamental domains for the multiplicative action of a fundamental unit $1+\sqrt{2}$ on $\mathbb{Z}[\sqrt{2}]$. In Section 3.4, we use a Polya-Vinogradov-type estimate to give bounds for linear sums of the binary symbol. In Section 3.5, we give bounds for general bilinear sums of the binary symbol, thus completing the proof of Theorem 3.1. In the final section, we show that if a governing field for the 16-rank in the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv -1(4)}$ were to exist, Theorem 3.1 would give error terms for certain prime-counting functions that are far better than any which could be obtained via the best known zero-free regions of L-functions.

Finally, we say a few words about the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 1(4)}$. Given a prime $p\equiv 1 \bmod 4$, the 4-rank of $\mathrm{Cl}(-8p)$ is equal to 1 if and only if $p\equiv 1 \bmod 8$. Then, given a prime $p\equiv 1 \bmod 8$ and a representation of p as $p=u^2-2v^2$ for integers $u\equiv 1 \bmod 4$ and v, $\mathrm{rk}_8\mathrm{Cl}(-8p)=1$ if and only if $\left(\frac{u}{p}\right)=1$ (see [30, 2.2, P.204]). Finally, $\mathrm{rk}_{16}\mathrm{Cl}(-8p)=1$ if and only if the binary symbol

$$\left(\frac{u}{p}\right)_4$$

is 1; see [30, Theorem 2, p.204]. Here the quantity $\left(\frac{u}{p}\right)_4$ is equal to 1 or -1 according to whether u is a fourth power modulo p or u is a square but not a fourth power modulo p, respectively. Heuristically, we once again expect that the value of this binary symbol is equidistributed as p ranges over the prime numbers congruent to 1 modulo 8 such that u is a square modulo p. However, although we could generalize most of the ingredients in the proof of Theorem 3.1 to this new setting, we are unable to obtain power-saving cancellation in the linear sums as in Section 3.4 without a Burgess-type estimate for short character (modulo q) sums of length $q^{\frac{1}{8}-\epsilon}$. As such a result on short character sums is currently well out of reach, we do not deal with the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 1(4)}$.

3.1 Governing symbols

The purpose of this section is to generalize [30, Theorem 3, p.205] and to develop a framework conducive to the analytic techniques of Friedlander, Iwaniec, Mazur, and Rubin [17].

Let χ be a character $(\mathbb{Z}/16\mathbb{Z})^\times \to \mathrm{Cl}^\times$ with kernel $\{\pm 1\}$. In other words, we have $\chi(\pm 1 \bmod 16) = 1$ and $\chi(\pm 7 \bmod 16) = -1$. Then our generalization of [30, Theorem 3, p.205] is as follows:

Proposition 3.1. *Let $p \equiv -1 \bmod 16$ be a prime number. Let u and v be integers such that $p = u^2 - 2v^2$ and such that $u > 0$ and $v \equiv 1 \bmod 4$. Then*

$$\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1 \Longleftrightarrow \left(\frac{v}{u}\right)\chi(u) = 1. \tag{3.4}$$

The choice of u and v in the proposition above is *not* unique. Let

$$\varepsilon = 1 + \sqrt{2}$$

be a *fundamental unit* in $\mathbb{Z}[\sqrt{2}]$, so that the group of units $\mathbb{Z}[\sqrt{2}]^\times$ is generated by ε and -1. As the norm of ε is -1, the norm of $\varepsilon^2 = 3 + 2\sqrt{2}$ is 1. Let $p \equiv -1 \bmod 16$ be a prime number as in Proposition 3.1. Given *one* integer solution $(u, v) = (u_0, v_0)$ to the system

$$\begin{cases} p = u^2 - 2v^2 \\ u > 0, v \equiv 1 \bmod 4 \end{cases}, \tag{3.5}$$

then the complete set of integer solutions (u, v) to the system (3.5) is of the form

$$u + v\sqrt{2} = \varepsilon^{2k}(u_0 + v_0\sqrt{2})$$

for some integer k. An interesting consequence of Proposition 3.1 is that the quantity

$$\left(\frac{v}{u}\right)\chi(u)$$

is *independent* of the choice of u and v satisfying (3.5). This allows us to make the following definition.

For a prime $p \equiv -1 \bmod 16$, we define the *governing symbol* for the 16-rank to be

$$[p] := \left(\frac{v}{u}\right)\chi(u), \tag{3.6}$$

where u and v are integers satisfying (3.5). The quantity $[p]$ determines the 16-rank of the class group $\mathrm{Cl}(-8p)$. It is interesting to note that the 16-rank of $\mathrm{Cl}(-8p)$ depends on a "quantitative" aspect of the splitting behavior of p in $\mathbb{Z}[\sqrt{2}]$ that appears to allow no description purely in terms of the "qualitative" splitting behavior of p in some normal extension of $\mathbb{Q}$.

Leonard and Williams claim that [30, Theorem 3, p.205] can be proved by numerous manipulations of Jacobi symbols and applications of quadratic reciprocity. We instead prove Proposition 3.1 by interpreting the Jacobi symbol $\left(\frac{v}{u}\right)$ as an Artin symbol of an ideal that depends on the decomposition of a prime p as $p = u^2 - 2v^2$ in an extension of $\mathbb{Q}(\sqrt{-8p})$ that depends on the same decomposition $p = u^2 - 2v^2$. Moreover, a by-product of our proof is the following proposition, which turns out to be essential for a successful application of the analytic tools we wish to use.

Proposition 3.2. *Let u_1 and v_1 be integers such that u_1 is odd and positive and such that $u_1^2 - 2v_1^2 > 0$. Define integers u_2 and v_2 by the equality*

$$u_2 + v_2\sqrt{2} = \varepsilon^8(u_1 + v_1\sqrt{2}).$$

Then

$$\left(\frac{v_1}{u_1}\right) = \left(\frac{v_2}{u_2}\right).$$

In other words, we have the equality of Jacobi symbols

$$\left(\frac{v_1}{u_1}\right) = \left(\frac{408u_1 + 577v_1}{577u_1 + 816v_1}\right).$$

The rest of this section is devoted to proving Proposition 3.1 and Proposition 3.2.

3.1.1 Preliminaries

We will use the following lemma several times.

Lemma 3.1. *Let E/F be an abelian extension of number fields, let L/F be a finite extension, and let*

$$\iota : \mathrm{Gal}(EL/L) \hookrightarrow \mathrm{Gal}(E/F)$$

be the restriction-to-E map. Then for every prime ideal $\mathfrak{p}$ of L that is coprime to $\mathrm{Disc}(E/F)$*, we have*

$$\iota\left(\frac{\mathfrak{p}}{EL/L}\right) = \left(\frac{\mathrm{Norm}_{L/F}(\mathfrak{p})}{E/F}\right).$$

Proof. See [25, Proposition 3.1, p. 103]. □

Ring class fields

To prove Proposition 3.2, we will have to work with a generalization of the Hilbert class field. Let $D < 0$ be any integer $\equiv 0, 1 \bmod 4$ that is not a square, and let $\mathcal{O}_D$ be the quadratic order of discriminant D, i.e.,

$$\mathcal{O}_D = \mathbb{Z}[(D + \sqrt{D})/2].$$

Let $K = \mathbb{Q}(\sqrt{D})$ be the field of fractions of $\mathcal{O}_D$. Then K is an imaginary quadratic number field of discriminant $\mathrm{Disc}(K)$ satisfying the equality

$$D = f^2\mathrm{Disc}(K)$$

for some positive integer f, called the *conductor* of $\mathcal{O}_D$. Let $\mathrm{Cl}(D)$ denote the class group of $\mathcal{O}_D$. Then there is a unique abelian extension R_D/K called the *ring class field* of $\mathcal{O}_D$ such that the Artin map induces a canonical isomorphism of groups

$$\left(\frac{\cdot}{R_D/K}\right) : \mathrm{Cl}(D) \longrightarrow \mathrm{Gal}(R_D/K). \tag{3.7}$$

In the case $f = 1$, so that $D = \mathrm{Disc}(K)$, the ring class field R_D coincides with the Hilbert class field of K.

The main property of ring class fields of imaginary quadratic orders that we will use is stated in the following lemma.

Lemma 3.2. *Let K be an imaginary quadratic number field of even discriminant, and let L/K be a cyclic extension such that:*

- *$L/\mathbb{Q}$ is a dihedral extension, and*
- *the conductor of L/K divides* (4).

Then L is contained in the ring class field R_D of the imaginary quadratic order $\mathcal{O}_D$ of discriminant $D = 16 \cdot \mathrm{Disc}(K)$.

Proof. See [8, Theorem 9.18, p. 191] and [8, Exercise 9.20, p. 195-196]. □

3.1.2 A special family of quadratic fields

Let u and v be coprime integers such that u is odd and positive and such that

$$n = u^2 - 2v^2 \tag{3.8}$$

is positive as well. Let K be the imaginary quadratic number field defined by

$$K = \mathbb{Q}(\sqrt{-2n}).$$

Note that $n \equiv \pm 1 \bmod 8$, and moreover $n \equiv 1 \bmod 8$ if and only if v is even. Let m and d be the unique positive integers such that m is squarefree and

$$n = d^2 m.$$

Then $K = \mathbb{Q}(\sqrt{-2m})$ and the discriminant of $K/\mathbb{Q}$ is

$$\mathrm{Disc}(K/\mathbb{Q}) = -8m.$$

We emphasize that both m and d are odd. As $\gcd(u, v) = 1$, every prime dividing n splits in $\mathbb{Q}(\sqrt{2})$. Hence there exist δ and μ in $\mathbb{Q}(\sqrt{2})$ of norm d and m, respectively, such that

$$u + v\sqrt{2} = \delta^2 \mu.$$

We define a quadratic extension G/K by

$$G = K(\sqrt{2}).$$

We call this field G because it coincides with the *genus field* of K in the case that n is a prime number congruent to -1 modulo 4.

Finally, we define a quadratic extension of G as follows. Define $\nu \in \mathbb{Z}[\sqrt{2}] \subset G$ by setting

$$\nu = u + v\sqrt{2}. \tag{3.9}$$

Then let

$$L = L_{u,v} = G(\sqrt{\varepsilon\nu}),$$

where $\varepsilon = 1 + \sqrt{2}$ as before. If n is a prime number congruent to -1 modulo 8 and u and v are chosen as in the statement of Proposition 3.1, we will see that L coincides with the 4-Hilbert class field H_4 of K.

Remark. The fields K and G are determined simply by n. In other words, had we started with another choice of integers u and v giving rise to the same n, the definitions of K and G would not change. However, the field L may depend on the specific choice of u and v. Since we fixed u and v in the beginning of the section, this should not cause any confusion.

We now introduce some notation and prove some properties of the extensions $K \subset G \subset L$. Let $\overline{\nu} = u - v\sqrt{2}$ be the conjugate of ν in $\mathbb{Q}(\sqrt{2})$. We now state a few consequences of the assumption that $\gcd(u, v) = 1$. It will be useful to consider the following field diagram.

$$\begin{tikzcd}
& L = G(\sqrt{\varepsilon\nu}) \arrow[dl, dash] \arrow[d, dash] \\
A = \mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon\nu}) \arrow[d, dash] & G = K(\sqrt{2}) \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & K = \mathbb{Q}(\sqrt{-2m}) \arrow[d, dash] \\
& \mathbb{Q}
\end{tikzcd}$$

Lemma 3.3. *The extension L/K is cyclic of degree* 4, *and the extension $L/\mathbb{Q}$ is dihedral of order* 8.

Proof. We have

$$\mathrm{Norm}_{G/K}(\varepsilon\nu) = \mathrm{Norm}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\varepsilon\nu) = -\nu\overline{\nu} = -n.$$

As

$$-n = 2 \cdot \left(\frac{1}{2}\sqrt{-2n}\right)^2 \in 2 \cdot (K^\times)^2,$$

the first claim follows from Lemma 2.2, part (3). Now let $A = \mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon\nu})$. As

$$-n \notin (\mathbb{Q}^\times)^2 \cup 2 \cdot (\mathbb{Q}^\times)^2,$$

part (1) of Lemma 2.2 implies that $L = A(\sqrt{-n})$ is the normal closure of $A/\mathbb{Q}$ and $\mathrm{Gal}(L/\mathbb{Q}) \cong D_8$. □

Let $\mathfrak{t}$ denote the prime of K lying above 2.

Lemma 3.4. *L/K is unramified at every prime other than possibly at $\mathfrak{t}$.*

Proof. Recall that $\nu = \delta^2\mu$, so $L = \mathbb{Q}(\sqrt{-2m}, \sqrt{2}, \sqrt{\varepsilon\mu})$. As the norm of μ is m, every prime that ramifies in $L/\mathbb{Q}$ must divide $2m$. Let p be a rational prime dividing m. Suppose p factors as $\pi\overline{\pi}$ in $\mathbb{Z}[\sqrt{2}]$, and, without loss of generality, suppose π divides $\overline{\nu}$. As u and v are coprime, ν and $\overline{\nu}$ are coprime in $\mathbb{Z}[\sqrt{2}]$ and hence π does not ramify in $A = \mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon\nu})$. Thus, as p splits in $\mathbb{Q}(\sqrt{2})$, its ramification index in $L/\mathbb{Q}$ is at most 2. But p already ramifies in $K/\mathbb{Q}$, and hence every prime $\mathfrak{p}$ of K lying above p must be unramified in L/K. □

By Lemma 3.4, the only prime that can divide the conductor $\mathfrak{f}$ of L/K is the prime $\mathfrak{t}$. The following lemma gives the precise power of $\mathfrak{t}$ dividing $\mathfrak{f}$.

Lemma 3.5. *Let $\mathfrak{f}$ denote the conductor of L/K. Then:*

1. *If $v \equiv 1 \bmod 4$, then L/K is unramified and $\mathfrak{f} = 1$.*

2. *If $v \equiv -1 \bmod 4$, then $\mathfrak{f} = \mathfrak{t}^2 = (2)$.*

3. *If $v \equiv 0 \bmod 2$, then $\mathfrak{f} = \mathfrak{t}^4 = (4)$.*

Proof. Since $\mathfrak{t}$ is the only prime that can divide $\mathfrak{f}$, we only need to study the extensions locally at the primes above 2. Let $\mathfrak{T}$ be a prime of G lying above $\mathfrak{t}$ and $\mathcal{T}$ a prime of L lying above $\mathfrak{T}$. Let $K_\mathfrak{t}$, $G_\mathfrak{T}$, and $L_\mathcal{T}$ denote the completions of K, G, and L with respect to the primes $\mathfrak{t}$, $\mathfrak{T}$, and $\mathcal{T}$, respectively.

If v is odd, then $n \equiv -1 \bmod 8$, and so $K_\mathfrak{t} = \mathbb{Q}_2(\sqrt{-2n}) = \mathbb{Q}_2(\sqrt{2})$ and $G_\mathfrak{T} = K_\mathfrak{t}(\sqrt{2}) = K_\mathfrak{t}$. Thus the extension $G_\mathfrak{T}/K_\mathfrak{t}$ is trivial and $L_\mathcal{T} = \mathbb{Q}_2(\sqrt{2}, \sqrt{\varepsilon\nu})$. The extension $\mathbb{Q}_2(\sqrt{2}, \sqrt{\varepsilon\nu})/\mathbb{Q}_2(\sqrt{2})$ is unramified if and only if $\varepsilon\nu$ is a square modulo $\mathfrak{t}^4$; here $\mathfrak{t} = (\sqrt{2})$ is the maximal ideal in $\mathbb{Z}_2[\sqrt{2}]$. If $v \equiv 1 \bmod 4$, then

$$\varepsilon\nu = (u + 2v) + (u + v)\sqrt{2} \equiv \begin{cases} 1 \bmod \mathfrak{t}^4 & \text{if } u \equiv -1 \bmod 4, \\ \varepsilon^2 \bmod \mathfrak{t}^4 & \text{if } u \equiv 1 \bmod 4, \end{cases}$$

and hence $L_\mathcal{T}/K_\mathfrak{t}$ is unramified. This proves part (1) of the lemma. Similarly, if $v \equiv 1 \bmod 4$, then

$$\varepsilon\nu \equiv 3 \text{ or } 1 + 2\sqrt{2} \bmod \mathfrak{t}^4.$$

In this case $\varepsilon\nu$ is not a square modulo $\mathfrak{t}^4$, and so $L_{\mathcal{T}}/K_{\mathfrak{t}}$ is ramified. The ramification is wild, and thus $\mathfrak{f}$ must be divisible by $\mathfrak{t}^2$. As $\varepsilon\nu \equiv 1 \bmod \mathfrak{t}^2$, the extension $L_{\mathcal{T}}/K_{\mathfrak{t}}$ can be generated by a root of the polynomial

$$X^2 + \sqrt{2}X + \frac{1-\varepsilon\nu}{2} = \frac{1}{2}\left(\left(\sqrt{2}X+1\right)^2 - \varepsilon\nu\right),$$

whose discriminant is $2 \bmod \mathfrak{t}^4$. Hence $\mathfrak{f} = \mathfrak{t}^2$ and part (2) of the lemma is proved.

Finally, suppose $v \equiv 0 \bmod 2$, so that $n \equiv 1 \bmod 8$. Then $K_{\mathfrak{t}} = \mathbb{Q}_2(\sqrt{-2n}) = \mathbb{Q}_2(\sqrt{-2})$ and $G_{\mathfrak{T}} = K_{\mathfrak{t}}(\sqrt{2}) = \mathbb{Q}_2(\zeta_8)$. The quadratic extension $G_{\mathfrak{T}}/K_{\mathfrak{t}}$ is ramified of conductor $\mathfrak{t}^2$, where $\mathfrak{t} = (\sqrt{-2})$ is the maximal ideal in $\mathbb{Z}_2[\sqrt{-2}]$. Let $s = 1 + \zeta_8$ be a generator of the maximal ideal $\mathfrak{s}$ in $\mathbb{Z}_2[\zeta_8]$. Note that $s^2 = \sqrt{2}\cdot\zeta_8\varepsilon$, so $\varepsilon\nu \equiv 1 \bmod \mathfrak{s}^2$. Hence the extension $L_{\mathcal{T}}/K_{\mathfrak{t}}$ can be generated by a root of the polynomial

$$X^2 + s^3\zeta_8^6\varepsilon^{-2}X + \frac{1-\varepsilon\nu}{s^2} = \frac{1}{s^2}\left((sX+1)^2 - \varepsilon\nu\right),$$

whose discriminant is $s^6 \bmod \mathfrak{s}^7$. Hence the discriminant of $L_{\mathcal{T}}/G_{\mathfrak{T}}$ is $\mathfrak{s}^6$.

To finish, we use the conductor-discriminant formula, i.e.,

$$\mathrm{Disc}(L_{\mathcal{T}}/K_{\mathfrak{t}}) = \mathrm{Disc}(G_{\mathfrak{T}}/K_{\mathfrak{t}})\mathfrak{f}(L_{\mathcal{T}}/K_{\mathfrak{t}})^2.$$

The discriminant formula for the tower of fields $K_{\mathfrak{t}} \subset G_{\mathfrak{T}} \subset L_{\mathcal{T}}$ gives

$$\mathrm{Disc}(L_{\mathcal{T}}/K_{\mathfrak{t}}) = \mathrm{Disc}(G_{\mathfrak{T}}/K_{\mathfrak{t}})^2\mathrm{Norm}_{G_{\mathfrak{T}}/K_{\mathfrak{t}}}(\mathrm{Disc}(L_{\mathcal{T}}/G_{\mathfrak{T}})),$$

so that

$$\mathfrak{f}(L_{\mathcal{T}}/K_{\mathfrak{t}})^2 = \mathrm{Disc}(G_{\mathfrak{T}}/K_{\mathfrak{t}})\mathrm{Norm}_{G_{\mathfrak{T}}/K_{\mathfrak{t}}}(\mathrm{Disc}(L_{\mathcal{T}}/G_{\mathfrak{T}})).$$

Substituting $\mathrm{Disc}(G_{\mathfrak{T}}/K_{\mathfrak{t}}) = \mathfrak{t}^2$ and $\mathrm{Disc}(L_{\mathcal{T}}/G_{\mathfrak{T}}) = \mathfrak{s}^6$ into the formula above implies that $\mathfrak{f}(L_{\mathcal{T}}/K_{\mathfrak{t}}) = \mathfrak{t}^4$, which completes the proof of part (3) of the lemma. □

Lemma 3.6. *L is contained in the ring class field R_D of the imaginary quadratic order $\mathcal{O}_D$ of discriminant $D = 16 \cdot -8m$.*

Proof. Combine Lemmas 3.2, 3.3, and 3.5. □

3.1.3 A computation of Artin symbols

This section contains the heart of the proof of both Proposition 3.1 and Proposition 3.2.

The integers u and v appearing in (3.8) are not unique. Given a representation $n = u^2 - 2v^2$, another representation can be obtained by multiplying $u + v\sqrt{2}$ by $3 + 2\sqrt{2}$. This transforms (u, v) into $(3u + 4v, 2u + 3v)$.

We will show how the quantity

$$\left(\frac{v}{u}\right)\chi(u),$$

where χ is a Dirichlet character from Proposition 3.2, naturally arises in the computation of a certain Artin symbol. This computation is somewhat delicate because the Artin symbol will take a value in a cyclic group of order 4, and such a group has a non-trivial automorphism.

Remark. In [23], Halter-Koch, Kaplan, and Williams compute Artin symbols in similar cyclic field extensions L/K of degree 4. Their results, however, involve computations of Artin symbols of ideals of K of order 2 in the class group of K, and hence only give information about the 8-rank in certain quadratic fields.

Let $f \in \{1, 4\}$. The case $f = 1$ will be used to prove Proposition 3.1, while the case $f = 4$ will be used to prove Proposition 3.2. Let $\tau = f\sqrt{-2n}$, so that $\mathbb{Z}[\tau]$ is the order of K of discriminant $-8nf^2$. We define a homomorphism

$$\psi_{u,v} : \mathbb{Z}[\tau] \to \mathbb{Z}/u\mathbb{Z}$$

by sending $\tau \mapsto 2vf \bmod u$. This homomorphism is well-defined since

$$\tau^2 = -2nf^2 = -2(u^2 - 2v^2)f^2 \equiv (2vf)^2 \bmod u.$$

Let

$$\mathfrak{u} = \ker \psi_{u,v}. \tag{3.10}$$

It is the ideal of $\mathbb{Z}[\tau]$ generated by u and $2vf - \tau$, i.e.,

$$\mathfrak{u} = (u, 2vf - \tau).$$

In case $n = p \equiv -1 \bmod 8$ and $f = 1$, the ideal class of $\mathfrak{u}$ turns out to have order 4, as we will see later. We remark that

$$2vf \equiv \tau \bmod \mathfrak{u}. \tag{3.11}$$

We also note that

$$\mathrm{Norm}(\mathfrak{u}) = u. \tag{3.12}$$

Let $\sqrt{\varepsilon\nu}$ be a square root of $\varepsilon\nu$. Then, by Lemma 2.2, the extension $G(\sqrt{\varepsilon\nu})/K$ is cyclic of degree 4. We are interested in computing the Artin symbol

$$\left(\frac{\mathfrak{u}}{G(\sqrt{\varepsilon\nu})/K}\right).$$

The key idea is to relate this Artin symbol to the Artin symbol associated to a different but related cyclic degree-4 extension of K. Let

$$\gamma = (2+\sqrt{2})v \in \mathbb{Z}[\sqrt{2}]. \tag{3.13}$$

Then again by Lemma 2.2, the extension $G(\sqrt{\gamma})/K$ is cyclic of degree 4. The element γ was chosen so that

$$\varepsilon\nu \equiv \gamma \bmod \mathfrak{u}, \tag{3.14}$$

and at the same time so that the extension $\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}$ mimics the cyclic degree-4 subextension of the cyclotomic extension $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$. Finally, let F be the compositum of $G(\sqrt{\varepsilon\nu})$ and $G(\sqrt{\gamma})$. We have the following field diagram.

$$\begin{tikzcd}
& & F = G(\sqrt{\varepsilon\nu}, \sqrt{\gamma}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
& G(\sqrt{\varepsilon\nu\gamma}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & G(\sqrt{\varepsilon\nu}) \arrow[d, dash] & G(\sqrt{\gamma}) \arrow[dl, dash] \\
K(\sqrt{\beta}) \arrow[dr, dash] & K(\sqrt{\beta'}) \arrow[d, dash] & G = K(\sqrt{2}) \arrow[dl, dash] & \\
& K = \mathbb{Q}(\sqrt{-2n}) & &
\end{tikzcd}$$

Here β and β' are elements of K that are conjugate over $\mathbb{Q}$. Let $\overline{\varepsilon\nu\gamma} \in \mathbb{Q}(\sqrt{2})$ be the conjugate of $\varepsilon\nu\gamma$ over $\mathbb{Q}$. Since

$$\left(\sqrt{2\varepsilon\nu\gamma} \pm \sqrt{2\overline{\varepsilon\nu\gamma}}\right)^2 = 4v((4u+6v) \pm \sqrt{-2n}) = \frac{4v}{f}\left((4u+6v)f \pm \tau\right),$$

we can take

$$\beta = v((4u+6v)f - \tau)$$

and

$$\beta' = v((4u+6v)f + \tau).$$

The inclusion $\mathrm{Gal}(F/K(\sqrt{\beta})) \subset \mathrm{Gal}(F/K)$ and projections $\mathrm{Gal}(F/K) \twoheadrightarrow \mathrm{Gal}(G(\sqrt{\varepsilon\nu})/K)$ and $\mathrm{Gal}(F/K) \twoheadrightarrow \mathrm{Gal}(G(\sqrt{\gamma})/K)$ induce canonical isomorphisms

$$\psi_1 : \mathrm{Gal}(F/K(\sqrt{\beta})) \xrightarrow{\sim} \mathrm{Gal}(G(\sqrt{\varepsilon\nu})/K)$$

and

$$\psi_2 : \mathrm{Gal}(F/K(\sqrt{\beta})) \xrightarrow{\sim} \mathrm{Gal}(G(\sqrt{\gamma})/K).$$

Using (3.11), we find that if $\mathfrak{p}$ is a prime ideal dividing $\mathfrak{u}$, then

$$\left(\frac{\beta}{\mathfrak{p}}\right) = \left(\frac{v((4u+6v)f-\tau)}{\mathfrak{p}}\right) = \left(\frac{4v^2f}{\mathfrak{p}}\right) = 1,$$

and so $\mathfrak{p}$ splits in $K(\sqrt{\beta})$. By Lemma 3.1, for any prime $\mathfrak{P}$ of $K(\sqrt{\beta})$ lying above a prime ideal $\mathfrak{p}$ dividing $\mathfrak{u}$, we have

$$\psi_1\left(\left(\frac{\mathfrak{P}}{F/K(\beta)}\right)\right) = \left(\frac{\mathfrak{p}}{G(\sqrt{\varepsilon\nu})/K}\right)$$

and

$$\psi_2\left(\left(\frac{\mathfrak{P}}{F/K(\beta)}\right)\right) = \left(\frac{\mathfrak{p}}{G(\sqrt{\gamma})/K}\right).$$

Multiplying over all prime ideals $\mathfrak{p}$ dividing $\mathfrak{u}$, we have proved the following key lemma.

Lemma 3.7. *Let* $\mathfrak{u}$ *be defined as in* (3.10). *Then*

$$\psi_2\circ\psi_1^{-1}\left(\left(\frac{\mathfrak{u}}{G(\sqrt{\varepsilon\nu})/K}\right)\right) = \left(\frac{\mathfrak{u}}{G(\sqrt{\gamma})/K}\right).$$

Now we apply Lemma 3.1 with $E=\mathbb{Q}(\sqrt{-2n})$, $F=\mathbb{Q}$, and $L=\mathbb{Q}(\sqrt{\gamma})$. We have

$$\iota\left(\left(\frac{\mathfrak{u}}{G(\sqrt{\gamma})/K}\right)\right) = \left(\frac{u}{\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}}\right),$$

so that, by Lemma 3.7, we have

$$\iota\circ\psi_2\circ\psi_1^{-1}\left(\left(\frac{\mathfrak{u}}{G(\sqrt{\gamma})/K}\right)\right) = \left(\frac{u}{\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}}\right).$$

Now observe that $\mathbb{Q}(\sqrt{\gamma})$ is a subfield of $\mathbb{Q}(\zeta_{16}\sqrt{v})$. Indeed, $\zeta_{16}\sqrt{v}+\zeta_{16}^{-1}\sqrt{v}=\gamma$. There is a canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{16}\sqrt{v})/\mathbb{Q}) \cong (\mathbb{Z}/16\mathbb{Z})^\times \cong \langle -1 \bmod 16\rangle \times \langle 3 \bmod 16\rangle$$

given by sending

$$\left(\zeta_{16}\sqrt{v}\mapsto\zeta_{16}^k\sqrt{v}\right)\mapsto(k \bmod 16).$$

Then $\mathbb{Q}(\sqrt{\gamma})$ is the subfield of $\mathbb{Q}(\zeta_{16}\sqrt{v})$ fixed by -1. For each prime p coprime to $2v$, we have

$$\left(\frac{p}{\mathbb{Q}(\zeta_{16}\sqrt{v})/\mathbb{Q}}\right) = p\left(\frac{v}{p}\right) \bmod 16,$$

so that if we identify

$$\psi_3:\langle 3 \bmod 16\rangle \xrightarrow{\sim} \mu_4=\langle i\rangle\subset\mathbb{C}^\times$$

by sending $3 \mapsto i = \sqrt{-1}$, we get

$$\psi_3\left(\left(\frac{p}{\mathbb{Q}(\sqrt{\gamma})/\mathbb{Q}}\right)\right) = \left(\frac{v}{p}\right)\chi(p).$$

Multiplying over all primes p dividing u and using Lemma 3.7, we finally obtain the following result.

Lemma 3.8. *Let $\psi : \mathrm{Gal}(G(\sqrt{\varepsilon\nu})/K) \xrightarrow{\sim} \mu_4$ be the isomorphism of cyclic groups of order 4 defined by $\psi = \psi_3 \circ \iota \circ \psi_2 \circ \psi_1^{-1}$. Then*

$$\psi\left(\left(\frac{\mathfrak{u}}{G(\sqrt{\varepsilon\nu})/K}\right)\right) = \left(\frac{v}{u}\right)\chi(u).$$

3.1.4 An ideal identity

We keep the same notation as in Sections 3.1.2 and 3.1.3. Recall that $\tau = f\sqrt{-2n}$, where $f \in \{1, 4\}$. Let $\mathfrak{t}_f$ be the ideal of $\mathbb{Z}[\tau]$ defined as the kernel of the homomorphism

$$\tau_f : \mathbb{Z}[\tau] \to \mathbb{Z}/2f^2\mathbb{Z}$$

given by sending $\tau \mapsto 2vf$. The homomorphism τ_f is well-defined because

$$\tau^2 = -2nf^2 = 4v^2f^2 - 2u^2f^2 \equiv (2vf)^2 \bmod 2f^2.$$

Then $\mathfrak{t}_f = (2vf - \tau, 2f^2)$. The following identity of between ideals in $\mathbb{Z}[\tau]$ will be useful in proofs of both Proposition 3.1 and Proposition 3.2.

Lemma 3.9. *Let $\mathfrak{u}$ be defined as in* (3.10). *Then*

$$(2vf - \tau) = \mathfrak{t}_f\mathfrak{u}^2.$$

Proof. The principal ideal $2vf - \tau$ is invertible of norm $2u^2f^2$. Since u is odd and $\gcd(u, v) = 1$, we deduce that $\mathfrak{u}$ is coprime to the discriminant $-8nf^2$ of $\mathbb{Z}[\tau]$ and is thus invertible. No rational primes can divide $2vf - \tau$ and $\mathfrak{u}$ divides $(2vf - \tau)$ by definition, so it must be that $\mathfrak{u}^2$ divides $(2vf - \tau)$.

The ideal $\mathfrak{t}_f$ of norm $2f^2$ contains $(2vf - \tau)$ and has the same norm as the invertible ideal $(2vf - \tau)\mathfrak{u}^{-2}$. Hence we must have $(2vf - \tau)\mathfrak{u}^{-2} = \mathfrak{t}_f$. □

3.1.5 Proof of Proposition 3.1

We apply the results of Sections 3.1.3 and 3.1.4 in the case $n = p \equiv -1 \bmod 8$ is a prime number and $f = 1$. Suppose $p \equiv -1 \bmod 8$ is a prime number. Then p splits in $\mathbb{Q}(\sqrt{2})$, so there exist integers u and v such that

$$p = u^2 - 2v^2.$$

Note that the congruence $p \equiv -1 \bmod 8$ immediately implies that both u and v are odd. Without loss of generality, we may assume that u is positive and

$$v \equiv 1 \bmod 4. \tag{3.15}$$

Since the 2-part of $\mathrm{Cl}(-8p)$ is cyclic, $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1$ if and only if $\mathrm{Cl}(-8p)$ has an element of order 16. To get started, we first produce an element of order 4 in $\mathrm{Cl}(-8p)$ that we can write explicitly in terms of u and v.

A class of order 4

We now produce an ideal generating a class of order 4 in the class group $\mathrm{Cl}(-8p)$ when p is a prime $\equiv -1 \bmod 8$. This is the main ingredient in [30].

When $n = p$ and $f = 1$, the ideal $\mathfrak{t} = \mathfrak{t}_f$ defined in Section 3.1.4 is the prime ideal lying above 2. If $\mathfrak{t} = (x + y\sqrt{-2p})$ for some $x, y \in \mathbb{Z}$, then

$$x^2 + 2py^2 = \mathrm{Norm}(\mathfrak{t}) = 2,$$

which is impossible. Hence the class of $\mathfrak{t}$ in $\mathrm{Cl}(-8p)$ has order 2.

Now let $\mathfrak{u}$ be defined as in (3.10) with u and v as above and $f = 1$. Lemma 3.9 shows that $\mathfrak{u}^2$ and $\mathfrak{t}$ are in the same ideal class in $\mathrm{Cl}(-8p)$. Hence we have proved the following result.

Lemma 3.10. *Let $\mathfrak{u}$ be the ideal of $\mathbb{Z}[\sqrt{-2p}]$ defined as above. Then the ideal class of $\mathfrak{u}$ has order 4 in $\mathrm{Cl}(-8p)$.*

Remark. Perhaps an easier, although more old-fashioned, way to prove Lemma 3.10 is via the theory of binary quadratic forms, as was done in [30]. Let $[a, b, c]$ denote the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of the form $ax^2 + bxy + cy^2$. The key observation is that $[u, -4v, 2u]$ has discriminant $16v^2 - 8u^2 = -8p$. To compose this class with itself, one can use the special case of the composition law for *concordant forms*, which yields the class $[u, -4v, 2u]^2 = [u^2, -4v, 2] = [2, 0, p]$. The classes $[u, -4v, 2u]$ and $[2, 0, p]$ correspond to the ideal classes of $\mathfrak{u}$ and $\mathfrak{t}$, respectively.

Generating the 4-Hilbert class field

Let p be a prime congruent to $-1 \bmod 8$ and let $K = \mathbb{Q}(\sqrt{-8p})$. The 2-Hilbert class field, also called the *genus field* of K, is known to be $H_2 = K(\sqrt{2})$. Lemma 3.10 implies that $\mathrm{rk}_4\mathrm{Cl}(-8p) = 1$, and our aim is to generate the 4-Hilbert class field H_4 over H_2 by adjoining an element that we can write explicitly in terms of u and v.

Define $\pi \in \mathbb{Z}[\sqrt{2}]$ by setting $\pi = \nu$ with ν as in (3.9), i.e.,

$$\pi = u + v\sqrt{2}.$$

The following proposition achieves our aim.

Proposition 3.3. *Let $K = \mathbb{Q}(\sqrt{-8p})$, and let π be as above. Then the 4-Hilbert class field of K is*

$$H_4 = H_2(\sqrt{\varepsilon\pi}).$$

Proof. Since the 2-part of the class group $\mathrm{Cl}(-8p)$ is cyclic, it suffices to show that $H_2(\sqrt{\varepsilon\pi})$ is an unramified, cyclic, degree-4 extension of K.

We apply the lemmas of Sections 3.1.2 and 3.1.3 with $n = m = p$, $e = 1$, and u and v as above. By Lemma 3.3, the extension $H_2(\sqrt{\varepsilon\pi})/K$ is cyclic of degree 4. By Lemma 3.4, $H_2(\sqrt{\varepsilon\pi})/K$ is unramified over the prime ideal $\mathfrak{p} = (p, \sqrt{-2p})$ of K lying over p. Finally, by part (1) of Lemma 3.5, $H_2(\sqrt{\varepsilon\pi})/K$ is unramified over the prime ideal $\mathfrak{t} = (2, \sqrt{-2p})$ of K lying over 2. □

Conclusion of the proof of Proposition 3.1

By Lemma 3.10, $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1$ if and only if the ideal class of $\mathfrak{u}$ belongs to $\mathrm{Cl}(-8p)^4$. By Proposition 3.3, this is true if and only if the Artin symbol of $\mathfrak{u}$ in $H_4 = H_2(\sqrt{\varepsilon\pi})$ is trivial. In the notation of Section 3.1.3, we have that $H_2 = G$, so that $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1$ if and only if

$$\left(\frac{\mathfrak{u}}{G(\sqrt{\varepsilon\pi})/K}\right) = \mathrm{Id}.$$

By Lemma 3.8, this occurs if and only if

$$\left(\frac{v}{u}\right)\chi(u) = 1,$$

which proves Proposition 3.1.

3.1.6 Proof of Proposition 3.2

As in the statement of Proposition 3.2, let u_1 and v_1 be integers such that u_1 is odd and positive and such that $u_1^2 - 2v_1^2 > 0$. We define u_2 and v_2 by the equality

$$u_2 + v_2\sqrt{2} = \varepsilon^8(u_1 + v_1\sqrt{2}) = (577u_1 + 816v_1) + (408u_1 + 577v_1)\sqrt{2}, \quad (3.16)$$

where, as before, $\varepsilon = 1 + \sqrt{2}$. Our goal is to prove the following equality of Jacobi symbols

$$\left(\frac{v_1}{u_1}\right) = \left(\frac{v_2}{u_2}\right). \quad (3.17)$$

By the Euclidean algorithm, we have the equality

$$\gcd(u_1, v_1) = \gcd(u_2, v_2).$$

First, if $\gcd(u_1, v_1) = \gcd(u_2, v_2) > 1$, then both sides of (3.17) are equal to 0, and hence (3.17) holds true.

Now suppose $\gcd(u_1, v_1) = \gcd(u_2, v_2) = 1$. Let

$$n = u_1^2 - 2v_1^2 = u_2^2 - 2v_2^2,$$

and let $K = \mathbb{Q}(\sqrt{-2n})$ as in Section 3.1.2. Set $\tau = 4\sqrt{-2n}$. Let $\mathfrak{u}_1$ (resp. $\mathfrak{u}_2$) be the ideal of the imaginary quadratic order $\mathbb{Z}[\tau]$ (of discriminant $16 \cdot -8n$) defined by (3.10) with $(u, v) = (u_1, v_1)$ (resp. $(u, v) = (u_2, v_2)$) and $f = 4$. The ideals $\mathfrak{u}_1$ and $\mathfrak{u}_2$ satisfy the following key property.

Lemma 3.11. *The ideals $\mathfrak{u}_1$ and $\mathfrak{u}_2$ belong to the same ideal class in the class group $\mathrm{Cl}(16 \cdot -8n)$ of the imaginary quadratic order $\mathbb{Z}[\tau]$.*

Proof. Let $k \in \{1, 2\}$. By Lemma 3.9, we have

$$(8v_k - \tau) = \mathfrak{t}_{4,k}\mathfrak{u}_k^2$$

where $\mathfrak{t}_{4,k} = (8v_k - \tau, 32)$ is as in Section 3.1.4. By (3.16), we have

$$8v_2 = 8(408u_1 + 577v_1) = 8v_1 + 32(102u_1 + 144v_1),$$

so that

$$\mathfrak{t}_{4,2} = (8v_2 - \tau, 32) = (8v_1 - \tau, 32) = \mathfrak{t}_{4,1}.$$

Therefore

$$\mathfrak{u}_2^2 = \frac{8v_2 - \tau}{8v_1 - \tau}\mathfrak{u}_1^2. \tag{3.18}$$

Let

$$\alpha = (17u_1 + 24v_1) + 3\tau.$$

We claim that

$$\left(\frac{\alpha}{u_1}\right)^2 = \frac{8v_2 - \tau}{8v_1 - \tau}. \tag{3.19}$$

We first note that

$$\begin{aligned} \frac{8v_2 - \tau}{8v_1 - \tau} &= \frac{8v_2 - \tau}{8v_1 - \tau} \cdot \frac{8v_1 + \tau}{8v_1 + \tau} \\ &= \frac{64v_1v_2 + 32n + 8(v_2 - v_1)\tau}{64v_1^2 + 32n} \\ &= \frac{64v_1(408u_1 + 577v_1) + 32n + 8(408u_1 + 576v_1)\tau}{32u_1^2} \\ &= \frac{n + 2v_1(408u_1 + 577v_1) + (102u_1 + 144v_1)\tau}{u_1^2}. \end{aligned} \tag{3.20}$$

Expanding α^2, we get

$$\begin{aligned} \alpha^2 &= 289u_1^2 + 576v_1^2 + 816u_1v_1 - 288n + (102u_1 + 144v_1)\tau \\ &= u_1^2 + 1152v_1^2 + 816u_1v_1 + (102u_1 + 144v_1)\tau \\ &= n + 1154v_1^2 + 816u_1v_1 + (102u_1 + 144v_1)\tau \\ &= n + 2v_1(408u_1 + 577v_1) + (102u_1 + 144v_1)\tau. \end{aligned} \tag{3.21}$$

Comparing the last line of (3.21) with the numerator in the last line of (3.20), we obtain (3.19).

Now (3.18) and (3.19) imply that

$$u_1^2\mathfrak{u}_2^2 = \alpha^2\mathfrak{u}_1^2. \tag{3.22}$$

By (3.12), $\mathrm{Norm}(\mathfrak{u}_2) = u_2$. Hence $\mathrm{Norm}(\mathfrak{u}_2)$ is odd, and since u_1 is also odd, we find that $u_1^2\mathfrak{u}_2^2$ is coprime to the conductor $f = 4$ of $\mathbb{Z}[\tau]$, and hence factors uniquely into prime ideals. Therefore (3.22) implies that

$$u_1\mathfrak{u}_2 = \alpha\mathfrak{u}_1,$$

which proves the lemma. □

Remark. There is a shorter proof of Lemma 3.11 via the theory of binary quadratic forms. The $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms of discriminant $16 \cdot -8n$ corresponding to the ideals $\mathfrak{u}_1$ and $\mathfrak{u}_2$ of $\mathbb{Z}[\tau]$ are $[u_1, 16v_1, 32u_1]$ and $[u_2, 16v_2, 32u_2]$, respectively. The matrix

$$\begin{pmatrix} 17 & 96 \\ 3 & 17 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

transforms the quadratic form $[u_1, 16v_1, 32u_1]$ into $[u_2, 16v_2, 32u_2]$, which proves [redacted] the lemma.

Now, for $k \in \{1, 2\}$, define $\nu_k = u_k + v_k\sqrt{2}$ similarly as in Section 3.1.2. Then

$$\nu_2 = \varepsilon^8\nu_1. \tag{3.23}$$

Since $\sqrt{2}$ is contained in $G = K(\sqrt{2})$, ϵ^8 is a square in G. Hence the fields $G(\sqrt{\varepsilon\nu_1})$ and $G(\sqrt{\varepsilon\nu_2})$ are equal, and so we define

$$L = G(\sqrt{\varepsilon\nu_1}) = G(\sqrt{\varepsilon\nu_2}).$$

By Lemma 3.6, L is contained in the ring class field of $\mathbb{Z}[\tau]$. Hence, by Lemma 3.11, the images of both $\mathfrak{u}_1$ and $\mathfrak{u}_2$ under the map (3.7) coincide, i.e.,

$$\left(\frac{\mathfrak{u}_1}{L/K}\right) = \left(\frac{\mathfrak{u}_2}{L/K}\right).$$

Applying Lemma 3.8, we get

$$\left(\frac{v_1}{u_1}\right)\chi(u_1) = \left(\frac{v_2}{u_2}\right)\chi(u_2).$$

Equation (3.16) implies that

$$u_2 = 577u_1 + 816v_1 \equiv u_1 \bmod 16. \tag{3.24}$$

Hence, as χ is a character modulo 16, we have $\chi(u_1) = \chi(u_2)$, and so Proposition 3.2 is finally proved.

3.2 Sums over primes

Above, we defined the governing symbol $[p]$ for a prime $p \equiv -1 \bmod 16$ in terms of particular integer solutions u and v to the equation $p = u^2 - 2v^2$. The main lemma that we will use to prove Theorem 3.1, i.e., that these governing symbols oscillate, is a proposition due to Friedlander, Iwaniec, Mazur and Rubin [17]. We now state this proposition in our context.

3.2.1 A result of Friedlander, Iwaniec, Mazur, and Rubin

Recall that an element $w = u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is *totally positive* if and only if $\mathrm{Norm}(w) = u^2 - 2v^2 > 0$ *and* $u > 0$. We sometimes write $w \succ 0$ to say that w is totally positive.

Since $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain and since the norm of the fundamental unit ε over $\mathbb{Q}$ is -1, an ideal $\mathfrak{n}$ in $\mathbb{Z}[\sqrt{2}]$ can always be generated by a totally positive element. For an ideal $\mathfrak{n}$ of $\mathbb{Z}[\sqrt{2}]$, recall that the norm of $\mathfrak{n}$ is given by

$$\mathrm{Norm}(\mathfrak{n}) := u^2 - 2v^2,$$

where $u + v\sqrt{2}$ is a totally positive generator of $\mathfrak{n}$.

We now define an analogue of the von Mangoldt function Λ for the ring $\mathbb{Z}[\sqrt{2}]$. For a non-zero ideal $\mathfrak{n}$ of $\mathbb{Z}[\sqrt{2}]$, we set

$$\Lambda(\mathfrak{n}) = \begin{cases} \log(\mathrm{Norm}(\mathfrak{p})) & \text{if } \mathfrak{n} = \mathfrak{p}^k \text{ for some prime ideal } \mathfrak{p} \text{ and integer } k \geq 1 \\ 0 & \text{otherwise.} \end{cases}$$

Hence Λ is supported on powers of prime ideals.

Given a sequence of complex numbers $\{a_\mathfrak{n}\}_\mathfrak{n}$ indexed by non-zero ideals in $\mathbb{Z}[\sqrt{2}]$, a good estimate for the sum of $a_\mathfrak{n}$ over prime ideals $\mathfrak{p}$ of norm $\mathrm{Norm}(\mathfrak{p}) \leq X$ can usually be derived from a good estimate of the "smoother" weighted sum

$$S(X) := \sum_{\mathrm{Norm}(\mathfrak{n}) \leq X} a_\mathfrak{n} \Lambda(\mathfrak{n}).$$

The idea in [17] (and even earlier in [19]), is to bound $S(X)$ by combinations of linear and bilinear sums in $a_\mathfrak{n}$. Given a non-zero ideal $\mathfrak{d}$ of $\mathbb{Z}[\sqrt{2}]$, we define the linear sum

$$A_\mathfrak{d}(X) := \sum_{\substack{\mathrm{Norm}(\mathfrak{n}) \leq X \\ \mathfrak{n} \equiv 0 \bmod \mathfrak{d}}} a_\mathfrak{n}. \tag{3.25}$$

Moreover, given two sequences of complex numbers $\{\alpha_\mathfrak{m}\}$ and $\{\beta_\mathfrak{n}\}$, each indexed by non-zero ideals in $\mathbb{Z}[\sqrt{2}]$, we define the bilinear sum

$$B(M, N) := \sum_{\mathrm{Norm}(\mathfrak{m}) \leq M} \sum_{\mathrm{Norm}(\mathfrak{n}) \leq N} \alpha_\mathfrak{m} \beta_\mathfrak{n} a_{\mathfrak{m}\mathfrak{n}}. \tag{3.26}$$

We consider bilinear sums where the complex numbers $\alpha_{\mathfrak{m}}$ and $\beta_{\mathfrak{n}}$ satisfy

$$|\alpha_{\mathfrak{m}}| \leq \Lambda(\mathfrak{m}) \text{ and } |\beta_{\mathfrak{n}}| \leq \tau(\mathfrak{n}), \tag{3.27}$$

where $\tau(\mathfrak{n})$ denotes the number of ideals in $\mathbb{Z}[\sqrt{2}]$ dividing $\mathfrak{n}$. We now state [17, Proposition 5.2, p.722] that we use to prove Theorem 3.1.

Proposition 3.4. *Let $a_{\mathfrak{n}}$ be a sequence of complex numbers bounded by 1 in absolute value and indexed by non-zero ideals of $\mathbb{Z}[\sqrt{2}]$. Suppose that there exist two real numbers $0 < \theta_1, \theta_2 < 1$ such that: for every $\epsilon > 0$, we have*

$$A_{\mathfrak{d}}(X) \ll_{\epsilon} X^{1-\theta_1+\epsilon} \tag{A}$$

uniformly for all non-zero ideals $\mathfrak{d}$ of $\mathbb{Z}[\sqrt{2}]$ and all $X \geq 2$, and

$$B(M,N) \ll_{\epsilon} (M+N)^{\theta_2}(MN)^{1-\theta_2+\epsilon} \tag{B}$$

uniformly for all $M, N \geq 2$ and sequences of complex numbers $\{\alpha_{\mathfrak{m}}\}$ and $\{\beta_{\mathfrak{n}}\}$ satisfying (3.27).
Then for all $X \geq 2$ and all $\epsilon > 0$, we have the bound

$$S(X) \ll_{\epsilon} X^{1-\frac{\theta_1\theta_2}{2+\theta_2}+\epsilon}.$$

In other words, power-saving estimates for linear and bilinear sums imply power-saving estimates for sums supported on primes. Note that this result is now classical in the context of rational integers, thanks to the pioneering work of Vinogradov [44].

3.2.2 Extending governing symbols

In light of Proposition 3.4, our current goal is to define a sequence $a_{\mathfrak{n}}$ over all non-zero ideals $\mathfrak{n}$ of $\mathbb{Z}[\sqrt{2}]$ so that if $p \equiv -1 \bmod 16$ is a prime and $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\sqrt{2}]$ lying above p, then $a_{\mathfrak{p}}$ coincides with the governing symbol $[p]$ defined in (3.6). We first define $[\cdot]$ for all totally positive elements of $\mathbb{Z}[\sqrt{2}]$. We put

$$[u+v\sqrt{2}] := \begin{cases} \left(\frac{v}{u}\right) & \text{if } u \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$$

We remark that $[\cdot]$ is supported on *primitive odd* elements $w \in \mathbb{Z}[\sqrt{2}]$, i.e. $w = u + v\sqrt{2}$ such that $\gcd(u,v) = 1$ and $\mathrm{Norm}(w) = u^2 - 2v^2$ is odd.

If $u + v\sqrt{2} \succ 0$ generates a prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\sqrt{2}]$ lying above a prime $p \equiv -1 \bmod 16$ and if $u \equiv 1 \bmod 16$, then $[u + v\sqrt{2}] = [p]$. The condition $u \equiv 1 \bmod 16$ is useful for two reasons. First, it ensures that $\chi(u) = 1$. Second, for each prime $p \equiv -1 \bmod 16$, there are two prime ideals in $\mathbb{Z}[\sqrt{2}]$ lying above p. If we write their totally positive generators in the form $u + v\sqrt{2}$, then one of them satisfies $v \equiv 1 \bmod 4$ while the other satisfies $v \equiv 3 \bmod 4$.

A priori, the definition (3.6) requires us to choose u and v coming from the prime ideal satisfying $v \equiv 1 \bmod 4$. However, if $u \equiv 1 \bmod 16$, then

$$\left(\frac{-v}{u}\right) = \left(\frac{v}{u}\right),$$

so that $[u + v\sqrt{2}] = [p]$ for *both* of the prime ideals $(u + v\sqrt{2})$ lying above p.

Proposition 3.2 states that $[w] = [\varepsilon^8 w]$ for any $w \in \mathbb{Z}[\sqrt{2}]$, so we might naively define

$$a_{\mathfrak{n}} := [w] + [\varepsilon^2 w] + [\varepsilon^4 w] + [\varepsilon^6 w], \tag{3.28}$$

where $w \succ 0$ is any totally positive generator of $\mathfrak{n}$.

A convenient fact is that if $p \equiv -1 \bmod 16$ is a prime, then exactly one of the four elements $\varepsilon^{2k} w = u_k + v_k\sqrt{2}$ $(0 \leq k \leq 3)$ satisfies $u_k \equiv 1 \bmod 16$. Indeed, multiplying $u + v\sqrt{2}$ by ε^2 (resp. ε^4) transforms (u, v) into $(3u + 4v, 2u + 3v)$ (resp. $(17u + 24v, 12u + 17v)$). If $p \equiv -1 \bmod 16$, then $u \equiv \pm 1 \bmod 8$ and v is odd. Hence $u_4 \equiv u + 8 \bmod 16$, and one can now easily check that multiplying $u+v\sqrt{2}$ successively by ε^2 cycles $u \bmod 16$ through the set $\{1, 7, 9, 15\}$.

The definition (3.28) does not quite suffice for our purposes because we want to isolate those p that are congruent to $-1 \bmod 16$ and representations $p = u^2 - 2v^2$ with $u \equiv 1 \bmod 16$. Hence we weight the formula (3.28) by Dirichlet characters modulo 16. More precisely, for each pair of Dirichlet characters ϕ and ψ modulo 16 and totally positive $u + v\sqrt{2}$, we set

$$[u + v\sqrt{2}]_{\phi,\psi} := \left(\frac{v}{u}\right) \phi(-u^2 + 2v^2)\psi(u). \tag{3.29}$$

For a non-zero ideal $\mathfrak{n}$ in $\mathbb{Z}[\sqrt{2}]$ generated by a totally positive element w, we set

$$a_{\phi,\psi,\mathfrak{n}} := [w]_{\phi,\psi} + [\varepsilon^2 w]_{\phi,\psi} + [\varepsilon^4 w]_{\phi,\psi} + [\varepsilon^6 w]_{\phi,\psi}. \tag{3.30}$$

This is still well-defined, i.e. independent of the choice of $w \succ 0$, by Proposition 3.2 and by (3.24). We will apply Proposition 3.4 to 8^2 sequences $\{a_{\phi,\psi,\mathfrak{n}}\}_{\mathfrak{n}}$, one for each pair of Dirichlet characters ϕ, ψ, and then add together the corresponding 8^2 sums $S_{\phi,\psi}(X)$ to obtain Theorem 3.1. The key lemma is then

Lemma 3.12. *If p is a prime and $\mathfrak{p}$ is a prime ideal lying above p, then we have*

$$\frac{1}{8^2}\sum_{\phi}\sum_{\psi} a_{\phi,\psi,\mathfrak{p}} = \begin{cases} [p] & \text{if } p \equiv -1 \bmod 16 \\ 0 & \text{otherwise.} \end{cases}$$

Hence, to prove Theorem 3.1, it now suffices to prove

Theorem 3.2. *Let $a_{\phi,\psi,\mathfrak{n}}$ be defined as in* (3.30)*. For every $\epsilon > 0$, there is a constant $C_\epsilon > 0$ depending only on ϵ such that for every $X \geq 2$, we have*

$$\left| \sum_{\text{Norm}(\mathfrak{n}) \leq X} a_{\phi,\psi,\mathfrak{n}} \Lambda(\mathfrak{n}) \right| \leq C_\epsilon X^{\frac{149}{150}+\epsilon}.$$

3.3 Fundamental domains

In order to obtain power-saving cancellation for linear and bilinear sums as in Proposition 3.4, we will have to choose generators of $\mathfrak{n}$ in (3.30) carefully. The problem reduces to finding a convenient fundamental domain for the action of $\varepsilon^2 = 3 + 2\sqrt{2}$ on totally positive elements of $\mathbb{Z}[\sqrt{2}]$.

In [17], the authors describe how to construct such a fundamental domain in a more general setting. We give simpler arguments tailored to our specific needs and describe a fundamental domain very explicitly. This explicit description along with the ancillary pictures is possible in large part because the degree of the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is 2.

Let

$$\Omega := \left\{ (u,v) \in \mathbb{R}^2 : u > 0, -u < \sqrt{2}v < u \right\}.$$

Then the lattice points $(u,v) \in \Omega \cap \mathbb{Z}^2$ precisely enumerate the totally positive elements $w = u + v\sqrt{2}$. The ring $\mathbb{Z}[\sqrt{2}]$ acts on itself by multiplication, and this induces an action

$$\mathbb{Z}[\sqrt{2}] \times \Omega \to \Omega$$

given by

$$(a,b) \cdot (u,v) := (au + 2bv, bu + av).$$

Since $\text{Norm}(\varepsilon^2) = 1$ and since the norm is multiplicative, it follows immediately that $\varepsilon^2 \cdot \Omega \subset \Omega$.

Let $\mathcal{D}$ be the subset of Ω defined by

$$\mathcal{D} := \left\{ (u,v) \in \mathbb{R}^2 : u > 0, -u < 2v \leq u \right\} \tag{3.31}$$

We claim that the region $\mathcal{D}$ in Figure 3.1 shown above is a fundamental domain for the action of ε^2 on Ω in the following sense.

Lemma 3.13. *For each element $(u,v) \in \Omega \cap \mathbb{Z}^2$, there exists exactly one integer k such that $\varepsilon^{2k} \cdot (u,v) \in \mathcal{D}$.*

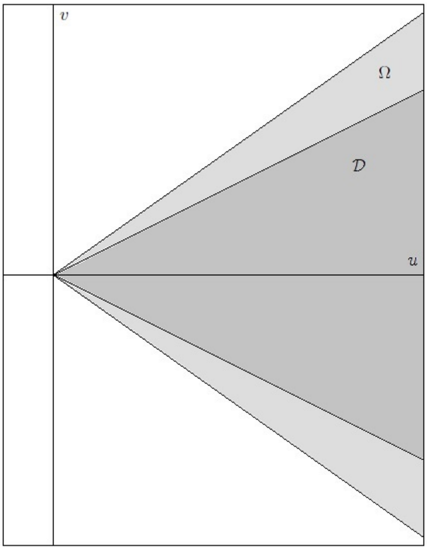


Figure 3.1: The region Ω and the fundamental domain $\mathcal{D}$

Proof. For an element $w = (u, v) \in \mathbb{R}^2$ with $u \neq 0$, define the *slope* of w to be

$$m(w) = \frac{v}{u}.$$

By definition, Ω is the subset of $\mathbb{R}^2$ consisting of w such that $u > 0$ and $|m(w)| < 1/\sqrt{2}$, and $\mathcal{D}$ is the subset of Ω consisting of w such that $-1/2 < m(w) \leq 1/2$.

For each integer k, define integers p_k and q_k by the equation

$$(3 + 2\sqrt{2})^{2k} = p_k + q_k\sqrt{2}.$$

Since $p_k^2 - 2q_k^2 = 1$, it follows that $q_k/p_k \to 1/\sqrt{2}$ as $k \to +\infty$. Moreover, $p_{-k} = p_k$ and $q_{-k} = -q_k$, so that $q_k/p_k \to -1/\sqrt{2}$ as $k \to -\infty$. We will also use the fact that $|q_k/p_k| < 1/\sqrt{2}$.

Now let $w = (u, v) \in \Omega \cap \mathbb{Z}^2$. We have

$$m(\varepsilon^{2k} \cdot w) = \frac{q_k u + p_k v}{p_k u + 2q_k v} = \frac{q_k}{p_k} + \frac{v}{p_k(p_k u + 2q_k v)}.$$

Since u and v are integers, so is $p_k u + 2q_k v$. If $p_k u + 2q_k v = 0$, then

$$\left|\frac{v}{u}\right| = \left|\frac{p_k}{2q_k}\right| > \frac{1}{\sqrt{2}},$$

which contradicts the assumption that $(u, v) \in \Omega$. Hence $p_k u + 2q_k v$ is a non-zero integer, so that $|p_k u + 2q_k v| \geq 1$, and since $p_k \to +\infty$ as $k \to +\infty$, we deduce that

$$m(\varepsilon^{2k} \cdot w) \to \pm\frac{1}{\sqrt{2}}$$

as $k \to \pm\infty$.

Moreover, we have

$$m(\varepsilon^2 \cdot w) - m(w) = \frac{2u + 3v}{3u + 4v} - \frac{v}{u} = \frac{2(u^2 - 2v^2)}{(3u + 4v)u}.$$

As $3\sqrt{2} > 4$, we deduce that

$$3u + 4v > 3\sqrt{2}|v| + 4v \geq 0,$$

and so $m(\varepsilon^2 \cdot w) - m(w) > 0$. Also, as $(u + 2v)^2 \geq 0$, we deduce that

$$2u^2 - 4v^2 \leq 3u^2 + 4uv,$$

so that $m(\varepsilon^2 \cdot w) - m(w) \leq 1$. Hence multiplying $w \in \Omega$ by ε^2 strictly increases its slope by at most 1 and multiplying $w \in \Omega$ by ε^{-2} strictly decreases its slope by at most 1. As $|m(w_1) - m(w_2)| < 1$ for any two elements $w_1, w_2 \in \mathcal{D}$, this proves that for each $w \in \Omega \cap \mathbb{Z}^2$, there exists an integer k such that $\varepsilon^{2k} w \in \mathcal{D}$.

To show that this integer k is unique, it remains to prove that if $w = (u, v) \in \mathcal{D}$, then $\varepsilon^2 \cdot w = (3u + 4v, 2u + 3v) \notin \mathcal{D}$. Suppose for sake of contradiction that $\varepsilon^2 \cdot w \in \mathcal{D}$. Then

$$2(2u + 3v) \leq 3u + 4v,$$

so that $-u \geq 2v$, which contradicts the assumption that $(u, v) \in \mathcal{D}$. □

An immediate consequence of Lemma 3.13 is the following proposition.

Proposition 3.5. *Suppose that* $\mathfrak{n}$ *is a non-zero ideal of* $\mathbb{Z}[\sqrt{2}]$. *Then* $\mathfrak{n}$ *has a unique generator in* $\mathcal{D}$.

3.3.1 Geometry of numbers in the fundamental domain: the Lipschitz principle

We now briefly turn to the problem of counting lattice points and boxes inside certain compact subsets of the fundamental domain $\mathcal{D}$. We state a lemma of Davenport (see [9] and [10]).

Let $\mathcal{R}$ be a compact, Lebesgue measurable subset of $\mathbb{R}^n$. Suppose that $\mathcal{R}$ satisfies the following two conditions:

1. Any line parallel to one of the n coordinate axes intersects $\mathcal{R}$ in a set of points which, if not empty, consists of at most h intervals, and
2. The same is true (with m in place of n) for any of the m-dimensional regions obtained by projecting $\mathcal{R}$ on one of the coordinate spaces defined by equating a selection of $n-m$ of the coordinates to zero; and this condition is satisfied for all m from 1 to $n-1$.

Lemma 3.14 (Davenport). *If $\mathcal{R}$ satisfies conditions (1) and (2) above, then*

$$|\mathcal{R} \cap \mathbb{Z}^n - \mathrm{Vol}(\mathcal{R})| \leq \sum_{m=0}^{n-1} h^{n-m} V_m$$

where V_m is the sum of the m-dimensional volumes of the projections of $\mathcal{R}$ on the various coordinate spaces obtained by equating any $n-m$ coordinates to zero, and $V_0 = 1$ by convention.

We will apply Lemma 3.14 to the fundamental domain $\mathcal{D} \subset \mathbb{R}^2$ as well as certain variations thereof.

Let k be a positive integer, and define

$$\mathcal{D}_k = \mathcal{D} \cup \varepsilon^2 \cdot \mathcal{D} \cdots \cup \varepsilon^{2k} \cdot \mathcal{D}.$$

Let $X > 0$. Then the region

$$\mathcal{D}_k(X) := \{(u, v) \in \mathcal{D}_k : u^2 - 2v^2 \leq X\}$$

is a compact subset of $\mathbb{R}^2$ and satisfies conditions (1) and (2) above with $h = 2$. Moreover, one can check that there exist positive real numbers a_k and ℓ_k such that

$$\mathrm{Vol}(\mathcal{D}_k(X)) = a_k X \tag{3.32}$$

and

$$\mathrm{Vol}(\partial(\mathcal{D}_k(X))) = \ell_k X^{\frac{1}{2}}.$$

Now let $L : \mathbb{R}^2 \to \mathbb{R}^2$ be an invertible linear transformation of the form

$$L\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix},$$

of determinant

$$D := ad - bc \neq 0.$$

Then $L(\mathcal{D}_k(X))$ is a compact subset of $\mathbb{R}^2$ that also satisfies conditions (1) and (2) above, also with $h = 2$.

We define the diameter of L to be

$$\mathrm{diam}(L) = |a| + |b| + |c| + |d|.$$

Then

$$\mathrm{Vol}(L(\mathcal{D}_k(X))) = |D|\mathrm{Vol}(\mathcal{D}_k(X))$$

and

$$\mathrm{Vol}(\partial(L(\mathcal{D}_k(X)))) = O(\mathrm{diam}(L) \cdot X^{\frac{1}{2}}),$$

where the implied constant is absolute.

3.4 Linear sums

In this section we prove that the estimate (A) from Proposition 3.4 holds for the sequence $\{a_{\phi,\psi,\mathfrak{n}}\}_{\mathfrak{n}}$ defined in (3.30) with $\theta_1 = 1/6$.

Proposition 3.6. *Let $a_{\mathfrak{n}} = a_{\phi,\psi,\mathfrak{n}}$, where $a_{\phi,\psi,\mathfrak{n}}$ is defined as in* (3.30)*, and let $A_{\mathfrak{d}}(X)$ be defined as in* (3.25)*. Then for all $\epsilon > 0$ and all $X \geq 2$, we have*

$$A_{\mathfrak{d}}(X) \ll_\epsilon X^{\frac{5}{6}+\epsilon}.$$

Proof. Recall that

$$A_{\mathfrak{d}}(X) = \sum_{\substack{\mathrm{Norm}(\mathfrak{n}) \leq X \\ \mathfrak{n} \equiv 0 \bmod \mathfrak{d}}} a_{\mathfrak{n}}.$$

Since the sequence $a_{\mathfrak{n}}$ is supported on odd ideals $\mathfrak{n}$, we see that $A_{\mathfrak{d}}(X) = 0$ unless $\mathfrak{d}$ is odd. Hence we may assume without loss of generality that $\mathfrak{d}$ is an odd ideal. Let

$$\mathcal{R}(X) := \mathcal{D}_4(X) = \left\{(u,v) \in \mathcal{D} \cup \varepsilon^2\mathcal{D} \cup \varepsilon^4\mathcal{D} \cup \varepsilon^6\mathcal{D} : u^2 - 2v^2 \leq X\right\}. \quad (3.33)$$

By Proposition 3.5 and definition (3.30), we have

$$A_{\mathfrak{d}}(X) = \sum_{\substack{(u,v) \in \mathcal{R}(X) \\ u+v\sqrt{2} \equiv 0 \bmod \mathfrak{d}}} [u + v\sqrt{2}]_{\phi,\psi},$$

where $[u + v\sqrt{2}]_{\phi,\psi}$ is defined as in (3.29).

We now reformulate the congruence condition $u + v\sqrt{2} \equiv 0 \bmod \mathfrak{d}$. Proposition 3.5 implies that there is an element $d_1 + d_2\sqrt{2} \in \mathcal{D}$ which generates $\mathfrak{d}$. Then the congruence above is equivalent to saying that there exist integers e_1 and e_2 such that $u + v\sqrt{2} = (d_1 + d_2\sqrt{2})(e_1 + e_2\sqrt{2})$, i.e. such that

$$u = d_1e_1 + 2d_2e_2$$

and

$$v = d_2e_1 + d_1e_2.$$

In other words, (u,v) is in the image of the linear transformation

$$L_{\mathfrak{d}} := \begin{pmatrix} d_1 & 2d_2 \\ d_2 & d_1 \end{pmatrix} : \mathbb{Z}^2 \to \mathbb{Z}^2$$

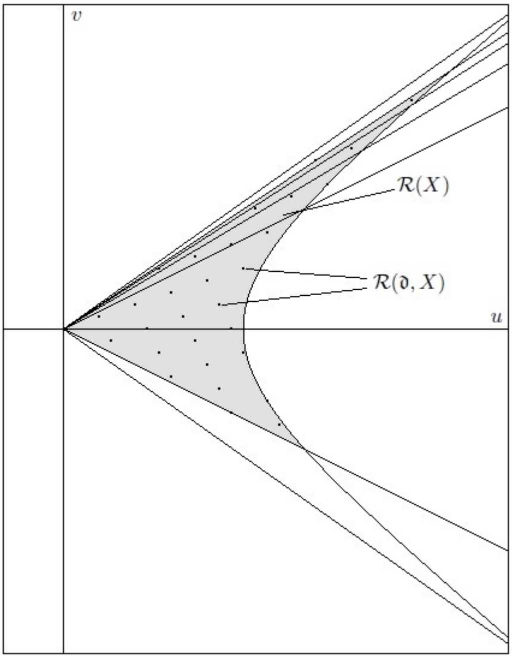


Figure 3.2: The region $\mathcal{R}(X)$ and the lattice points $\mathcal{R}(\mathfrak{d}, X)$

of determinant

$$D := \mathrm{Norm}(\mathfrak{d}) = d_1^2 - 2d_2^2.$$

Hence we define

$$\mathcal{R}(\mathfrak{d}, X) := \{(u, v) \in \mathcal{R}(X) : (u, v) \in \mathrm{Image}(L_{\mathfrak{d}})\}$$

(depicted in Figure 3.2), and we rewrite the sum $A_{\mathfrak{d}}(X)$ as

$$A_{\mathfrak{d}}(X) = \sum_{(u,v)\in\mathcal{R}(\mathfrak{d},X)} [u + v\sqrt{2}]_{\phi,\psi}.$$

Using the fact that $|[u + v\sqrt{2}]_{\phi,\psi}| \leq 1$, we obtain the trivial bound

$$|A_{\mathfrak{d}}(X)| \leq \sum_{(u,v)\in\mathcal{R}(\mathfrak{d},X)} 1 = \sum_{L_{\mathfrak{d}}^{-1}\mathcal{R}(X)\cap\mathbb{Z}^2} 1. \qquad (3.34)$$

Since $d_1 + d_2\sqrt{2} \in \mathcal{D}$, we have the inequalities

$$\frac{d_1^2}{2} \leq D \leq d_1^2,$$

which implies that $\operatorname{diam}(L_{\mathfrak{d}}^{-1}) \ll D^{-1/2}$. Hence Lemma 3.14 gives

$$|A_{\mathfrak{d}}(X)| \leq a_4 X D^{-1} + O(D^{-\frac{1}{2}} X^{\frac{1}{2}} + 1) \ll X D^{-1} + X^{\frac{1}{2}} D^{-\frac{1}{2}} + 1, \qquad (3.35)$$

where the implied constant is absolute. This estimate will be useful when D is large compared to X.

Next we split the sum $A_{\mathfrak{d}}(X)$ into $8 \cdot 16$ sums where the congruence classes of u and v modulo 16 are fixed, say $u \equiv u_0 \bmod 16$ and $v \equiv v_0 \bmod 16$ for some congruence classes u_0 and v_0 modulo 16 with u_0 invertible modulo 16. For u and v satisfying these congruences, we have

$$[u + v\sqrt{2}]_{\phi,\psi} = \delta(u_0, v_0) \left(\frac{v}{u}\right),$$

where $\delta(u_0, v_0) \in \{\pm 1\}$ depends only on the congruence classes u_0 and v_0 modulo 16. Hence it remains to give estimates for sums of the type

$$A_{\mathfrak{d}}(u_0, v_0, X) := \sum_{(u,v) \in \mathcal{R}(u_0, v_0, \mathfrak{d}, X)} \left(\frac{v}{u}\right),$$

where

$$\mathcal{R}(u_0, v_0, \mathfrak{d}, X) := \{(u, v) \in \mathcal{R}(\mathfrak{d}, X) : (u, v) \equiv (u_0, v_0) \bmod 16\}.$$

Splitting the sum according to the value of u, we obtain

$$A_{\mathfrak{d}}(u_0, v_0, X) = \sum_{\substack{0 \leq u \leq R_1(X) \\ u \equiv u_0 \bmod 16}} A_{u,\mathfrak{d}}(v_0, X), \qquad (3.36)$$

where

$$A_{u,\mathfrak{d}}(v_0, X) := \sum_{\substack{v \in I_u \\ (u,v) \in L_{\mathfrak{d}}(\mathbb{Z}^2) \\ v \equiv v_0 \bmod 16}} \left(\frac{v}{u}\right).$$

Here

$$R_1(X) = \sup\{u \in \mathbb{R} : \ (u, v) \in \mathcal{R}(X)\} \ll X^{\frac{1}{2}}$$

and I_u is an interval (or a union of 2 disjoint intervals) of size $\leq 2R_2(X)$, where

$$R_2(X) = \sup\{|v| \in \mathbb{R} : \ (u, v) \in \mathcal{R}(X)\} \ll X^{\frac{1}{2}}.$$

We now unwind the condition $(u, v) \in L_{\mathfrak{d}}(\mathbb{Z}^2)$, i.e. that (u, v) is in the image of $L_{\mathfrak{d}}$. Consider the system of equations in x and y:

$$\begin{cases} u = d_1 x + 2 d_2 y \\ v = d_2 x + d_1 y. \end{cases} \qquad (3.37)$$

Let $d := \gcd(d_1, d_2)$ and write $d_1 = dd_1'$, $d_2 = dd_2'$. Recall that $\mathfrak{d}$ and so also d_1 is odd, so that $d = \gcd(d_1, 2d_2)$. If the system (3.37) has a solution over $\mathbb{Z}$, then d must divide u. This means that

$$A_{\mathfrak{d}}(u_0, v_0, X) = \sum_{\substack{0 \leq u \leq R_1(X) \\ u \equiv u_0 \bmod 16 \\ u \equiv 0 \bmod d}} A_{u,\mathfrak{d}}(v_0, X).$$

Now suppose $u \equiv 0 \bmod d$, and let $x_u, y_u \in \mathbb{Z}$ be such that

$$u = d_1 x_u + 2d_2 y_u.$$

Then all solutions $(x, y) \in \mathbb{Z}^2$ to the first equation in (3.37) are given by

$$(x, y) = (x_u - 2d_2'k, y_u + d_1'k), \quad k \in \mathbb{Z}.$$

Hence

$$v = d_2 \left(x_u - 2d_2'k\right) + d_1 \left(y_u + d_1'k\right) = d_2 x_u + d_1 y_u + Dk/d,$$

which means that (3.37) has a solution over $\mathbb{Z}$ if and only if

$$v \equiv d_2 x_u + d_1 y_u \bmod D/d.$$

Note that D is odd, so that D/d and 16 are coprime. Let v_u be the congruence class modulo $16D/d$ such that

$$\begin{cases} v_u \equiv d_2 x_u + d_1 y_u \bmod D/d \\ v_u \equiv v_0 \bmod 16. \end{cases}$$

Thus we have proved that if $u \equiv 0 \bmod d$, then

$$A_{u,\mathfrak{d}}(v_0, X) = \sum_{\substack{v \in I_u \\ v \equiv v_u \bmod 16D/d}} \left(\frac{v}{u}\right).$$

Let $e_u = \gcd(v_u, 16D/d)$, write $16D/d = e_u d_u$, $v_u = e_u v_u'$, and perform a change of variables $v = e_u v'$, so that

$$A_{u,\mathfrak{d}}(v_0, X) = \left(\frac{e_u}{u}\right) \sum_{\substack{v' \in I_u' \\ v' \equiv v_u' \bmod d_u}} \left(\frac{v'}{u}\right),$$

where $I_u' = I_u/e_u$. Since $\gcd(v_u', d_u) = 1$, we can now detect the congruence condition $v' \equiv v_u' \bmod d_u$ via Dirichlet characters modulo d_u. In other words,

$$A_{u,\mathfrak{d}}(v_0, X) = \frac{1}{\varphi(d_u)} \left(\frac{e_u}{u}\right) \chi(\overline{v_u'}) \sum_{\chi \bmod d_u} \sum_{v' \in I_u'} \chi(v') \left(\frac{v'}{u}\right), \tag{3.38}$$

where $\overline{v'_u}$ denotes the multiplicative inverse of v'_u modulo d_u. Let χ be a Dirichlet character modulo d_u. If the character

$$v' \mapsto \chi(v') \left(\frac{v'}{u}\right)$$

is trivial, then $u = fg^2$ for some f dividing d_u (and therefore dividing $16D/d$) and some integer g. The number of such $u \leq R_1(X)$ is

$$\leq \tau(16D/d) R_1(X)^{\frac{1}{2}} \ll_\epsilon D^\epsilon X^{\frac{1}{4}}.$$

In this case we use the trivial bound

$$\sum_{v' \in I'_u} \chi(v') \left(\frac{v'}{u}\right) \ll \# I'_u \leq \# I_u \ll X^{\frac{1}{2}},$$

where the implied constant in $\ll$ is absolute. Hence the contribution of such u to $A_{\mathfrak{d}}(u_0, v_0, X)$ is

$$\ll_\epsilon D^\epsilon X^{\frac{3}{4}}. \tag{3.39}$$

On the other hand, if the character

$$v' \mapsto \chi(v') \left(\frac{v'}{u}\right)$$

is not trivial, its conductor is at most

$$16Du/d \ll DX^{\frac{1}{2}},$$

and so the Polya-Vinogradov inequality gives the estimate

$$\sum_{v' \in I'_u} \chi(v') \left(\frac{v'}{u}\right) \ll_\epsilon D^{\frac{1}{2}} X^{\frac{1}{4}+\epsilon}.$$

Combining this with (3.36), (3.38), and (3.39), we have proved the bound

$$A_{\mathfrak{d}}(X) \ll_\epsilon D^{\frac{1}{2}} X^{\frac{3}{4}+\epsilon}. \tag{3.40}$$

We use (3.40) for $D < X^{1/6}$ and (3.35) for $D \geq X^{1/6}$ to obtain

$$A_{\mathfrak{d}}(X) \ll_\epsilon X^{\frac{5}{6}+\epsilon}.$$

□

3.5 Bilinear sums

We are left with proving the estimate (B) from Proposition 3.4, which we do with $\theta_2 = 1/12$ in much the same way as in [19, Sections 19-21, p. 1018-1028].

Proposition 3.7. *Let $a_{\mathfrak{n}} = a_{\phi,\psi,\mathfrak{n}}$, where $a_{\phi,\psi,\mathfrak{n}}$ is defined as in* (3.30)*, and let $B(M,N)$ be defined as in* (3.26)*. Then for all $\epsilon > 0$ and all $M, N \geq 2$, we have*

$$B(M,N) \ll_\epsilon (M+N)^{\frac{1}{12}} (MN)^{\frac{11}{12}+\epsilon}.$$

Before we begin the proof of Proposition 3.7, we first define a quantity $\gamma(w,z)$ that oscillates in both arguments $w, z \in \mathbb{Z}[\sqrt{2}]$.

3.5.1 The symbol $\gamma(w,z)$

Let σ denote the non-trivial automorphism of $\mathbb{Q}(\sqrt{2})$. Define the *rational part* of an element $w \in \mathbb{Z}[\sqrt{2}]$ to be

$$\mathrm{r}(w) := \frac{1}{2}(w + \sigma(w)).$$

In other words, if $w = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$, then $\mathrm{r}(w) = a$.

We say that an element $w = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is *primitive* if and only if $\gcd(a,b) = 1$.

Suppose w and z are primitive. Then wz need *not* be primitive. Nonetheless, we have the following lemma.

Lemma 3.15. *Suppose w and z are primitive. Let $d = \mathrm{Norm}(\gcd(w, \sigma(z))$. Then wz/d is primitive. In particular, wz is primitive whenever* $\gcd(w, \sigma(z)) =$ [redacted] 1.

Proof. If p is inert in $\mathbb{Z}[\sqrt{2}]$ and $p|wz$, then by unique prime factorization in $\mathbb{Z}[\sqrt{2}]$, p divides either w or z, which contradicts the assumption that w and z are primitive. Now suppose that p splits in $\mathbb{Z}[\sqrt{2}]$ (resp. $p = 2$), so that $p = \xi\sigma(\xi)$ (resp. $p = -\xi\sigma(\xi)$) for some prime $\xi \in \mathbb{Z}[\sqrt{2}]$. If p^k is the exact power of p dividing wz, then the assumption that w and z are primitive implies that $\xi^k|w$ and $\sigma(\xi^k)|z$, which is true if and only if $\xi^k|\gcd(w_1, \sigma(w_2))$. The lemma now follows by unique factorization in $\mathbb{Z}[\sqrt{2}]$. □

Given an odd, totally positive, primitive $w \in \mathbb{Z}[\sqrt{2}]$ a totally positive $z \in \mathbb{Z}[\sqrt{2}]$, we define the *generalized Dirichlet symbol* $\gamma(w,z)$ to be

$$\gamma(w,z) := \left(\frac{\mathrm{r}(wz)}{\mathrm{Norm}(w)}\right), \tag{3.41}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi symbol. More concretely, if we write $w = a + b\sqrt{2}$ and $z = c + d\sqrt{2}$, then

$$\gamma(w,z) = \left(\frac{ac+2bd}{a^2-2b^2}\right).$$

Our choice of terminology is inspired by the Dirichlet symbol defined in a slightly different setting in [19, Section 19, p. 1018-1021].

The symbol $\gamma(w,z)$ is almost multiplicative in the second argument. More precisely, for an odd, totally positive $w = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, define

$$\mathrm{m}(w) := \left(\frac{\mathrm{r}(w)}{\mathrm{Norm}(w)}\right) = \left(\frac{a}{a^2-2b^2}\right). \tag{3.42}$$

Note that w is primitive if and only if $\mathrm{m}(w) \neq 0$. In this case, the law of quadratic reciprocity implies that

$$\left(\frac{a}{a^2-2b^2}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{a^2-2b^2-1}{2}}\left(\frac{-2}{a}\right),$$

and so $\mathrm{m}(w) \in \{\pm 1\}$ depends only on the residue class of w modulo 8. We have

Lemma 3.16. *Let $w \in \mathbb{Z}[\sqrt{2}]$ be odd, totally positive, and primitive, and let $z_1, z_2 \in \mathbb{Z}[\sqrt{2}]$ be totally positive. Then*

$$\gamma(w, z_1z_2) = \gamma(w,z_1)\gamma(w,z_2)\mathrm{m}(w). \tag{3.43}$$

Proof. Write $w = a + b\sqrt{2}$, $z_1 = c_1 + d_1\sqrt{2}$, and $z_2 = c_2 + d_2\sqrt{2}$. Then

$$\gamma(w,z_1)\gamma(w,z_2) = \left(\frac{a^2c_1c_2 + 2ab(c_1d_2+c_2d_1) + 4b^2d_1d_2}{a^2-2b^2}\right).$$

Using the facts that $4b^2 \equiv 2a^2 \bmod a^2-2b^2$ and that $z_1z_2 = (c_1c_2+2d_1d_2) + (c_1d_2+c_2d_1)\sqrt{2}$, we deduce that

$$\begin{aligned}\gamma(w,z_1)\gamma(w,z_2) &= \left(\frac{a^2(c_1c_2+2d_1d_2)+2ab(c_1d_2+c_2d_1)}{a^2-2b^2}\right)\\ &= \left(\frac{a}{a^2-2b^2}\right)\left(\frac{a(c_1c_2+2d_1d_2)+2b(c_1d_2+c_2d_1)}{a^2-2b^2}\right)\\ &= \mathrm{m}(w)\gamma(w,z_1z_2).\end{aligned}$$

□

The symbol $\gamma(w,z)$ also satisfies a reciprocity law.

Lemma 3.17. *Let w and z be odd, totally positive, and primitive elements of $\mathbb{Z}[\sqrt{2}]$. Then*

$$\gamma(w,z)\gamma(z,w) = \mathrm{m}(wz). \tag{3.44}$$

In particular, if $\gamma(w,z) = 0$ whenever $\gcd(w,\sigma(z)) \neq 1$.

Proof. We have

$$\gamma(w,z)\gamma(z,w) = \left(\frac{\mathrm{r}(wz)}{\mathrm{Norm}(w)}\right)\left(\frac{\mathrm{r}(wz)}{\mathrm{Norm}(z)}\right) = \left(\frac{\mathrm{r}(wz)}{\mathrm{Norm}(wz)}\right) = \mathrm{m}(wz).$$

□

Finally, we remark that $\gamma(w,z_1) = \gamma(w,z_2)$ whenever $z_1 \equiv z_2 \bmod \mathrm{Norm}(w)$. [redacted]

3.5.2 Twisted multiplicativity of governing symbols

Recall that if $u+v\sqrt{2}$ is a totally positive odd element of $\mathbb{Z}[\sqrt{2}]$, we define the governing symbol $[u+v\sqrt{2}]$ to be

$$[u+v\sqrt{2}] = \left(\frac{v}{u}\right).$$

Thus $[u+v\sqrt{2}] = 0$ whenever $u+v\sqrt{2}$ is not primitive.

A key feature of the governing symbol $[\cdot]$ which leads to significant cancellation in (3.26) is that $[\cdot]$ is *not* multiplicative, i.e. the relation

$$[wz] = [w][z],$$

does *not* hold for all totally positive w and z. Instead, the equation above becomes essentially valid when twisted by $\gamma(w,z)$. We now state our result more precisely.

We now introduce notation that will simplify the subsequent arguments. Suppose that f_1 and f_2 are functions $\mathbb{Z}^r \to \mathbb{C}$. For $x \in \mathbb{Z}^r$, we write $f_1 \sim f_2$ (or more conveniently $f_1(x) \sim f_2(x)$) if there exists a function $\delta : \mathbb{Z}^r \to \{\pm 1\}$ such that δ factors though $(\mathbb{Z}/16\mathbb{Z})^r$, i.e. the value of $\delta(x)$ depends only on the congruence classes of the coordinates of x modulo 16, and such that

$$f_1(x) = \delta(x) f_2(x)$$

for all $x \in \mathbb{Z}^r$. For instance, $[u+v\sqrt{2}]_{\phi,\psi} \sim [u+v\sqrt{2}]_{\phi',\psi'}$ for any four Dirichlet characters ϕ, ψ, ϕ', ψ'.

The following proposition is analogous to [19, Lemma 20.1, p. 1021].

Proposition 3.8. *Let $w = a+b\sqrt{2}$ and $z = c+d\sqrt{2}$ be two primitive, totally positive, odd elements of $\mathbb{Z}[\sqrt{2}]$. Then*

$$[wz] \sim [w][z]\gamma(w,z).$$

Proof. When wz is not primitive, then $[wz] = 0$ and $\gamma(w,z) = 0$, and so the result follows. Hence we may assume that wz is primitive.

First note that

$$wz = (ac+2bd) + (ad+bc)\sqrt{2}.$$

We set $\rho = (a,d)$ and define a_1 and d_1 by the equalities $a = \rho a_1$ and $d = \rho d_1$, respectively. Then

$$[wz] = \left(\frac{ad+bc}{ac+2bd}\right) = \left(\frac{ad+bc}{\rho}\right)\left(\frac{ad+bc}{a_1c+2bd_1}\right),$$

and since ρ divides ad, the above simplifies to

$$[wz] = \left(\frac{bc}{\rho}\right)\left(\frac{ad+bc}{a_1c+2bd_1}\right).$$

Now, since w is primitive, a_1 is relatively prime to b and hence also to a_1c+2bd_1. Hence we may write

$$c \equiv -2bd_1/a_1 \pmod{a_1c+2bd_1},$$

so that the second factor in the expression above becomes

$$\left(\frac{ad+bc}{a_1c+2bd_1}\right) = \left(\frac{ad-2b^2d_1/a_1}{a_1c+2bd_1}\right) = \left(\frac{a_1d_1}{a_1c+2bd_1}\right)\left(\frac{\rho^2-2b^2/a_1^2}{a_1c+2bd_1}\right).$$

As $a^2-2b^2 = a_1^2(\rho^2-2b^2/a_1^2)$, we deduce that

$$[wz] \sim \left(\frac{bc}{\rho}\right)\left(\frac{a_1d_1}{a_1c+2bd_1}\right)\left(\frac{a^2-2b^2}{a_1c+2bd_1}\right).$$

We write the last factor in the expression above as

$$\left(\frac{a^2-2b^2}{a_1c+2bd_1}\right) = \left(\frac{a^2-2b^2}{\rho}\right)\left(\frac{a^2-2b^2}{ac+2bd}\right),$$

and use the fact that

$$\left(\frac{a^2-2b^2}{\rho}\right) = \left(\frac{-2b^2}{\rho}\right) = \left(\frac{-2}{\rho}\right)$$

to conclude that

$$[wz] \sim \left(\frac{-2bc}{\rho}\right)\left(\frac{a_1d_1}{a_1c+2bd_1}\right)\left(\frac{a^2-2b^2}{ac+2bd}\right).$$

The law of quadratic reciprocity implies that

$$\left(\frac{a^2-2b^2}{ac+2bd}\right) \sim \left(\frac{ac+2bd}{a^2-2b^2}\right),$$

so that

$$[wz] \sim \left(\frac{-2bc}{\rho}\right)\left(\frac{a_1d_1}{a_1c+2bd_1}\right)\gamma(w,z).$$

We again use the law of quadratic reciprocity to treat the middle term above. We get

$$\left(\frac{a_1}{a_1c+2bd_1}\right) = (-1)^{\nu_1(a,b,c,d,\rho)}\left(\frac{2}{a_1}\right)\left(\frac{bd_1}{a_1}\right),$$

where

$$\nu_1(a,b,c,d,\rho) \equiv \frac{a_1-1}{2}\cdot\frac{r_1-1}{2} \bmod 2$$

and

$$r_1 = a_1 c + 2bd_1.$$

Similarly, we write d_1 as

$$d_1 = 2^e d_2,$$

where d_2 is odd, and compute that

$$\left(\frac{d_1}{a_1 c + 2bd_1}\right) = (-1)^{\nu_2(a,b,c,d,\rho)} \left(\frac{d_1}{a_1 c}\right),$$

where now

$$\nu_2(a,b,c,d,\rho) \equiv e\frac{r_1^2 - 1}{8} + \frac{d_2 - 1}{2} \cdot \frac{r_1 - 1}{2} + \frac{d_2 - 1}{2} \cdot \frac{a_1 c - 1}{2} + e\frac{a_1^2 c^2 - 1}{8} \bmod 2.$$

We thus have

$$[wz] \sim (-1)^{\nu_1 + \nu_2} \left(\frac{2}{a_1}\right) \left(\frac{-2bc}{\rho}\right) \left(\frac{b}{a_1}\right) \left(\frac{d_1}{c}\right) \gamma(w,z),$$

which simplifies to

$$[wz] \sim (-1)^{\nu_1 + \nu_2 + \nu_3} \left(\frac{-1}{\rho}\right) \left(\frac{b}{a}\right) \left(\frac{d}{c}\right) \gamma(w,z),$$

where

$$\nu_3 = \nu_3(c,\rho) \equiv \frac{\rho - 1}{2} \cdot \frac{c - 1}{2} \bmod 2.$$

It remains to show that

$$(-1)^{\nu_1 + \nu_2 + \nu_3} \left(\frac{-1}{\rho}\right)$$

depends only on the residue classes of a, b, c, d modulo 16. First note that whether $e = 0$, $e = 1$, or $e \geq 2$ depends only on the residue class of d modulo 4 (and hence also modulo 16). Hence we can split into cases $e = 0$, $e = 1$, and $e \geq 2$.

Note that if $e \geq 2$ or $e = 1$ and $b \equiv 0 \bmod 2$, then $r_1 \equiv a_1 c \bmod 8$. Using this observation and the definitions of ν_1, ν_2, and ν_3, we find that

$$\nu_2 \equiv \begin{cases} \frac{d_1 - 1}{2} \bmod 2 & \text{if } e = 0 \text{ and } b \equiv 1 \bmod 2 \\ 1 \bmod 2 & \text{if } e = 1 \text{ and } b \equiv 1 \bmod 2 \\ 0 \bmod 2 & \text{otherwise.} \end{cases}$$

First suppose $e \geq 2$. Then $r_1 \equiv a_1 c \bmod 8$ and $\nu_2 \equiv 0 \bmod 2$. Suppose first that $c \equiv 1 \bmod 4$. Then $\nu_3 \equiv 0 \bmod 2$ as well. Moreover, $a_1 \equiv r_1 \bmod 4$, so that

$$\nu_1 \equiv \frac{a_1 - 1}{2} \cdot \frac{a_1 - 1}{2} \equiv \frac{a_1 - 1}{2} \bmod 2.$$

Finally, as $a = a_1\rho$,

$$\left(\frac{-1}{a}\right) = \left(\frac{-1}{a_1}\right)\left(\frac{-1}{\rho}\right)$$

and so $\nu_1 + (\rho-1)/2 \equiv (a-1)/2 \bmod 2$. Now suppose $c \equiv 3 \bmod 4$. Then ρ and $c\rho$ are odd and different modulo 2, and so $\nu_3 + (\rho-1)/2 \equiv 1 \bmod 2$. Moreover, $r_1 \equiv 3a_1 \bmod 4$, so that r_1 and a_1 are odd and different modulo 4. Hence at least one of $(r_1-1)/2$ and $(a_1-1)/2$ is $0 \bmod 2$ and so $\nu_1 = 0$. Collecting these results, we get

$$\nu_1 + \nu_2 + \nu_3 + \frac{\rho-1}{2} \equiv \begin{cases} \frac{a-1}{2} \bmod 2 & \text{if } c \equiv 1 \bmod 4 \\ 1 \bmod 2 & \text{if } c \equiv 3 \bmod 4. \end{cases}$$

Now suppose $e = 1$. Then splitting into cases similarly as above, we get

$$\nu_1 + \nu_2 + \nu_3 + \frac{\rho-1}{2} \equiv \begin{cases} \frac{a-1}{2} \bmod 2 & \text{if } b \equiv 0 \bmod 2 \text{ and } c \equiv 1 \bmod 4 \\ 0 \bmod 2 & \text{if } b \equiv 0 \bmod 2 \text{ and } c \equiv 3 \bmod 4 \\ \frac{a-1}{2} + 1 \bmod 2 & \text{if } b \equiv 1 \bmod 2 \text{ and } c \equiv 1 \bmod 4 \\ 1 \bmod 2 & \text{if } b \equiv 1 \bmod 2 \text{ and } c \equiv 3 \bmod 4. \end{cases}$$

Finally, suppose $e = 0$. Then

$$\nu_1 + \nu_2 + \nu_3 + \frac{\rho-1}{2} \equiv \begin{cases} \frac{a-1}{2} \bmod 2 & \text{if } b \equiv 0 \bmod 2 \text{ and } c \equiv 1 \bmod 4 \\ 0 \bmod 2 & \text{if } b \equiv 0 \bmod 2 \text{ and } c \equiv 3 \bmod 4 \\ \frac{d-1}{2} \bmod 2 & \text{if } b \equiv 1 \bmod 2 \text{ and } c \equiv 1 \bmod 4 \\ \frac{a-1}{2} + \frac{d-1}{2} \bmod 2 & \text{if } b \equiv 1 \bmod 2 \text{ and } c \equiv 3 \bmod 4. \end{cases}$$

This proves the lemma. □

3.5.3 Proof of Proposition 3.7

We are now ready to prove Proposition 3.7. Let

$$\mathcal{D}(X) := \left\{(u,v) \in \mathcal{D} : u^2 - 2v^2 \leq X\right\},$$

where again $\mathcal{D}$ is defined as in (3.31). We will say that $u + v\sqrt{2} \in \mathcal{D}(X)$ to mean that $(u,v) \in \mathcal{D}(X)$. Then the bilinear sum (3.26) can be written as

$$B(M,N) = \sum_{k=0}^{3} B_k(M,N),$$

where

$$B_k(M,N) = \sum_{w \in \mathcal{D}(M)} \sum_{z \in \mathcal{D}(N)} \alpha_w \beta_z [\varepsilon^{2k} wz]_{\phi,\psi}. \tag{3.45}$$

Here $\alpha_w = \alpha_{(w)}$ and $\beta_z = \beta_{(z)}$, i.e. α_w (resp. β_z) depends only on the ideal generated by w (resp. z).

It is enough to estimate (3.45) for each $0 \leq k \leq 3$. First, suppose $u+v\sqrt{2} \succ 0$ is primitive and odd. Then by Proposition 3.8, we have

$$[\varepsilon^{2k}(u+v\sqrt{2})] \sim [u+v\sqrt{2}][\varepsilon^{2k}]\gamma(\varepsilon^{2k}, u+v\sqrt{2}) \sim [u+v\sqrt{2}].$$

We write $w = a+b\sqrt{2}$ and $z = c+d\sqrt{2}$ and split (3.45) into $8^2 \cdot 16^2$ sums by fixing congruence classes of a, b, c, and d modulo 16 (where the congruence classes of a and c are invertible). Then it suffices to estimate each sum

$$\pm \sum_{\substack{w\in\mathcal{D}(M)\\ w\equiv w_0 \bmod 16}} \sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv z_0 \bmod 16}} \alpha_w\beta_z[wz].$$

Unless both w and z are primitive, wz is not primitive, and hence $[wz] = 0$. Using Proposition 3.8 again and replacing α_w by $\alpha_w[w]$ and β_z by $\beta_z[z]$, we are left to estimate sums of the type

$$Q^*(M,N) := \sum_{\substack{w\in\mathcal{D}(M)\\ w\equiv w_0 \bmod 16}}^{*} \sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv z_0 \bmod 16}}^{*} \alpha_w\beta_z\gamma(w,z), \tag{3.46}$$

where $*$ restricts the summation to primitive elements of $\mathbb{Z}[\sqrt{2}]$. The cancellation in the bilinear sum (3.46) comes from the double oscillation of the term $\gamma(w,z)$ in the formula above.

We also define the closely related sum

$$Q(M,N) := \sum_{\substack{w\in\mathcal{D}(M)\\ w\equiv w_0 \bmod 16}}^{*} \sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv z_0 \bmod 16}} \alpha_w\beta_z\gamma(w,z), \tag{3.47}$$

and note that $Q^*(M,N)$ is a special case of $Q(M,N)$ where the complex numbers β_z are supported on primitive elements z.

The Cauchy-Schwarz inequality implies that

$$|Q(M,N)|^2 \leq \sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv z_0(16)}} |\beta_z|^2 \sum_{\substack{w_1\in\mathcal{D}(M)\\ w_1\equiv w_0(16)}} \sum_{\substack{w_2\in\mathcal{D}(M)\\ w_2\equiv w_0(16)}} \alpha_{w_1}\overline{\alpha_{w_2}} \sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv z_0(16)}} \gamma(w_1,z)\gamma(w_2,z).$$

Since β_z is bounded in modulus by N^ϵ, Lemma 3.14 applied to $L = \mathrm{Id}$ gives

$$\sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv z_0(16)}} |\beta_z|^2 \ll_\epsilon N^\epsilon \mathrm{Vol}(\mathcal{D}(N)) + N^\epsilon O(\mathrm{Vol}(\partial(\mathcal{D}(N))) + 1) \ll_\epsilon N^{1+\epsilon}. \tag{3.48}$$

Recall that $\gamma(w,z_1) = \gamma(w,z_2)$ whenever $z_1 \equiv z_2 \bmod \mathrm{Norm}(w)$. Set

$$q := \mathrm{Norm}(w_1w_2).$$

Hence we can split the inner sum over z into residue classes modulo $16q$. More precisely, we write $z_0 = z_{01}+z_{02}\sqrt{2}$ and define L to be the linear transformation $L = 16q \cdot \mathrm{Id} + (z_{01}, z_{02}) : \mathbb{R}^2 \to \mathbb{R}^2$. Then Lemma 3.14 gives

$$\begin{aligned}
\sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv z_0(16)}} \gamma(w_1,z)\gamma(w_2,z) &= \sum_{\substack{\zeta \bmod 16q\\ \zeta\equiv z_0 \bmod 16}} \gamma(w_1,z)\gamma(w_2,z) \sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv\zeta \bmod 16q}} 1\\
&= \sum_{\substack{\zeta \bmod 16q\\ \zeta\equiv z_0 \bmod 16}} \gamma(w_1,z)\gamma(w_2,z)\left(\frac{a_0N}{(16q)^2} + O\left(\frac{N^{\frac{1}{2}}}{q}+1\right)\right)\\
&= \frac{a_0N}{(16q)^2} \sum_{\substack{\zeta \bmod 16q\\ \zeta\equiv z_0 \bmod 16}} \gamma(w_1,z)\gamma(w_2,z) + O\left(q^2\left(\frac{N^{\frac{1}{2}}}{q}+1\right)\right),
\end{aligned}$$

where a_0 is defined as in (3.32). The following proposition, analogous to [19, Lemma 21.1, p. 1025], helps us estimate the sum above. It gives a lot of cancellation for most w_1 and w_2.

Proposition 3.9. *Let w_0 and z_0 be odd congruence classes modulo 16 in $\mathbb{Z}[\sqrt{2}]$. Let $w_1, w_2 \in \mathbb{Z}[\sqrt{2}]$ be primitive, totally positive, and odd. Suppose $w_1 \equiv w_2 \equiv w_0 \bmod 16$. Let σ be the non-trivial automorphism of $\mathbb{Q}(\sqrt{2})$. Let $\gcd(w_1, \sigma(w_2))$ denote a totally positive generator for the greatest common divisor of the ideals (w_1) and $(\sigma(w_2))$ in $\mathbb{Z}[\sqrt{2}]$. Let $q := \mathrm{Norm}(w_1w_2)$ and $d := \mathrm{Norm}(\gcd(w_1, \sigma(w_2)))$ (so that $d^2|q$). Then we have*

$$\left|\sum_{\substack{z \bmod 16q\\ z\equiv z_0 \bmod 16}} \gamma(w_1,z)\gamma(w_2,z)\right| = \begin{cases} q\varphi(d)\varphi(q/d) & \text{if } q \text{ and } d \text{ are squares}\\ 0 & \text{otherwise.}\end{cases}$$

Proof. We write $z = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. Our first goal is to show that

$$\gamma(w_1,z)\gamma(w_2,z) = \delta\left(\frac{a^2-2b^2}{d}\right)\gamma(w_1w_2/d, z), \tag{3.49}$$

where $\delta \in \{\pm 1\}$ possibly depends on w_1, w_2 and the fixed congruence class $z_0 \bmod 16$ but *not* on z.

It is possible that z is not primitive, so that we cannot directly apply the reciprocity law from Lemma 3.17 to $\gamma(w_1, z)$ and $\gamma(w_2, z)$. However, we can factor out the greatest common factor of a and b to obtain

$$z = gz',$$

where $g = \gcd(a, b)$, $a = ga'$, $b = gb'$, and $z' = a' + b'\sqrt{2}$. Now z' is primitive.

First assume that

$$\gcd(w_1w_2, \sigma(z)) = 1. \tag{3.50}$$

Under this assumption, we claim that

$$\gcd(d, a^2 - 2b^2) = \gcd(q, g) = \gcd(d, g) = 1. \tag{3.51}$$

These equalities will be useful in subsequent manipulations of Jacobi symbols. We now prove the claim.

First, suppose that there is a prime p dividing d and $a^2 - 2b^2$. Let $\xi = \gcd(w_1, \sigma(w_2))$, so that $d = \xi\sigma(\xi)$. Suppose p divides ξ or $\sigma(\xi)$. In the former case, this would mean that p divides w_1, while in the latter case it would mean that p divides w_2. Both of these cases contradict the assumption that w_1 and w_2 are primitive. Hence p cannot divide either ξ or $\sigma(\xi)$. Since $z \equiv z_0 \bmod 16$ and z_0 is an odd congruence class modulo 16, we see that $a^2 - 2b^2$ is odd, and so also that p is odd. If p is inert in $\mathbb{Z}[\sqrt{2}]$, then since p divides d, p must divide either ξ or $\sigma(\xi)$, and this is a contradiction. Hence we may assume that p splits in $\mathbb{Z}[\sqrt{2}]$, i.e. $p = \pi\sigma(\pi)$ for some prime π in $\mathbb{Z}[\sqrt{2}]$. Again, as p divides neither ξ nor $\sigma(\xi)$, we can assume without loss of generality that π divides ξ and $\sigma(\pi)$ divides $\sigma(\xi)$. This means that π divides w_1 and $\sigma(\pi)$ divides w_2. Now, since p (and hence π) divides $a^2 - 2b^2 = z\sigma(z)$, we find that π divides z or $\sigma(z)$. In the former case, $\sigma(\pi)$ divides $\sigma(z)$, which means that $\sigma(\pi)$ divides $\gcd(w_2, \sigma(z))$, and this contradicts assumption (3.50). In the latter case, π divides $\gcd(w_1, \sigma(z))$, which again contradicts (3.50). Hence we have shown that $(d, a^2 - 2b^2) = 1$.

Now suppose that there is a prime p dividing q and g. As g is a rational integer, $\sigma(g) = g$, and so, as $z = gz'$, we see that p divides $\sigma(z)$. Since w_1 and w_2 are odd, p must be odd. If p divides w_1 or w_2, then p divides $\gcd(w_1w_2, \sigma(z))$, which contradicts assumption (3.50). Hence p cannot divide either w_1 or w_2. If p is inert in $\mathbb{Z}[\sqrt{2}]$, then, as $q = w_1w_2\sigma(w_1)\sigma(w_2)$, p divides at least one of w_1, w_2, $\sigma(w_1)$, and $\sigma(w_2)$. In fact, as $p = \sigma(p)$, we see that p must divide either w_1 or w_2, which is a contradiction. Hence we may assume that p splits in $\mathbb{Z}[\sqrt{2}]$, i.e. $p = \pi\sigma(\pi)$ for some prime π in $\mathbb{Z}[\sqrt{2}]$. Again, as p divides neither w_1 nor w_2, we can assume without loss of generality that π divides w_1. But then π divides $\gcd(w_1, \sigma(z))$, which contradicts assumption (3.50). Hence we have shown that $\gcd(q, g) = 1$.

Finally, as d divides q, we immediately deduce that $\gcd(d, g) = 1$. This finishes the proof of (3.51).

By definition of $\gamma(\cdot, \cdot)$, as g is a rational integer, we have

$$\gamma(w_i, z) = \left(\frac{g}{\mathrm{Norm}(w_i)}\right)\gamma(w_i, z')$$

for $i = 1, 2$. Hence

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right)\gamma(w_1, z')\gamma(w_2, z').$$

Now we can apply the reciprocity law from Lemma 3.17 twice to obtain

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right) (\gamma(z', w_1)\mathrm{m}(w_1 z')) (\gamma(z', w_2)\mathrm{m}(w_2 z')) .$$

Recall that $\mathrm{m}(\alpha)$ depends only on the residue class of α modulo 8. Using the fact that $w_1 \equiv w_2 \bmod 16$, we deduce that $w_1 z' \equiv w_2 z' \bmod 16$, and so $\mathrm{m}(w_1 z') = \mathrm{m}(w_2 z')$. The assumption $\gcd(w_1 w_2, \sigma(z)) = 1$ ensures that $w_i z'$ is primitive (see Lemma 3.15), and so that $\mathrm{m}(w_i z') \in \{\pm 1\}$ for $i = 1, 2$. Hence $\mathrm{m}(w_1 z')\mathrm{m}(w_2 z') = \mathrm{m}(w_1 z')^2 = 1$ and the expression above simplifies to

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right) \gamma(z', w_1)\gamma(z', w_2).$$

Lemma 3.15 ensures that $w_1 w_2 / d$ is primitive. Hence we can now use the multiplicativity formula from Lemma 3.16 twice to obtain

$$\begin{aligned} \gamma(w_1, z)\gamma(w_2, z) &= \left(\frac{g}{q}\right) \gamma(z', w_1 w_2)\mathrm{m}(z') \\ &= \left(\frac{g}{q}\right) (\gamma(z', d)\gamma(z', w_1 w_2/d)\mathrm{m}(z'))\, \mathrm{m}(z'). \end{aligned}$$

Again, z' is primitive, so $\mathrm{m}(z') \in \{\pm 1\}$. The above simplifies to

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right) \gamma(z', d)\gamma(z', w_1 w_2/d).$$

We again use the reciprocity law from Lemma 3.17 on $\gamma(z', w_1 w_2/d)$ to obtain

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right) \gamma(z', d)\gamma(w_1 w_2/d, z')\mathrm{m}(z' w_1 w_2/d).$$

As before, since g is a rational integer,

$$\gamma(w_1 w_2/d, z) = \left(\frac{g}{q/d^2}\right) \gamma(w_1 w_2/d, z').$$

By equation (3.51), the Jacobi symbols $\left(\frac{g}{q}\right)$ and $\left(\frac{g}{q/d^2}\right)$ are non-zero. Hence

$$\left(\frac{g}{q}\right)\left(\frac{g}{q/d^2}\right) = \left(\frac{g}{q^2/d^2}\right) = 1,$$

and the above simplifies to

$$\gamma(w_1, z)\gamma(w_2, z) = \gamma(z', d)\gamma(w_1 w_2/d, z)\mathrm{m}(z' w_1 w_2/d). \tag{3.52}$$

By definition of $\gamma(\cdot, \cdot)$,

$$\gamma(z', d) = \left(\frac{a' d}{a'^2 - 2b'^2}\right) = \mathrm{m}(z') \left(\frac{d}{a'^2 - 2b'^2}\right). \tag{3.53}$$

By equation (3.51), we use the law of quadratic reciprocity to write

$$\left(\frac{d}{a'^2-2b'^2}\right)=\epsilon(d,a'^2-2b'^2)\left(\frac{a'^2-2b'^2}{d}\right)=\epsilon(d,a'^2-2b'^2)\left(\frac{a^2-2b^2}{d}\right), \tag{3.54}$$

where for odd integers r and s,

$$\epsilon(r,s)=(-1)^{\frac{r-1}{2}\frac{s-1}{2}}=\left(\frac{-1}{s}\right)^{\frac{r-1}{2}}.$$

Note that $\epsilon(r,s)$ depends only on the congruence classes of r and s modulo 4. Since g is odd, $g^2\equiv 1 \bmod 4$, and so $\epsilon(d,a'^2-2b'^2)=\epsilon(d,a^2-2b^2)$. In particular, as $z\equiv z_0 \bmod 16$, $\epsilon(d,a'^2-2b'^2)$ depends only on the congruence classes of d and z_0 modulo 4, and not on z.

Putting together (3.52), (3.53), and (3.54), we see that to accomplish our goal (3.49), it remains to show that the value of the factor

$$\mathrm{m}(z')\mathrm{m}(z'w_1w_2/d)$$

is independent of z. By definition of $\mathrm{m}(\cdot)$, the law of quadratic reciprocity, and the fact that $g^2\equiv 1 \bmod 4$, we have

$$\mathrm{m}(z')=\epsilon(a',a^2-2b^2)\left(\frac{-2}{a'}\right). \tag{3.55}$$

As $a=ga'$, we have

$$\left(\frac{-1}{a'}\right)=\left(\frac{-1}{a}\right)\left(\frac{-1}{g}\right),$$

that is, $(a'-1)/2\equiv(a-1)/2+(g-1)/2 \bmod 2$. Hence

$$\epsilon(a',a^2-2b^2)=\epsilon(a,a^2-2b^2)\left(\frac{-1}{a^2-2b^2}\right)^{\frac{g-1}{2}}. \tag{3.56}$$

Again, as $a=ga'$, we also have

$$\left(\frac{-2}{a'}\right)=\left(\frac{-2}{a}\right)\left(\frac{-2}{g}\right). \tag{3.57}$$

Combining (3.55), (3.56), and (3.57), and using the definition of $\mathrm{m}(\cdot)$, we get

$$\mathrm{m}(z')=\mathrm{m}(z)\left(\frac{-1}{a^2-2b^2}\right)^{\frac{g-1}{2}}\left(\frac{-2}{g}\right), \tag{3.58}$$

where we note that $\mathrm{m}(z)$ depends only on the fixed congruence class z_0 modulo 16 and *not* on z.

We now define integers e and f by the equation

$$w_1 w_2/d = e + f\sqrt{2},$$

and define integers x, y, x', and y' by the equations

$$z w_1 w_2/d = x + y\sqrt{2} = g(x' + y'\sqrt{2}).$$

Proceeding in the same way as for (3.55), we get

$$\mathrm{m}(z' w_1 w_2/d) = \epsilon(x', x^2 - 2y^2)\left(\frac{-2}{x'}\right). \tag{3.59}$$

As $x = gx'$, we have

$$\left(\frac{-1}{x'}\right) = \left(\frac{-1}{x}\right)\left(\frac{-1}{g}\right),$$

that is, $(x'-1)/2 \equiv (x-1)/2 + (g-1)/2 \bmod 2$. Hence

$$\epsilon(x', x^2 - 2y^2) = \epsilon(x, x^2 - 2y^2)\left(\frac{-1}{x^2 - 2y^2}\right)^{\frac{g-1}{2}}. \tag{3.60}$$

Again, as $x = gx'$, we also have

$$\left(\frac{-2}{x'}\right) = \left(\frac{-2}{x}\right)\left(\frac{-2}{g}\right). \tag{3.61}$$

Combining (3.59), (3.60), and (3.61) as before, and using the definition of $\mathrm{m}(\cdot)$, we get

$$\mathrm{m}(z' w_1 w_2/d) = \mathrm{m}(z w_1 w_2/d)\left(\frac{-1}{x^2 - 2y^2}\right)^{\frac{g-1}{2}}\left(\frac{-2}{g}\right), \tag{3.62}$$

where again the factor $\mathrm{m}(z w_1 w_2/d)$ depends on w_1, w_2 and the fixed congruence class z_0 modulo 16 but *not* on z. Combining (3.58) and (3.62), and using the fact that $x^2 - 2y^2 = (a^2 - 2b^2)(e^2 - 2f^2)$, we find that

$$\mathrm{m}(z')\mathrm{m}(z' w_1 w_2/d) = \delta(w_1, w_2, z_0)\left(\frac{-1}{(a^2 - 2b^2)^2(e^2 - 2f^2)}\right)^{\frac{g-1}{2}},$$

where $\delta(w_1, w_2, z_0) \in \{\pm 1\}$ depends only on w_1, w_2 and the residue class of z_0 modulo 16. Finally, note that

$$e^2 - 2f^2 = \mathrm{Norm}(w_1 w_2/d) = \frac{\mathrm{Norm}(w_1 w_2)}{d^2}$$

and that $\mathrm{Norm}(w_1) \equiv \mathrm{Norm}(w_2) \bmod 4$ (since again $w_1 \equiv w_2 \equiv w_0 \bmod 16$). Hence $e^2 - 2f^2 \equiv \mathrm{Norm}(w_1)^2 \equiv 1 \bmod 4$, and so

$$\mathrm{m}(z')\mathrm{m}(z' w_1 w_2/d) = \delta(w_1, w_2, z_0).$$

Thus, in the case that $\gcd(w_1w_2, \sigma(z)) = 1$ (see (3.50)), we have proved (3.49).

Suppose now that (3.50) is not satisfied, i.e., $(w_1w_2, \sigma(z)) \neq 1$. Then, by Lemma 3.17, either $\gamma(w_1, z) = 0$ or $\gamma(w_1, z) = 0$. Moreover, either $(w_1w_2/d, \sigma(z)) = 1$ or $(w_1w_2/d, \sigma(z)) \neq 1$. In the former case, $(w_1w_2/d, \sigma(z))$ divides both d and $z\sigma(z) = a^2 - 2b^2$, so that $(a^2 - 2b^2, d) \neq 1$. In the latter case, $(w_1w_2/d, \sigma(z)) \neq 1$, so $\gamma(w_1w_2/d, z) = 0$ again by Lemma 3.17. As $0 = 0$, we have once again proved

$$\gamma(w_1, z)\gamma(w_2, z) = \delta\left(\frac{a^2 - 2b^2}{d}\right)\gamma(w_1w_2/d, z),$$

so that the goal (3.49) has been established in all cases.

Writing $z_0 = a_0 + b_0\sqrt{2}$, we then get

$$\sum_{\substack{z \bmod 16q \\ z \equiv z_0 \bmod 16}} \gamma(w_1, z)\gamma(w_2, z) = \epsilon_1\epsilon_2 \sum_{\substack{a \bmod 16q \\ a \equiv a_0 \bmod 16}} \sum_{\substack{b \bmod 16q \\ a \equiv b_0 \bmod 16}} \left(\frac{a^2 - 2b^2}{d}\right)\left(\frac{ae + 2bf}{q/d^2}\right).$$

Note that there exists an integer t such that $t^2 \equiv 2 \bmod q$ because q is a norm of an element in $\mathbb{Z}[\sqrt{2}]$. Let t be such that $t \equiv 2f/e \bmod q/d^2$; this is possible since, by definition, $q/d^2 = e^2 - 2f^2$ and w_1w_2/d is primitive. Then, as d divides q, we may rewrite the above sum as

$$\sum_{\substack{z \bmod 16q \\ z \equiv z_0 \bmod 16}} \gamma(w_1, z)\gamma(w_2, z) = \epsilon_1\epsilon_2 \left(\frac{e}{q^2/d}\right) \sum_{\substack{a \bmod 16q \\ a \equiv a_0 \bmod 16}} \sum_{\substack{b \bmod 16q \\ a \equiv b_0 \bmod 16}} \left(\frac{a - bt}{d}\right)\left(\frac{a + bt}{q/d}\right).$$

Write $a = a_0 + 16a_1$ and $b = b_0 + 16b_1$ and set $x_0 = a_0 + b_0t$, $y_0 = a_0 - b_0t$, $x = a_1 + b_1t$, $y = a_1 - b_1t$. Then $a + bt = x_0 + 16x$ and $a - bt = y_0 + 16y$. Note that the map $(a_1, b_1) \mapsto (x, y)$ is bijective on $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, and hence

$$\sum_{\substack{z \bmod 16q \\ z \equiv z_0 \bmod 16}} \gamma(w_1, z)\gamma(w_2, z) = \pm \sum_{y \bmod q} \left(\frac{y}{d}\right) \sum_{x \bmod q} \left(\frac{x}{q/d}\right) = q \sum_{y \bmod d} \left(\frac{y}{d}\right) \sum_{x \bmod q/d} \left(\frac{x}{q/d}\right),$$

and this implies the desired result. □

Since $\varphi(d)\varphi(q/d) \leq q$ and $q \leq M^2$, we deduce that whenever q and d are both squares,

$$\sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv z_0(16)}} \gamma(w_1, z)\gamma(w_2, z) \ll q^2\left(\frac{N}{q^2} + O\left(\frac{N^{\frac{1}{2}}}{q}\right)\right) + O\left(qN^{\frac{1}{2}} + q^2\right) \ll N + M^2N^{\frac{1}{2}} + M^4.$$

By unique factorization in $\mathbb{Z}[\sqrt{2}]$, the number of elements $w \in \mathcal{D}$ such that $\mathrm{Norm}(w) = n$ is at most $\tau(n)$, the number of divisors of n. Hence, setting

$m_1 = \mathrm{Norm}(w_1)$ and $m_2 = \mathrm{Norm}(w_2)$, and using (3.27) and (3.48), we get the upper bound

$$|Q(M,N)|^2 \ll N \left(\sum_{\substack{m_1, m_2 \le M \\ m_1 m_2 \text{ square}}} \sum \tau(m_1 m_2) \left(N + M^2 N^{\frac{1}{2}} + M^4 \right) + M^4 N^{\frac{1}{2}} + M^6 \right) (MN)^{\epsilon}.$$

Using the estimate $\tau(n) \ll_{\epsilon} n^{\epsilon}$, we obtain

Lemma 3.18. *Let $Q(M,N)$ be defined as in* (3.47)*. Then*

$$Q(M,N) \ll_{\epsilon} \left(M^{\frac{1}{2}} N + M^2 N^{\frac{3}{4}} + M^3 N^{\frac{1}{2}} \right) (MN)^{\epsilon}.$$

We now apply Hölder's inequality with k even to (3.47) to get

$$|Q(M,N)|^k \le \left(\sum_w |\alpha_w|^{\frac{k}{k-1}} \right)^{k-1} \sum_w \left| \sum_z \beta_z \gamma(w,z) \right|^k. \tag{3.63}$$

Since $\gamma(w,z)$ is multiplicative in the second argument up to a unit factor depending only on w (see (3.16)), we can write

$$Q'(M, N^k) := \sum_w \left| \sum_z \beta_z \gamma(w,z) \right|^k =: \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv w_0 \bmod 16}} \sum_{\substack{z \in \mathcal{D}(N^k) \\ z \equiv z_0' \bmod 16}} \alpha_w' \beta_z' \gamma(w,z),$$

for some α_w' with $|\alpha_w'| \ll M^{\epsilon}$ and

$$\beta_z' = \sum_{\substack{z_1 \cdots z_k = \varepsilon^{2j} z \\ z \in \mathcal{D}(N^k)}} \beta_{z_1} \overline{\beta_{z_2}} \cdots \beta_{z_{k-1}} \overline{\beta_{z_k}}.$$

By Lemma 3.18, we have

$$Q'(M, N^k) \ll_{\epsilon} \left(M^{\frac{1}{2}} N^k + M^2 N^{\frac{3k}{4}} + M^3 N^{\frac{k}{2}} \right) (MN)^{\epsilon}.$$

Using this estimate with $k = 6$ along with the upper bound (proved similarly as (3.48))

$$\sum_{\substack{w \in \mathcal{D}(N) \\ w \equiv w_0 (16)}} |\alpha_w|^2 \ll M^{1+\epsilon}, \tag{3.64}$$

inside the inequality (3.63), we get

$$Q(M,N) \ll_{\epsilon} \left(M^{\frac{11}{12}} N + M^{\frac{7}{6}} N^{\frac{3}{4}} + M^{\frac{4}{3}} N^{\frac{1}{2}} \right) (MN)^{\epsilon}$$

We now use the reciprocity law (3.44) to interchange the roles of w and z in (3.46). As the value of $\mathrm{m}(wz)$ depends only on the residue classes of w and z modulo 16, we can apply the above estimate to get that $Q(M, N)$

$$\ll_\epsilon \min\left\{M^{\frac{11}{12}}N + M^{\frac{7}{6}}N^{\frac{3}{4}} + M^{\frac{4}{3}}N^{\frac{1}{2}}, N^{\frac{11}{12}}M + N^{\frac{7}{6}}M^{\frac{3}{4}} + N^{\frac{4}{3}}M^{\frac{1}{2}}\right\}(MN)^\epsilon .$$

For $M < N$, we have $M^{11/12}N > M^{7/6}N^{3/4}$ and $M^{11/12}N > M^{4/3}N^{1/2}$, so that

$$Q(M,N) \ll_\epsilon \left(M^{\frac{11}{12}}N + N^{\frac{11}{12}}M\right)(MN)^\epsilon \ll_\epsilon (M+N)^{\frac{1}{12}}(MN)^{\frac{11}{12}+\epsilon} .$$

This completes the proof of Theorem 3.2 and hence also Theorem 3.1.

3.6 Counting primes

In this section we give evidence that a governing field for the 16-rank of the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 3(4)}$ does *not* exist. To explain why, we first define a prime counting function. Suppose $M/\mathbb{Q}$ is a normal extension. Let S be a subset of $\mathrm{Gal}(M/\mathbb{Q})$ which is a union of conjugacy classes. We define

$$\pi(M,S,X) := \#\{p \leq X : \text{the Artin class of } p \text{ in } \mathrm{Gal}(M/\mathbb{Q}) \text{ is a subset of } S\}$$

Given any normal extension $M/\mathbb{Q}$ of degree d and a subset S of $\mathrm{Gal}(M/\mathbb{Q})$ stable under conjugation, the Čebotarev Density Theorem using the best known zero-free regions of L-functions gives [39, Théorème 2, p. 132], for some constant $c > 0$,

$$\pi(M,S,X) = \frac{\#S}{\#\mathrm{Gal}(M/\mathbb{Q})}\mathrm{Li}(X) + O(\#SX\exp(-cd^{-1/2}\log^{1/2}X)).$$

Hence given any two subsets S_1 and S_2 of $\mathrm{Gal}(M/\mathbb{Q})$ which are stable under conjugation and of the same size,

$$\pi(M,S_1,X) - \pi(M,S_2,X) \ll \#SX\exp(-cd^{-1/2}\log^{1/2}X)$$

is the best known bound. Note that this bound is weaker than $X^{1-\delta}$ for any $\delta > 0$. For instance, it is *not* known if

$$\#\{p \leq X \text{ prime} : \ p \equiv 1 \bmod 4\} - \#\{p \leq X \text{ prime} : \ p \equiv -1 \bmod 4\} \ll X^{0.9999}.$$ [redacted]

However, we have the following result.

Theorem 3.3. *Suppose that there exists a governing field M for the* 16*-rank of the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 3(4)}$. Then there exist disjoint subsets S_1 and S_2 of* $\mathrm{Gal}(M/\mathbb{Q})$ *which are stable under conjugation and of equal size such that*

$$\pi(M,S_1,X) - \pi(M,S_2,X) \ll_\varepsilon X^{\frac{149}{150}+\epsilon}$$

Proof. We simply let S_1 be the union of Artin classes c_p for primes p satisfying $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1$ and S_2 be the union of Artin classes c_p for primes p satisfying $\mathrm{rk}_8\mathrm{Cl}(-8p) = 1$ but $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 0$. The result now immediately follows from Theorem 3.1. □

However, with our current methods of complex analysis applied to L-functions, we are not able to produce an error term of the form $O(x^{1-\delta_M})$ for any $\delta_M > 0$. This leads us to believe that a governing field M for the 16-rank of the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 3(4)}$ is unlikely to exist.

Bibliography

[1] Pierre Barrucand and Harvey Cohn. Note on primes of type $x^2 + 32y^2$, class number, and residuacity. *J. Reine Angew. Math.*, 238:67–70, 1969.

[2] Manjul Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1):217–250, 2004.

[3] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.

[4] 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.

[5] 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.

[6] 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.

[7] Harvey Cohn and George Cooke. Parametric form of an eight class field. *Acta Arith.*, 30(4):367–377, 1976.

[8] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[9] H. Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, 26:179–183, 1951.

[10] H. Davenport. Corrigendum: "On a principle of Lipschitz". *J. London Math. Soc.*, 39:580, 1964.

[11] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[12] Etienne Fouvry and Henryk Iwaniec. Gaussian primes. *Acta Arith.*, 79(3):249–287, 1997.

[13] Étienne Fouvry and Jürgen Klüners. Cohen-Lenstra heuristics of quadratic number fields. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 40–55. Springer, Berlin, 2006.

[14] Étienne Fouvry and Jürgen Klüners. On the 4-rank of class groups of quadratic number fields. *Invent. Math.*, 167(3):455–513, 2007.

[15] Étienne Fouvry and Jürgen Klüners. On the negative Pell equation. *Ann. of Math. (2)*, 172(3):2035–2104, 2010.

[16] Étienne Fouvry and Jürgen Klüners. The parity of the period of the continued fraction of $\sqrt{d}$. *Proc. Lond. Math. Soc. (3)*, 101(2):337–391, 2010.

[17] J. B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin. The spin of prime ideals. *Invent. Math.*, 193(3):697–749, 2013.

[18] John Friedlander and Henryk Iwaniec. Asymptotic sieve for primes. *Ann. of Math. (2)*, 148(3):1041–1065, 1998.

[19] John Friedlander and Henryk Iwaniec. The polynomial $X^2 + Y^4$ captures its primes. *Ann. of Math. (2)*, 148(3):945–1040, 1998.

[20] John Friedlander and Henryk Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[21] Carl Friedrich 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.

[22] Frank Gerth, III. Extension of conjectures of Cohen and Lenstra. *Exposition. Math.*, 5(2):181–184, 1987.

[23] Franz Halter-Koch, Pierre Kaplan, and Kenneth S. Williams. An Artin character and representations of primes by binary quadratic forms. II. *Manuscripta Math.*, 37(3):357–381, 1982.

[24] Helmut Hasse. Über die Klassenzahl des Körpers $P(\sqrt{} - 2p)$ mit einer Primzahl $p \neq 2$. *J. Number Theory*, 1:231–234, 1969.

[25] Gerald J. Janusz. *Algebraic number fields*. Academic Press [A Subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973. Pure and Applied Mathematics, Vol. 55.

[26] Pierre Kaplan. Cycles d'ordre au moins 16 dans le 2-groupe des classes d'idéaux de certains corps quadratiques. *Bull. Soc. Math. France Mém.*, (49-50):113–124, 1977. Utilisation des calculateurs en mathématiques pures (Conf., Limoges, 1975).

[27] J. C. Lagarias. Signatures of units and congruences (mod 4) in certain real quadratic fields. II. *J. Reine Angew. Math.*, 320:115–126, 1980.

[28] Jeffrey Clark Lagarias. *The 4-part of the class groups of a quadratic field*. ProQuest LLC, Ann Arbor, MI, 1974. Thesis (Ph.D.)–Massachusetts Institute of Technology.

[29] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[30] Philip A. Leonard and Kenneth S. Williams. On the divisibility of the class numbers of $Q(\sqrt{-p})$ and $Q(\sqrt{-2p})$ by 16. *Canad. Math. Bull.*, 25(2):200–206, 1982.

[31] D. Milovic. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \bmod 4$. *ArXiv e-prints*, November 2015.

[32] D. Milovic. The infinitude of $\mathbb{Q}(\sqrt{-p})$ with class number divisible by 16. *ArXiv e-prints*, February 2015.

[33] Bernard Oriat. Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques $Q(\sqrt{2p})$ et $Q(\sqrt{-2})$. *J. Math. Soc. Japan*, 30(2):279–285, 1978.

[34] 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.

[35] Ladislaus Rédei. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I. *J. Reine Angew. Math.*, 180:1–43, 1939.

[36] Hans Reichardt. Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 170:75–82, 1934.

[37] Lowell Schoenfeld. Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$. II. *Math. Comp.*, 30(134):337–360, 1976.

[38] Arnold Scholz. Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$. *Math. Z.*, 39(1):95–111, 1935.

[39] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[40] Peter 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.

[41] Peter Stevenhagen. Divisibility by 2-powers of certain quadratic class numbers. *J. Number Theory*, 43(1):1–19, 1993.

[42] Peter Stevenhagen. The number of real quadratic fields having units of negative norm. *Experiment. Math.*, 2(2):121–136, 1993.

[43] Takashi Taniguchi and Frank Thorne. Secondary terms in counting functions for cubic fields. *Duke Math. J.*, 162(13):2451–2508, 2013.

[44] I. M. Vinogradov. *The method of trigonometrical sums in the theory of numbers.* Dover Publications, Inc., Mineola, NY, 2004. Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation.

[45] Kenneth S. Williams. On the class number of $\mathbf{Q}(\sqrt{-p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime. *Acta Arith.*, 39(4):381–398, 1981.

Abstract

We prove two new density results about 16-ranks of class groups of quadratic number fields. They can be stated informally as follows.

Theorem A. *The class group of* $\mathbb{Q}(\sqrt{-p})$ *has an element of order* 16 *for one-fourth of prime numbers* p *of the form* $a^2 + 16c^4$.

Theorem B. *The class group of* $\mathbb{Q}(\sqrt{-2p})$ *has an element of order* 16 *for one-eighth of prime numbers* $p \equiv -1 \bmod 4$.

These density results are interesting for several reasons. First, they are the first non-trivial density results about the 16-rank of class groups in a family of quadratic number fields. Second, they prove an instance of the Cohen-Lenstra conjectures. Third, both of their proofs involve new applications of powerful sieving techniques developed by Friedlander and Iwaniec. Fourth, we give an explicit description of the 8-Hilbert class field of $\mathbb{Q}(\sqrt{-p})$ whenever p is a prime number of the form $a^2 + 16c^4$; the lack of such an explicit description for the 8-Hilbert class field of $\mathbb{Q}(\sqrt{d})$ is the main obstacle to improving the estimates for the density of positive discriminants d for which the negative Pell equation $x^2 - dy^2 = -1$ is solvable.

In case of Theorem B, we give an explicit description of an element of order 4 in the class group of $\mathbb{Q}(\sqrt{-2p})$ and we compute its Artin symbol in the 4-Hilbert class field of $\mathbb{Q}(\sqrt{-2p})$, thereby generalizing a result of Leonard and Williams. Finally, we prove a power-saving error term for a prime-counting function related to the 16-rank of the class group of $\mathbb{Q}(\sqrt{-2p})$, thereby giving strong evidence against a conjecture of Cohn and Lagarias that the 16-rank is governed by a Čebotarev-type criterion.

Samenvatting

We bewijzen twee nieuwe dichtheidsstellingen over de 16-rang van klassengroepen van kwadratische getallenlichamen. Informeel geformuleerd zijn het de volgende.

Stelling A. *De klassengroep van* $\mathbb{Q}(\sqrt{-p})$ *een element heeft van orde* 16 *voor een vierde van de priemgetallen* p *van de vorm* $a^2 + 16c^4$.

Stelling B. *De klassengroep van* $\mathbb{Q}(\sqrt{-2p})$ *een element heeft van orde* 16 *voor een achtste van de priemgetallen van de vorm* $p \equiv -1 \bmod 4$.

Deze dichtheidsstellingen zijn om een aantal redenen belangrijk. Ten eerste zijn het de eerste niet-triviale dichtheidsstellingen over de 16-rang van klassengroepen in een familie van kwadratische getallenlichamen. Ten tweede bewijzen deze dichtheidstellingen een speciaal geval van het Cohen-Lenstra vermoeden. Ten derde bevatten beide bewijzen nieuwe toepassingen van geavanceerde zeeftechnieken van Friedlander en Iwaniec. Ten vierde geven we een expliciete beschrijving van het 8-Hilbert klassenlichaam van $\mathbb{Q}(\sqrt{-p})$ als p een priemgetal is van de vorm $a^2 + 16c^4$; het gebrek aan een dergelijke beschrijving voor het 8-Hilbert klassenlichaam van $\mathbb{Q}(\sqrt{d})$ is het grootste obstakel tot het verbeteren van de afschattingen voor de dichtheid van positieve discriminanten d waarvoor de negatieve Pell-vergelijking $x^2 - dy^2 = -1$ oplosbaar is.

In het bewijs van Stelling B geven we een expliciete beschrijving van een element van orde 4 in de klassengroep van $\mathbb{Q}(\sqrt{-2p})$ en berekenen we het Artin-symbool van dat element in het 4-Hilbert klassenlichaam van $\mathbb{Q}(\sqrt{-2p})$. Dit is een generalisatie van een resultaat van Leonard en Williams. Tenslotte bewijzen we een dusdanig goede foutterm voor een priemgetal-telfunctie gerelateerd aan de 16-rang van de klassengroep van $\mathbb{Q}(\sqrt{-p})$, dat het een sterke indicatie geeft tegen een vermoeden van Cohn en Lagarias over het bestaan van Čebotarev-achtige criteria voor de 16-rang.

Résumé

Nous démontrons deux nouveaux résultats de densité à propos du 16-rang des groupes des classes de corps de nombres quadratiques.

Théorème A. *Le groupe des classes de* $\mathbb{Q}(\sqrt{-p})$ *a un élément d'ordre* 16 *pour un quart des nombres premiers* p *de la forme* $a^2 + 16c^4$.

Théorème B. *Le groupe des classes de* $\mathbb{Q}(\sqrt{-2p})$ *a un élément d'ordre* 16 *pour un huitième des nombres premiers* $p \equiv -1 \bmod 4$.

Ces résultats de densité sont intéressants pour plusieurs raisons. D'abord, ils sont les premiers résultats non triviaux de densité sur le 16-rang des groupes des classes dans une famille de corps de nombres quadratiques. Deuxièmement, ils prouvent une instance des conjectures de Cohen et Lenstra. Troisièmement, leurs preuves impliquent de nouvelles applications des cribles développés par Friedlander et Iwaniec. Quatrièmement, nous donnons une description explicite du sous-corps du corps de classes de Hilbert de degré 8 de $\mathbb{Q}(\sqrt{-p})$ lorsque p est un nombre premier de la forme $a^2 + 16c^4$; l'absence d'une telle description explicite pour le sous-corps du corps de classes de Hilbert de degré 8 de $\mathbb{Q}(\sqrt{d})$ est le frein principal à l'amélioration des estimations de la densité des discriminants positifs d pour lesquels l'équation de Pell négative $x^2 - dy^2 = -1$ est résoluble.

Dans le cas de Théorème B, nous donnons une description explicite d'un élément d'ordre 4 dans le groupe des classes de $\mathbb{Q}(\sqrt{-2p})$ et on calcule son symbole de Artin dans le sous-corps du corps de classes de Hilbert de degré 4 de $\mathbb{Q}(\sqrt{-2p})$, généralisant ainsi un résultat de Leonard et Williams. Enfin, nous démontrons un très bon terme d'erreur pour une fonction de comptage des nombres premiers qui est liée au 16-rang du groupe des classes de $\mathbb{Q}(\sqrt{-2p})$, donnant ainsi des indications fortes contre une conjecture de Cohn et Lagarias que le 16-rang est contrôlé par un critère de type Chebotarev.

Acknowledgements

I am very grateful to my advisors Étienne Fouvry and Peter Stevenhagen for their guidance during the past three years, both mathematical and otherwise.

Prof. Stevenhagen shared his immense expertise in class field theory and gave me the algebraic tools necessary to attack problems related to class groups of quadratic number fields. In our very first mathematical discussion, he introduced me to the problems about the 16-rank that captivated my curiosity and whose solutions form the backbone of my thesis. His help was unceasing, even in the face of great tribulations.

Prof. Fouvry used his great knowledge of analytic techniques to help me overcome many obstacles in the course of my research. He always made sure that I made timely progress and also that I had a platform to share my results with the wider mathematical community. Above all, his greatest contribution to my thesis are his many words of encouragement – he showed great trust in me and made me believe that anything is possible.

I would also like to thank Régis de la Bretèche, Kevin Destagnol, Christian Elsholtz, Jan-Hendrik Evertse, Florent Jouve, Hendrik Lenstra, Peter Koymans, Ramon Moreira Nunes, Carlo Pagano, Marco Steng, and other professors and colleagues for creating a rich mathematical environment conducive to creativity.

Ila Varma deserves special thanks for telling me about the ALGANT program.

Thank you Corneel, Dawid, Chiara, Giacomo, Sydney, Giulio, Rosa, Abtien, Corina, Simon, Mima, Nikola, Iuliana, Liu, Chloe, Yan, Sudi, Drew, Pauline, Dino, Pınar, Martin, Kaitlin, Dušan, Izabela, Thanos, Rossella, Andrea, Bianca and other friends for sharing many wonderful experiences and helping me grow as a person during the past five years.

Mama, Tata, Anđo, i Mlađo, hvala vam na vašoj podršci. Volim vas!

CV

Djordjo Zeljko Milovic was born in Belgrade, Serbia, on March 27, 1989. He spent an idyllic early childhood in Rušanj, a village in the suburbs of Belgrade. He finished the first four grades of elementary school at Zmaj Jova Jovanovič in Belgrade. His family then moved to Irvine, California, where he attended Culverdale Elementary, South Lake Middle, and University High schools. After graduating from high school in 2007, Djordjo studied mathematics at Princeton University. He graduated in 2011 cum laude, and wrote a thesis titled "Random Polynomials" under the supervision of Peter Sarnak.

Following undergraduate studies, Djordjo attended the European ALGANT Master program. He spent the first year in Milan and the second year in Orsay, France, where he met one of his eventual PhD supervisors, Étienne Fouvry. Under Fouvry's supervision, Djordjo wrote a thesis titled "On the 4-rank of class groups of quadratic number fields."

Djordjo continued his work on class groups as a PhD student in the ALGANT Doctorate program, under the joint supervision of Étienne Fouvry, Université Paris-Sud 11, and Peter Stevenhagen, Universiteit Leiden. In the second year of his PhD program, Djordjo won the KWG Prize for PhD students. He plans to spend the next year at the Institute for Advanced Study in Princeton working under the mentorship of Peter Sarnak.