ON THE 16-RANK OF CLASS GROUPS OF $\mathbb{Q}(\sqrt{-8p})$ FOR $p \equiv -1 \bmod 4$

DJORDJO MILOVIC

Abstract. We use a variant of Vinogradov's method to show that the density of the set of prime numbers $p \equiv -1 \bmod\ 4$ for which the class group of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-8p})$ has an element of order 16 is equal to 1/16, as predicted by the Cohen-Lenstra heuristics.

1. Introduction and motivation

Let $\mathrm{Cl}(D)$ denote the (narrow) class group of the quadratic number field $\mathbb{Q}(\sqrt{D})$ of discriminant D, and let $h(D) := \#\mathrm{Cl}(D)$ denote its class number. Although the class group $\mathrm{Cl}(D)$ encodes important arithmetic information about the ring of integers in $\mathbb{Q}(\sqrt{D})$, very little is known about its average behavior as D varies in some natural family of discriminants. The 2-part of $\mathrm{Cl}(D)$ is perhaps the most accessible. In [12], Gauss proved that the 2-rank (in other words, the "width" of the 2-part) is given by the formula

$$\mathrm{rk}_2\mathrm{Cl}(D) := \dim_{\mathbb{F}_2}(\mathrm{Cl}(D)/2\mathrm{Cl}(D)) = \omega(D) - 1,$$

where $\omega(D)$ is the number of distinct prime divisors of D. In particular, if $\omega(D) = 1$, then the 2-part of $\mathrm{Cl}(D)$ is trivial, so class groups with the simplest non-trivial 2-parts arise from discriminants that have exactly two distinct prime divisors. We focus on one family of such discriminants, namely the family $\{-8p\}_p$, where p ranges over prime numbers congruent to -1 modulo 4. The 2-part of $\mathrm{Cl}(-8p)$ is cyclic and hence completely determined by the highest power of 2 dividing $h(-8p)$. Therefore a natural problem is to determine, for each integer $k \geq 1$, the natural density of the set of prime numbers $p \equiv -1 \bmod 4$ such that 2^k divides $h(-8p)$. In that vein, for each integer $k \geq 1$ and real number $X > 2$, we set

$$\rho(X; 2^k) := \frac{\#\{p \leq X : \ p \equiv -1 \bmod 4,\ 2^k | h(-8p)\}}{\#\{p \leq X\}},$$

and we define $\rho(2^k) := \lim_{X\to\infty} \rho(X; 2^k)$, if the limit exists. Rédei's [19] and Reichardt's [20] work from the 1930's implies that 4 divides $h(-8p)$ if and only if $p \equiv -1 \bmod 8$ and that 8 divides $h(-8p)$ if and only if $p \equiv -1 \bmod 16$. It now follows from the Čebotarev Density Theorem that $\rho(2^k) = 2^{-k}$ for $1 \leq k \leq 3$. We prove that $\rho(16) = \frac{1}{16}$. More precisely, we prove the following equidistribution result.

Institute for Advanced Study, Einstein Drive, Princeton, NJ 08540, USA
E-mail address: dmilovic@math.ias.edu.

Date: January 23, 2017.
2010 *Mathematics Subject Classification.* 11N45, 11R29, 11R44, 11N36.

Theorem 1. *For a prime number $p \equiv -1 \bmod 16$, let $e_p = 1$ if 16 divides $h(-8p)$ and let $e_p = -1$ otherwise. Then for all $X > 0$, we have*

$$\sum_{\substack{p \leq X \\ p \equiv -1\ (16)}} e_p \ll X^{\frac{199}{200}},$$

where the implied constant is absolute. In particular, the natural density of the set of prime numbers p such that $p \equiv -1 \bmod 4$ and such that 16 divides $h(-8p)$ is equal to $\frac{1}{16}$.

In other words, if we define the 2^k-rank of $\mathrm{Cl}(D)$ to be

$$\mathrm{rk}_{2^k}\mathrm{Cl}(D) = \dim_{\mathbb{F}_2}(2^{k-1}\mathrm{Cl}(D)/2^k\mathrm{Cl}(D)),$$

Theorem 1 states that the natural density of the set of prime numbers p such that $p \equiv -1 \bmod 4$ and such that $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1$ is equal to $\frac{1}{16}$. Aside from giving a numerical density for the 16-rank, the main novelty of Theorem 1 is that the power-saving in X gives strong evidence that the behavior of the 16-rank is different from the behavior of the lower 2-power ranks in a very essential way. In the terminology used by Serre to describe equidistribution phenomena [21], the 8-rank in families of quadratic fields of the type $\{\mathrm{Cl}(dp)\}_p$, where d is a fixed integer and p varies among primes such that dp is a discriminant, is "motivated" – that is, $\mathrm{rk}_8\mathrm{Cl}(dp)$ is given by the trace of the Frobenius conjugacy class of p in a Galois representation associated to a motive depending only on d; however, the 16-rank in the family $\{\mathrm{Cl}(-8p)\}_{p\equiv -1 \bmod 4}$ appears not to be "motivated." We now explain the various consequences of Theorem 1 in more detail.

1.1. **Cohen-Lenstra heuristics.**

Cohen and Lenstra [1] proposed a heuristic model to predict the average behavior of class groups. They 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. Hence the cyclic group of order 2^{k-1} should 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 noted above, the 2-part of the class group $\mathrm{Cl}(-8p)$ is cyclic, and so it is natural to make the following conjecture.

Conjecture 1. *For all $k \geq 1$, we have $\rho(2^k) = 2^{-k}$.*

Conjecture 1 for $k \leq 3$ was implicit in the work of Rédei and Reichardt mentioned above (although the case $k = 3$ first appeared explicitly in literature as a result Hasse [14]). Moreover, Conjecture 1 is supported by strong numerical evidence (for instance, the percentages of primes p that are $< 10^6$ such that $p \equiv -1 \bmod 4$ and such that $\mathrm{rk}_{2^k}\mathrm{Cl}(-8p) = 1$ for $k = 1$, 2, 3, 4, 5, and 6 are 50.09, 25.06, 12.53, 6.40, 3.16, and 1.62%, respectively). Theorem 1 gives a positive answer to Conjecture 1 for the case $k = 4$.

1.2. **Methods for proving density results about the 2-part of the class group.**

Rédei [19] showed that the 4-rank of $\mathrm{Cl}(D)$ is essentially determined by the quadratic residue symbols $(\frac{p_1}{p_2})$ for distinct prime divisors p_1 and p_2 of D. Fouvry and Klüners [7, 8, 9] combined this characterization with analytic and combinatorial techniques to obtain many interesting results about the 4-rank of $\mathrm{Cl}(D)$

and the negative Pell equation $x^2 - Dy^2 = -1$.

The 8-rank is already more subtle. The main method to prove density results for the 8-rank has been to construct certain governing fields and apply the Čebotarev Density Theorem. More precisely, Stevenhagen [23] proved that if d is a non-zero integer, then there exists a normal extension $M_d/\mathbb{Q}$ such that the 8-rank of $\mathrm{Cl}(dp)$ (when dp is a fundamental discriminant) is determined by the Artin conjugacy class $(p, M_d/\mathbb{Q})$ in $\mathrm{Gal}(M_d/\mathbb{Q})$. Knowing such a governing field M_d explicitly makes it easy to study the density of primes p for which $\mathrm{rk}_8\mathrm{Cl}(dp) = r$ for any fixed integer r. For instance, a governing field for the 8-rank in the family $\{\mathrm{Cl}(-8p)\}_{p\equiv -1(4)}$ is $\mathbb{Q}(\zeta_{16})$, where ζ_{16} is a primitive 16th root of unity.

Cohn and Lagarias [2] made the bold conjecture that governing fields $M_{d,2^k}$ for the 2^k-rank in the family $\{\mathrm{Cl}(dp)\}_p$ as above should exist for every 2-power 2^k (see also [3]). However, a governing field has *not* been found for the 16- or higher 2-power ranks in *any* family. This is the main reason that density results for the 16-rank have been out of reach for such a long time (see [24, p. 16-18]).

Instead of exhibiting a governing field for the 16-rank in the family $\{\mathrm{Cl}(-8p)\}_p$, we introduce another method to the study of the 2-part of class groups of quadratic number fields.

1.3. **Vinogradov's method.**

In late 1940's, I.M. Vinogradov [25, 26] was able to prove cancellation in the sum over primes

$$\sum_{p\leq X} \exp(2\pi i\sqrt{p})\log p$$

by expanding it into sums of type I

$$\sum_{n\leq X,\ n\equiv 0 \bmod d} a_n$$

and sums of type II

$$\sum_{m\leq M, n\leq N}\sum \alpha_m\beta_n a_{mn},$$

where $a_n = \exp(2\pi i\sqrt{n})$, d is any positive integer, and $\{\alpha_n\}_n$ and $\{\beta_m\}_m$ are very general sequences of complex numbers that do not grow too quickly. We prove Theorem 1 by using a modern version of Vinogradov's method developed by Friedlander, Iwaniec, Mazur, and Rubin [10, Proposition 5.2, p.722].

One important feature of Vinogradov's estimates is that the bound for the sum over primes saves a power of X, i.e., there exists a small real number $\delta > 0$ such that

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

On the other hand, the best zero-free regions of classical L-functions generally give the much worse error estimates of the type $X\log(-c\sqrt{\log X})$. This suggests that the a_p are not "motivated" – they do not arise naturally as coefficients of a finite sum of classical L-functions, and in particular are not naturally related to an Artin symbol of p in a fixed normal extension $M/\mathbb{Q}$. In other words, the proof of Theorem 1 gives strong evidence that a governing field for the 16-rank in the family $\{\mathrm{Cl}(-8p)\}_{p\equiv -1(4)}$ in fact does *not* exist. For a more precise discussion of this phenomenon, see Section 7.

1.4. **A few words about the proof.** Leonard and Williams [17] found the following criterion for the 16-rank. Since we were unable to verify their proof of this criterion, we give another proof of a slightly more general statement in Section 2. A prime $p \equiv -1 \bmod 16$ can be written as

$$p = u^2 - 2v^2 \tag{1.1}$$

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

$$u \equiv 1 \bmod 16. \tag{1.2}$$

Given such a representation, [17, Theorem 3, p.205] (or our Proposition 1) states that

$$e_p = \left(\frac{v}{u}\right), \tag{1.3}$$

where e_p is defined as in Theorem 1 and $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi symbol. The first few primes satisfying the above criterion are 127, 223, 479, 719, ... Note that integers $u > 0$ and v satisfying (1.1) and (1.2) are *not* unique. Nonetheless, the criterion (1.3) is valid for *any* choice of integers $u > 0$ and v satisfying (1.1) and (1.2). Hence Theorem 1 is a corollary of the following theorem, which we will prove using Vinogradov's method.

Theorem 2. *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 prime p in the sum above, u and v are taken to be integers satisfying (1.1) *and* (1.2).

Theorem 2 is an equidistribution result reminiscent of [11, Theorem 2, p. 948]. In [11], Friedlander and Iwaniec associate a *spin symbol* (i.e., a quantity taking values in $S^1 \subset \mathbb{C}^\times$) to each non-zero ideal in the Gaussian integers $\mathbb{Z}[i]$ and show, also using Vinogradov's method, that its value is equidistributed over prime ideals in $\mathbb{Z}[i]$ ordered by their norms.

To apply Vinogradov's method to the sum $\sum_{p\leq X} e_p$, the most important task is to define a sequence $\{e_n\}_n$ in a way that one can prove good estimates for sums of type I and type II. Generalizing the proof in [11] to our setting is made difficult by the fact that an odd ideal in the quadratic ring $\mathbb{Z}[\sqrt{2}]$ does not have a canonical generator – the group of units $\mathbb{Z}[\sqrt{2}]^\times$ is infinite. We resort to averaging over four carefully chosen generators to define an analogous spin symbol. Proving that the resulting quantity is well-defined already requires significant new ideas. Proposition 2 in Section 2 is a key result in this direction; it describes the twisting of $\left(\frac{v}{u}\right)$ by the fundamental unit $1 + \sqrt{2}$. Section 2 also contains the class field theoretic construction of the *governing (spin) symbol* $e_p = \left(\frac{v}{u}\right)\chi(u)$ for the 16-rank in the family $\{\mathrm{Cl}(-8p)\}_{p\equiv -1(4)}$ (see Proposition 1). In Section 3, we construct spin symbols that both encode behavior of the 16-rank in our family and are conducive to analytic techniques (see Equations (3.4) and (3.5)). We also reduce Theorem 2 to a purely analytic statement (see Theorem 3) that can be attacked by the machinery of Friedlander, Iwaniec, Mazur, and Rubin (see Proposition 4). The goal of Section 4 is to construct convenient fundamental domains for the multiplicative action of a fundamental unit $1+\sqrt{2}$ on $\mathbb{Z}[\sqrt{2}]$. In Section 5, we use a Polya-Vinogradov-type estimate to give bounds for sums of type I for the spin symbol. In Section 6, we give bounds for sums of type II of the spin symbol, thus completing the proof of Theorem 2. In the final section, we discuss the implications of the power-saving bound in Theorem 1 on the existence of governing fields for the 16-rank.

1.5. **Generalizations.** While it would be desirable to prove density results about the 16-rank in any family of the type $\{\mathrm{Cl}(dp)\}_p$ with d fixed and p varying, there are serious technical limitations on both algebraic and analytic sides of the problem. On the algebraic side, the 2-part of $\mathrm{Cl}(dp)$ might no longer be cyclic, and hence one would have to account for the possible interactions between the spin symbols arising from different prime divisors of d. On the analytic side, one would have to account for the possibility that the class group of $\mathbb{Q}(\sqrt{d})$ need not be trivial.

Perhaps an even more basic problem is that applying Vinogradov's method in this setting generally requires one to carry out analytic estimates over a number ring instead of $\mathbb{Z}$, and many such estimates require bounds on incomplete character sums that are well beyond anything currently available. For instance, similar proofs of density results about the 16-rank in the families $\{\mathrm{Cl}(-8p)\}_{p\equiv 1(4)}$ and $\{\mathrm{Cl}(-4p)\}_p$ would require Burgess-type estimates for short character (modulo q) sums of length $q^{\frac{1}{8}-\epsilon}$.

Theorem 1 thus lives on the very edge of unconditional density results about the 2-part of class groups of quadratic number fields. So while the statement of our main theorem is not as general as one might hope for, our work nevertheless demonstrates two important ideas: that yet another classical analytic method is applicable to modern problems concerning class groups; and that the nature of the 16-rank is of a type not seen before in the study of the 2-part of class groups.

Acknowledgments. I would like to give special thanks to my PhD advisors Étienne Fouvry and Peter Stevenhagen for checking my work and helping me improve some arguments. I would also like to thank Hendrik Lenstra, Peter Sarnak, and Marco Streng for useful discussions. This research was partially supported by an ALGANT Erasmus Mundus Scholarship and by National Science Foundation agreement No. DMS-1128155.

2. Governing symbols

The purpose of this section is to generalize [17, Theorem 3, p.205] and to develop a framework conducive to the analytic techniques of Friedlander, Iwaniec, Mazur, and Rubin [10].

Let χ be a character $(\mathbb{Z}/16\mathbb{Z})^\times \to \mathbb{C}^\times$ 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 [17, Theorem 3, p.205] is as follows:

Proposition 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*

$$\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1 \Longleftrightarrow \left(\frac{v}{u}\right)\chi(u) = 1. \tag{2.1}$$

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 1. Given *one* integer solution $(u, v) = (u_0, v_0)$ to the system

$$\begin{cases} p = u^2 - 2v^2 \\ u > 0, v \equiv 1 \bmod 4 \end{cases}, \tag{2.2}$$

then the complete set of integer solutions (u, v) to the system (2.2) 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 1 is that the quantity $\left(\frac{v}{u}\right)\chi(u)$ is *independent* of the choice of u and v satisfying (2.2). For a prime $p \equiv -1 \bmod 16$, we can thus define the *governing symbol* for the 16-rank to be

$$\langle p \rangle := \left(\frac{v}{u}\right)\chi(u), \tag{2.3}$$

where u and v are integers satisfying (2.2). The quantity $\langle p \rangle$ 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 [17, Theorem 3, p.205] can be proved by numerous manipulations of Jacobi symbols and applications of quadratic reciprocity. We instead prove Proposition 1 by interpreting the Jacobi symbol $\left(\frac{v}{u}\right)$ as an Artin symbol of an ideal $\mathfrak{u}$ defined via the decomposition $p = u^2 - 2v^2$ in an extension of $\mathbb{Q}(\sqrt{-8p})$ defined via the *same* decomposition $p = u^2 - 2v^2$. Moreover, a byproduct 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 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 1 and Proposition 2.

2.1. **Preliminaries.**

2.1.1. *Galois theory.* We will make extensive use of the following lemma from Galois theory (see [16, Chapter VI, Exercise 4, p.321]).

Lemma 1. *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.*

2.1.2. *The Artin map and Artin symbols.* Let E/F be a finite abelian extension of number fields. Let 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

$$\left(\frac{\cdot}{E/F}\right) : I_F \to \mathrm{Gal}(E/F)$$

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 $\mathrm{Norm}(\mathfrak{p})$ 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 $\mathrm{Gal}(E/F)$ such that

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

for all α in E. We then extend $\left(\frac{\cdot}{E/F}\right)$ multiplicatively to I_F.

We will use the following lemma several times.

Lemma 2. *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 [15, Proposition 3.1, p. 103]. □

2.1.3. *2^n-Hilbert class fields.* Let $K = \mathbb{Q}(\sqrt{-8p})$ and $\mathrm{Cl} = \mathrm{Cl}(-8p)$. Recall that the *Hilbert class field* H of K is the maximal unramified abelian extension of K. The Artin symbol induces a canonical isomorphism of groups

$$\left(\frac{\cdot}{H/K}\right) : \mathrm{Cl} \longrightarrow \mathrm{Gal}(H/K). \tag{2.4}$$

Suppose for the moment that $\mathrm{rk}_{2^n}\mathrm{Cl}(-8p) = 1$. Then $2^n\mathrm{Cl}$ 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 $2^n\mathrm{Cl}$ under the isomorphism (2.4). Since the 2-primary part of Cl is cyclic, it follows immediately that H_{2^n} is the unique unramified, cyclic, degree-2^n extension of K. Moreover, (2.4) induces a canonical isomorphism of cyclic groups of order 2^n

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

The main idea of the proof of Proposition 1 is to write down explicitly, for $p \equiv -1 \bmod 8$, *both*

- the 4-Hilbert class field H_4 of K, *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

$$\left(\frac{\mathfrak{u}}{H_4/K}\right) = 1. \tag{2.6}$$

The isomorphism (2.5) for $n = 2$ and the equality (2.6) then imply that the class of order 4 in Cl in fact belongs to 4Cl, which proves that Cl has an element of order 16.

2.1.4. *Ring class fields.* To prove Proposition 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

$$\left(\frac{\cdot}{R_D/K}\right) : \mathrm{Cl}(D) \longrightarrow \mathrm{Gal}(R_D/K). \tag{2.7}$$

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. *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 [4, Theorem 9.18, p. 191] and [4, Exercise 9.20, p. 195-196]. □

2.2. **A special family of quadratic fields.** Let u and v be coprime integers such that u is odd and positive and such that

$$n = u^2 - 2v^2 \tag{2.8}$$

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 such that $n = d^2 m$. Then $K = \mathbb{Q}(\sqrt{-2m})$ and the discriminant of $K/\mathbb{Q}$ is equal to $-8m$. 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 $u + v\sqrt{2} = \delta^2 \mu$.

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

$$\nu = u + v\sqrt{2}. \tag{2.9}$$

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 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.

$$\begin{tikzcd}
 & L = G(\sqrt{\varepsilon\nu}) \arrow[dl, no head] \arrow[d, no head] \\
A = \mathbb{Q}(\sqrt{2}, \sqrt{\varepsilon\nu}) \arrow[d, no head] & G = K(\sqrt{2}) \arrow[dl, no head] \arrow[d, no head] \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, no head] & K = \mathbb{Q}(\sqrt{-2m}) \arrow[d, no head] \\
 & \mathbb{Q}
\end{tikzcd}$$

Lemma 4. *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 1, 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 1 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 5. *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 5, 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 6. *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 7. *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, 4, and 6. □

2.3. **A computation of Artin symbols.** This section contains the heart of the proof of both Proposition 1 and Proposition 2.

The integers u and v appearing in (2.8) 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 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 [13], 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 1, while the case $f = 4$ will be used to prove Proposition 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

$$\mathfrak{u} = \ker \psi_{u,v}. \tag{2.10}$$

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

$$2vf \equiv \tau \bmod \mathfrak{u} \tag{2.11}$$

and that

$$\mathrm{Norm}(\mathfrak{u}) = u. \tag{2.12}$$

Let $\sqrt{\varepsilon\nu}$ be a square root of $\varepsilon\nu$. Then, by Lemma 1, 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

$$\gamma = (2 + \sqrt{2})v \in \mathbb{Z}[\sqrt{2}]. \tag{2.13}$$

Then again by Lemma 1, the extension $G(\sqrt{\gamma})/K$ is cyclic of degree 4. The element γ was chosen so that

$$\varepsilon\nu \equiv \gamma \bmod \mathfrak{u}, \tag{2.14}$$

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

$$\beta = v((4u+6v)f - \tau) \qquad \text{and} \qquad \beta' = v((4u+6v)f + \tau).$$

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

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

and so $\mathfrak{p}$ splits in $K(\sqrt{\beta})$. By Lemma 2, 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 8. *Let $\mathfrak{u}$ be defined as in* (2.10). *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 2 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 8, 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 q coprime to $2v$, we have

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

so that if we identify $\psi_3 : \langle 3 \bmod 16\rangle \cong \mu_4 = \langle i\rangle \subset \mathbb{C}^{\times}$ by sending $3 \mapsto i = \sqrt{-1}$, we get

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

Multiplying over all primes q dividing u and using Lemma 8, we finally obtain the following result.

Lemma 9. *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*

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

2.4. **An ideal identity.** We keep the same notation as in Sections 2.2 and 2.3. 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 1 and Proposition 2.

Lemma 10. *Let $\mathfrak{u}$ be defined as in* (2.10). *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 $(2vf - \tau)\mathfrak{u}^{-2} = \mathfrak{t}_f$. □

2.5. **Proof of Proposition 1.** We apply the results of Sections 2.3 and 2.4 in the case $n = p \equiv -1 \bmod 8$ is a prime number and $f = 1$. In this case there exist integers u and v such that $p = u^2 - 2v^2$, and 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

$$v \equiv 1 \bmod 4. \tag{2.15}$$

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.

2.5.1. *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 [17].

When $n = p$ and $f = 1$, the ideal $\mathfrak{t} = \mathfrak{t}_f$ defined in Section 2.4 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 (2.10) with u and v as above and $f = 1$. Lemma 10 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 11. *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 11 is via the theory of binary quadratic forms, as was done in [17]. 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.

2.5.2. *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 11 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 (2.9), i.e., $\pi = u + v\sqrt{2}$. The following proposition achieves our aim.

Proposition 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 2.2 and 2.3 with $n = m = p$, $e = 1$, and u and v as above. By Lemma 4, the extension $H_2(\sqrt{\varepsilon\pi})/K$ is cyclic of degree 4. By Lemma 5, $H_2(\sqrt{\varepsilon\pi})/K$ is unramified over the prime ideal $\mathfrak{p} = (p, \sqrt{-2p})$ of K lying over p. Finally, by part (1) of Lemma 6, $H_2(\sqrt{\varepsilon\pi})/K$ is unramified over the prime ideal $\mathfrak{t} = (2, \sqrt{-2p})$ of K lying over 2. □

2.5.3. *Conclusion of the proof of Proposition 1.* By Lemma 11, $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1$ if and only if the ideal class of $\mathfrak{u}$ belongs to $\mathrm{Cl}(-8p)^4$. By Proposition 3, 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 2.3, 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 9, this occurs if and only if $\left(\frac{v}{u}\right)\chi(u) = 1$, which proves Proposition 1.

2.6. **Proof of Proposition 2.** As in the statement of Proposition 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

$$u_2 + v_2\sqrt{2} = \varepsilon^8(u_1 + v_1\sqrt{2}) = (577u_1 + 816v_1) + (408u_1 + 577v_1)\sqrt{2}, \tag{2.16}$$

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

$$\left(\frac{v_1}{u_1}\right) = \left(\frac{v_2}{u_2}\right). \tag{2.17}$$

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 (2.17) are equal to 0, and hence (2.17) 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 2.2. 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 (2.10) 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 12. *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 10, 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 2.4. By (2.16), 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

$$\mathfrak{u}_2^2 = \frac{8v_2 - \tau}{8v_1 - \tau}\mathfrak{u}_1^2. \tag{2.18}$$

Let $\alpha = (17u_1 + 24v_1) + 3\tau$. We claim that

$$\left(\frac{\alpha}{u_1}\right)^2 = \frac{8v_2 - \tau}{8v_1 - \tau}. \tag{2.19}$$

We first note that

$$\begin{aligned} \frac{8v_2 - \tau}{8v_1 - \tau} &= \frac{8v_2 - \tau}{8v_1 - \tau} \cdot \frac{8v_1 + \tau}{8v_1 + \tau} \\ &= \frac{64v_1v_2 + 32n + 8(v_2 - v_1)\tau}{64v_1^2 + 32n} \\ &= \frac{64v_1(408u_1 + 577v_1) + 32n + 8(408u_1 + 576v_1)\tau}{32u_1^2} \\ &= \frac{n + 2v_1(408u_1 + 577v_1) + (102u_1 + 144v_1)\tau}{u_1^2}. \end{aligned} \tag{2.20}$$

Expanding α^2, we get

$$\begin{aligned} \alpha^2 &= 289u_1^2 + 576v_1^2 + 816u_1v_1 - 288n + (102u_1 + 144v_1)\tau \\ &= u_1^2 + 1152v_1^2 + 816u_1v_1 + (102u_1 + 144v_1)\tau \\ &= n + 1154v_1^2 + 816u_1v_1 + (102u_1 + 144v_1)\tau \\ &= n + 2v_1(408u_1 + 577v_1) + (102u_1 + 144v_1)\tau. \end{aligned} \tag{2.21}$$

Comparing the last line of (2.21) with the numerator in the last line of (2.20), we obtain (2.19).

Now (2.18) and (2.19) imply that

$$u_1^2\mathfrak{u}_2^2 = \alpha^2\mathfrak{u}_1^2. \tag{2.22}$$

By (2.12), $\mathrm{Norm}(\mathfrak{u}_2) = u_2$. 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 (2.22) implies that $u_1\mathfrak{u}_2 = \alpha\mathfrak{u}_1$, which proves the lemma. □

Remark. There is a shorter proof of Lemma 12 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 the lemma.

Now, for $k \in \{1, 2\}$, define $\nu_k = u_k + v_k\sqrt{2}$ similarly as in Section 2.2. Then

$$\nu_2 = \varepsilon^8\nu_1. \tag{2.23}$$

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 7, L is contained in the ring class field of $\mathbb{Z}[\tau]$. Hence, by Lemma 12, the images of both $\mathfrak{u}_1$ and $\mathfrak{u}_2$ under the map (2.7) coincide, i.e.,

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

Applying Lemma 9, we get

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

Equation (2.16) implies that

$$u_2 = 577u_1 + 816v_1 \equiv u_1 \bmod 16. \tag{2.24}$$

Hence, as χ is a character modulo 16, we have $\chi(u_1) = \chi(u_2)$, and so Proposition 2 is finally proved.

3. Sums over primes

Above, we defined the governing symbol $\langle p\rangle$ 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 2, i.e., that these governing symbols oscillate, is a proposition due to Friedlander, Iwaniec, Mazur and Rubin [10]. We now state this proposition in our context.

3.1. 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 [10] (and even earlier in [11]), 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

$$A_{\mathfrak{d}}(X) := \sum_{\substack{\mathrm{Norm}(\mathfrak{n}) \leq X \\ \mathfrak{n} \equiv 0 \bmod \mathfrak{d}}} a_{\mathfrak{n}}. \tag{3.1}$$

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

$$B(M, N) := \sum_{\mathrm{Norm}(\mathfrak{m}) \leq M} \sum_{\mathrm{Norm}(\mathfrak{n}) \leq N} \alpha_{\mathfrak{m}} \beta_{\mathfrak{n}} a_{\mathfrak{m}\mathfrak{n}}. \tag{3.2}$$

We consider bilinear sums where the complex numbers $\alpha_{\mathfrak{m}}$ and $\beta_{\mathfrak{n}}$ satisfy

$$|\alpha_{\mathfrak{m}}| \leq \Lambda(\mathfrak{m}) \text{ and } |\beta_{\mathfrak{n}}| \leq \tau(\mathfrak{n}), \tag{3.3}$$

where $\tau(\mathfrak{n})$ denotes the number of ideals in $\mathbb{Z}[\sqrt{2}]$ dividing $\mathfrak{n}$. We now state [10, Proposition 5.2, p.722] that we use to prove Theorem 2.

Proposition 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 (3.3).
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 [25].

3.2. **Extending governing symbols.** In light of Proposition 4, our current goal is to define a sequence $\{a_{\mathfrak{n}}\}$ indexed by 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 $\langle p \rangle$ defined in (2.3). We first define a spin symbol $[\cdot]$ for all totally positive elements of $\mathbb{Z}[\sqrt{2}]$. We put

$$[u + v\sqrt{2}] := \begin{cases} \left(\frac{v}{u}\right) & \text{if } u \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$$

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 $[u+v\sqrt{2}] = \langle p \rangle$, by definition (2.3). Indeed, the condition

$u \equiv 1 \bmod 16$ implies that $\chi(u) = 1$ and also that $\left(\frac{-v}{u}\right) = \left(\frac{v}{u}\right)$ (note that one of v and $-v$ is congruent to $1 \bmod 4$). It is also convenient that exactly one of the four elements $\varepsilon^{2k}(u + v\sqrt{2}) = u_k + v_k\sqrt{2}$ $(0 \leq k \leq 3)$ 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. $(17u+24v, 12u+17v)$), and hence $u_2 \equiv u_0+8 \bmod 16$; one can now easily check that multiplying $u+v\sqrt{2}$ successively by ε^2 cycles $u \bmod 16$ through the set $\{1, 7, 9, 15\}$.

Proposition 2 states that $[w] = [\varepsilon^8 w]$ for any odd and totally positive $w \in \mathbb{Z}[\sqrt{2}]$, so, in light of the preceding discussion, we might naively define $a_{\mathfrak{n}} = \sum_{k=0}^{3}[\varepsilon^{2k}w]$, where $w \succ 0$ is any totally positive generator of $\mathfrak{n}$. This definition 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 weigh the expression above 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

$$[u + v\sqrt{2}]_{\phi,\psi} := [u + v\sqrt{2}]\phi(-u^2 + 2v^2)\psi(u). \tag{3.4}$$

For a non-zero ideal $\mathfrak{n}$ in $\mathbb{Z}[\sqrt{2}]$ generated by a totally positive element w, we set

$$a_{\phi,\psi,\mathfrak{n}} := \sum_{k=0}^{3}[\varepsilon^{2k}w]_{\phi,\psi}. \tag{3.5}$$

This is still well-defined, i.e., independent of the choice of $w \succ 0$, by Proposition 2 and by (2.24). We will apply Proposition 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 2. It is now easy to check

Lemma 13. *If p is a prime and $\mathfrak{p}$ is a prime ideal lying above p, then we have*

$$\frac{1}{8^2}\sum_{\phi}\sum_{\psi}a_{\phi,\psi,\mathfrak{p}} = \begin{cases}\langle p\rangle & \text{if } p \equiv -1 \bmod 16\\ 0 & \text{otherwise.}\end{cases}$$

Hence, to prove Theorem 2, it now suffices to prove

Theorem 3. *Let $a_{\phi,\psi,\mathfrak{n}}$ be defined as in (3.5). For every $\epsilon > 0$, there is a constant $C_\epsilon > 0$ depending only on ϵ such that for every $X \geq 2$, we have*

$$\left|\sum_{\mathrm{Norm}(\mathfrak{n})\leq X}a_{\phi,\psi,\mathfrak{n}}\Lambda(\mathfrak{n})\right| \leq C_\epsilon X^{\frac{149}{150}+\epsilon}.$$

4. Fundamental domains

In order to obtain power-saving cancellation for linear and bilinear sums as in Proposition 4, we will have to choose generators of $\mathfrak{n}$ in (3.5) carefully. The problem reduces to constructing a convenient fundamental domain for the action of $\varepsilon^2 = 3+2\sqrt{2}$ on totally positive elements of $\mathbb{Z}[\sqrt{2}]$. Such constructions are standard (see for instance [18, Chapter 6] or [10, Section 4]). For the sake of completeness and explicitness, we give a simple argument tailored to our specific needs. Let

$$\Omega := \left\{(u, v) \in \mathbb{R}^2 : u > 0, -u < \sqrt{2}v < u\right\}. \tag{4.1}$$

Then the lattice points $(u,v) \in \Omega \cap \mathbb{Z}^2$ precisely enumerate the totally positive elements $w = u + v\sqrt{2}$. The group $\langle \varepsilon^2 \rangle$ of totally positive units of $\mathbb{Z}[\sqrt{2}]$ acts on the totally positive elements of $\mathbb{Z}[\sqrt{2}]$ by multiplication, and this induces an action $\langle \varepsilon^2 \rangle \times \Omega \to \Omega$ given by

$$a + b\sqrt{2} \cdot (u,v) := (au + 2bv, bu + av).$$

Let $\mathcal{D}$ be the subset of Ω defined by

$$\mathcal{D} := \left\{(u,v) \in \mathbb{R}^2 : u > 0, -u < 2v \leq u\right\} \tag{4.2}$$

We claim that the region $\mathcal{D}$ is a fundamental domain for the action of ε^2 on Ω in the following sense.

Lemma 14. *For each element $(u,v) \in \Omega \cap \mathbb{Z}^2$, there exists exactly one integer k such that $\varepsilon^{2k} \cdot (u,v) \in \mathcal{D}$.*

Proof. Since $\varepsilon^2 = 3+2\sqrt{2} > 1$, we have that $\varepsilon^{2k} > \varepsilon^{2j}$ whenever $k > j$, that $\varepsilon^{2k} \to 0$ as $k \to -\infty$, and that $\varepsilon^{2k} \to \infty$ as $k \to \infty$. Moreover, given $(u,v) \in \Omega \cap \mathbb{Z}^2$, we have

$$\frac{\varepsilon^2(u + v\sqrt{2})}{\varepsilon^{-2}(u - v\sqrt{2})} = \varepsilon^4 \cdot \frac{u + v\sqrt{2}}{u - v\sqrt{2}}.$$

Hence, given $(u,v) \in \Omega \cap \mathbb{Z}^2$, there exists a unique integer k such that

$$\varepsilon^{-2} < \frac{\varepsilon^{2k}(u + v\sqrt{2})}{\varepsilon^{-2k}(u - v\sqrt{2})} \leq \varepsilon^2.$$

The lemma follows upon noticing that for $(u,v) \in \Omega$, we have $(u,v) \in \mathcal{D}$ if and only if $\varepsilon^{-2} < (u + v\sqrt{2})/(u - v\sqrt{2}) \leq \varepsilon^2$. □

An immediate consequence of Lemma 14 is the following proposition.

Proposition 5. *Suppose that $\mathfrak{n}$ is a non-zero ideal of $\mathbb{Z}[\sqrt{2}]$. Then $\mathfrak{n}$ has a unique generator in $\mathcal{D}$.*

4.1. 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 [5] and [6]).

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 15 (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 15 to the fundamental domain $\mathcal{D} \subset \mathbb{R}^2$ as well as certain variations thereof.

Let $k \geq 0$ be an 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

$$\mathcal{D}_k(X) := \{(u,v) \in \mathcal{D}_k : u^2 - 2v^2 \leq X\} \tag{4.3}$$

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

$$\mathrm{Vol}(\mathcal{D}_k(X)) = a_k X \qquad \text{and} \qquad \mathrm{Vol}(\partial(\mathcal{D}_k(X))) = \ell_k X^{\frac{1}{2}}. \tag{4.4}$$

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.

5. Linear sums

In this section we prove that the estimate (A) from Proposition 4 holds for the sequence $\{a_{\phi,\psi,\mathfrak{n}}\}_{\mathfrak{n}}$ defined in (3.5) with $\theta_1 = 1/6$.

Proposition 6. *Let $a_{\mathfrak{n}} = a_{\phi,\psi,\mathfrak{n}}$, where $a_{\phi,\psi,\mathfrak{n}}$ is defined as in* (3.5)*, and let $A_{\mathfrak{d}}(X)$ be defined as in* (3.1)*. 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

$$\mathcal{R}(X) := \mathcal{D}_4(X) = \left\{(u,v) \in \mathcal{D} \cup \varepsilon^2\mathcal{D} \cup \varepsilon^4\mathcal{D} \cup \varepsilon^6\mathcal{D} : u^2 - 2v^2 \leq X\right\}. \tag{5.1}$$

By Proposition 5 and definition (3.5), 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 (3.4).

We now reformulate the congruence condition $u + v\sqrt{2} \equiv 0 \bmod \mathfrak{d}$. Proposition 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

$$L_{\mathfrak{d}} := \begin{pmatrix} d_1 & 2d_2 \\ d_2 & d_1 \end{pmatrix} : \mathbb{Z}^2 \to \mathbb{Z}^2$$

of determinant $D := \mathrm{Norm}(\mathfrak{d}) = d_1^2 - 2d_2^2$. Hence we define

$$\mathcal{R}(\mathfrak{d}, X) := \{(u,v) \in \mathcal{R}(X) : (u,v) \in \mathrm{Image}(L_{\mathfrak{d}})\},$$

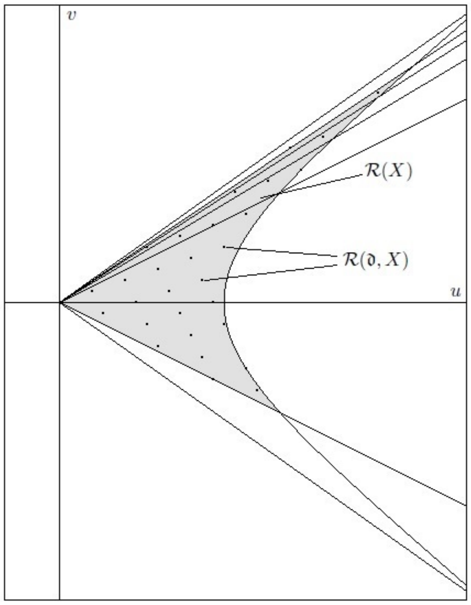

FIGURE 1. The region $\mathcal{R}(X)$ and the lattice points $\mathcal{R}(\mathfrak{d}, X)$

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

$$|A_{\mathfrak{d}}(X)| \leq \sum_{(u,v)\in\mathcal{R}(\mathfrak{d},X)} 1 = \sum_{L_{\mathfrak{d}}^{-1}\mathcal{R}(X)\cap\mathbb{Z}^2} 1. \tag{5.2}$$

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 15 gives

$$|A_{\mathfrak{d}}(X)| \leq a_4 X D^{-1} + O(D^{-\frac{1}{2}}X^{\frac{1}{2}} + 1) \ll XD^{-1} + X^{\frac{1}{2}}D^{-\frac{1}{2}} + 1, \tag{5.3}$$

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

$$A_{\mathfrak{d}}(u_0,v_0,X) = \sum_{\substack{0\leq u\leq R_1(X)\\ u\equiv u_0 \bmod 16}} A_{u,\mathfrak{d}}(v_0,X), \tag{5.4}$$

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:

$$\begin{cases} u = d_1x + 2d_2y \\ v = d_2x + d_1y. \end{cases} \tag{5.5}$$

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 (5.5) has a solution over $\mathbb{Z}$, then d must divide u. This means that

$$A_{\mathfrak{d}}(u_0,v_0,X) = \sum_{\substack{0 \le u \le R_1(X) \\ u \equiv u_0 \bmod 16 \\ u \equiv 0 \bmod d}} A_{u,\mathfrak{d}}(v_0,X).$$

Now suppose $u \equiv 0 \bmod d$, and let $x_u, y_u \in \mathbb{Z}$ be such that

$$u = d_1x_u + 2d_2y_u.$$

Then all solutions $(x,y) \in \mathbb{Z}^2$ to the first equation in (5.5) are given by

$$(x,y) = (x_u - 2d_2'k, y_u + d_1'k), \quad k \in \mathbb{Z}.$$

Hence

$$v = d_2\left(x_u - 2d_2'k\right) + d_1\left(y_u + d_1'k\right) = d_2x_u + d_1y_u + Dk/d,$$

which means that (5.5) has a solution over $\mathbb{Z}$ if and only if

$$v \equiv d_2x_u + d_1y_u \bmod D/d.$$

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

$$\begin{cases} v_u \equiv d_2x_u + d_1y_u \bmod D/d \\ v_u \equiv v_0 \bmod 16. \end{cases}$$

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 $16D/d = e_ud_u$, $v_u = e_uv_u'$, and perform a change of variables $v = e_uv'$, 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,

$$A_{u,\mathfrak{d}}(v_0,X) = \frac{1}{\varphi(d_u)} \left(\frac{e_u}{u}\right) \chi(\overline{v_u'}) \sum_{\chi \bmod d_u} \sum_{v' \in I_u'} \chi(v') \left(\frac{v'}{u}\right), \tag{5.6}$$

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

$$\ll_\epsilon D^\epsilon X^{\frac{3}{4}}. \tag{5.7}$$

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 (5.4), (5.6), and (5.7), we have proved the bound

$$A_{\mathfrak{d}}(X) \ll_\epsilon D^{\frac{1}{2}} X^{\frac{3}{4}+\epsilon}. \tag{5.8}$$

We use (5.8) for $D < X^{1/6}$ and (5.3) for $D \geq X^{1/6}$ to obtain

$$A_{\mathfrak{d}}(X) \ll_\epsilon X^{\frac{5}{6}+\epsilon}.$$

□

6. Bilinear sums

We are left with proving the estimate (B) from Proposition 4, which we do with $\theta_2 = 1/12$ in much the same way as in [11, Sections 19-21, p. 1018-1028].

Proposition 7. *Let $a_{\mathfrak{n}} = a_{\phi,\psi,\mathfrak{n}}$, where $a_{\phi,\psi,\mathfrak{n}}$ is defined as in* (3.5)*, and let $B(M,N)$ be defined as in* (3.2)*. Then for all $\epsilon > 0$ and all $M, N \geq 2$, we have*

$$B(M,N) \ll_\epsilon (M+N)^{\frac{1}{12}} (MN)^{\frac{11}{12}+\epsilon}.$$

Our basic strategy will be to prove a factorization formula of the type $[wz] = [w][z]\gamma(w,z)$, where $\gamma(w,z)$ is a quantity which oscillates in both arguments $w, z \in \mathbb{Z}[\sqrt{2}]$. We first develop some background necessary to define $\gamma(w,z)$ and then prove power-saving cancellation for general bilinear sums of the type $\sum\sum_{w,z} \alpha_w \beta_z \gamma(w,z)$.

6.1. Primitivity.

We say that an ideal $\mathfrak{a}$ in $\mathbb{Z}[\sqrt{2}]$ is *primitive* if whenever $\mathfrak{p}$ is a prime ideal dividing $\mathfrak{a}$, then $\mathfrak{p}$ is unramified, of residue degree one, and $\overline{\mathfrak{p}}$ does not divide $\mathfrak{a}$. Here and after, if x is an element or an ideal in $\mathbb{Z}[\sqrt{2}]$ we will use $\overline{x}$ to denote the conjugate of x over $\mathbb{Q}$. The main property of primitive ideals that we will use is that the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{2}]$ induces an isomorphism

$$\mathbb{Z}/(\mathrm{Norm}(\mathfrak{a})) \xrightarrow{\sim} \mathbb{Z}[\sqrt{2}]/\mathfrak{a}. \tag{6.1}$$

We call an ideal $\mathfrak{a}$ (resp. element w) in $\mathbb{Z}[\sqrt{2}]$ *odd* if $\mathrm{Norm}(\mathfrak{a})$ (resp. $\mathrm{Norm}(w)$) is an odd integer. An ideal in $\mathbb{Z}[\sqrt{2}]$ is odd if and only if every prime ideal that divides

$\mathfrak{a}$ is unramified. Hence, an ideal $\mathfrak{a}$ is primitive if and only if $\mathfrak{a}$ is odd and there is no rational prime p dividing $\mathfrak{a}$ (i.e., no rational prime p such that (p) divides $\mathfrak{a}$).

Remark. For instance, $\mathrm{Norm}(7) = 49$, but $\mathbb{Z}[\sqrt{2}]/(7) \cong \mathbb{Z}[\sqrt{2}]/(3+\sqrt{2}) \times \mathbb{Z}[\sqrt{2}]/(3-\sqrt{2}) \cong \mathbb{Z}/(7) \times \mathbb{Z}/(7) \not\cong \mathbb{Z}/(49)$.

For every integer n we have the equality of quadratic residue symbols

$$\left(\frac{n}{\mathrm{Norm}(\mathfrak{a})}\right) = \left(\frac{n}{\mathfrak{a}}\right), \tag{6.2}$$

where the symbol on the left is the usual Jacobi symbol while the symbol on the right is the quadratic residue symbol in $\mathbb{Z}[\sqrt{2}]$, i.e., for $\alpha \in \mathbb{Z}[\sqrt{2}]$,

$$\left(\frac{\alpha}{\mathfrak{a}}\right) := \prod_{\mathfrak{p}^{k_\mathfrak{p}} \| \mathfrak{a}} \left(\frac{\alpha}{\mathfrak{p}}\right)^{k_\mathfrak{p}},$$

where

$$\left(\frac{\alpha}{\mathfrak{p}}\right) := \begin{cases} 1 & \text{if } (\alpha, \mathfrak{p}) = 1 \text{ and } \alpha \equiv \square \bmod \mathfrak{a} \\ -1 & \text{if } (\alpha, \mathfrak{p}) = 1 \text{ and } \alpha \not\equiv \square \bmod \mathfrak{a} \\ 0 & \text{otherwise.} \end{cases}$$

Now it follows immediately from (6.1) and (6.2) that

$$\sum_{z \in \mathbb{Z}[\sqrt{2}]/\mathfrak{a}} \left(\frac{z}{\mathfrak{a}}\right) = \sum_{n \in \mathbb{Z}/(\mathrm{Norm}(\mathfrak{a}))} \left(\frac{n}{\mathrm{Norm}(\mathfrak{a})}\right). \tag{6.3}$$

The following is yet another characterization of primitive ideals.

Lemma 16. *Suppose $\mathfrak{a} \subset \mathbb{Z}[\sqrt{2}]$ is an odd ideal. Then $\mathfrak{a}$ is primitive if and only if* $\gcd(\mathfrak{a}, \overline{\mathfrak{a}}) = (1)$.

Proof. If $\mathfrak{a}$ is not primitive, then there is a rational prime p dividing $\mathfrak{a}$. As p is rational, it also divides $\overline{\mathfrak{a}}$, and so $\gcd(\mathfrak{a}, \overline{\mathfrak{a}}) \neq (1)$. Conversely, if $\gcd(\mathfrak{a}, \overline{\mathfrak{a}}) \neq (1)$, then there is a prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\sqrt{2}]$ such that both $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ divide $\mathfrak{a}$. If $\mathfrak{p}$ is a prime of degree 2, then $\mathfrak{p} = (p)$ for some rational prime p and automatically $\mathfrak{a}$ is not primitive. Otherwise, as $\mathfrak{a}$ is odd and the only prime that ramifies in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is 2, we conclude that $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are coprime, and hence that $\mathfrak{p}\overline{\mathfrak{p}}$ divides $\mathfrak{a}$. Once again, as $\mathfrak{p}\overline{\mathfrak{p}} = (p)$ for a rational prime p, $\mathfrak{a}$ is not primitive. □

Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathbb{Z}[\sqrt{2}]$. If one of $\mathfrak{a}$ and $\mathfrak{b}$ is not primitive, then clearly their product $\mathfrak{a}\mathfrak{b}$ is not primitive. Even if both $\mathfrak{a}$ and $\mathfrak{b}$ are primitive, the product $\mathfrak{a}\mathfrak{b}$ need *not* be primitive. Nonetheless, we have the following lemma.

Lemma 17. *Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are primitive. Let $\mathfrak{r} = \gcd(\mathfrak{a}, \overline{\mathfrak{b}})$ and $r = \mathrm{Norm}(\mathfrak{r})$. Then $\mathfrak{a}\mathfrak{b}/(r)$ is primitive. In particular, $\mathfrak{a}\mathfrak{b}$ is primitive if and only if* $\gcd(\mathfrak{a}, \overline{\mathfrak{b}}) = (1)$.

Proof. Suppose p is a rational prime such that p divides $\mathfrak{a}\mathfrak{b}$. Then (p) cannot be a prime in $\mathbb{Z}[\sqrt{2}]$, because otherwise either $\mathfrak{a}$ or $\mathfrak{b}$ is not primitive. Hence there exists a prime ideal $\mathfrak{p} \subset \mathbb{Z}[\sqrt{2}]$ such that $p = \mathfrak{p}\overline{\mathfrak{p}}$ and $\mathfrak{p} | \mathfrak{a}$. If p^k is the exact power of p dividing $\mathfrak{a}\mathfrak{b}$, then the assumption that $\mathfrak{a}$ and $\mathfrak{b}$ are primitive implies that $\mathfrak{p}^k | \mathfrak{a}$ and $\overline{\mathfrak{p}}^k | \mathfrak{b}$, which is true if and only if $\mathfrak{p}^k | \mathfrak{r}$. □

There is another way to obtain a primitive ideal from a product of two odd primitive ideals $\mathfrak{a}$ and $\mathfrak{b}$. We can write

$$\mathfrak{a} = \prod_{p \text{ split}} \mathfrak{p}^{a_p}\overline{\mathfrak{p}}^{\overline{a}_p} \qquad \text{and} \qquad \mathfrak{b} = \prod_{p \text{ split}} \mathfrak{p}^{b_p}\overline{\mathfrak{p}}^{\overline{b}_p},$$

where $a_p\overline{a}_p = b_p\overline{b}_p = 0$ for every p. Let $\mathfrak{r} = \gcd(\mathfrak{a}, \mathfrak{b})$ and let $r = \text{Norm}(\mathfrak{r})$. If a prime p divides r, after possibly interchanging the roles of $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ in the products above, we can assume that $\mathfrak{p}$ divides $\mathfrak{r}$. For every such prime p, define

$$\mathfrak{c}_{a,p} = \begin{cases} \mathfrak{p}^{a_p} & \text{if } a_p \leq \overline{b}_p, \\ 1 & \text{otherwise,} \end{cases} \qquad \text{and} \qquad \mathfrak{c}_{b,p} = \begin{cases} 1 & \text{if } a_p \leq \overline{b}_p, \\ \overline{\mathfrak{p}}^{\overline{b}_p} & \text{otherwise,} \end{cases}$$

and set

$$\mathfrak{c}_a = \prod_p \mathfrak{c}_{a,p}, \qquad \mathfrak{c}_b = \prod_p \mathfrak{c}_{b,p}, \qquad \text{and} \qquad \mathfrak{c} = \mathfrak{c}_a\mathfrak{c}_b.$$

Then clearly

$$\text{Norm}(\mathfrak{c}) = \text{Norm}(\mathfrak{r}) = r.$$

Moreover, by construction

$$\gcd\left(\frac{\mathfrak{a}}{\mathfrak{c}_a}, \frac{\mathfrak{b}}{\mathfrak{c}_b}\right) = (1),$$

so by Lemma 16, we conclude $\mathfrak{a}\mathfrak{b}/\mathfrak{c}$ is primitive. By construction, $\mathfrak{c}$ is also primitive and coprime to $\mathfrak{a}\mathfrak{b}/\mathfrak{c}$. Therefore, using the Chinese Remainder Theorem and applying (6.1) twice, we conclude that

$$\mathbb{Z}[\sqrt{2}]/\mathfrak{a}\mathfrak{b} \cong \mathbb{Z}[\sqrt{2}]/(\mathfrak{a}\mathfrak{b}/\mathfrak{c}) \times \mathbb{Z}[\sqrt{2}]/\mathfrak{c} \cong \mathbb{Z}/(W/r) \times \mathbb{Z}/(r), \tag{6.4}$$

where $W = \text{Norm}(\mathfrak{a}\mathfrak{b})$.

Finally, we say that an element $w \in \mathbb{Z}[\sqrt{2}]$ is *primitive* if and only if the principal ideal generated by w is primitive. An equivalent definition is that $w = a + b\sqrt{d}$ is odd and $\gcd(a, b) = 1$.

6.2. **A quasi-bilinear symbol with a reciprocity law.**

For $w, z \in \mathbb{Z}[\sqrt{2}]$ with w odd, we define the *generalized Dirichlet symbol* $\gamma(w, z)$ to be

$$\gamma(w, z) := \left(\frac{\overline{wz}}{(w)}\right), \tag{6.5}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the quadratic residue symbol in $\mathbb{Q}(\sqrt{2})$. Our choice of terminology is inspired by the Dirichlet symbol defined in a slightly different context in [11, Section 19, p. 1018-1021].

The symbol $\gamma(w, z)$ factors as

$$\gamma(w, z) = \text{m}(w)\left(\frac{z}{(\overline{w})}\right), \tag{6.6}$$

where, for odd $w \in \mathbb{Z}[\sqrt{2}]$, we define

$$\text{m}(w) := \gamma(w, 1) = \left(\frac{\overline{w}}{(w)}\right). \tag{6.7}$$

By Lemma 6.2, if $w \in \mathbb{Z}[\sqrt{2}]$ is odd, then

$$\mathrm{m}(w) \neq 0 \Longleftrightarrow \gcd((w), (\overline{w})) = (1) \Longleftrightarrow w \text{ is primitive.}$$

Hence the factor $\mathrm{m}(w)$ restricts the support of $\gamma(w, z)$ to w that are primitive. Furthermore, if w is primitive, then $\gcd((w), (\overline{wz})) = \gcd((w), (\overline{z}))$, and so in this case $\gamma(w, z) = 0$ if and only if $\gcd((w), (\overline{z})) \neq (1)$.

The factor $\left(\frac{z}{(\overline{w})}\right)$ is completely multiplicative in z, so it follows from (6.6) that

$$\gamma(w, z_1)\gamma(w, z_2) = \gamma(w, z_1 z_2)\mathrm{m}(w), \tag{6.8}$$

for any w, z_1, and z_2 in $\mathbb{Z}[\sqrt{2}]$ such that w is odd. Hence the symbol $\gamma(w, z)$ is multiplicative in z except for a twist by $\mathrm{m}(w)$.

The symbol $\gamma(w, z)$ also satisfies a reciprocity law, which is an important ingredient in our proof of Proposition 7.

Lemma 18. *Let $w, z \in \mathbb{Z}[\sqrt{2}]$ such that both w and z are odd. Then*

$$\gamma(w, z)\gamma(z, w) = \mathrm{m}(wz).$$

Proof. We have

$$\gamma(w, z)\gamma(z, w) = \left(\frac{\overline{wz}}{(w)}\right)\left(\frac{\overline{zw}}{(z)}\right) = \left(\frac{\overline{wz}}{(wz)}\right) = \mathrm{m}(wz).$$

□

Finally, we note that $\gamma(w, z)$ is periodic in the second argument. In fact, $\gamma(w, z_1) = \gamma(w, z_2)$ whenever $z_1 \equiv z_2 \bmod (\overline{w})$. In other words, $\gamma(w, \cdot)$ is a function on $\mathbb{Z}[\sqrt{2}]/(\overline{w})$. This allows us to prove the following analogue of [11, Lemma 21.1, p. 1025], which will provide all of the cancellation that we need for Proposition 7.

Lemma 19. *Let $w_1, w_2 \in \mathbb{Z}[\sqrt{2}]$ be primitive. Let $\mathfrak{r} = \gcd((w_1), (\overline{w}_2))$, $r = \mathrm{Norm}(r)$, $W = \mathrm{Norm}(w_1 w_2)$. Then*

$$\left|\sum_{z \in \mathbb{Z}[\sqrt{2}]/(W)} \gamma(w_1, z)\gamma(w_2, z)\right| = \begin{cases} W\varphi(r)\varphi(W/r) & \text{if } W \text{ and } r \text{ are squares} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By (6.6), we have

$$\gamma(w_1, z)\gamma(w_2, z) = \mathrm{m}(w_1)\mathrm{m}(w_2)\left(\frac{\overline{z}}{(w_1 w_2)}\right),$$

and, as w_1 and w_2 are odd and primitive, $\mathrm{m}(w_1)\mathrm{m}(w_2) \neq 0$. Hence

$$\left|\sum_{z \in \mathbb{Z}[\sqrt{2}]/(W)} \gamma(w_1, z)\gamma(w_2, z)\right| = \left|\sum_{z \in \mathbb{Z}[\sqrt{2}]/(W)} \left(\frac{\overline{z}}{(w_1 w_2)}\right)\right|.$$

Now, as W is rational, the map $z \mapsto \overline{z}$ is an automorphism of the group $\mathbb{Z}[\sqrt{2}]/(W)$. Thus, we obtain

$$\sum_{z \in \mathbb{Z}[\sqrt{2}]/(W)} \left(\frac{\overline{z}}{(w_1 w_2)}\right) = \sum_{z \in \mathbb{Z}[\sqrt{2}]/(W)} \left(\frac{z}{(w_1 w_2)}\right).$$

As $\left(\frac{\cdot}{(w_1w_2)}\right)$ is already a function on $\mathbb{Z}[\sqrt{2}]/(w_1w_2)$, and

$$\#\left(\mathbb{Z}[\sqrt{2}]/(W)\right) = W \cdot \#\left(\mathbb{Z}[\sqrt{2}]/(w_1w_2)\right),$$

we have

$$\sum_{z\in\mathbb{Z}[\sqrt{2}]/(W)} \left(\frac{z}{(w_1w_2)}\right) = W \sum_{z\in\mathbb{Z}[\sqrt{2}]/(w_1w_2)} \left(\frac{z}{(w_1w_2)}\right).$$

By (6.4), we have

$$\mathbb{Z}[\sqrt{2}]/(w_1w_2) \cong \mathbb{Z}[\sqrt{2}]/(\alpha) \times \mathbb{Z}[\sqrt{2}]/(\beta),$$

where (α) and (β) are coprime primitive ideals of norm W/r and r, respectively, satisfying $(w_1w_2) = (\alpha\beta)$. Hence

$$\sum_{z\in\mathbb{Z}[\sqrt{2}]/(w_1w_2)} \left(\frac{z}{(w_1w_2)}\right) = \sum_{\substack{z_{01} \bmod \alpha \\ z_{02} \bmod \beta}}\sum \left(\frac{z}{(\alpha\beta)}\right),$$

where

$$z = z_{01}\cdot\beta\cdot\beta' + z_{02}\cdot\alpha\cdot\alpha'$$

and α' and β' are some elements of $\mathbb{Z}[\sqrt{2}]$ such that $\alpha\alpha' \equiv 1 \bmod \beta$ and $\beta\beta' \equiv 1 \bmod \alpha$. With these choices, we have

$$\left(\frac{z}{(\alpha\beta)}\right) = \left(\frac{z}{(\alpha)}\right)\left(\frac{z}{(\beta)}\right) = \left(\frac{z_{01}}{(\alpha)}\right)\left(\frac{z_{02}}{(\beta)}\right).$$

Then, by (6.3), we have

$$\sum_{z_{01} \bmod \alpha} \left(\frac{z_{01}}{(\alpha)}\right) \sum_{z_{02} \bmod \beta} \left(\frac{z_{02}}{(\beta)}\right) = \sum_{a\in\mathbb{Z}/(W/r)} \left(\frac{a}{W/r}\right) \sum_{b\in\mathbb{Z}/(r)} \left(\frac{b}{r}\right),$$

where the symbols on the right-hand side of the equality are the usual Jacobi symbols. For any positive integer n, we have

$$\sum_{a\in\mathbb{Z}/(n)} \left(\frac{a}{n}\right) = \begin{cases} \varphi(n) & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases}$$

Combining all of the equations above, we conclude the proof of the proposition. □

We conclude this section by expressing $\gamma(w, z)$ as a Jacobi symbol. Suppose $w = a + b\sqrt{2}$ and $z = c + d\sqrt{2}$, with w primitive and totally positive. Then

$$\left(\frac{\overline{wz}}{(w)}\right) = \left(\frac{wz + \overline{wz}}{(w)}\right) = \left(\frac{2ac + 4bd}{a^2 - 2b^2}\right).$$

Moreover, as w is primitive, every prime factor of $\mathrm{Norm}(w) = a^2 - 2b^2$ is congruent to ±1 modulo 8, so $\left(\frac{2}{a^2-2b^2}\right) = 1$. Hence

$$\gamma(w, z) = \left(\frac{ac + 2bd}{a^2 - 2b^2}\right). \tag{6.9}$$

6.3. **Double oscillation of $\gamma(w,z)$.** We can now prove some general bilinear sum estimates that we will use to deduce Proposition 7. Let $\alpha = \{\alpha_w\}$ and $\beta = \{\beta_z\}$ be two sequences of complex numbers, each indexed by non-zero elements in $\mathbb{Z}[\sqrt{2}]$, such that

$$|\alpha_w| \leq \log(\mathrm{Norm}(w))\tau(w) \text{ and } |\beta_z| \leq \log(\mathrm{Norm}(z))\tau(z) \tag{6.10}$$

for all w and z in $\mathbb{Z}[\sqrt{2}]$. For a positive real number X, let $\mathcal{D}(X) = \mathcal{D}_0(X)$ as in (4.3). Set

$$C := \limsup_{X\to\infty}\{u : \ (u,v) \in \mathcal{D}(X)\} \cdot X^{-\frac{1}{2}}.$$

and note that $C < \infty$. Next, for a positive real number X, we define the "cone"

$$\mathcal{B}(X) := \{(u,v) \in \Omega : \ 0 < u \leq CX^{\frac{1}{2}}\},$$

where Ω is the region, defined in (4.1), which enumerates the totally positive elements in $\mathbb{Z}[\sqrt{2}]$. Hence the set of elements in $\mathbb{Z}[\sqrt{2}]$ enumerated by $\cup_{X>0}\mathcal{B}(X) = \Omega$ is closed under multiplication. Note also that $\mathcal{D}(X) \subset \mathcal{B}(X)$ for every real number X. For a subset $\mathcal{S}$ of $\mathbb{R}^2$ and an element $u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, we will say that $u + v\sqrt{2} \in \mathcal{S}$ to mean that $(u,v) \in \mathcal{S} \cap \mathbb{Z}^2$. Finally, for positive real numbers M and N, we define the bilinear sum

$$Q(M,N;\alpha,\beta) := \sum_{w\in\mathcal{D}(M)}{}^{*} \sum_{z\in\mathcal{B}(N)} \alpha_w\beta_z\gamma(w,z), \tag{6.11}$$

where $\sum^{*}_{w}$ restricts the summation to primitive w. The first result we prove is a standard consequence of the Cauchy-Schwartz inequality and Lemma 19.

Lemma 20. *For every $\epsilon > 0$, there is a constant $C_\epsilon > 0$ such that for every pair of sequences of complex numbers $\alpha = \{\alpha_w\}$ and $\beta = \{\beta_z\}$ satisfying* (6.10) *and every pair of real numbers $M, N > 1$, we have*

$$|Q(M,N;\alpha,\beta)| \leq C_\epsilon\left(M^{\frac{1}{2}}N + M^2N^{\frac{3}{4}} + M^3N^{\frac{1}{2}}\right)(MN)^\epsilon.$$

Proof. Let $Q(M,N) = Q(M,N;\alpha,\beta)$. Applying the Cauchy-Schwarz inequality to the sum over z and expanding the square, we obtain

$$|Q(M,N)|^2 \leq \sum_{z\in\mathcal{B}(N)}|\beta_z|^2 \sum_{w_1\in\mathcal{D}(M)}{}^{*} \sum_{w_2\in\mathcal{D}(M)}{}^{*} \alpha_{w_1}\overline{\alpha_{w_2}}R(N;w_1,w_2),$$

where

$$R(N;w_1,w_2) = \sum_{z\in\mathcal{B}(N)}\gamma(w_1,z)\gamma(w_2,z).$$

Since β_z is bounded in modulus by N^ϵ, Lemma 15 applied to $L = \mathrm{Id}$ gives

$$\sum_{z\in\mathcal{B}(N)}|\beta_z|^2 \ll_\epsilon N^\epsilon\mathrm{Vol}(\mathcal{B}(N)) + N^\epsilon O(\mathrm{Vol}(\partial(\mathcal{B}(N))) + 1) \ll_\epsilon N^{1+\epsilon}. \tag{6.12}$$

Next, recall that $\gamma(w,z_1) = \gamma(w,z_2)$ whenever $z_1 \equiv z_2 \bmod \mathrm{Norm}(w)$. Hence we can split the inner sum over z into residue classes modulo W. More precisely, if

$\zeta = \zeta_1 + \zeta_2\sqrt{2}$, we define L to be the linear transformation $L = W \cdot \mathrm{Id} + (\zeta_1, \zeta_2) : \mathbb{R}^2 \to \mathbb{R}^2$. Then Lemma 15 gives

$$\begin{aligned} R(N; w_1, w_2) &= \sum_{\zeta \bmod W} \gamma(w_1, \zeta)\gamma(w_2, \zeta) \sum_{\substack{z \in \mathcal{B}(N) \\ z \equiv \zeta \bmod W}} 1 \\ &= \sum_{\zeta \bmod W} \gamma(w_1, \zeta)\gamma(w_2, \zeta) \left(\frac{2C^2N}{W^2} + O\left(\frac{N^{\frac{1}{2}}}{W} + 1 \right) \right) \\ &= \frac{2C^2N}{W^2} \sum_{\zeta \bmod W} \gamma(w_1, z)\gamma(w_2, z) + O\left(W^2 \left(\frac{N^{\frac{1}{2}}}{W} + 1 \right) \right). \end{aligned}$$

Now set $r = \mathrm{Norm}(\gcd((w_1), (\overline{w}_2)))$. Note that $W\varphi(r)\varphi(W/r) \leq W^2$. Then using Lemma 19, we obtain the estimate

$$R(N; w_1, w_2) \ll \begin{cases} N + WN^{\frac{1}{2}} + W^2 & \text{if } W \text{ and } r \text{ are squares} \\ WN^{\frac{1}{2}} + W^2 & \text{otherwise.} \end{cases}$$

By unique factorization in $\mathbb{Z}[\sqrt{2}]$, the number of primitive elements $w \in \mathcal{D}$ such that $\mathrm{Norm}(w) = n$ is at most $2^{\omega(n)} \leq \tau(n) \ll_\epsilon n^\epsilon$. Hence, using the bound $W \ll M^2$ and setting $m_1 = \mathrm{Norm}(w_1)$ and $m_2 = \mathrm{Norm}(w_2)$, we get

$$\begin{aligned} &|Q(M, N)|^2 \\ &\ll_\epsilon N \left(\sum\sum_{\substack{m_1, m_2 \leq M \\ m_1 m_2 = \square}} \left(N + M^2N^{\frac{1}{2}} + M^4 \right) + M^2 \left(M^2N^{\frac{1}{2}} + M^4 \right) \right) (MN)^\epsilon. \end{aligned}$$

We deduce that

$$Q(M, N) \ll_\epsilon \left(M^{\frac{1}{2}}N + M^{\frac{3}{2}}N^{\frac{3}{4}} + M^{\frac{5}{2}}N^{\frac{1}{2}} + M^2N^{\frac{3}{4}} + M^3N^{\frac{1}{2}} \right) (MN)^\epsilon,$$

and the inequality $M \geq 1$ now implies the desired result. □

The following method, which appears in [11], exploits the multiplicativity of $\gamma(w, z)$ in z to improve the quality of the estimate when M and N are close to each other.

Lemma 21. *For every $\epsilon > 0$, there is a constant $C_\epsilon > 0$ such that for every pair of sequences of complex numbers $\alpha = \{\alpha_w\}$ and $\beta = \{\beta_z\}$ satisfying* (6.10) *and every pair of real numbers $M, N > 1$, we have*

$$|Q(M, N; \alpha, \beta)| \leq C_\epsilon \left(M^{\frac{11}{12}}N + M^{\frac{7}{6}}N^{\frac{3}{4}} + M^{\frac{4}{3}}N^{\frac{1}{2}} \right) (MN)^\epsilon.$$

Proof. Let $Q(M, N) = Q(M, N; \alpha, \beta)$. We apply Hölder's inequality to get

$$|Q(M, N)|^6 \leq \left({\sum_w}^* |\alpha_w|^{\frac{6}{5}} \right)^5 {\sum_w}^* \left| \sum_z \beta_z \gamma(w, z) \right|^6. \tag{6.13}$$

By (6.8), we can write the second factor above as

$${\sum_w}^* \left| \sum_z \beta_z \gamma(w, z) \right|^6 =: {\sum_{w \in \mathcal{D}(M)}}^* \sum_{z \in \Omega} \alpha'_w \beta'_z \gamma(w, z), \tag{6.14}$$

where $\alpha'_w = \mathrm{m}(w)^5$ and

$$\beta'_z = \sum_{\substack{z_1 \cdots z_6 = z \\ z_1, \ldots, z_6 \in \mathcal{B}(N)}} \beta_{z_1} \overline{\beta_{z_2}} \cdots \beta_{z_5} \overline{\beta_{z_6}}.$$

Note that β_z is supported on $z \in \mathcal{B}(27C^6N^3)$. Now using Lemma 20 to estimate the sum (6.14), and substituting back into (6.13), we obtain the desired result. □

The final step is to exploit the symmetry of the symbol $\gamma(w, z)$ coming from its reciprocity law. Suppose that $w = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is primitive and totally positive. By (6.9) and the law of quadratic reciprocity, we have

$$\mathrm{m}(w) = \gamma(w, 1) = \left(\frac{a}{a^2 - 2b^2}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{a^2 - 2b^2 - 1}{2}} \left(\frac{-2}{a}\right),$$

and so $\mathrm{m}(w) \in \{\pm 1\}$ depends only on the residue class of w modulo $8\mathbb{Z}[\sqrt{2}]$. Lemma 18 then implies that for every pair of odd and totally positive $w, z \in \mathbb{Z}[\sqrt{2}]$, we have

$$\gamma(w, z) = \delta \cdot \gamma(z, w),$$

where $\delta = \delta(w \bmod 8, z \bmod 8) := \mathrm{m}(wz) \in \{\pm 1\}$ depends only on the congruence classes of w and z modulo $8\mathbb{Z}[\sqrt{2}]$. We are thus led to decompose the sum $Q(M, N; \alpha, \beta)$ as

$$Q(M, N; \alpha, \beta) = \sum_{\substack{w_0 \bmod 8 \\ z_0 \bmod 8}} \sum Q(M, N; \alpha(w_0), \beta(z_0)),$$

where $\alpha(w_0)$ and $\beta(z_0)$ are sequences indexed by non-zero elements of $\mathbb{Z}[\sqrt{2}]$ defined by

$$\alpha(w_0)_w := \alpha_w \cdot \mathbf{1}(w \equiv w_0 \bmod 8)$$

and

$$\beta(z_0)_z := \beta_z \cdot \mathbf{1}(z \equiv z_0 \bmod 8).$$

Here $\mathbf{1}(P)$ is the indicator function of a property P. We will now prove

Lemma 22. *For every $\epsilon > 0$, there is a constant $C_\epsilon > 0$ such that for every pair of sequences of complex numbers $\alpha = \{\alpha_w\}$ and $\beta = \{\beta_z\}$ such that* (6.10) *holds and such that β is supported on primitive $z \in \mathcal{D}(N)$, and for every pair of real numbers $M, N > 1$, we have*

$$|Q(M, N; \alpha, \beta)| \leq C_\epsilon \, (M + N)^{\frac{1}{12}} \, (MN)^{\frac{11}{12} + \epsilon}.$$

Proof. It suffices to establish the desired estimate for the sequences $\alpha(w_0)$ and $\beta(z_0)$ for each pair of congruence classes w_0 and z_0 modulo $8\mathbb{Z}[\sqrt{2}]$. So fix congruence classes w_0 and z_0 modulo $8\mathbb{Z}[\sqrt{2}]$. Note that the sum $Q(N, M; \beta(z_0), \alpha(w_0))$ satisfies the assumptions of Lemma 21. Thus, applying Lemma 21 gives the estimate

$$Q(M, N; \alpha(w_0), \beta(z_0)) \ll_\epsilon \left(M^{\frac{11}{12}} N + M^{\frac{7}{6}} N^{\frac{3}{4}} + M^{\frac{4}{3}} N^{\frac{1}{2}}\right) (MN)^\epsilon. \tag{6.15}$$

As discussed above, by Lemma 18, we have

$$Q(M, N; \alpha(w_0), \beta(z_0)) = \delta(w_0, z_0) \cdot Q(N, M; \beta(z_0), \alpha(w_0)).$$

Applying Lemma 21 to the right-hand side above, we also get

$$Q(M,N;\alpha(w_0),\beta(z_0)) \ll_\epsilon \left(N^{\frac{11}{12}}M + N^{\frac{7}{6}}M^{\frac{3}{4}} + N^{\frac{4}{3}}M^{\frac{1}{2}}\right)(MN)^\epsilon. \tag{6.16}$$

Finally, taking the minimum of the terms in (6.15) and (6.16) in the appropriate ranges, we obtain

$$Q(M,N;\alpha(w_0),\beta(z_0)) \ll_\epsilon \left(M^{\frac{11}{12}}N + N^{\frac{11}{12}}\right)(MN)^\epsilon,$$

and then the inequality

$$M^{\frac{1}{12}} + N^{\frac{1}{12}} \leq 2\max\{M,N\}^{\frac{1}{12}} \leq 2(M+N)^{\frac{1}{12}}$$

gives the desired result. □

6.4. **Twisted multiplicativity of governing symbols.** Recall that if $u+v\sqrt{2}$ is a totally positive odd element of $\mathbb{Z}[\sqrt{2}]$, we defined 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 (3.2) 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' modulo 16.

The following proposition is analogous to [11, Lemma 20.1, p. 1021]. It is perhaps the most surprising part of the proof of Proposition 7.

Proposition 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, by (6.9),

$$[wz] \sim \left(\frac{-2bc}{\rho}\right)\left(\frac{a_1d_1}{a_1c+2bd_1}\right)\gamma(w,z)$$

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

$$r_1 = a_1c+2bd_1.$$

Similarly, we write d_1 as

$$d_1 = 2^e d_2,$$

where d_2 is odd, and compute that

$$\left(\frac{d_1}{a_1c+2bd_1}\right) = (-1)^{\nu_2(a,b,c,d,\rho)}\left(\frac{d_1}{a_1c}\right),$$

where now

$$\nu_2(a,b,c,d,\rho) \equiv e\frac{r_1^2-1}{8} + \frac{d_2-1}{2}\cdot\frac{r_1-1}{2} + \frac{d_2-1}{2}\cdot\frac{a_1c-1}{2} + e\frac{a_1^2c^2-1}{8} \bmod 2.$$

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 $r_1 \equiv a_1c \bmod 8$. 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 $r_1 \equiv a_1c \bmod 8$ 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 mod 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. □

6.5. **Proof of Proposition 7.** We are now ready to conclude the proof of Proposition 7. The bilinear sum (3.2) can be written as

$$B(M, N) = \sum_{k=0}^{3} B_k(M, N),$$

where

$$B_k(M, N) = \sum_{w \in \mathcal{D}(M)} \sum_{z \in \mathcal{D}(N)} \alpha_w \beta_z [\varepsilon^{2k} wz]_{\phi,\psi}. \tag{6.17}$$

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 (6.17) for each $0 \leq k \leq 3$. First, suppose $u + v\sqrt{2} \succ 0$ is primitive and odd. Then by Proposition 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 (6.17) 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

$$\sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv w_0 \bmod 16}} \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv z_0 \bmod 16}} \alpha_w \beta_z [wz].$$

Unless both w and z are primitive, wz is not primitive, and hence $[wz] = 0$. Using Proposition 8 again and replacing α_w by $\alpha_w[w]\mathbf{1}(w \equiv w_0 \bmod 16)$ and β_z by $\beta_z[z]\mathbf{1}(w \equiv w_0 \bmod 16)$, it now suffices to estimate sums of the type

$$\sideset{}{^*}\sum_{w \in \mathcal{D}(M)} \sideset{}{^*}\sum_{z \in \mathcal{D}(N)} \alpha_w \beta_z \gamma(w, z).$$

This is exactly a sum of the type $Q(M, N; \alpha, \beta)$ as in Lemma 22, and so Proposition 7 follows. This completes the proof of Theorem 3 and hence also Theorem 2.

7. 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 [22, 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 cardinality,

$$\pi(M,S_1,X) - \pi(M,S_2,X) \ll \#S_1X\exp(-cd^{-1/2}\log^{1/2}X)$$

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

$$\#\{p \leq X \text{ prime}: \ p \equiv 1 \bmod 4\} - \#\{p \leq X \text{ prime}: \ p \equiv -1 \bmod 4\} \ll X^{0.9999}.$$

However, we have the following result.

Theorem 4. *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*

$$\pi(M,S_1,X) - \pi(M,S_2,X) \ll X^{\frac{199}{200}}$$

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 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.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] H. Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, 26:179–183, 1951.

[6] H. Davenport. Corrigendum: "On a principle of Lipschitz". *J. London Math. Soc.*, 39:580, 1964.

[7] Étienne Fouvry and Jürgen Klüners. On the 4-rank of class groups of quadratic number fields. *Invent. Math.*, 167(3):455–513, 2007.

[8] Étienne Fouvry and Jürgen Klüners. On the negative Pell equation. *Ann. of Math. (2)*, 172(3):2035–2104, 2010.

[9] 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.

[10] J. B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin. The spin of prime ideals. *Invent. Math.*, 193(3):697–749, 2013.

[11] John Friedlander and Henryk Iwaniec. The polynomial $X^2 + Y^4$ captures its primes. *Ann. of Math. (2)*, 148(3):945–1040, 1998.

[12] 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.

[13] 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.

[14] Helmut Hasse. Über die Klassenzahl des Körpers $P(\sqrt{}-2p)$ mit einer Primzahl $p \neq 2$. *J. Number Theory*, 1:231–234, 1969.

[15] 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.

[16] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.

[17] 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.

[18] Daniel A. Marcus. *Number fields.* Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[19] 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.

[20] Hans Reichardt. Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 170:75–82, 1934.

[21] Jean-Pierre Serre. Minerva Lectures 2012 - J.P. Serre Talk 1: Equidistribution.

[22] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[23] 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.

[24] Peter Stevenhagen. Divisibility by 2-powers of certain quadratic class numbers. *J. Number Theory*, 43(1):1–19, 1993.

[25] I. M. Vinogradov. The method of trigonometrical sums in the theory of numbers. *Trav. Inst. Math. Stekloff*, 23:109, 1947.

[26] 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.