Chapter 3

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

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

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

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

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

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

if it exists.

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

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

Furthermore, Hasse [24] proved that

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

Both congruence conditions on p in the criteria above can be interpreted as splitting conditions on p in the degree-8 cyclotomic extension $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$. Now

the Čhebotarev's Density Theorem implies that $\rho(2^k;-1) = 2^{-k}$ for $1 \leq k \leq 3$.

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

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

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

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

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

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

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

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

Theorem B gives a positive answer to Conjecture 3.1 for $k = 4$ *without appealing to a governing field.* Instead, we use a criterion for the 16-rank of $\mathrm{Cl}(-8p)$ that is conducive to analytic techniques. In [30, Theorem 3, p.205], Leonard

and Williams stated the following criterion. A prime $p \equiv -1 \bmod 16$ can be written as

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

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

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

Given such a representation, we have

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

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

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

Hence Theorem B is a corollary of the following theorem:

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

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

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

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

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

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

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

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

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

3.1 Governing symbols

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

Let χ be a character $(\mathbb{Z}/16\mathbb{Z})^\times \to \mathrm{Cl}^\times$ with kernel $\{\pm 1\}$. In other words,

we have $\chi(\pm 1 \bmod 16) = 1$ and $\chi(\pm 7 \bmod 16) = -1$. Then our generalization of [30, Theorem 3, p.205] is as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Then

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

In other words, we have the equality of Jacobi symbols

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

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

3.1.1 Preliminaries

We will use the following lemma several times.

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

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

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

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

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

Ring class fields

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

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

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

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

for some positive integer f, called the *conductor* of $\mathcal{O}_D$. Let $\mathrm{Cl}(D)$ denote the class group of $\mathcal{O}_D$. Then there is a unique abelian extension R_D/K called the

ring class field of $\mathcal{O}_D$ such that the Artin map induces a canonical isomorphism of groups

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

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

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

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

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

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

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

3.1.2 A special family of quadratic fields

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

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

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

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

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

$$n = d^2 m.$$

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

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

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

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

We define a quadratic extension G/K by

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

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

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

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

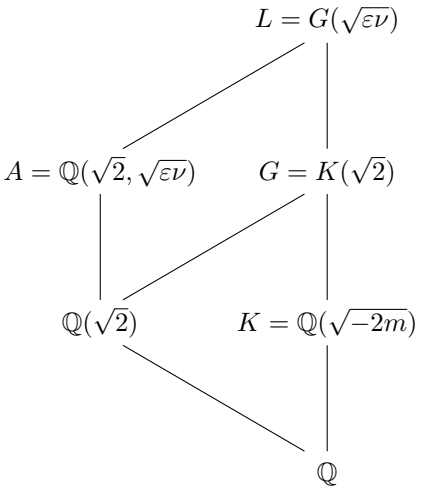
Then let

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

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

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

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



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

Proof. We have

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

As

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

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

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

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

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

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

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

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

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

1. *If $v \equiv 1 \bmod 4$, then L/K is unramified and $\mathfrak{f} = 1$.*
2. *If $v \equiv -1 \bmod 4$, then $\mathfrak{f} = \mathfrak{t}^2 = (2)$.*
3. *If $v \equiv 0 \bmod 2$, then $\mathfrak{f} = \mathfrak{t}^4 = (4)$.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

so that

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

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

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

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

3.1.3 A computation of Artin symbols

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

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

We will show how the quantity

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

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

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

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

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

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

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

Let

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

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

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

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

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

We also note that

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

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

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

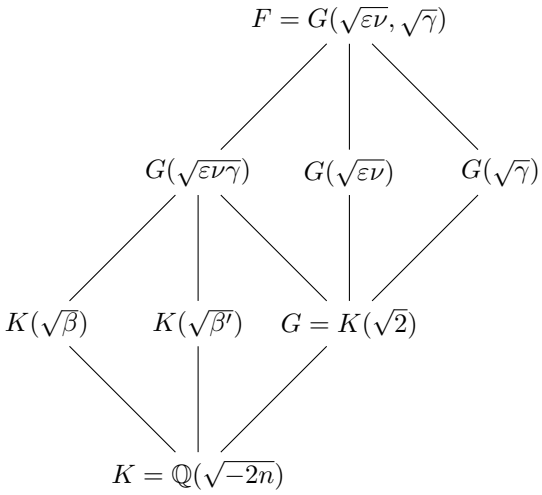
The key idea is to relate this Artin symbol to the Artin symbol associated to a different but related cyclic degree-4 extension of K. Let

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

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

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

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



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

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

we can take

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

and

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

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

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

and

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

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

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

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

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

and

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

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

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

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

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

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

so that, by Lemma 3.7, we have

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

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

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

given by sending

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

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

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

so that if we identify

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

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

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

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

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

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

3.1.4 An ideal identity

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

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

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

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

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

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

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

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

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

3.1.5 Proof of Proposition 3.1

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

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

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

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

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

A class of order 4

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

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

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

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

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

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

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

Generating the 4-Hilbert class field

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

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

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

The following proposition achieves our aim.

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

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

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

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

Conclusion of the proof of Proposition 3.1

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

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

By Lemma 3.8, this occurs if and only if

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

which proves Proposition 3.1.

3.1.6 Proof of Proposition 3.2

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

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

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

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

By the Euclidean algorithm, we have the equality

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

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

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

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

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

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

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

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

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

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

so that

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

Therefore

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

Let

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

We claim that

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

We first note that

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

Expanding α^2, we get

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

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

Now (3.18) and (3.19) imply that

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

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

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

which proves the lemma. □

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

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

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

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

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

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

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

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

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

Applying Lemma 3.8, we get

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

Equation (3.16) implies that

$$u_2 = 577u_1 + 816v_1 \equiv u_1 \bmod 16. \tag{3.24}$$

Hence, as χ is a character modulo 16, we have $\chi(u_1) = \chi(u_2)$, and so Proposition 3.2 is finally proved.

3.2 Sums over primes

Above, we defined the governing symbol $[p]$ for a prime $p \equiv -1 \bmod 16$ in terms of particular integer solutions u and v to the equation $p = u^2 - 2v^2$. The main lemma that we will use to prove Theorem 3.1, i.e., that these governing symbols oscillate, is a proposition due to Friedlander, Iwaniec, Mazur and Rubin [17]. We now state this proposition in our context.

3.2.1 A result of Friedlander, Iwaniec, Mazur, and Rubin

Recall that an element $w = u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is *totally positive* if and only if $\mathrm{Norm}(w) = u^2 - 2v^2 > 0$ *and* $u > 0$. We sometimes write $w \succ 0$ to say that w is totally positive.

Since $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain and since the norm of the fundamental unit ε over $\mathbb{Q}$ is -1, an ideal $\mathfrak{n}$ in $\mathbb{Z}[\sqrt{2}]$ can always be generated by a totally positive element. For an ideal $\mathfrak{n}$ of $\mathbb{Z}[\sqrt{2}]$, recall that the norm of $\mathfrak{n}$ is given by

$$\mathrm{Norm}(\mathfrak{n}) := u^2 - 2v^2,$$

where $u + v\sqrt{2}$ is a totally positive generator of $\mathfrak{n}$.

We now define an analogue of the von Mangoldt function Λ for the ring $\mathbb{Z}[\sqrt{2}]$. For a non-zero ideal $\mathfrak{n}$ of $\mathbb{Z}[\sqrt{2}]$, we set

$$\Lambda(\mathfrak{n}) = \begin{cases} \log(\mathrm{Norm}(\mathfrak{p})) & \text{if } \mathfrak{n} = \mathfrak{p}^k \text{ for some prime ideal } \mathfrak{p} \text{ and integer } k \geq 1 \\ 0 & \text{otherwise.} \end{cases}$$

Hence Λ is supported on powers of prime ideals.

Given a sequence of complex numbers $\{a_{\mathfrak{n}}\}_{\mathfrak{n}}$ indexed by non-zero ideals in $\mathbb{Z}[\sqrt{2}]$, a good estimate for the sum of $a_{\mathfrak{n}}$ over prime ideals $\mathfrak{p}$ of norm $\mathrm{Norm}(\mathfrak{p}) \leq X$ can usually be derived from a good estimate of the "smoother" weighted sum

$$S(X) := \sum_{\mathrm{Norm}(\mathfrak{n}) \leq X} a_{\mathfrak{n}} \Lambda(\mathfrak{n}).$$

The idea in [17] (and even earlier in [19]), is to bound $S(X)$ by combinations of linear and bilinear sums in $a_{\mathfrak{n}}$. Given a non-zero ideal $\mathfrak{d}$ of $\mathbb{Z}[\sqrt{2}]$, we define the linear sum

$$A_{\mathfrak{d}}(X) := \sum_{\substack{\mathrm{Norm}(\mathfrak{n}) \leq X \\ \mathfrak{n} \equiv 0 \bmod \mathfrak{d}}} a_{\mathfrak{n}}. \tag{3.25}$$

Moreover, given two sequences of complex numbers $\{\alpha_{\mathfrak{m}}\}$ and $\{\beta_{\mathfrak{n}}\}$, each indexed by non-zero ideals in $\mathbb{Z}[\sqrt{2}]$, we define the bilinear sum

$$B(M, N) := \sum_{\mathrm{Norm}(\mathfrak{m}) \leq M} \sum_{\mathrm{Norm}(\mathfrak{n}) \leq N} \alpha_{\mathfrak{m}} \beta_{\mathfrak{n}} a_{\mathfrak{m}\mathfrak{n}}. \tag{3.26}$$

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

$$|\alpha_{\mathfrak{m}}| \leq \Lambda(\mathfrak{m}) \text{ and } |\beta_{\mathfrak{n}}| \leq \tau(\mathfrak{n}), \tag{3.27}$$

where $\tau(\mathfrak{n})$ denotes the number of ideals in $\mathbb{Z}[\sqrt{2}]$ dividing $\mathfrak{n}$. We now state [17, Proposition 5.2, p.722] that we use to prove Theorem 3.1.

Proposition 3.4. *Let $a_{\mathfrak{n}}$ be a sequence of complex numbers bounded by 1 in absolute value and indexed by non-zero ideals of $\mathbb{Z}[\sqrt{2}]$. Suppose that there exist two real numbers $0 < \theta_1, \theta_2 < 1$ such that: for every $\epsilon > 0$, we have*

$$A_{\mathfrak{d}}(X) \ll_{\epsilon} X^{1-\theta_1+\epsilon} \tag{A}$$

uniformly for all non-zero ideals $\mathfrak{d}$ of $\mathbb{Z}[\sqrt{2}]$ and all $X \geq 2$, and

$$B(M,N) \ll_{\epsilon} (M+N)^{\theta_2}(MN)^{1-\theta_2+\epsilon} \tag{B}$$

uniformly for all $M, N \geq 2$ and sequences of complex numbers $\{\alpha_{\mathfrak{m}}\}$ and $\{\beta_{\mathfrak{n}}\}$ satisfying (3.27).
Then for all $X \geq 2$ and all $\epsilon > 0$, we have the bound

$$S(X) \ll_{\epsilon} X^{1-\frac{\theta_1\theta_2}{2+\theta_2}+\epsilon}.$$

In other words, power-saving estimates for linear and bilinear sums imply power-saving estimates for sums supported on primes. Note that this result is now classical in the context of rational integers, thanks to the pioneering work of Vinogradov [44].

3.2.2 Extending governing symbols

In light of Proposition 3.4, our current goal is to define a sequence $a_{\mathfrak{n}}$ over all non-zero ideals $\mathfrak{n}$ of $\mathbb{Z}[\sqrt{2}]$ so that if $p \equiv -1 \bmod 16$ is a prime and $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\sqrt{2}]$ lying above p, then $a_{\mathfrak{p}}$ coincides with the governing symbol $[p]$ defined in (3.6). We first define $[\cdot]$ for all totally positive elements of $\mathbb{Z}[\sqrt{2}]$. We put

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

We remark that $[\cdot]$ is supported on *primitive odd* elements $w \in \mathbb{Z}[\sqrt{2}]$, i.e. $w = u + v\sqrt{2}$ such that $\gcd(u,v) = 1$ and $\mathrm{Norm}(w) = u^2 - 2v^2$ is odd.

If $u + v\sqrt{2} \succ 0$ generates a prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\sqrt{2}]$ lying above a prime $p \equiv -1 \bmod 16$ and if $u \equiv 1 \bmod 16$, then $[u+v\sqrt{2}] = [p]$. The condition $u \equiv 1 \bmod 16$ is useful for two reasons. First, it ensures that $\chi(u) = 1$. Second, for each prime $p \equiv -1 \bmod 16$, there are two prime ideals in $\mathbb{Z}[\sqrt{2}]$ lying above p. If we write their totally positive generators in the form $u + v\sqrt{2}$, then one of them satisfies $v \equiv 1 \bmod 4$ while the other satisfies $v \equiv 3 \mod 4$.

A priori, the definition (3.6) requires us to choose u and v coming from the prime ideal satisfying $v \equiv 1 \bmod 4$. However, if $u \equiv 1 \bmod 16$, then

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

so that $[u + v\sqrt{2}] = [p]$ for *both* of the prime ideals $(u + v\sqrt{2})$ lying above p.

Proposition 3.2 states that $[w] = [\varepsilon^8 w]$ for any $w \in \mathbb{Z}[\sqrt{2}]$, so we might naively define

$$a_{\mathfrak{n}} := [w] + [\varepsilon^2 w] + [\varepsilon^4 w] + [\varepsilon^6 w], \tag{3.28}$$

where $w \succ 0$ is any totally positive generator of $\mathfrak{n}$.

A convenient fact is that if $p \equiv -1 \bmod 16$ is a prime, then exactly one of the four elements $\varepsilon^{2k} w = u_k + v_k\sqrt{2}$ $(0 \le k \le 3)$ satisfies $u_k \equiv 1 \bmod 16$. Indeed, multiplying $u + v\sqrt{2}$ by ε^2 (resp. ε^4) transforms (u, v) into $(3u + 4v, 2u + 3v)$ (resp. $(17u + 24v, 12u + 17v)$). If $p \equiv -1 \bmod 16$, then $u \equiv \pm 1 \bmod 8$ and v is odd. Hence $u_4 \equiv u + 8 \bmod 16$, and one can now easily check that multiplying $u+v\sqrt{2}$ successively by ε^2 cycles u mod 16 through the set $\{1, 7, 9, 15\}$.

The definition (3.28) does not quite suffice for our purposes because we want to isolate those p that are congruent to -1 mod 16 and representations $p = u^2 - 2v^2$ with $u \equiv 1 \bmod 16$. Hence we weight the formula (3.28) by Dirichlet characters modulo 16. More precisely, for each pair of Dirichlet characters ϕ and ψ modulo 16 and totally positive $u + v\sqrt{2}$, we set

$$[u + v\sqrt{2}]_{\phi,\psi} := \left(\frac{v}{u}\right) \phi(-u^2 + 2v^2)\psi(u). \tag{3.29}$$

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

$$a_{\phi,\psi,\mathfrak{n}} := [w]_{\phi,\psi} + [\varepsilon^2 w]_{\phi,\psi} + [\varepsilon^4 w]_{\phi,\psi} + [\varepsilon^6 w]_{\phi,\psi}. \tag{3.30}$$

This is still well-defined, i.e. independent of the choice of $w \succ 0$, by Proposition 3.2 and by (3.24). We will apply Proposition 3.4 to 8^2 sequences $\{a_{\phi,\psi,\mathfrak{n}}\}_{\mathfrak{n}}$, one for each pair of Dirichlet characters ϕ, ψ, and then add together the corresponding 8^2 sums $S_{\phi,\psi}(X)$ to obtain Theorem 3.1. The key lemma is then

Lemma 3.12. *If p is a prime and $\mathfrak{p}$ is a prime ideal lying above p, then we have*

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

Hence, to prove Theorem 3.1, it now suffices to prove

Theorem 3.2. *Let $a_{\phi,\psi,\mathfrak{n}}$ be defined as in* (3.30)*. For every $\epsilon > 0$, there is a constant $C_\epsilon > 0$ depending only on ϵ such that for every $X \geq 2$, we have*

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

3.3 Fundamental domains

In order to obtain power-saving cancellation for linear and bilinear sums as in Proposition 3.4, we will have to choose generators of $\mathfrak{n}$ in (3.30) carefully. The problem reduces to finding a convenient fundamental domain for the action of $\varepsilon^2 = 3 + 2\sqrt{2}$ on totally positive elements of $\mathbb{Z}[\sqrt{2}]$.

In [17], the authors describe how to construct such a fundamental domain in a more general setting. We give simpler arguments tailored to our specific needs and describe a fundamental domain very explicitly. This explicit description along with the ancillary pictures is possible in large part because the degree of the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is 2.

Let

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

Then the lattice points $(u, v) \in \Omega \cap \mathbb{Z}^2$ precisely enumerate the totally positive elements $w = u + v\sqrt{2}$. The ring $\mathbb{Z}[\sqrt{2}]$ acts on itself by multiplication, and this induces an action

$$\mathbb{Z}[\sqrt{2}] \times \Omega \to \Omega$$

given by

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

Since $\mathrm{Norm}(\varepsilon^2) = 1$ and since the norm is multiplicative, it follows immediately that $\varepsilon^2 \cdot \Omega \subset \Omega$.

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

$$\mathcal{D} := \left\{ (u, v) \in \mathbb{R}^2 : u > 0, -u < 2v \leq u \right\} \tag{3.31}$$

We claim that the region $\mathcal{D}$ in Figure 3.1 shown above is a fundamental domain for the action of ε^2 on Ω in the following sense.

Lemma 3.13. *For each element $(u, v) \in \Omega \cap \mathbb{Z}^2$, there exists exactly one integer k such that $\varepsilon^{2k} \cdot (u, v) \in \mathcal{D}$.*

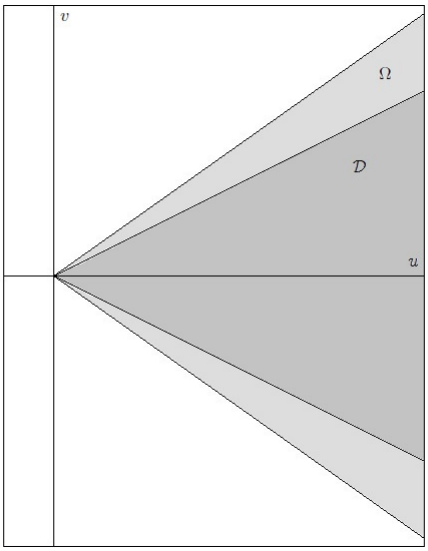


Figure 3.1: The region Ω and the fundamental domain $\mathcal{D}$

Proof. For an element $w = (u, v) \in \mathbb{R}^2$ with $u \neq 0$, define the *slope* of w to be

$$m(w) = \frac{v}{u}.$$

By definition, Ω is the subset of $\mathbb{R}^2$ consisting of w such that $u > 0$ and $|m(w)| < 1/\sqrt{2}$, and $\mathcal{D}$ is the subset of Ω consisting of w such that $-1/2 < m(w) \leq 1/2$.

For each integer k, define integers p_k and q_k by the equation

$$(3 + 2\sqrt{2})^{2k} = p_k + q_k\sqrt{2}.$$

Since $p_k^2 - 2q_k^2 = 1$, it follows that $q_k/p_k \to 1/\sqrt{2}$ as $k \to +\infty$. Moreover, $p_{-k} = p_k$ and $q_{-k} = -q_k$, so that $q_k/p_k \to -1/\sqrt{2}$ as $k \to -\infty$. We will also use the fact that $|q_k/p_k| < 1/\sqrt{2}$.

Now let $w = (u, v) \in \Omega \cap \mathbb{Z}^2$. We have

$$m(\varepsilon^{2k} \cdot w) = \frac{q_k u + p_k v}{p_k u + 2q_k v} = \frac{q_k}{p_k} + \frac{v}{p_k(p_k u + 2q_k v)}.$$

Since u and v are integers, so is $p_k u + 2q_k v$. If $p_k u + 2q_k v = 0$, then

$$\left|\frac{v}{u}\right| = \left|\frac{p_k}{2q_k}\right| > \frac{1}{\sqrt{2}},$$

which contradicts the assumption that $(u, v) \in \Omega$. Hence $p_k u + 2q_k v$ is a non-zero integer, so that $|p_k u + 2q_k v| \geq 1$, and since $p_k \to +\infty$ as $k \to +\infty$, we deduce that

$$m(\varepsilon^{2k} \cdot w) \to \pm \frac{1}{\sqrt{2}}$$

as $k \to \pm\infty$.

Moreover, we have

$$m(\varepsilon^2 \cdot w) - m(w) = \frac{2u + 3v}{3u + 4v} - \frac{v}{u} = \frac{2(u^2 - 2v^2)}{(3u + 4v)u}.$$

As $3\sqrt{2} > 4$, we deduce that

$$3u + 4v > 3\sqrt{2}|v| + 4v \geq 0,$$

and so $m(\varepsilon^2 \cdot w) - m(w) > 0$. Also, as $(u + 2v)^2 \geq 0$, we deduce that

$$2u^2 - 4v^2 \leq 3u^2 + 4uv,$$

so that $m(\varepsilon^2 \cdot w) - m(w) \leq 1$. Hence multiplying $w \in \Omega$ by ε^2 strictly increases its slope by at most 1 and multiplying $w \in \Omega$ by ε^{-2} strictly decreases its slope by at most 1. As $|m(w_1) - m(w_2)| < 1$ for any two elements $w_1, w_2 \in \mathcal{D}$, this proves that for each $w \in \Omega \cap \mathbb{Z}^2$, there exists an integer k such that $\varepsilon^{2k} w \in \mathcal{D}$.

To show that this integer k is unique, it remains to prove that if $w = (u, v) \in \mathcal{D}$, then $\varepsilon^2 \cdot w = (3u + 4v, 2u + 3v) \notin \mathcal{D}$. Suppose for sake of contradiction that $\varepsilon^2 \cdot w \in \mathcal{D}$. Then

$$2(2u + 3v) \leq 3u + 4v,$$

so that $-u \geq 2v$, which contradicts the assumption that $(u, v) \in \mathcal{D}$. □

An immediate consequence of Lemma 3.13 is the following proposition.

Proposition 3.5. *Suppose that* $\mathfrak{n}$ *is a non-zero ideal of* $\mathbb{Z}[\sqrt{2}]$. *Then* $\mathfrak{n}$ *has a unique generator in* $\mathcal{D}$.

3.3.1 Geometry of numbers in the fundamental domain: the Lipschitz principle

We now briefly turn to the problem of counting lattice points and boxes inside certain compact subsets of the fundamental domain $\mathcal{D}$. We state a lemma of Davenport (see [9] and [10]).

Let $\mathcal{R}$ be a compact, Lebesgue measurable subset of $\mathbb{R}^n$. Suppose that $\mathcal{R}$ satisfies the following two conditions:

1. Any line parallel to one of the n coordinate axes intersects $\mathcal{R}$ in a set of points which, if not empty, consists of at most h intervals, and

2. The same is true (with m in place of n) for any of the m-dimensional regions obtained by projecting $\mathcal{R}$ on one of the coordinate spaces defined by equating a selection of $n-m$ of the coordinates to zero; and this condition is satisfied for all m from 1 to $n-1$.

Lemma 3.14 (Davenport)**.** *If $\mathcal{R}$ satisfies conditions (1) and (2) above, then*

$$|\mathcal{R} \cap \mathbb{Z}^n - \mathrm{Vol}(\mathcal{R})| \leq \sum_{m=0}^{n-1} h^{n-m} V_m$$

where V_m is the sum of the m-dimensional volumes of the projections of $\mathcal{R}$ on the various coordinate spaces obtained by equating any $n-m$ coordinates to zero, and $V_0 = 1$ by convention.

We will apply Lemma 3.14 to the fundamental domain $\mathcal{D} \subset \mathbb{R}^2$ as well as certain variations thereof.

Let k be a positive integer, and define

$$\mathcal{D}_k = \mathcal{D} \cup \varepsilon^2 \cdot \mathcal{D} \cdots \cup \varepsilon^{2k} \cdot \mathcal{D}.$$

Let $X > 0$. Then the region

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

is a compact subset of $\mathbb{R}^2$ and satisfies conditions (1) and (2) above with $h = 2$. Moreover, one can check that there exist positive real numbers a_k and ℓ_k such that

$$\mathrm{Vol}(\mathcal{D}_k(X)) = a_k X \tag{3.32}$$

and

$$\mathrm{Vol}(\partial(\mathcal{D}_k(X))) = \ell_k X^{\frac{1}{2}}.$$

Now let $L : \mathbb{R}^2 \to \mathbb{R}^2$ be an invertible linear transformation of the form

$$L\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix},$$

of determinant

$$D := ad - bc \neq 0.$$

Then $L(\mathcal{D}_k(X))$ is a compact subset of $\mathbb{R}^2$ that also satisfies conditions (1) and (2) above, also with $h = 2$.

We define the diameter of L to be

$$\mathrm{diam}(L) = |a| + |b| + |c| + |d|.$$

Then

$$\mathrm{Vol}(L(\mathcal{D}_k(X))) = |D|\mathrm{Vol}(\mathcal{D}_k(X))$$

and

$$\mathrm{Vol}(\partial(L(\mathcal{D}_k(X)))) = O(\mathrm{diam}(L) \cdot X^{\frac{1}{2}}),$$

where the implied constant is absolute.

3.4 Linear sums

In this section we prove that the estimate (A) from Proposition 3.4 holds for the sequence $\{a_{\phi,\psi,\mathfrak{n}}\}_{\mathfrak{n}}$ defined in (3.30) with $\theta_1 = 1/6$.

Proposition 3.6. *Let $a_{\mathfrak{n}} = a_{\phi,\psi,\mathfrak{n}}$, where $a_{\phi,\psi,\mathfrak{n}}$ is defined as in (3.30), and let $A_{\mathfrak{d}}(X)$ be defined as in (3.25). Then for all $\epsilon > 0$ and all $X \geq 2$, we have*

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

Proof. Recall that

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

Since the sequence $a_{\mathfrak{n}}$ is supported on odd ideals $\mathfrak{n}$, we see that $A_{\mathfrak{d}}(X) = 0$ unless $\mathfrak{d}$ is odd. Hence we may assume without loss of generality that $\mathfrak{d}$ is an odd ideal. Let

$$\mathcal{R}(X) := \mathcal{D}_4(X) = \left\{(u,v) \in \mathcal{D} \cup \varepsilon^2\mathcal{D} \cup \varepsilon^4\mathcal{D} \cup \varepsilon^6\mathcal{D} : u^2 - 2v^2 \leq X\right\}. \quad (3.33)$$

By Proposition 3.5 and definition (3.30), we have

$$A_{\mathfrak{d}}(X) = \sum_{\substack{(u,v) \in \mathcal{R}(X) \\ u+v\sqrt{2} \equiv 0 \bmod \mathfrak{d}}} [u + v\sqrt{2}]_{\phi,\psi},$$

where $[u + v\sqrt{2}]_{\phi,\psi}$ is defined as in (3.29).

We now reformulate the congruence condition $u + v\sqrt{2} \equiv 0 \bmod \mathfrak{d}$. Proposition 3.5 implies that there is an element $d_1 + d_2\sqrt{2} \in \mathcal{D}$ which generates $\mathfrak{d}$. Then the congruence above is equivalent to saying that there exist integers e_1 and e_2 such that $u + v\sqrt{2} = (d_1 + d_2\sqrt{2})(e_1 + e_2\sqrt{2})$, i.e. such that

$$u = d_1e_1 + 2d_2e_2$$

and

$$v = d_2e_1 + d_1e_2.$$

In other words, (u, v) is in the image of the linear transformation

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

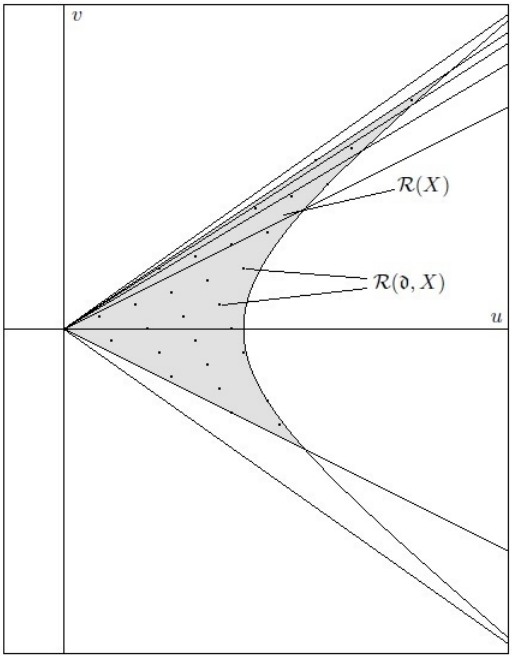


Figure 3.2: The region $\mathcal{R}(X)$ and the lattice points $\mathcal{R}(\mathfrak{d}, X)$

of determinant

$$D := \mathrm{Norm}(\mathfrak{d}) = d_1^2 - 2d_2^2.$$

Hence we define

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

(depicted in Figure 3.2), and we rewrite the sum $A_{\mathfrak{d}}(X)$ as

$$A_{\mathfrak{d}}(X) = \sum_{(u,v)\in\mathcal{R}(\mathfrak{d},X)} [u + v\sqrt{2}]_{\phi,\psi}.$$

Using the fact that $|[u + v\sqrt{2}]_{\phi,\psi}| \leq 1$, we obtain the trivial bound

$$|A_{\mathfrak{d}}(X)| \leq \sum_{(u,v)\in\mathcal{R}(\mathfrak{d},X)} 1 = \sum_{L_{\mathfrak{d}}^{-1}\mathcal{R}(X)\cap\mathbb{Z}^2} 1. \tag{3.34}$$

Since $d_1 + d_2\sqrt{2} \in \mathcal{D}$, we have the inequalities

$$\frac{d_1^2}{2} \leq D \leq d_1^2,$$

which implies that $\mathrm{diam}(L_{\mathfrak{d}}^{-1}) \ll D^{-1/2}$. Hence Lemma 3.14 gives

$$|A_{\mathfrak{d}}(X)| \leq a_4 X D^{-1} + O(D^{-\frac{1}{2}} X^{\frac{1}{2}} + 1) \ll X D^{-1} + X^{\frac{1}{2}} D^{-\frac{1}{2}} + 1, \qquad (3.35)$$

where the implied constant is absolute. This estimate will be useful when D is large compared to X.

Next we split the sum $A_{\mathfrak{d}}(X)$ into $8 \cdot 16$ sums where the congruence classes of u and v modulo 16 are fixed, say $u \equiv u_0 \bmod 16$ and $v \equiv v_0 \bmod 16$ for some congruence classes u_0 and v_0 modulo 16 with u_0 invertible modulo 16. For u and v satisfying these congruences, we have

$$[u + v\sqrt{2}]_{\phi,\psi} = \delta(u_0, v_0) \left(\frac{v}{u}\right),$$

where $\delta(u_0, v_0) \in \{\pm 1\}$ depends only on the congruence classes u_0 and v_0 modulo 16. Hence it remains to give estimates for sums of the type

$$A_{\mathfrak{d}}(u_0, v_0, X) := \sum_{(u,v) \in \mathcal{R}(u_0, v_0, \mathfrak{d}, X)} \left(\frac{v}{u}\right),$$

where

$$\mathcal{R}(u_0, v_0, \mathfrak{d}, X) := \{(u, v) \in \mathcal{R}(\mathfrak{d}, X) : (u, v) \equiv (u_0, v_0) \bmod 16\}.$$

Splitting the sum according to the value of u, we obtain

$$A_{\mathfrak{d}}(u_0, v_0, X) = \sum_{\substack{0 \leq u \leq R_1(X) \\ u \equiv u_0 \bmod 16}} A_{u,\mathfrak{d}}(v_0, X), \qquad (3.36)$$

where

$$A_{u,\mathfrak{d}}(v_0, X) := \sum_{\substack{v \in I_u \\ (u,v) \in L_{\mathfrak{d}}(\mathbb{Z}^2) \\ v \equiv v_0 \bmod 16}} \left(\frac{v}{u}\right).$$

Here

$$R_1(X) = \sup\{u \in \mathbb{R} : \ (u, v) \in \mathcal{R}(X)\} \ll X^{\frac{1}{2}}$$

and I_u is an interval (or a union of 2 disjoint intervals) of size $\leq 2R_2(X)$, where

$$R_2(X) = \sup\{|v| \in \mathbb{R} : \ (u, v) \in \mathcal{R}(X)\} \ll X^{\frac{1}{2}}.$$

We now unwind the condition $(u, v) \in L_{\mathfrak{d}}(\mathbb{Z}^2)$, i.e. that (u, v) is in the image of $L_{\mathfrak{d}}$. Consider the system of equations in x and y:

$$\begin{cases} u = d_1 x + 2d_2 y \\ v = d_2 x + d_1 y. \end{cases} \qquad (3.37)$$

Let $d := \gcd(d_1, d_2)$ and write $d_1 = dd_1'$, $d_2 = dd_2'$. Recall that $\mathfrak{d}$ and so also d_1 is odd, so that $d = \gcd(d_1, 2d_2)$. If the system (3.37) has a solution over $\mathbb{Z}$, then d must divide u. This means that

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

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

$$u = d_1 x_u + 2d_2 y_u.$$

Then all solutions $(x, y) \in \mathbb{Z}^2$ to the first equation in (3.37) are given by

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

Hence

$$v = d_2 (x_u - 2d_2' k) + d_1 (y_u + d_1' k) = d_2 x_u + d_1 y_u + Dk/d,$$

which means that (3.37) has a solution over $\mathbb{Z}$ if and only if

$$v \equiv d_2 x_u + d_1 y_u \bmod D/d.$$

Note that D is odd, so that D/d and 16 are coprime. Let v_u be the congruence class modulo $16D/d$ such that

$$\begin{cases} v_u \equiv d_2 x_u + d_1 y_u \bmod D/d \\ v_u \equiv v_0 \bmod 16. \end{cases}$$

Thus we have proved that if $u \equiv 0 \bmod d$, then

$$A_{u,\mathfrak{d}}(v_0, X) = \sum_{\substack{v \in I_u \\ v \equiv v_u \bmod 16D/d}} \left(\frac{v}{u}\right).$$

Let $e_u = \gcd(v_u, 16D/d)$, write $16D/d = e_u d_u$, $v_u = e_u v_u'$, and perform a change of variables $v = e_u v'$, so that

$$A_{u,\mathfrak{d}}(v_0, X) = \left(\frac{e_u}{u}\right) \sum_{\substack{v' \in I_u' \\ v' \equiv v_u' \bmod d_u}} \left(\frac{v'}{u}\right),$$

where $I_u' = I_u/e_u$. Since $\gcd(v_u', d_u) = 1$, we can now detect the congruence condition $v' \equiv v_u' \bmod d_u$ via Dirichlet characters modulo d_u. In other words,

$$A_{u,\mathfrak{d}}(v_0, X) = \frac{1}{\varphi(d_u)} \left(\frac{e_u}{u}\right) \chi(\overline{v_u'}) \sum_{\chi \bmod d_u} \sum_{v' \in I_u'} \chi(v') \left(\frac{v'}{u}\right), \tag{3.38}$$

where $\overline{v'_u}$ denotes the multiplicative inverse of v'_u modulo d_u. Let χ be a Dirichlet character modulo d_u. If the character

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

is trivial, then $u = fg^2$ for some f dividing d_u (and therefore dividing $16D/d$) and some integer g. The number of such $u \leq R_1(X)$ is

$$\leq \tau(16D/d) R_1(X)^{\frac{1}{2}} \ll_\epsilon D^\epsilon X^{\frac{1}{4}}.$$

In this case we use the trivial bound

$$\sum_{v' \in I'_u} \chi(v') \left(\frac{v'}{u}\right) \ll \#I'_u \leq \#I_u \ll X^{\frac{1}{2}},$$

where the implied constant in $\ll$ is absolute. Hence the contribution of such u to $A_{\mathfrak{d}}(u_0, v_0, X)$ is

$$\ll_\epsilon D^\epsilon X^{\frac{3}{4}}. \tag{3.39}$$

On the other hand, if the character

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

is not trivial, its conductor is at most

$$16Du/d \ll DX^{\frac{1}{2}},$$

and so the Polya-Vinogradov inequality gives the estimate

$$\sum_{v' \in I'_u} \chi(v') \left(\frac{v'}{u}\right) \ll_\epsilon D^{\frac{1}{2}} X^{\frac{1}{4}+\epsilon}.$$

Combining this with (3.36), (3.38), and (3.39), we have proved the bound

$$A_{\mathfrak{d}}(X) \ll_\epsilon D^{\frac{1}{2}} X^{\frac{3}{4}+\epsilon}. \tag{3.40}$$

We use (3.40) for $D < X^{1/6}$ and (3.35) for $D \geq X^{1/6}$ to obtain

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

□

3.5 Bilinear sums

We are left with proving the estimate (B) from Proposition 3.4, which we do with $\theta_2 = 1/12$ in much the same way as in [19, Sections 19-21, p. 1018-1028].

Proposition 3.7. *Let $a_{\mathfrak{n}} = a_{\phi,\psi,\mathfrak{n}}$, where $a_{\phi,\psi,\mathfrak{n}}$ is defined as in (3.30), and let $B(M,N)$ be defined as in (3.26). Then for all $\epsilon > 0$ and all $M, N \geq 2$, we have*

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

Before we begin the proof of Proposition 3.7, we first define a quantity $\gamma(w,z)$ that oscillates in both arguments $w, z \in \mathbb{Z}[\sqrt{2}]$.

3.5.1 The symbol $\gamma(w,z)$

Let σ denote the non-trivial automorphism of $\mathbb{Q}(\sqrt{2})$. Define the *rational part* of an element $w \in \mathbb{Z}[\sqrt{2}]$ to be

$$\mathrm{r}(w) := \frac{1}{2}(w + \sigma(w)).$$

In other words, if $w = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$, then $\mathrm{r}(w) = a$.

We say that an element $w = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is *primitive* if and only if $\gcd(a,b) = 1$.

Suppose w and z are primitive. Then wz need *not* be primitive. Nonetheless, we have the following lemma.

Lemma 3.15. *Suppose w and z are primitive. Let $d = \mathrm{Norm}(\gcd(w, \sigma(z))$. Then wz/d is primitive. In particular, wz is primitive whenever $\gcd(w,\sigma(z)) = 1$.*

Proof. If p is inert in $\mathbb{Z}[\sqrt{2}]$ and $p|wz$, then by unique prime factorization in $\mathbb{Z}[\sqrt{2}]$, p divides either w or z, which contradicts the assumption that w and z are primitive. Now suppose that p splits in $\mathbb{Z}[\sqrt{2}]$ (resp. $p = 2$), so that $p = \xi\sigma(\xi)$ (resp. $p = -\xi\sigma(\xi)$) for some prime $\xi \in \mathbb{Z}[\sqrt{2}]$. If p^k is the exact power of p dividing wz, then the assumption that w and z are primitive implies that $\xi^k | w$ and $\sigma(\xi^k)|z$, which is true if and only if $\xi^k | \gcd(w_1, \sigma(w_2))$. The lemma now follows by unique factorization in $\mathbb{Z}[\sqrt{2}]$. □

Given an odd, totally positive, primitive $w \in \mathbb{Z}[\sqrt{2}]$ a totally positive $z \in \mathbb{Z}[\sqrt{2}]$, we define the *generalized Dirichlet symbol* $\gamma(w,z)$ to be

$$\gamma(w,z) := \left(\frac{\mathrm{r}(wz)}{\mathrm{Norm}(w)}\right), \tag{3.41}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi symbol. More concretely, if we write $w = a + b\sqrt{2}$ and $z = c + d\sqrt{2}$, then

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

Our choice of terminology is inspired by the Dirichlet symbol defined in a slightly different setting in [19, Section 19, p. 1018-1021].

The symbol $\gamma(w,z)$ is almost multiplicative in the second argument. More precisely, for an odd, totally positive $w = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, define

$$\mathrm{m}(w) := \left(\frac{\mathrm{r}(w)}{\mathrm{Norm}(w)}\right) = \left(\frac{a}{a^2-2b^2}\right). \tag{3.42}$$

Note that w is primitive if and only if $\mathrm{m}(w) \neq 0$. In this case, the law of quadratic reciprocity implies that

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

and so $\mathrm{m}(w) \in \{\pm 1\}$ depends only on the residue class of w modulo 8. We have

Lemma 3.16. *Let $w \in \mathbb{Z}[\sqrt{2}]$ be odd, totally positive, and primitive, and let $z_1, z_2 \in \mathbb{Z}[\sqrt{2}]$ be totally positive. Then*

$$\gamma(w, z_1 z_2) = \gamma(w, z_1)\gamma(w, z_2)\mathrm{m}(w). \tag{3.43}$$

Proof. Write $w = a + b\sqrt{2}$, $z_1 = c_1 + d_1\sqrt{2}$, and $z_2 = c_2 + d_2\sqrt{2}$. Then

$$\gamma(w, z_1)\gamma(w, z_2) = \left(\frac{a^2c_1c_2 + 2ab(c_1d_2 + c_2d_1) + 4b^2d_1d_2}{a^2-2b^2}\right).$$

Using the facts that $4b^2 \equiv 2a^2 \bmod a^2 - 2b^2$ and that $z_1z_2 = (c_1c_2 + 2d_1d_2) + (c_1d_2 + c_2d_1)\sqrt{2}$, we deduce that

$$\begin{aligned}
\gamma(w, z_1)\gamma(w, z_2) &= \left(\frac{a^2(c_1c_2 + 2d_1d_2) + 2ab(c_1d_2 + c_2d_1)}{a^2-2b^2}\right) \\
&= \left(\frac{a}{a^2-2b^2}\right)\left(\frac{a(c_1c_2 + 2d_1d_2) + 2b(c_1d_2 + c_2d_1)}{a^2-2b^2}\right) \\
&= \mathrm{m}(w)\gamma(w, z_1z_2).
\end{aligned}$$

□

The symbol $\gamma(w,z)$ also satisfies a reciprocity law.

Lemma 3.17. *Let w and z be odd, totally positive, and primitive elements of $\mathbb{Z}[\sqrt{2}]$. Then*

$$\gamma(w, z)\gamma(z, w) = \mathrm{m}(wz). \tag{3.44}$$

In particular, if $\gamma(w,z) = 0$ whenever $\gcd(w, \sigma(z)) \neq 1$.

Proof. We have

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

□

Finally, we remark that $\gamma(w, z_1) = \gamma(w, z_2)$ whenever $z_1 \equiv z_2 \bmod \mathrm{Norm}(w)$.

3.5.2 Twisted multiplicativity of governing symbols

Recall that if $u+v\sqrt{2}$ is a totally positive odd element of $\mathbb{Z}[\sqrt{2}]$, we define the governing symbol $[u+v\sqrt{2}]$ to be

$$[u+v\sqrt{2}] = \left(\frac{v}{u}\right).$$

Thus $[u+v\sqrt{2}] = 0$ whenever $u+v\sqrt{2}$ is not primitive.

A key feature of the governing symbol $[\cdot]$ which leads to significant cancellation in (3.26) is that $[\cdot]$ is *not* multiplicative, i.e. the relation

$$[wz] = [w][z],$$

does *not* hold for all totally positive w and z. Instead, the equation above becomes essentially valid when twisted by $\gamma(w,z)$. We now state our result more precisely.

We now introduce notation that will simplify the subsequent arguments. Suppose that f_1 and f_2 are functions $\mathbb{Z}^r \to \mathbb{C}$. For $x \in \mathbb{Z}^r$, we write $f_1 \sim f_2$ (or more conveniently $f_1(x) \sim f_2(x)$) if there exists a function $\delta : \mathbb{Z}^r \to \{\pm 1\}$ such that δ factors though $(\mathbb{Z}/16\mathbb{Z})^r$, i.e. the value of $\delta(x)$ depends only on the congruence classes of the coordinates of x modulo 16, and such that

$$f_1(x) = \delta(x) f_2(x)$$

for all $x \in \mathbb{Z}^r$. For instance, $[u+v\sqrt{2}]_{\phi,\psi} \sim [u+v\sqrt{2}]_{\phi',\psi'}$ for any four Dirichlet characters ϕ, ψ, ϕ', ψ'.

The following proposition is analogous to [19, Lemma 20.1, p. 1021].

Proposition 3.8. *Let $w = a+b\sqrt{2}$ and $z = c+d\sqrt{2}$ be two primitive, totally positive, odd elements of $\mathbb{Z}[\sqrt{2}]$. Then*

$$[wz] \sim [w][z]\gamma(w,z).$$

Proof. When wz is not primitive, then $[wz] = 0$ and $\gamma(w,z) = 0$, and so the result follows. Hence we may assume that wz is primitive.

First note that

$$wz = (ac+2bd) + (ad+bc)\sqrt{2}.$$

We set $\rho = (a,d)$ and define a_1 and d_1 by the equalities $a = \rho a_1$ and $d = \rho d_1$, respectively. Then

$$[wz] = \left(\frac{ad+bc}{ac+2bd}\right) = \left(\frac{ad+bc}{\rho}\right)\left(\frac{ad+bc}{a_1 c + 2bd_1}\right),$$

and since ρ divides ad, the above simplifies to

$$[wz] = \left(\frac{bc}{\rho}\right)\left(\frac{ad+bc}{a_1c+2bd_1}\right).$$

Now, since w is primitive, a_1 is relatively prime to b and hence also to a_1c+2bd_1. Hence we may write

$$c \equiv -2bd_1/a_1 \pmod{a_1c+2bd_1},$$

so that the second factor in the expression above becomes

$$\left(\frac{ad+bc}{a_1c+2bd_1}\right) = \left(\frac{ad-2b^2d_1/a_1}{a_1c+2bd_1}\right) = \left(\frac{a_1d_1}{a_1c+2bd_1}\right)\left(\frac{\rho^2-2b^2/a_1^2}{a_1c+2bd_1}\right).$$

As $a^2-2b^2 = a_1^2(\rho^2-2b^2/a_1^2)$, we deduce that

$$[wz] \sim \left(\frac{bc}{\rho}\right)\left(\frac{a_1d_1}{a_1c+2bd_1}\right)\left(\frac{a^2-2b^2}{a_1c+2bd_1}\right).$$

We write the last factor in the expression above as

$$\left(\frac{a^2-2b^2}{a_1c+2bd_1}\right) = \left(\frac{a^2-2b^2}{\rho}\right)\left(\frac{a^2-2b^2}{ac+2bd}\right),$$

and use the fact that

$$\left(\frac{a^2-2b^2}{\rho}\right) = \left(\frac{-2b^2}{\rho}\right) = \left(\frac{-2}{\rho}\right)$$

to conclude that

$$[wz] \sim \left(\frac{-2bc}{\rho}\right)\left(\frac{a_1d_1}{a_1c+2bd_1}\right)\left(\frac{a^2-2b^2}{ac+2bd}\right).$$

The law of quadratic reciprocity implies that

$$\left(\frac{a^2-2b^2}{ac+2bd}\right) \sim \left(\frac{ac+2bd}{a^2-2b^2}\right),$$

so that

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

We again use the law of quadratic reciprocity to treat the middle term above. We get

$$\left(\frac{a_1}{a_1c+2bd_1}\right) = (-1)^{\nu_1(a,b,c,d,\rho)}\left(\frac{2}{a_1}\right)\left(\frac{bd_1}{a_1}\right),$$

where

$$\nu_1(a,b,c,d,\rho) \equiv \frac{a_1-1}{2}\cdot\frac{r_1-1}{2} \bmod 2$$

and

$$r_1 = a_1 c + 2bd_1.$$

Similarly, we write d_1 as

$$d_1 = 2^e d_2,$$

where d_2 is odd, and compute that

$$\left(\frac{d_1}{a_1 c + 2bd_1}\right) = (-1)^{\nu_2(a,b,c,d,\rho)} \left(\frac{d_1}{a_1 c}\right),$$

where now

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

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 $r_1 \equiv a_1 c \bmod 8$. Using this observation and the definitions of ν_1, ν_2, and ν_3, we find that

$$\nu_2 \equiv \begin{cases} \frac{d_1-1}{2} \bmod 2 & \text{if } e = 0 \text{ and } b \equiv 1 \bmod 2 \\ 1 \bmod 2 & \text{if } e = 1 \text{ and } b \equiv 1 \bmod 2 \\ 0 \bmod 2 & \text{otherwise.} \end{cases}$$

First suppose $e \geq 2$. Then $r_1 \equiv a_1 c \bmod 8$ and $\nu_2 \equiv 0 \bmod 2$. Suppose first that $c \equiv 1 \bmod 4$. Then $\nu_3 \equiv 0 \bmod 2$ as well. Moreover, $a_1 \equiv r_1 \bmod 4$, so that

$$\nu_1 \equiv \frac{a_1-1}{2}\cdot\frac{a_1-1}{2} \equiv \frac{a_1-1}{2} \bmod 2.$$

Finally, as $a = a_1\rho$,

$$\left(\frac{-1}{a}\right) = \left(\frac{-1}{a_1}\right)\left(\frac{-1}{\rho}\right)$$

and so $\nu_1 + (\rho-1)/2 \equiv (a-1)/2 \bmod 2$. Now suppose $c \equiv 3 \bmod 4$. Then ρ and $c\rho$ are odd and different modulo 2, and so $\nu_3 + (\rho-1)/2 \equiv 1 \bmod 2$. Moreover, $r_1 \equiv 3a_1 \bmod 4$, so that r_1 and a_1 are odd and different modulo 4. Hence at least one of $(r_1-1)/2$ and $(a_1-1)/2$ is 0 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. □

3.5.3 Proof of Proposition 3.7

We are now ready to prove Proposition 3.7. Let

$$\mathcal{D}(X) := \left\{(u,v) \in \mathcal{D} : u^2 - 2v^2 \le X\right\},$$

where again $\mathcal{D}$ is defined as in (3.31). We will say that $u + v\sqrt{2} \in \mathcal{D}(X)$ to mean that $(u,v) \in \mathcal{D}(X)$. Then the bilinear sum (3.26) can be written as

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

where

$$B_k(M,N) = \sum_{w \in \mathcal{D}(M)} \sum_{z \in \mathcal{D}(N)} \alpha_w \beta_z [\varepsilon^{2k} wz]_{\phi,\psi}. \tag{3.45}$$

Here $\alpha_w = \alpha_{(w)}$ and $\beta_z = \beta_{(z)}$, i.e. α_w (resp. β_z) depends only on the ideal generated by w (resp. z).

It is enough to estimate (3.45) for each $0 \le k \le 3$. First, suppose $u+v\sqrt{2} \succ 0$ is primitive and odd. Then by Proposition 3.8, we have

$$[\varepsilon^{2k}(u+v\sqrt{2})] \sim [u+v\sqrt{2}][\varepsilon^{2k}]\gamma(\varepsilon^{2k}, u+v\sqrt{2}) \sim [u+v\sqrt{2}].$$

We write $w = a+b\sqrt{2}$ and $z = c+d\sqrt{2}$ and split (3.45) into $8^2 \cdot 16^2$ sums by fixing congruence classes of a, b, c, and d modulo 16 (where the congruence classes of a and c are invertible). Then it suffices to estimate each sum

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

Unless both w and z are primitive, wz is not primitive, and hence $[wz] = 0$. Using Proposition 3.8 again and replacing α_w by $\alpha_w[w]$ and β_z by $\beta_z[z]$, we are left to estimate sums of the type

$$Q^*(M,N) := \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv w_0 \bmod 16}}^{*} \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv z_0 \bmod 16}}^{*} \alpha_w \beta_z \gamma(w,z), \tag{3.46}$$

where $*$ restricts the summation to primitive elements of $\mathbb{Z}[\sqrt{2}]$. The cancellation in the bilinear sum (3.46) comes from the double oscillation of the term $\gamma(w,z)$ in the formula above.

We also define the closely related sum

$$Q(M,N) := \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv w_0 \bmod 16}}^{*} \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv z_0 \bmod 16}} \alpha_w \beta_z \gamma(w,z), \tag{3.47}$$

and note that $Q^*(M,N)$ is a special case of $Q(M,N)$ where the complex numbers β_z are supported on primitive elements z.

The Cauchy-Schwarz inequality implies that

$$|Q(M,N)|^2 \le \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv z_0 (16)}} |\beta_z|^2 \sum_{\substack{w_1 \in \mathcal{D}(M) \\ w_1 \equiv w_0 (16)}} \sum_{\substack{w_2 \in \mathcal{D}(M) \\ w_2 \equiv w_0 (16)}} \alpha_{w_1} \overline{\alpha_{w_2}} \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv z_0 (16)}} \gamma(w_1,z)\gamma(w_2,z).$$

Since β_z is bounded in modulus by N^ϵ, Lemma 3.14 applied to $L = \mathrm{Id}$ gives

$$\sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv z_0 (16)}} |\beta_z|^2 \ll_\epsilon N^\epsilon \mathrm{Vol}(\mathcal{D}(N)) + N^\epsilon O(\mathrm{Vol}(\partial(\mathcal{D}(N))) + 1) \ll_\epsilon N^{1+\epsilon}. \tag{3.48}$$

Recall that $\gamma(w,z_1) = \gamma(w,z_2)$ whenever $z_1 \equiv z_2 \bmod \mathrm{Norm}(w)$. Set

$$q := \mathrm{Norm}(w_1 w_2).$$

Hence we can split the inner sum over z into residue classes modulo $16q$. More precisely, we write $z_0 = z_{01}+z_{02}\sqrt{2}$ and define L to be the linear transformation $L = 16q \cdot \mathrm{Id} + (z_{01}, z_{02}) : \mathbb{R}^2 \to \mathbb{R}^2$. Then Lemma 3.14 gives

$$\begin{aligned}\sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv z_0(16)}} \gamma(w_1,z)\gamma(w_2,z) &= \sum_{\substack{\zeta \bmod 16q\\ \zeta\equiv z_0 \bmod 16}} \gamma(w_1,z)\gamma(w_2,z) \sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv\zeta \bmod 16q}} 1\\ &= \sum_{\substack{\zeta \bmod 16q\\ \zeta\equiv z_0 \bmod 16}} \gamma(w_1,z)\gamma(w_2,z)\left(\frac{a_0 N}{(16q)^2} + O\left(\frac{N^{\frac12}}{q}+1\right)\right)\\ &= \frac{a_0 N}{(16q)^2}\sum_{\substack{\zeta \bmod 16q\\ \zeta\equiv z_0 \bmod 16}} \gamma(w_1,z)\gamma(w_2,z) + O\left(q^2\left(\frac{N^{\frac12}}{q}+1\right)\right),\end{aligned}$$

where a_0 is defined as in (3.32). The following proposition, analogous to [19, Lemma 21.1, p. 1025], helps us estimate the sum above. It gives a lot of cancellation for most w_1 and w_2.

Proposition 3.9. *Let w_0 and z_0 be odd congruence classes modulo 16 in $\mathbb{Z}[\sqrt{2}]$. Let $w_1, w_2 \in \mathbb{Z}[\sqrt{2}]$ be primitive, totally positive, and odd. Suppose $w_1 \equiv w_2 \equiv w_0 \bmod 16$. Let σ be the non-trivial automorphism of $\mathbb{Q}(\sqrt{2})$. Let $\gcd(w_1, \sigma(w_2))$ denote a totally positive generator for the greatest common divisor of the ideals (w_1) and $(\sigma(w_2))$ in $\mathbb{Z}[\sqrt{2}]$. Let $q := \mathrm{Norm}(w_1 w_2)$ and $d := \mathrm{Norm}(\gcd(w_1, \sigma(w_2)))$ (so that $d^2|q$). Then we have*

$$\left|\sum_{\substack{z \bmod 16q\\ z\equiv z_0 \bmod 16}} \gamma(w_1,z)\gamma(w_2,z)\right| = \begin{cases} q\varphi(d)\varphi(q/d) & \text{if } q \text{ and } d \text{ are squares}\\ 0 & \text{otherwise.}\end{cases}$$

Proof. We write $z = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. Our first goal is to show that

$$\gamma(w_1,z)\gamma(w_2,z) = \delta\left(\frac{a^2-2b^2}{d}\right)\gamma(w_1 w_2/d, z), \tag{3.49}$$

where $\delta \in \{\pm 1\}$ possibly depends on w_1, w_2 and the fixed congruence class $z_0 \bmod 16$ but *not* on z.

It is possible that z is not primitive, so that we cannot directly apply the reciprocity law from Lemma 3.17 to $\gamma(w_1, z)$ and $\gamma(w_2, z)$. However, we can factor out the greatest common factor of a and b to obtain

$$z = gz',$$

where $g = \gcd(a, b)$, $a = ga'$, $b = gb'$, and $z' = a' + b'\sqrt{2}$. Now z' is primitive.

First assume that

$$\gcd(w_1 w_2, \sigma(z)) = 1. \tag{3.50}$$

Under this assumption, we claim that

$$\gcd(d, a^2 - 2b^2) = \gcd(q, g) = \gcd(d, g) = 1. \tag{3.51}$$

These equalities will be useful in subsequent manipulations of Jacobi symbols. We now prove the claim.

First, suppose that there is a prime p dividing d and $a^2 - 2b^2$. Let $\xi = \gcd(w_1, \sigma(w_2))$, so that $d = \xi\sigma(\xi)$. Suppose p divides ξ or $\sigma(\xi)$. In the former case, this would mean that p divides w_1, while in the latter case it would mean that p divides w_2. Both of these cases contradict the assumption that w_1 and w_2 are primitive. Hence p cannot divide either ξ or $\sigma(\xi)$. Since $z \equiv z_0 \bmod 16$ and z_0 is an odd congruence class modulo 16, we see that $a^2 - 2b^2$ is odd, and so also that p is odd. If p is inert in $\mathbb{Z}[\sqrt{2}]$, then since p divides d, p must divide either ξ or $\sigma(\xi)$, and this is a contradiction. Hence we may assume that p splits in $\mathbb{Z}[\sqrt{2}]$, i.e. $p = \pi\sigma(\pi)$ for some prime π in $\mathbb{Z}[\sqrt{2}]$. Again, as p divides neither ξ nor $\sigma(\xi)$, we can assume without loss of generality that π divides ξ and $\sigma(\pi)$ divides $\sigma(\xi)$. This means that π divides w_1 and $\sigma(\pi)$ divides w_2. Now, since p (and hence π) divides $a^2 - 2b^2 = z\sigma(z)$, we find that π divides z or $\sigma(z)$. In the former case, $\sigma(\pi)$ divides $\sigma(z)$, which means that $\sigma(\pi)$ divides $\gcd(w_2, \sigma(z))$, and this contradicts assumption (3.50). In the latter case, π divides $\gcd(w_1, \sigma(z))$, which again contradicts (3.50). Hence we have shown that $(d, a^2 - 2b^2) = 1$.

Now suppose that there is a prime p dividing q and g. As g is a rational integer, $\sigma(g) = g$, and so, as $z = gz'$, we see that p divides $\sigma(z)$. Since w_1 and w_2 are odd, p must be odd. If p divides w_1 or w_2, then p divides $\gcd(w_1 w_2, \sigma(z))$, which contradicts assumption (3.50). Hence p cannot divide either w_1 or w_2. If p is inert in $\mathbb{Z}[\sqrt{2}]$, then, as $q = w_1 w_2 \sigma(w_1)\sigma(w_2)$, p divides at least one of w_1, w_2, $\sigma(w_1)$, and $\sigma(w_2)$. In fact, as $p = \sigma(p)$, we see that p must divide either w_1 or w_2, which is a contradiction. Hence we may assume that p splits in $\mathbb{Z}[\sqrt{2}]$, i.e. $p = \pi\sigma(\pi)$ for some prime π in $\mathbb{Z}[\sqrt{2}]$. Again, as p divides neither w_1 nor w_2, we can assume without loss of generality that π divides w_1. But then π divides $\gcd(w_1, \sigma(z))$, which contradicts assumption (3.50). Hence we have shown that $\gcd(q, g) = 1$.

Finally, as d divides q, we immediately deduce that $\gcd(d, g) = 1$. This finishes the proof of (3.51).

By definition of $\gamma(\cdot, \cdot)$, as g is a rational integer, we have

$$\gamma(w_i, z) = \left(\frac{g}{\mathrm{Norm}(w_i)}\right)\gamma(w_i, z')$$

for $i = 1, 2$. Hence

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right)\gamma(w_1, z')\gamma(w_2, z').$$

Now we can apply the reciprocity law from Lemma 3.17 twice to obtain

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right) \left(\gamma(z', w_1)\mathrm{m}(w_1 z')\right) \left(\gamma(z', w_2)\mathrm{m}(w_2 z')\right).$$

Recall that $\mathrm{m}(\alpha)$ depends only on the residue class of α modulo 8. Using the fact that $w_1 \equiv w_2 \bmod 16$, we deduce that $w_1 z' \equiv w_2 z' \bmod 16$, and so $\mathrm{m}(w_1 z') = \mathrm{m}(w_2 z')$. The assumption $\gcd(w_1 w_2, \sigma(z)) = 1$ ensures that $w_i z'$ is primitive (see Lemma 3.15), and so that $\mathrm{m}(w_i z') \in \{\pm 1\}$ for $i = 1, 2$. Hence $\mathrm{m}(w_1 z')\mathrm{m}(w_2 z') = \mathrm{m}(w_1 z')^2 = 1$ and the expression above simplifies to

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right) \gamma(z', w_1)\gamma(z', w_2).$$

Lemma 3.15 ensures that $w_1 w_2/d$ is primitive. Hence we can now use the multiplicativity formula from Lemma 3.16 twice to obtain

$$\begin{aligned} \gamma(w_1, z)\gamma(w_2, z) &= \left(\frac{g}{q}\right) \gamma(z', w_1 w_2)\mathrm{m}(z') \\ &= \left(\frac{g}{q}\right) \left(\gamma(z', d)\gamma(z', w_1 w_2/d)\mathrm{m}(z')\right) \mathrm{m}(z'). \end{aligned}$$

Again, z' is primitive, so $\mathrm{m}(z') \in \{\pm 1\}$. The above simplifies to

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right) \gamma(z', d)\gamma(z', w_1 w_2/d).$$

We again use the reciprocity law from Lemma 3.17 on $\gamma(z', w_1 w_2/d)$ to obtain

$$\gamma(w_1, z)\gamma(w_2, z) = \left(\frac{g}{q}\right) \gamma(z', d)\gamma(w_1 w_2/d, z')\mathrm{m}(z' w_1 w_2/d).$$

As before, since g is a rational integer,

$$\gamma(w_1 w_2/d, z) = \left(\frac{g}{q/d^2}\right) \gamma(w_1 w_2/d, z').$$

By equation (3.51), the Jacobi symbols $\left(\frac{g}{q}\right)$ and $\left(\frac{g}{q/d^2}\right)$ are non-zero. Hence

$$\left(\frac{g}{q}\right) \left(\frac{g}{q/d^2}\right) = \left(\frac{g}{q^2/d^2}\right) = 1,$$

and the above simplifies to

$$\gamma(w_1, z)\gamma(w_2, z) = \gamma(z', d)\gamma(w_1 w_2/d, z)\mathrm{m}(z' w_1 w_2/d). \tag{3.52}$$

By definition of $\gamma(\cdot, \cdot)$,

$$\gamma(z', d) = \left(\frac{a'd}{a'^2 - 2b'^2}\right) = \mathrm{m}(z') \left(\frac{d}{a'^2 - 2b'^2}\right). \tag{3.53}$$

By equation (3.51), we use the law of quadratic reciprocity to write

$$\left(\frac{d}{a'^2-2b'^2}\right)=\epsilon(d,a'^2-2b'^2)\left(\frac{a'^2-2b'^2}{d}\right)=\epsilon(d,a'^2-2b'^2)\left(\frac{a^2-2b^2}{d}\right), \tag{3.54}$$

where for odd integers r and s,

$$\epsilon(r,s)=(-1)^{\frac{r-1}{2}\frac{s-1}{2}}=\left(\frac{-1}{s}\right)^{\frac{r-1}{2}}.$$

Note that $\epsilon(r,s)$ depends only on the congruence classes of r and s modulo 4. Since g is odd, $g^2\equiv 1 \bmod 4$, and so $\epsilon(d,a'^2-2b'^2)=\epsilon(d,a^2-2b^2)$. In particular, as $z\equiv z_0 \bmod 16$, $\epsilon(d,a'^2-2b'^2)$ depends only on the congruence classes of d and z_0 modulo 4, and not on z.

Putting together (3.52), (3.53), and (3.54), we see that to accomplish our goal (3.49), it remains to show that the value of the factor

$$\mathrm{m}(z')\mathrm{m}(z'w_1w_2/d)$$

is independent of z. By definition of $\mathrm{m}(\cdot)$, the law of quadratic reciprocity, and the fact that $g^2\equiv 1 \bmod 4$, we have

$$\mathrm{m}(z')=\epsilon(a',a^2-2b^2)\left(\frac{-2}{a'}\right). \tag{3.55}$$

As $a=ga'$, we have

$$\left(\frac{-1}{a'}\right)=\left(\frac{-1}{a}\right)\left(\frac{-1}{g}\right),$$

that is, $(a'-1)/2\equiv(a-1)/2+(g-1)/2 \bmod 2$. Hence

$$\epsilon(a',a^2-2b^2)=\epsilon(a,a^2-2b^2)\left(\frac{-1}{a^2-2b^2}\right)^{\frac{g-1}{2}}. \tag{3.56}$$

Again, as $a=ga'$, we also have

$$\left(\frac{-2}{a'}\right)=\left(\frac{-2}{a}\right)\left(\frac{-2}{g}\right). \tag{3.57}$$

Combining (3.55), (3.56), and (3.57), and using the definition of $\mathrm{m}(\cdot)$, we get

$$\mathrm{m}(z')=\mathrm{m}(z)\left(\frac{-1}{a^2-2b^2}\right)^{\frac{g-1}{2}}\left(\frac{-2}{g}\right), \tag{3.58}$$

where we note that $\mathrm{m}(z)$ depends only on the fixed congruence class z_0 modulo 16 and *not* on z.

We now define integers e and f by the equation

$$w_1 w_2/d = e + f\sqrt{2},$$

and define integers x, y, x', and y' by the equations

$$zw_1 w_2/d = x + y\sqrt{2} = g(x' + y'\sqrt{2}).$$

Proceeding in the same way as for (3.55), we get

$$\mathrm{m}(z' w_1 w_2/d) = \epsilon(x', x^2 - 2y^2) \left(\frac{-2}{x'}\right). \tag{3.59}$$

As $x = gx'$, we have

$$\left(\frac{-1}{x'}\right) = \left(\frac{-1}{x}\right)\left(\frac{-1}{g}\right),$$

that is, $(x'-1)/2 \equiv (x-1)/2 + (g-1)/2 \bmod 2$. Hence

$$\epsilon(x', x^2 - 2y^2) = \epsilon(x, x^2 - 2y^2) \left(\frac{-1}{x^2 - 2y^2}\right)^{\frac{g-1}{2}}. \tag{3.60}$$

Again, as $x = gx'$, we also have

$$\left(\frac{-2}{x'}\right) = \left(\frac{-2}{x}\right)\left(\frac{-2}{g}\right). \tag{3.61}$$

Combining (3.59), (3.60), and (3.61) as before, and using the definition of $\mathrm{m}(\cdot)$, we get

$$\mathrm{m}(z' w_1 w_2/d) = \mathrm{m}(z w_1 w_2/d) \left(\frac{-1}{x^2 - 2y^2}\right)^{\frac{g-1}{2}} \left(\frac{-2}{g}\right), \tag{3.62}$$

where again the factor $\mathrm{m}(zw_1w_2/d)$ depends on w_1, w_2 and the fixed congruence class z_0 modulo 16 but *not* on z. Combining (3.58) and (3.62), and using the fact that $x^2 - 2y^2 = (a^2 - 2b^2)(e^2 - 2f^2)$, we find that

$$\mathrm{m}(z')\mathrm{m}(z' w_1 w_2/d) = \delta(w_1, w_2, z_0) \left(\frac{-1}{(a^2 - 2b^2)^2 (e^2 - 2f^2)}\right)^{\frac{g-1}{2}},$$

where $\delta(w_1, w_2, z_0) \in \{\pm 1\}$ depends only on w_1, w_2 and the residue class of z_0 modulo 16. Finally, note that

$$e^2 - 2f^2 = \mathrm{Norm}(w_1 w_2/d) = \frac{\mathrm{Norm}(w_1 w_2)}{d^2}$$

and that $\mathrm{Norm}(w_1) \equiv \mathrm{Norm}(w_2) \bmod 4$ (since again $w_1 \equiv w_2 \equiv w_0 \bmod 16$). Hence $e^2 - 2f^2 \equiv \mathrm{Norm}(w_1)^2 \equiv 1 \bmod 4$, and so

$$\mathrm{m}(z')\mathrm{m}(z' w_1 w_2/d) = \delta(w_1, w_2, z_0).$$

Thus, in the case that $\gcd(w_1w_2, \sigma(z)) = 1$ (see (3.50)), we have proved (3.49).

Suppose now that (3.50) is not satisfied, i.e., $(w_1w_2, \sigma(z)) \neq 1$. Then, by Lemma 3.17, either $\gamma(w_1, z) = 0$ or $\gamma(w_1, z) = 0$. Moreover, either $(w_1w_2/d, \sigma(z)) = 1$ or $(w_1w_2/d, \sigma(z)) \neq 1$. In the former case, $(w_1w_2/d, \sigma(z))$ divides both d and $z\sigma(z) = a^2 - 2b^2$, so that $(a^2 - 2b^2, d) \neq 1$. In the latter case, $(w_1w_2/d, \sigma(z)) \neq 1$, so $\gamma(w_1w_2/d, z) = 0$ again by Lemma 3.17. As $0 = 0$, we have once again proved

$$\gamma(w_1, z)\gamma(w_2, z) = \delta\left(\frac{a^2 - 2b^2}{d}\right)\gamma(w_1w_2/d, z),$$

so that the goal (3.49) has been established in all cases.

Writing $z_0 = a_0 + b_0\sqrt{2}$, we then get

$$\sum_{\substack{z \bmod 16q \\ z \equiv z_0 \bmod 16}} \gamma(w_1, z)\gamma(w_2, z) = \epsilon_1\epsilon_2 \sum_{\substack{a \bmod 16q \\ a \equiv a_0 \bmod 16}} \sum_{\substack{b \bmod 16q \\ a \equiv b_0 \bmod 16}} \left(\frac{a^2 - 2b^2}{d}\right)\left(\frac{ae + 2bf}{q/d^2}\right).$$

Note that there exists an integer t such that $t^2 \equiv 2 \bmod q$ because q is a norm of an element in $\mathbb{Z}[\sqrt{2}]$. Let t be such that $t \equiv 2f/e \bmod q/d^2$; this is possible since, by definition, $q/d^2 = e^2 - 2f^2$ and w_1w_2/d is primitive. Then, as d divides q, we may rewrite the above sum as

$$\sum_{\substack{z \bmod 16q \\ z \equiv z_0 \bmod 16}} \gamma(w_1, z)\gamma(w_2, z) = \epsilon_1\epsilon_2\left(\frac{e}{q^2/d}\right) \sum_{\substack{a \bmod 16q \\ a \equiv a_0 \bmod 16}} \sum_{\substack{b \bmod 16q \\ a \equiv b_0 \bmod 16}} \left(\frac{a - bt}{d}\right)\left(\frac{a + bt}{q/d}\right).$$

Write $a = a_0 + 16a_1$ and $b = b_0 + 16b_1$ and set $x_0 = a_0 + b_0t$, $y_0 = a_0 - b_0t$, $x = a_1 + b_1t$, $y = a_1 - b_1t$. Then $a + bt = x_0 + 16x$ and $a - bt = y_0 + 16y$. Note that the map $(a_1, b_1) \mapsto (x, y)$ is bijective on $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, and hence

$$\sum_{\substack{z \bmod 16q \\ z \equiv z_0 \bmod 16}} \gamma(w_1, z)\gamma(w_2, z) = \pm \sum_{y \bmod q}\left(\frac{y}{d}\right) \sum_{x \bmod q}\left(\frac{x}{q/d}\right) = q \sum_{y \bmod d}\left(\frac{y}{d}\right) \sum_{x \bmod q/d}\left(\frac{x}{q/d}\right),$$

and this implies the desired result. □

Since $\varphi(d)\varphi(q/d) \leq q$ and $q \leq M^2$, we deduce that whenever q and d are both squares,

$$\sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv z_0(16)}} \gamma(w_1, z)\gamma(w_2, z) \ll q^2\left(\frac{N}{q^2} + O\left(\frac{N^{\frac{1}{2}}}{q}\right)\right) + O\left(qN^{\frac{1}{2}} + q^2\right) \ll N + M^2N^{\frac{1}{2}} + M^4.$$

By unique factorization in $\mathbb{Z}[\sqrt{2}]$, the number of elements $w \in \mathcal{D}$ such that $\mathrm{Norm}(w) = n$ is at most $\tau(n)$, the number of divisors of n. Hence, setting

$m_1 = \mathrm{Norm}(w_1)$ and $m_2 = \mathrm{Norm}(w_2)$, and using (3.27) and (3.48), we get the upper bound

$$|Q(M,N)|^2 \ll N \left(\sum_{\substack{m_1,m_2 \leq M \\ m_1 m_2 \text{ square}}} \sum \tau(m_1 m_2) \left(N + M^2 N^{\frac{1}{2}} + M^4 \right) + M^4 N^{\frac{1}{2}} + M^6 \right) (MN)^{\epsilon}.$$

Using the estimate $\tau(n) \ll_\epsilon n^\epsilon$, we obtain

Lemma 3.18. *Let $Q(M,N)$ be defined as in* (3.47). *Then*

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

We now apply Hölder's inequality with k even to (3.47) to get

$$|Q(M,N)|^k \leq \left(\sum_w |\alpha_w|^{\frac{k}{k-1}} \right)^{k-1} \sum_w \left| \sum_z \beta_z \gamma(w,z) \right|^k. \tag{3.63}$$

Since $\gamma(w,z)$ is multiplicative in the second argument up to a unit factor depending only on w (see (3.16)), we can write

$$Q'(M,N^k) := \sum_w \left| \sum_z \beta_z \gamma(w,z) \right|^k =: \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv w_0 \bmod 16}} \sum_{\substack{z \in \mathcal{D}(N^k) \\ z \equiv z_0' \bmod 16}} \alpha_w' \beta_z' \gamma(w,z),$$

for some α_w' with $|\alpha_w'| \ll M^\epsilon$ and

$$\beta_z' = \sum_{\substack{z_1 \cdots z_k = \varepsilon^{2j} z \\ z \in \mathcal{D}(N^k)}} \beta_{z_1} \overline{\beta_{z_2}} \cdots \beta_{z_{k-1}} \overline{\beta_{z_k}}.$$

By Lemma 3.18, we have

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

Using this estimate with $k = 6$ along with the upper bound (proved similarly as (3.48))

$$\sum_{\substack{w \in \mathcal{D}(N) \\ w \equiv w_0 (16)}} |\alpha_w|^2 \ll M^{1+\epsilon}, \tag{3.64}$$

inside the inequality (3.63), we get

$$Q(M,N) \ll_\epsilon \left(M^{\frac{11}{12}} N + M^{\frac{7}{6}} N^{\frac{3}{4}} + M^{\frac{4}{3}} N^{\frac{1}{2}} \right) (MN)^{\epsilon}$$

We now use the reciprocity law (3.44) to interchange the roles of w and z in (3.46). As the value of $\mathrm{m}(wz)$ depends only on the residue classes of w and z modulo 16, we can apply the above estimate to get that $Q(M,N)$

$$\ll_\epsilon \min\left\{M^{\frac{11}{12}}N + M^{\frac{7}{6}}N^{\frac{3}{4}} + M^{\frac{4}{3}}N^{\frac{1}{2}}, N^{\frac{11}{12}}M + N^{\frac{7}{6}}M^{\frac{3}{4}} + N^{\frac{4}{3}}M^{\frac{1}{2}}\right\}(MN)^{\epsilon}.$$

For $M < N$, we have $M^{11/12}N > M^{7/6}N^{3/4}$ and $M^{11/12}N > M^{4/3}N^{1/2}$, so that

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

This completes the proof of Theorem 3.2 and hence also Theorem 3.1.

3.6 Counting primes

In this section we give evidence that a governing field for the 16-rank of the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 3(4)}$ does *not* exist. To explain why, we first define a prime counting function. Suppose $M/\mathbb{Q}$ is a normal extension. Let S be a subset of $\mathrm{Gal}(M/\mathbb{Q})$ which is a union of conjugacy classes. We define

$$\pi(M,S,X) := \#\{p \le X : \text{the Artin class of } p \text{ in } \mathrm{Gal}(M/\mathbb{Q}) \text{ is a subset of } S\}$$

Given any normal extension $M/\mathbb{Q}$ of degree d and a subset S of $\mathrm{Gal}(M/\mathbb{Q})$ stable under conjugation, the Čebotarev Density Theorem using the best known zero-free regions of L-functions gives [39, Théorème 2, p. 132], for some constant $c > 0$,

$$\pi(M,S,X) = \frac{\#S}{\#\mathrm{Gal}(M/\mathbb{Q})}\mathrm{Li}(X) + O(\#SX\exp(-cd^{-1/2}\log^{1/2}X)).$$

Hence given any two subsets S_1 and S_2 of $\mathrm{Gal}(M/\mathbb{Q})$ which are stable under conjugation and of the same size,

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

is the best known bound. Note that this bound is weaker than $X^{1-\delta}$ for any $\delta > 0$. For instance, it is *not* known if

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

However, we have the following result.

Theorem 3.3. *Suppose that there exists a governing field M for the* 16*-rank of the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 3(4)}$. Then there exist disjoint subsets S_1 and S_2 of $\mathrm{Gal}(M/\mathbb{Q})$ which are stable under conjugation and of equal size such that*

$$\pi(M,S_1,X) - \pi(M,S_2,X) \ll_\varepsilon X^{\frac{149}{150}+\epsilon}$$

Proof. We simply let S_1 be the union of Artin classes c_p for primes p satisfying $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1$ and S_2 be the union of Artin classes c_p for primes p satisfying $\mathrm{rk}_8\mathrm{Cl}(-8p) = 1$ but $\mathrm{rk}_{16}\mathrm{Cl}(-8p) = 0$. The result now immediately follows from Theorem 3.1. □

However, with our current methods of complex analysis applied to L-functions, we are not able to produce an error term of the form $O(x^{1-\delta_M})$ for any $\delta_M > 0$. This leads us to believe that a governing field M for the 16-rank of the family $\{\mathbb{Q}(\sqrt{-8p})\}_{p\equiv 3(4)}$ is unlikely to exist.