On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \bmod 4$

Peter Koymans*[1] and Djordjo Milovic†[2]

[1]Mathematisch Instituut, Leiden University
[2]Department of Mathematics, University College London

January 5, 2018

Abstract

We use Vinogradov's method to prove equidistribution of a spin symbol governing the 16-rank of class groups of quadratic number fields $\mathbb{Q}(\sqrt{-2p})$, where $p \equiv 1 \bmod 4$ is a prime.

1 Introduction

Recently, the authors have used Vinogradov's method to prove density results about elements of order 16 in class groups in certain *thin* families of quadratic number fields parametrized by a single prime number, namely the families $\{\mathbb{Q}(\sqrt{-2p})\}_{p\equiv -1 \bmod 4}$ and $\{\mathbb{Q}(\sqrt{-p})\}_p$ [17, 13]. In this paper, we establish a density result for the family $\{\mathbb{Q}(\sqrt{-2p})\}_{p\equiv 1 \bmod 4}$, thereby completing the picture for the 16-rank in families of imaginary quadratic fields with cyclic 2-class groups and even discriminant. Although our overarching methods are similar to those originally developed in the work of Friedlander et al. [10], the technical difficulties in the present case are different and require a more careful study of the spin symbols governing the 16-rank. The main distinguishing feature of the present work is that this careful study allows us to avoid relying on a conjecture about short character sums appearing in [10, 13], thus making our results unconditional.

More generally, given a sequence of complex numbers $\{a_n\}_n$ indexed by natural numbers, a problem of interest in analytic number theory is to prove an asymptotic formula for the sum over primes

$$S(X) := \sum_{\substack{p \text{ prime} \\ p \leq X}} a_p$$

as $X \to \infty$. Many sequences $\{a_n\}_n$ admit asymptotic formulas for $S(X)$ via various generalizations of the Prime Number Theorem, with essentially the best known error terms coming from ideas of de la Valée Poussin already in 1899 [4]. In 1947, Vinogradov [25, 26] invented another method to treat certain sequences which could not be handled with a variant of the Prime Number Theorem. His method has since been clarified and made easier to apply,

*Niels Bohrweg 1, 2333 CA Leiden, Netherlands, p.h.koymans@math.leidenuniv.nl
†Gower Street, London, United Kingdom, djordjo.milovic@ucl.ac.uk

most notably by Vaughan [24] and, for applications relating to more general number fields, by Friedlander et al. [10]. Nonetheless, there is a relative paucity of interesting sequences $\{a_n\}_n$ that admit an asymptotic formula for $S(X)$ via Vinogradov's method. The purpose of this paper is to present yet another such sequence, of a similar nature as those appearing in [10, 13]; similarly as in [13], the asymptotics we obtain have implications in the arithmetic statistics of class groups of number fields.

Let $p \equiv 1 \bmod 4$ be a prime number, and let $\mathrm{Cl}(-8p)$ denote the class group of the quadratic number field $\mathbb{Q}(\sqrt{-2p})$ of discriminant $-8p$. The finite abelian group $\mathrm{Cl}(-8p)$ measures the failure of unique factorization in the ring $\mathbb{Z}[\sqrt{-2p}]$. By Gauss's genus theory [12], the 2-part of $\mathrm{Cl}(-8p)$ is cyclic and non-trivial, and hence determined by the largest power of 2 dividing the order of $\mathrm{Cl}(-8p)$. For each integer $k \geq 1$, we define a density $\delta(2^k)$, if it exists, as

$$\delta(2^k) := \lim_{X\to\infty} \frac{\#\{p \leq X : \ p \equiv 1 \bmod 4, \ 2^k | \#\mathrm{Cl}(-8p)\}}{\#\{p \leq X : \ p \equiv 1 \bmod 4\}}.$$

As stated above, the 2-part of $\mathrm{Cl}(-8p)$ is cyclic and non-trivial, so $\delta(2) = 1$. It follows from the Chebotarev Density Theorem (a generalization of the Prime Number Theorem) that $\delta(4) = \frac{1}{2}$ and $\delta(8) = \frac{1}{4}$; indeed, Rédei [19] proved that $4|\#\mathrm{Cl}(-8p)$ if and only if p splits completely in $\mathbb{Q}(\zeta_8)$, and Stevenhagen [23] proved that $8|\#\mathrm{Cl}(-8p)$ if and only if p splits completely in $\mathbb{Q}(\zeta_8, \sqrt[4]{2})$, where ζ_8 denotes a primitive 8th root of unity. The qualitative behavior of divisibility by 16 departs from that of divisibility by lower 2-powers in that it can no longer be proved by a simple application of the Chebotarev Density Theorem. We instead use Vinogradov's method to prove

Theorem 1. *For a prime number $p \equiv 1 \bmod 4$, let $e_p = 0$ if $\mathrm{Cl}(-8p)$ does not have an element of order 8, let $e_p = 1$ if $\mathrm{Cl}(-8p)$ has an element of order 16, and let $e_p = -1$ otherwise. Then for all $X > 0$, we have*

$$\sum_{\substack{p \leq X \\ p\equiv 1 \bmod 4}} e_p \ll X^{1-\frac{1}{3200}},$$

where the implied constant is absolute. In particular, $\delta(16) = \frac{1}{8}$.

In combination with [17], we get

Corollary 2. *For a prime number p, let $h_2(-2p)$ denote the cardinality of the 2-part of the class group $\mathrm{Cl}(-8p)$. For an integer $k \geq 0$, let $\delta'(2^k)$ denote the natural density (in the set of all primes) of primes p such that $h_2(-2p) = 2^k$, if it exists. Then $\delta'(1) = 0$, $\delta'(2) = \frac{1}{2}$, $\delta'(4) = \frac{1}{4}$, and $\delta'(8) = \frac{1}{8}$.*

The power-saving bound in Theorem 1, similarly to the main results in [17] and [13], is another piece of evidence that *governing fields* for the 16-rank do *not* exist. For a sampling on previous work about governing fields, see [2], [3], [18], and [22].

The strategy to prove Theorem 1 is to construct a sequence $\{a_n\}_n$ which simultaneously carries arithmetic information about divisibility by 16 when n is a prime number congruent to 1 modulo 4 and is conducive to Vinogradov's method. On one hand, the criterion for divisibility by 16 cannot be stated naturally over the rational numbers $\mathbb{Q}$. For instance, even the criterion for divisibility by 8 is most naturally stated over a field of degree 8 over $\mathbb{Q}$. On the other hand, proving analytic estimates in a number field generally becomes more difficult as the degree of the number field increases, as exemplified by the reliance on a conjecture on short character sums in [10]. We manage to work over $\mathbb{Q}(\zeta_8)$, a field of degree 4. Although the methods of Friedlander et al. [10] narrowly miss the mark of being unconditional for number fields of degree 4, we manage to exploit the arithmetic structure of our sequence to ensure that Theorem 1 is unconditional.

Lastly, for work concerning the average behavior of the 2-parts of class groups of quadratic number fields in families that are *not* thin, i.e., for which the average number of primes dividing the discriminant grows as the discriminant grows, we point the reader to the extensive work of Fouvry and Klüners [5, 6, 7, 8] on the 4-rank and certain cases of the 8-rank and more recently to the work of Smith on the 8- and higher 2-power-ranks [20, 21]. While Smith's methods in [21] appear to be very powerful, the authors believe that they are unlikely to be applicable to thin families of the type appearing in this paper.

Funding

This work was supported by the National Science Foundation [DMS-1128155 to D.Z.M.].

Acknowledgements

The authors would like to thank Jan-Hendrik Evertse and Carlo Pagano for useful discussions.

2 Encoding the 16-rank of $\mathrm{Cl}(-8p)$ into sequences $\{a_\mathfrak{n}\}_\mathfrak{n}$

Given an integer $k \geq 1$, the 2^k-rank of a finite abelian group G, denoted by $\mathrm{rk}_{2^k} G$, is defined as the dimension of the $\mathbb{F}_2$-vector space $2^{k-1}G/2^kG$. If the 2-part of G is cyclic, then $\mathrm{rk}_{2^k} G \in \{0, 1\}$, and $\mathrm{rk}_{2^k} G = 1$ if and only if $2^k | \#G$. The order of a class group is called the class number, and we denote the class number of $\mathrm{Cl}(-8p)$ by $h(-8p)$.

The criterion for divisibility of $h(-8p)$ by 16 that we will use is due to Leonard and Williams [16, Theorem 2, p. 204]. Given a prime number $p \equiv 1 \bmod 8$ (so that $4|h(-8p)$), there exist integers u and v such that

$$p = u^2 - 2v^2, \qquad u > 0. \tag{2.1}$$

The integers u and v are *not* uniquely determined by p; nevertheless, if (u_0, v_0) is one such pair, then, every such pair (u, v) is of the form $u + v\sqrt{2} = \varepsilon^{2m}(u_0 \pm v_0\sqrt{2})$ for some $m \in \mathbb{Z}$, where $\varepsilon = 1 + \sqrt{2}$. The criterion for divisibility by 8 can be restated in terms of a quadratic residue symbol; one has

$$8|h(-8p) \Longleftrightarrow \left(\frac{u}{p}\right)_2 = 1.$$

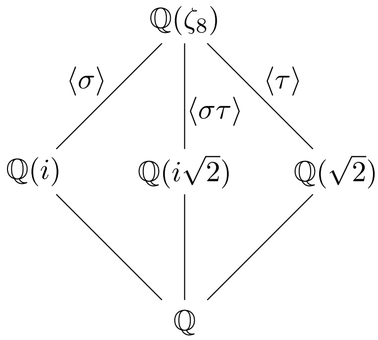
Note that $1 = (u/p)_2 = (p/u)_2 = (-2/u)_2$, so that $8|h(-8p)$ if and only if $u \equiv 1, 3 \bmod 8$. As $\varepsilon^2(u + v\sqrt{2}) = (3u + 4v) + (2u + 3v)\sqrt{2}$ and v is even, we can always choose u and v in (2.1) so that $u \equiv 1 \bmod 8$. The criterion for divisibility of $h(-8p)$ by 16 states that if u and v are integers satisfying (2.1) and $u \equiv 1 \bmod 8$, then

$$16|h(-8p) \Longleftrightarrow \left(\frac{u}{p}\right)_4 = 1,$$

where $(u/p)_4$ is equal to 1 or -1 depending on whether or not u is a fourth power modulo p. To take advantage of the multiplicative properties of the fourth-power residue symbol, one has to work over a field containing $i = \sqrt{-1}$, a primitive fourth root of unity. Since u appears naturally via the splitting of p in $\mathbb{Q}(\sqrt{2})$, we see that the natural setting for the criterion above is the number field

$$M := \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8),$$

of degree 4 over $\mathbb{Q}$. It is straightforward to check that the class number of M and each of its subfields is 1, that 2 is totally ramified in M, and that the unit group of its ring of integers $\mathcal{O}_M = \mathbb{Z}[\zeta_8]$ is generated by ζ_8 and $\varepsilon = 1 + \sqrt{2}$. Note that $M/\mathbb{Q}$ is a normal extension with Galois group isomorphic to the Klein four group, say $\{1, \sigma, \tau, \sigma\tau\}$, where σ fixes $\mathbb{Q}(i)$ and τ fixes $\mathbb{Q}(\sqrt{2})$.



Let $p \equiv 1 \bmod 8$ be a prime, so that p splits completely in M. Then there exists $w \in \mathcal{O}_M$ such that $\mathrm{N}(w) = p$, i.e., such that $p = w\sigma(w)\tau(w)\sigma\tau(w)$. Note that the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_M$ induces an isomorphism $\mathbb{Z}/(p) \cong \mathcal{O}_M/(w)$, so that an integer n is a fourth power modulo p exactly when it is a fourth power modulo w. As $w\tau(w) \in \mathbb{Z}[\sqrt{2}]$, there exist integers u and v such that $w\tau(w) = u + v\sqrt{2}$. Then $u = (w\tau(w) + \sigma(w)\sigma\tau(w))/2$. With this in mind, we define, for any $\alpha \in \mathbb{Z}[\sqrt{2}]$,

$$\mathrm{r}(\alpha) = \frac{1}{2}\left(\alpha + \sigma(\alpha)\right)$$

and, for *any odd* (i.e., coprime to 2) $w \in \mathcal{O}_M$, not necessarily prime,

$$[w] := \left(\frac{\mathrm{r}(w\tau(w))}{w}\right)_4,$$

where $(\cdot/\cdot)_4$ is the quartic residue symbol in M; we recall the definition of $(\cdot/\cdot)_4$ in the next section. A simple computation shows that $\mathrm{r}(w\tau(w)) > 0$ for any non-zero $w \in \mathcal{O}_M$. Hence $16|h(-8p)$ if and only if $[w] = 1$, where w is any element of $\mathcal{O}_M$ such that $\mathrm{N}(w) = p$ and $\mathrm{r}(w) \equiv 1 \bmod 8$.

Given a Dirichlet character χ modulo 8, we define, for any odd $w \in \mathcal{O}_M$,

$$[w]_\chi := [w] \cdot \chi(\mathrm{r}(w\tau(w))).$$

Then

$$\frac{1}{4}\sum_{\chi \bmod 8} [w]_\chi = \begin{cases} [w] & \text{if } \mathrm{r}(w\tau(w)) \equiv 1 \bmod 8, \\ 0 & \text{otherwise,} \end{cases}$$

where the sum is over all Dirichlet characters modulo 8. Another simple computation shows that, for all odd $w \in \mathcal{O}_M$, we have $[\zeta_8 w] = [w]$. We note that $\mathrm{r}(\varepsilon^2\alpha) \equiv 3 \cdot \mathrm{r}(\alpha) \bmod 8$ for any

$\alpha \in \mathbb{Z}[\sqrt{2}]$, so that $\chi(\mathrm{r}(\varepsilon^2 w\tau(\varepsilon^2 w))) = \chi(\mathrm{r}(w\tau(w)))$ for every Dirichlet character χ modulo 8. Finally, we note that

$$[w] = \left(\frac{16\mathrm{r}(w\tau(w))}{w}\right)_4 = \left(\frac{8\sigma(w)\sigma\tau(w)}{w}\right)_4, \tag{2.2}$$

so that

$$[\varepsilon w] = \left(\frac{\sigma(\varepsilon)}{w}\right)_2 [w],$$

and hence $[\varepsilon^2 w] = [w]$. Having determined the action of the units $\mathcal{O}_M^\times$ on $[\cdot]_\chi$, we can define, for each Dirichlet character χ modulo 8, a sequence $\{a(\chi)_\mathfrak{n}\}_\mathfrak{n}$ indexed by *ideals* of $\mathcal{O}_M$ by setting $a(\chi)_\mathfrak{n} = 0$ if $\mathfrak{n}$ is even, and otherwise

$$a(\chi)_\mathfrak{n} := [w]_\chi + [\varepsilon w]_\chi, \tag{2.3}$$

where w is any generator of the odd ideal $\mathfrak{n}$. Again because $\mathrm{r}(\varepsilon^2\alpha) \equiv 3 \cdot \mathrm{r}(\alpha) \bmod 8$ for any $\alpha \in \mathbb{Z}[\sqrt{2}]$, we see that if $8|h(-8p)$, then exactly one of $\mathrm{r}(w\tau(w))$ and $\mathrm{r}(\varepsilon w\tau(\varepsilon w))$ is 1 mod 8, and if $8 \nmid h(-8p)$, then neither is 1 mod 8. We have proved

Proposition 2.1. *Let $p \equiv 1 \bmod 8$ be a prime, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_M$ lying above p. Then*

$$\frac{1}{4}\sum_{\chi \bmod 8} a(\chi)_\mathfrak{p} = \begin{cases} 1 & \text{if } 16|h(-8p), \\ -1 & \text{if } 8|h(-8p) \text{ but } 16 \nmid h(-8p), \\ 0 & \text{otherwise,} \end{cases}$$

where the sum is over Dirichlet characters modulo 8.

3 Prerequisites

We now collect some definitions and facts that we will use in our proof of Theorem 1.

3.1 Quartic residue symbols and quartic reciprocity

Let L be a number field with ring of integers $\mathcal{O}_L$. Let $\mathfrak{p}$ be an odd prime ideal of $\mathcal{O}_L$ and let $\alpha \in \mathcal{O}_L$. One defines the *quadratic residue symbol* $(\alpha/\mathfrak{p})_{L,2}$ by setting

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{L,2} := \begin{cases} 0 & \text{if } \alpha \in \mathfrak{p} \\ 1 & \text{if } \alpha \notin \mathfrak{p} \text{ and } \alpha \equiv \beta^2 \bmod \mathfrak{p} \text{ for some } \beta \in \mathcal{O}_L \\ -1 & \text{otherwise.} \end{cases}$$

Then we have $(\alpha/\mathfrak{p})_{L,2} \equiv \alpha^{\frac{\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p})-1}{2}} \bmod \mathfrak{p}$. The quadratic residue symbol is then extended multiplicatively to all odd ideals $\mathfrak{n}$, and then also to all odd elements β in $\mathcal{O}_L$ by setting $(\alpha/\beta)_{L,2} = (\alpha/\beta\mathcal{O}_L)_{L,2}$. To define the quartic residue symbol, we assume that L contains $\mathbb{Q}(i)$. Then one can define the *quartic residue symbol* $(\alpha/\mathfrak{p})_{L,4}$ as the element of $\{\pm 1, \pm i, 0\}$ such that

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{L,4} \equiv \alpha^{\frac{\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p})-1}{4}} \bmod \mathfrak{p},$$

and extend this to all odd ideals $\mathfrak{n}$ and odd elements β in the same way as the quadratic residue symbol. A key property of the quartic residue symbol that we will use extensively is the following weak version of quartic reciprocity in $M := \mathbb{Q}(\zeta_8)$.

Lemma 3.1. *Let $\alpha, \beta \in \mathcal{O}_M$ with β odd. Then $(\alpha/\beta)_{M,4}$ depends only on the congruence class of β modulo $16\alpha\mathcal{O}_M$. Moreover, if α is also odd, then*

$$\left(\frac{\alpha}{\beta}\right)_{M,4} = \mu \cdot \left(\frac{\beta}{\alpha}\right)_{M,4},$$

where $\mu \in \{\pm 1, \pm i\}$ depends only on the congruence classes of α and β modulo $16\mathcal{O}_M$.

Proof. This follows from [15, Proposition 6.11, p. 199]. □

3.2 Field lowering

A key feature of our proof is the reduction of quartic residue symbols in a quartic number field to quadratic residue symbols in a quadratic field. We do this by using the following three lemmas.

Lemma 3.2. *Let K be a number field and let $\mathfrak{p}$ be an odd prime ideal of K. Suppose that L is a quadratic extension of K such that L contains $\mathbb{Q}(i)$ and $\mathfrak{p}$ splits in L. Denote by ψ the non-trivial element in Gal(L/K). Then if ψ fixes $\mathbb{Q}(i)$ we have for all $\alpha \in \mathcal{O}_K$*

$$\left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_L}\right)_{L,4} = \left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_K}\right)_{K,2}$$

and if ψ does not fix $\mathbb{Q}(i)$ we have for all $\alpha \in \mathcal{O}_K$ with $\mathfrak{p} \nmid \alpha$

$$\left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_L}\right)_{L,4} = 1$$

Proof. Since $\mathfrak{p}$ splits in L, we can write $\mathfrak{p} = \mathfrak{q}\psi(\mathfrak{q})$ for some prime ideal $\mathfrak{q}$ of L. Hence we have

$$\left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_L}\right)_{L,4} = \left(\frac{\alpha}{\mathfrak{q}}\right)_{L,4} \left(\frac{\alpha}{\psi(\mathfrak{q})}\right)_{L,4}.$$

If ψ fixes i we find that

$$\left(\frac{\alpha}{\mathfrak{q}}\right)_{L,4} = \psi\left(\left(\frac{\alpha}{\mathfrak{q}}\right)_{L,4}\right) = \left(\frac{\psi(\alpha)}{\psi(\mathfrak{q})}\right)_{L,4} = \left(\frac{\alpha}{\psi(\mathfrak{q})}\right)_{L,4}.$$

Combining this with the previous identity gives

$$\left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_L}\right)_{L,4} = \left(\frac{\alpha}{\mathfrak{q}}\right)_{L,4}^2 = \left(\frac{\alpha}{\mathfrak{q}}\right)_{L,2} = \left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_K}\right)_{K,2},$$

establishing the first part of the lemma. If ψ does not fix i we find that

$$\left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_L}\right)_{L,4} = \left(\frac{\alpha}{\mathfrak{q}}\right)_{L,4} \left(\frac{\alpha}{\psi(\mathfrak{q})}\right)_{L,4} = \left(\frac{\alpha}{\mathfrak{q}}\right)_{L,4} \psi\left(\left(\frac{\alpha}{\mathfrak{q}}\right)_{L,4}\right) = 1$$

by checking this for all values of $(\alpha/\mathfrak{q})_{L,4} \in \{\pm 1, \pm i\}$. This completes the proof. □

Lemma 3.3. *Let K be a number field and let $\mathfrak{p}$ be an odd prime ideal of K of degree 1 lying above p. Suppose that L is a quadratic extension of K such that L contains $\mathbb{Q}(i)$ and $\mathfrak{p}$ stays inert in L. Then we have for all $\alpha \in \mathcal{O}_K$*

$$\left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_L}\right)_{L,4} = \left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_K}\right)_{K,2}^{\frac{p+1}{2}}.$$

Proof. We have

$$\left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_L}\right)_{L,4} \equiv \alpha^{\frac{\mathrm{N}_L(\mathfrak{p})-1}{4}} \equiv \alpha^{\frac{p^2-1}{4}} \equiv \left(\alpha^{\frac{p-1}{2}}\right)^{\frac{p+1}{2}} \equiv \left(\alpha^{\frac{\mathrm{N}_K(\mathfrak{p})-1}{2}}\right)^{\frac{p+1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}\mathcal{O}_K}\right)_{K,2}^{\frac{p+1}{2}} \bmod \mathfrak{p},$$

which immediately implies the lemma. □

Note that the previous lemmas only work if $\alpha \in \mathcal{O}_K$. Our last lemma gives a way to ensure that $\alpha \in \mathcal{O}_K$.

Lemma 3.4. *Let K be a number field and let L be a quadratic extension of K. Denote by ψ the non-trivial element in Gal(L/K). Suppose that $\mathfrak{p}$ is a prime ideal of K that does not ramify in L and further suppose that $\beta \in \mathcal{O}_L$ satisfies $\beta \equiv \psi(\beta) \bmod \mathfrak{p}\mathcal{O}_L$. Then there is $\beta' \in \mathcal{O}_K$ such that $\beta' \equiv \beta \bmod \mathfrak{p}\mathcal{O}_L$.*

Proof. Since by assumption $\mathfrak{p}$ does not ramify in L, we may assume that $\mathfrak{p}$ splits or stays inert in L. Let us first do the case that $\mathfrak{p}$ stays inert, which means precisely that $\psi(\mathfrak{p}) = \mathfrak{p}$. We conclude that ψ is in the decomposition group of $\mathfrak{p}$. Furthermore, the inertia group of $\mathfrak{p}$ is trivial by the assumption that $\mathfrak{p}$ does not ramify. Since ψ is not the identity, it follows that ψ must become the Frobenius map of the finite field extension $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{p}$. Then $\beta \equiv \psi(\beta) \bmod \mathfrak{p}\mathcal{O}_L$ means that β is fixed by the Frobenius map. We conclude that β comes from $\mathcal{O}_K/\mathfrak{p}$, which we had to prove.

We still have to prove the lemma if $\mathfrak{p}$ splits. In this case we can write $\mathfrak{p} = \mathfrak{q}\psi(\mathfrak{q})$ for some prime ideal $\mathfrak{q}$ of L. Note that

$$\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathfrak{q} \times \mathcal{O}_L/\psi(\mathfrak{q}). \tag{3.1}$$

One checks that ψ is the automorphism of $\mathcal{O}_L/\mathfrak{q} \times \mathcal{O}_L/\psi(\mathfrak{q})$ that maps (x, y) to $(\psi(y), \psi(x))$. Hence $\beta \equiv \psi(\beta) \bmod \mathfrak{p}\mathcal{O}_L$ implies that there is some $x \in \mathcal{O}_L/\mathfrak{q}$ such that $\beta = (x, \psi(x))$ as an element of $\mathcal{O}_L/\mathfrak{q} \times \mathcal{O}_L/\psi(\mathfrak{q})$. Since $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_L/\mathfrak{q}$, we can pick $\beta' \in \mathcal{O}_K$ such that β' maps to x under the natural inclusion $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{q}$. Then it follows that β maps to $(\beta', \psi(\beta'))$ under the maps given as in (3.1). This implies that $\beta' \equiv \beta \bmod \mathfrak{p}\mathcal{O}_L$ as desired. □

3.3 A fundamental domain for the action of $\mathcal{O}_M^\times$

In defining $a(\chi)_\mathfrak{n}$ for odd ideals $\mathfrak{n}$ of $\mathcal{O}_M$, we had to choose a generator w for the ideal $\mathfrak{n}$. There are many such choices, since the group of units of $\mathcal{O}_M$ is quite large, i.e.,

$$\mathcal{O}_M^\times = \langle \zeta_8 \rangle \times \langle \varepsilon \rangle,$$

where $\varepsilon = 1 + \sqrt{2}$ as before. It will be important to us that we can choose generators that are in some sense as small as possible. We will do so by constructing a fundamental domain for the action (by multiplication) of $\mathcal{O}_M^\times$ on $\mathcal{O}_M$. The lemma that follows is usually implicitly proved in most number theory textbooks, but we have not been able to find a reference stating exactly the somewhat peculiar version that we will need. Below we deduce this version from [14, Lemma 1, p. 131].

More generally, let F be a number field of degree n over $\mathbb{Q}$ with ring of integers $\mathcal{O}_F$. Let $\sigma_1, \ldots, \sigma_r : F \hookrightarrow \mathbb{R}$ be the real embeddings of F and let $\tau_1, \bar{\tau}_1, \ldots, \tau_s, \bar{\tau}_s : F \hookrightarrow \mathbb{C}$ be the pairs of non-real complex conjugate embeddings of F (so that $r + 2s = n$). Let T be the subgroup of the unit group $\mathcal{O}_F^\times$ consisting of units of finite order. By Dirichlet's Unit Theorem, there exists a free abelian subgroup $V \subset \mathcal{O}_F^\times$ of rank $r + s - 1$ such that $\mathcal{O}_F^\times = T \times V$; fix one such V.

Let $\eta = \{\eta_1, \ldots, \eta_n\}$ be an integral basis for $\mathcal{O}_F$; it defines an isomorphism $i_\eta : \mathbb{Q}^n \to F$ via the map $(a_1, \ldots, a_n) \mapsto a_1\eta_1 + \cdots a_n\eta_n$. For a subset $S \subset \mathbb{R}^n$ and an element $\alpha = a_1\eta_1 + \cdots + a_n\eta_n \in F$, we will say that α is in S (or $\alpha \in S$) to mean that $(a_1, \ldots, a_n) \in S$. Let $f_\eta \in \mathbb{Z}[x_1, \ldots, x_n]$ be the homogeneous polynomial of degree n in n variables defined by $f_\eta(x_1, \ldots, x_n) = \mathrm{N}(x_1\eta_1 + \cdots + x_n\eta_n)$. For a subset $S \subset \mathbb{R}^n$ and a real number $X > 0$, let $S(X)$ be the set of all $(s_1, \ldots, s_n) \in S$ such that $|f_\eta(s_1, \ldots, s_n)| \leq X$.

Lemma 3.5. *There exists a subset $\mathcal{D} \subset \mathbb{R}^n$ such that:*

(1) for all $\alpha \in \mathcal{O}_F \setminus \{0\}$, there exists a unique $v \in V$ such that $v\alpha \in \mathcal{D}$; moreover, the complete set of $u \in \mathcal{O}_F^\times$ such that $u\alpha \in \mathcal{D}$ is $\{\mu v : \mu \in T\}$;

(2) $\mathcal{D}(1)$ has an $(n-1)$-Lipschitz parametrizable boundary; and

(3) there exists a constant $C_\eta > 0$ such that for all $\alpha = a_1\eta_1 + \cdots + a_n\eta_n \in \mathcal{D}$ (with $a_i \in \mathbb{Z}$), we have $|a_i| \leq C_\eta \cdot |\mathrm{N}(\alpha)|^{\frac{1}{n}}$.

Proof. Let $J = \mathbb{R}^r \times \mathbb{C}^s$. Then $j = (\sigma_1, \ldots, \sigma_r, \tau_1, \ldots, \tau_s)$ defines an embedding $j : F \hookrightarrow J$. Moreover, $j \circ i_\eta : \mathbb{Q}^n \to J$ is a *linear* map of $\mathbb{Q}$-vector spaces. By extension of scalars, we extend this to a linear map

$$\bar{j} : \mathbb{R}^n \to J.$$

It follows from [14, Lemma 1, p. 131] and its proof that there is a subset $D \subset J^\times$ such that:

(1') for all $\alpha \in J^\times$, there exists a unique $v \in V$ such that $v\alpha \in D$; moreover, the complete set of $u \in \mathcal{O}_F^\times$ such that $u\alpha \in D$ is $\{\mu v : \mu \in T\}$; and

(2') $D(1) = \{(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s) \in D : \prod_{i=1}^r |\alpha_i| \prod_{j=1}^s |\beta_j|^2 \leq 1\}$ has an $(n-1)$-Lipschitz parametrizable boundary.

(3') for all non-zero $t \in \mathbb{R}$, we have $tD = D$.

Let $\mathcal{D} = \bar{j}^{-1}(D)$. Then (1) follows immediately from (1'). Since $\bar{j}$ is linear and hence Lipschitz continuous, (2') immediately implies (2) (after also taking into account the definitions of $D(1)$, f_η, and $\mathcal{D}(1)$). By (2), the set $\mathcal{D}(1) \subset \mathbb{R}^n$ is bounded, so we can set

$$C_\eta = \sup\{|a_i| : (a_1, \ldots, a_n) \in \mathcal{D}(1)\}.$$

Finally, again because $\bar{j}$ is linear, (3') implies that $t\mathcal{D} = \mathcal{D}$ for all non-zero $t \in \mathbb{R}$, so that $\mathcal{D}(t) = t^{1/n}\mathcal{D}(1)$. This proves (3). □

3.4 General bilinear sum estimates

Let F, n, η, and V be as in Section 3.3. Fix a fundamental domain $\mathcal{D}$ for the action of V on $\mathcal{O}_F$ as in Lemma 3.5. Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be a pair of translates of $\mathcal{D}$, i.e., $\mathcal{D}_i = v_i\mathcal{D}$ for some

$v_i \in V$. Let $\mathfrak{f}$ be a non-zero ideal in $\mathcal{O}_F$, and let $S_{\mathfrak{f}}$ be the set of elements in $\mathcal{O}_F$ coprime to $\mathfrak{f}$. Suppose γ is a map

$$\gamma : S_{\mathfrak{f}} \times \mathcal{O}_F \to \{-1, 0, 1\}$$

satisfying the following properties:

(P1) for every pair of invertible congruence classes ω and ζ modulo $\mathfrak{f}$, there exists $\mu(\omega, \zeta) \in \{\pm 1\}$ such that $\gamma(w, z) = \mu(\omega, \zeta)\gamma(z, w)$ whenever $w \equiv \omega \bmod \mathfrak{f}$ and $z \equiv \zeta \bmod \mathfrak{f}$;

(P2) for all $z_1, z_2 \in \mathcal{O}_F$ and all $w \in S_{\mathfrak{f}}$, we have $\gamma(w, z_1z_2) = \gamma(w, z_1)\gamma(w, z_2)$; similarly, for all $w_1, w_2 \in S_{\mathfrak{f}}$ and all $z \in \mathcal{O}_F$, we have $\gamma(w_1w_2, z) = \gamma(w_1, z)\gamma(w_2, z)$; and

(P3) for all $w \in S_{\mathfrak{f}}$, if $z_1, z_2 \in \mathcal{O}_F$ satisfy $z_1 \equiv z_2 \bmod \mathrm{N}(w)$ (i.e., $z_1 - z_2 = N(w)\alpha$ for some $\alpha \in \mathcal{O}_F$), then we have $\gamma(w, z_1) = \gamma(w, z_2)$; moreover, if $|\mathrm{N}(w)|$ is not a square in $\mathbb{Z}$, we have $\sum_{\xi \bmod \mathrm{N}(w)} \gamma(w, \xi) = 0$.

We will consider bilinear sums of the type

$$B(M, N; \omega, \zeta) := \sum_{\substack{w \in \mathcal{D}_1(M) \\ w \equiv \omega \bmod \mathfrak{f}}} \sum_{\substack{z \in \mathcal{D}_2(N) \\ z \equiv \zeta \bmod \mathfrak{f}}} \alpha_w \beta_z \gamma(w, z), \tag{3.2}$$

where $\{\alpha_w\}_w$ and $\{\beta_z\}_z$ are bounded sequences of complex numbers, ω and ζ are invertible congruence classes modulo $\mathfrak{f}$, and M and N are positive real numbers. Recall that $w \in \mathcal{D}_1(M)$ if and only if $w \in \mathcal{D}_1$ and $|\mathrm{N}(w)| \leq M$, and similarly for $\mathcal{D}_2(N)$. Also recall that n is the degree of $F/\mathbb{Q}$. The following proposition is analogous to the bilinear sum estimates in [9, 10].

Proposition 3.6. *We have*

$$B(M, N; \omega, \zeta) \ll_\epsilon \left(M^{-\frac{1}{6n}} + N^{-\frac{1}{6n}}\right)(MN)^{1+\epsilon},$$

where the implied constant depends on ϵ, on the units v_1 and v_2, on the supremum norms of $\{\alpha_w\}_w$ and $\{\beta_z\}_z$, and the congruence classes ω and ζ modulo $\mathfrak{f}$.

Proof. We will prove that

$$B(M, N; \omega, \zeta) \ll_\epsilon M^{-\frac{1}{6n}}(MN)^{1+\epsilon} \tag{3.3}$$

whenever $N \geq M$; the proposition then immediately follows from the symmetry of the sum $B(M, N; \omega, \zeta)$ coming from property (P1). So suppose that $N \geq M$. We fix an integer $k \geq 2n$, and we apply Hölder's inequality (with $1 = \frac{k-1}{k} + \frac{1}{k}$) to the w variable to get

$$|B(M, N; \omega, \zeta)|^k \leq \left(\sum_w |\alpha_w|^{\frac{k}{k-1}}\right)^{k-1} \sum_w \left|\sum_z \beta_z \gamma(w, z)\right|^k,$$

where the summations over w and z are as above in (3.2). The first factor above is bounded trivially by $\ll M^{k-1}$, where the implied constant depends on the supremum norm of the sequence $\{\alpha_w\}_w$, on the fixed unit v_1, and on the constant C_η from part (3) of Lemma 3.5.

We use property (P2), as well as the identity $|\alpha|^k = \alpha^k \cdot (|\alpha|/\alpha)^k$, to expand the inner sum in the second factor above, getting

$$|B(M,N;\omega,\zeta)|^k \ll M^{k-1} \sum_w \varepsilon(w) \sum_z \beta'_z \gamma(w,z),$$

where

$$\beta'_z = \sum_{\substack{z=z_1\cdots z_k \\ z_1,\ldots,z_k \in \mathcal{D}_2(N) \\ z_1 \equiv \cdots \equiv z_k \equiv \zeta \bmod \mathfrak{f}}} \beta_{z_1} \cdots \beta_{z_k},$$

where $\varepsilon(w) = (|\sum_z \beta_z \gamma(w,z)|/\sum_z \beta_z \gamma(w,z))^k$, and where once again the summation conditions for w are as in (3.2). Since an ideal $\mathfrak{n}$ in $\mathcal{O}_F$ can be written as a product of k ideals in at most $\ll_\epsilon \mathrm{N}(\mathfrak{n})^\epsilon$ ways, and since $\mathcal{D}_2$ contains at most one generator of any principal ideal, we see that $\beta'_z \ll_\epsilon N^\epsilon$. Moreover, the coordinates of each $z_i \in \mathcal{D}_2$ $(1 \leq i \leq k)$ of absolute norm at most N in the basis η are bounded by $N^{\frac{1}{n}}$ times a constant depending on the unit v_2 and on C_η from Lemma 3.5. Hence we may assume that the sum $\sum_z \beta'_z \gamma(w,z)$ above is over $z = a_1\eta_1 + \cdots + a_n\eta_n$ in a box $\mathcal{B}$ defined by $|a_j| \ll N^{\frac{k}{n}}$ $(1 \leq j \leq n)$, with the implied constant depending on v_2 and on the integral basis η. Next, we apply the Cauchy-Schwarz inequality to the z variable above and use property (P2) to get

$$\left| \sum_w \varepsilon(w) \sum_z \beta'_z \gamma(w,z) \right|^2 \ll_\epsilon N^{k+\epsilon} \sum_{w_1} \sum_{w_2} \varepsilon(w_1)\overline{\varepsilon(w_2)} \sum_z \gamma(w_1 w_2, z),$$

where the summation conditions for w_1 and w_2 are as those for w in (3.2), while the inner sum is over $z \in \mathcal{B}$. We break up the sum over z into congruence classes ξ modulo $\mathrm{N}(w_1w_2)$ and note that, by property (P3),

$$\sum_{\xi \bmod \mathrm{N}(w_1w_2)} \gamma(w_1w_2, z) = 0$$

unless $|\mathrm{N}(w_1w_2)|$ is a square. By counting points z in the box $\mathcal{B}$ and noting that $|\mathrm{N}(w_1w_2)| \leq M^2$, this gives

$$\sum_z \gamma(w_1w_2,z) \ll \begin{cases} N^k & \text{if } |\mathrm{N}(w_1w_2)| = \square \\ \sum_{i=1}^n M^{2i} N^{k(1-\frac{i}{n})} & \text{otherwise.} \end{cases}$$

Since we took $k \geq 2n$ and since $N \geq M$, we have $N^{\frac{k}{n}} \geq M^2$, so the last bound can be simplified to $M^2 N^{k(1-\frac{1}{n})}$. Hence, putting together all of the bounds above, we get

$$\begin{aligned} |B(M,N;\omega,\zeta)|^{2k} &\ll_\epsilon M^{2k-2}N^k \left(M \cdot N^k + M^2 \cdot M^2 N^{k(1-\frac{1}{n})} \right) (MN)^\epsilon \\ &\ll_\epsilon \left(M^{2k-1}N^{2k} + M^{2k+2} N^{2k(1-\frac{1}{2n})} \right) (MN)^\epsilon. \end{aligned}$$

Since $N \geq M$, if we take $k = 3n$, we get that $N^{2k\frac{1}{2n}} \geq M^3$, so that the first term above dominates the second term. With this choice of k, we get

$$|B(M,N;\omega,\zeta)| \ll_\epsilon M^{-\frac{1}{6n}} (MN)^{1+\epsilon},$$

and this finishes the proof of (3.3). $\square$

3.5 The sieve

We will prove Theorem 1 by a sieve of Friedlander et al. [10] that generalizes the ideas of Vinogradov [25, 26] to the setting of number fields. Let χ be a Dirichlet character modulo 8, and let $a(\chi)_{\mathfrak{n}}$ be defined as in (2.3). We will prove the following two propositions.

Proposition 3.7. *For every $\epsilon > 0$, we have*

$$\sum_{\mathrm{N}(\mathfrak{n})\leq X,\ \mathfrak{m}|\mathfrak{n}} a(\chi)_{\mathfrak{n}} \ll_\epsilon X^{1-\frac{1}{64}+\epsilon}$$

uniformly for all non-zero ideals $\mathfrak{m}$ of $\mathcal{O}_M$ and all $X \geq 2$.

Proposition 3.8. *For every $\epsilon > 0$, we have*

$$\sum_{\mathrm{N}(\mathfrak{m})\leq M}\sum_{\mathrm{N}(\mathfrak{n})\leq N} \alpha_{\mathfrak{m}}\beta_{\mathfrak{n}}a(\chi)_{\mathfrak{mn}} \ll_\epsilon (M+N)^{\frac{1}{24}}(MN)^{1-\frac{1}{24}+\epsilon}$$

uniformly for all $M, N \geq 2$ and sequences of complex numbers $\{\alpha_{\mathfrak{m}}\}$ and $\{\beta_{\mathfrak{n}}\}$ satisfying $|\alpha_{\mathfrak{m}}|, |\beta_{\mathfrak{n}}| \leq 1$.

From these two propositions we can apply [10, Proposition 5.2, p. 722] with $\theta_1 = \frac{1}{64}$ and $\theta_2 = \frac{1}{24}$ to prove

$$\sum_{\mathrm{N}(\mathfrak{n})\leq X} a(\chi)_{\mathfrak{n}}\Lambda(\mathfrak{n}) \ll_\theta X^{1-\theta}$$

for all $\theta < 1/(49\cdot 64) = 1/3136$. By partial summation, it follows that, say,

$$\sum_{\mathrm{N}(\mathfrak{p})\leq X} a(\chi)_{\mathfrak{p}} \ll X^{1-\frac{1}{3200}}. \tag{3.4}$$

As

$$\sum_{\substack{\mathrm{N}(\mathfrak{p})\leq X \\ \mathfrak{p}\text{ lies over } p\not\equiv 1 \bmod 8}} 1 \ll X^{\frac{1}{2}},$$

Theorem 1 follows from (3.4) and Proposition 2.1. It now remains to prove Propositions 3.7 and 3.8.

4 Proof of Proposition 3.7

Let χ be a Dirichlet character modulo 8. Let $\mathfrak{m}$ be an odd ideal of $\mathcal{O}_M$. In view of Proposition 2.1 we must bound the following sum

$$A(x) = A(x;\chi,\mathfrak{m}) := \sum_{\substack{\mathrm{N}(\mathfrak{a})\leq x \\ (\mathfrak{a},2)=1,\ \mathfrak{m}|\mathfrak{a}}} \left([\alpha]_\chi + [\varepsilon\alpha]_\chi\right),$$

where α is chosen to be any generator of $\mathfrak{a}$. Our proof is based on the argument in [13, Section 3, p. 12-19], which is in turn based on [10, Section 6, p. 722-733]. Let $\mathcal{D}$ be a fundamental domain for the action of $\mathcal{O}_M^\times$ on $\mathcal{O}_M \setminus \{0\}$ as in Lemma 3.5, with respect to the integral basis $\eta = \{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$. Each non-zero ideal $\mathfrak{a}$ has exactly 8 generators $\alpha \in \mathcal{D}$. Set $u_1 = 1$

and $u_2 = \varepsilon$. Set $F = 16$. Note that $\chi(\mathrm{r}(\alpha\tau(\alpha)))$ depends only on the congruence class of α modulo 8. After splitting the above sum into congruence classes modulo F, and using (2.2) and Lemma 3.1, we find that

$$A(x) = \frac{1}{8}\sum_{i=1}^{2}\sum_{\substack{\rho \bmod F\\(\rho,F)=1}}\mu(\rho,u_i)A(x;\rho,u_i),$$

where $\mu(\rho,u_i) \in \{\pm1,\pm i\}$ depends only on ρ and u_i and where

$$A(x;\rho,u_i) := \sum_{\substack{\alpha\in u_i\mathcal{D},\ \mathrm{N}(\alpha)\le x\\ \alpha\equiv\rho \bmod F\\ \alpha\equiv 0 \bmod \mathfrak{m}}}\left(\frac{\sigma(\alpha)}{\alpha}\right)_{M,4}\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{M,4}.$$

Our goal is to estimate $A(x;\rho,u_i)$ separately for each congruence class $\rho \bmod F$, $(\rho,F)=1$ and unit u_i. We view $\mathcal{O}_M$ as a $\mathbb{Z}$-module of rank 4 and decompose it as $\mathcal{O}_M = \mathbb{Z}\oplus\mathbb{M}$, where $\mathbb{M} = \mathbb{Z}\zeta_8\oplus\mathbb{Z}\zeta_8^2\oplus\mathbb{Z}\zeta_8^3$ is a free $\mathbb{Z}$-module of rank 3. We can write α uniquely as

$$\alpha = a+\beta, \text{ with } a\in\mathbb{Z}, \beta\in\mathbb{M},$$

so that the summation conditions above are equivalent to

$$a+\beta\in u_i\mathcal{D},\quad \mathrm{N}(a+\beta)\le x,\quad a+\beta\equiv\rho \bmod F,\quad a+\beta\equiv 0 \bmod \mathfrak{m}. \tag{$*$}$$

We may assume that $\sigma(\beta)\neq\beta$ and $\sigma\tau(\beta)\neq\beta$. Indeed, if $\sigma(\beta)=\beta$ or $\sigma\tau(\beta)=\beta$, the residue symbol in $A(x;\rho,u_i)$ is zero. We are now going to rewrite $(\sigma(\alpha)/\alpha)_{M,4}$ and $(\sigma\tau(\alpha)/\alpha)_{M,4}$ by using the same trick as in [10, p. 725]. Put

$$\sigma(\beta)-\beta = \eta^2c_0c \quad\text{ and }\quad \sigma\tau(\beta)-\beta = \eta'^2c_0'c'$$

with $c_0,c_0',c,c',\eta,\eta'\in\mathcal{O}_M$, $c_0,c_0' \mid F$ squarefree, $\eta,\eta' \mid F^\infty$ and $(c,F)=(c',F)=1$. By multiplying with an appropriate unit we can even ensure that $c\in\mathbb{Z}[i]$ and $c'\in\mathbb{Z}[\sqrt{-2}]$. Indeed, observe that

$$\alpha' := \frac{\sigma(\alpha)-\alpha}{\zeta_8} = \frac{\sigma(\beta)-\beta}{\zeta_8}\in\mathbb{Z}[i], \tag{4.1}$$

and we have a similar identity for $\sigma\tau(\beta)-\beta$. Then we obtain, just as in [13, p. 14], by Lemma 3.1,

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)_{M,4} = \mu_1\cdot\left(\frac{a+\beta}{c\mathcal{O}_M}\right)_{M,4} \quad\text{ and }\quad \left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{M,4} = \mu_2\cdot\left(\frac{a+\beta}{c'\mathcal{O}_M}\right)_{M,4},$$

where $\mu_1,\mu_2\in\{\pm1,\pm i\}$ depend only on ρ and β. Hence

$$A(x;\rho,u_i)\le\sum_{\beta\in\mathbb{M}}|T(x;\beta,\rho,u_i)|,$$

where

$$T(x;\beta,\rho,u_i) := \sum_{\substack{a\in\mathbb{Z}\\ a+\beta \text{ sat. } (*)}}\left(\frac{a+\beta}{c\mathcal{O}_M}\right)_{M,4}\left(\frac{a+\beta}{c'\mathcal{O}_M}\right)_{M,4}.$$

From now on we treat β as fixed and estimate $T(x;\beta,\rho,u_i)$. It is here that we deviate from [10] and [13]. Since we chose $c' \in \mathbb{Z}[\sqrt{-2}]$, we can factor the principal ideal $(c') \subset \mathbb{Z}[\sqrt{-2}]$ into prime ideals in $\mathbb{Z}[\sqrt{-2}]$ that do not ramify in M, say, $(c') = \prod_{i=1}^k \mathfrak{p}_i^{e_i}$, so that

$$\left(\frac{a+\beta}{c'\mathcal{O}_M}\right)_{M,4} = \prod_{i=1}^k \left(\frac{a+\beta}{\mathfrak{p}_i\mathcal{O}_M}\right)_{M,4}^{e_i}.$$

We claim that $((a+\beta)/\mathfrak{p}\mathcal{O}_M)_{M,4} = 1$ if $\mathfrak{p} \nmid a+\beta$. As a first step we can replace β by some $\beta' \in \mathbb{Z}[\sqrt{-2}]$ due to Lemma 3.4. Then Lemma 3.2 proves the claim if $\mathfrak{p}$ splits in M. Finally suppose that $\mathfrak{p}$ stays inert in M. If we define $p := \mathfrak{p} \cap \mathbb{Z}$, we find that $p \equiv 3 \bmod 8$. Hence Lemma 3.3 finishes the proof of the claim.

The factor $((a+\beta)/c\mathcal{O}_M)_{M,4}$ is handled more similarly to [10, (6.21), p. 727]. Since we chose $c \in \mathbb{Z}[i]$, we factor $(c) \subset \mathbb{Z}[i]$ in $\mathbb{Z}[i]$ as $(c) = \mathfrak{g}\mathfrak{q}$ in the unique way so that $q := N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{q})$ is a squarefree odd integer and $g := N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{g})$ is an odd squarefull integer coprime with q.

Lemma 3.4 and the Chinese remainder theorem imply that there exists $\beta' \in \mathbb{Z}[i]$ such that $\beta \equiv \beta' \bmod \mathfrak{q}\mathcal{O}_M$. Next, Lemma 3.2 and Lemma 3.3 imply that $((a+\beta')/\mathfrak{q}\mathcal{O}_M)_{M,4} = ((a+\beta')/\mathfrak{q})_{\mathbb{Q}(i),2}$. Finally, as q is squarefree, the Chinese remainder theorem guarantees the existence of a rational integer b such that $\beta' \equiv b \bmod \mathfrak{q}$. Combining all of this gives

$$\left(\frac{a+\beta}{c\mathcal{O}_M}\right)_{M,4} = \left(\frac{a+\beta}{\mathfrak{g}\mathcal{O}_M}\right)_{M,4} \left(\frac{a+b}{\mathfrak{q}}\right)_{\mathbb{Q}(i),2}.$$

Since c depends on β and not on a, we find that b depends on β and not on a. Now define g_0 as the radical of g, i.e., $g_0 := \prod_{p|g} p$. We observe that the quartic residue symbol $(\alpha/\mathfrak{g}\mathcal{O}_M)_{M,4}$ is periodic in α modulo $\mathfrak{g}^* := \prod_{\mathfrak{p}|\mathfrak{g}} \mathfrak{p}$. But clearly $\mathfrak{g}^*$ divides g_0, and hence we conclude that $((a+\beta)/\mathfrak{g}\mathcal{O}_M)_{M,4}$ is periodic of period g_0 when viewed as a function of $a \in \mathbb{Z}$. So we split $T(x;\beta,\rho,u_i)$ into congruence classes modulo g_0, giving

$$|T(x;\beta,\rho,u_i)| \leq \sum_{a_0 \bmod g_0} |T(x;\beta,\rho,u_i,a_0)|,$$

where

$$T(x;\beta,\rho,u_i,a_0) = \sum_{\substack{a\in\mathbb{Z} \\ a+\beta \text{ sat. } (*) \\ a\equiv a_0 \bmod g_0}} \left(\frac{a+b}{\mathfrak{q}}\right)_{\mathbb{Q}(i),2} \left(\frac{a+\beta}{c'\mathcal{O}_M}\right)_{M,4}.$$

We have already proven that $((a+\beta)/c'\mathcal{O}_M)_{M,4} = 1$ unless $\gcd(a+\beta, c') \neq (1)$ and in this case we have $((a+\beta)/c'\mathcal{O}_M)_{M,4} = 0$. An application of inclusion-exclusion gives

$$|T(x;\beta,\rho,u_i,a_0)| \leq \sum_{\substack{\mathfrak{d}|c'\mathcal{O}_M \\ \mathfrak{d} \text{ square-free}}} |T(x;\beta,\rho,u_i,a_0,\mathfrak{d})|,$$

where

$$T(x;\beta,\rho,u_i,a_0,\mathfrak{d}) := \sum_{\substack{a\in\mathbb{Z} \\ a+\beta \text{ sat. } (*) \\ a\equiv a_0 \bmod g_0 \\ a+\beta\equiv 0 \bmod \mathfrak{d}}} \left(\frac{a+b}{\mathfrak{q}}\right)_{\mathbb{Q}(i),2}. \tag{4.2}$$

We unwrap the summation conditions above similarly as in [10, p. 728]. Certainly $a+\beta \in u_i\mathcal{D}$ implies that $|a| \leq Cx^{\frac{1}{4}}$, where $C > 0$ depends only on one of the two fixed units u_i. The condition $\mathrm{N}_{M/\mathbb{Q}}(a+\beta) \leq x$ is for fixed β and x a polynomial inequality of degree 4 in a. Hence the summation variable $a \in \mathbb{Z}$ runs over at most 4 intervals of length $\leq Cx^{1/4}$ with endpoints depending on β and x.

Next, the congruence conditions $a+\beta \equiv \rho \bmod F$, $a+\beta \equiv 0 \bmod \mathfrak{m}$, $a \equiv a_0 \bmod g_0$ and $a+\beta \equiv 0 \bmod \mathfrak{d}$ imply that a runs over some arithmetic progression of modulus k dividing g_0mdF, where we define $m := \mathrm{N}_{M/\mathbb{Q}}(\mathfrak{m})$ and $d := \mathrm{N}_{M/\mathbb{Q}}(\mathfrak{d})$. Moreover, as $q = \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{q})$ is squarefree, $(\cdot/\mathfrak{q})_{\mathbb{Q}(i),2} : \mathbb{Z} \to \{\pm 1, 0\}$ is the real primitive Dirichlet character of modulus q.

All in all, the sum in (4.2) can be rewritten as at most 4 incomplete real character sums of length $\ll x^{\frac{1}{4}}$ and modulus $q \ll x^{\frac{1}{2}}$, each of which runs over an arithmetic progression of modulus k. When the modulus q of the Dirichlet character divides the modulus k of the arithmetic progression, one does not get the desired cancellation. So for now we assume that $q \nmid k$, and we will handle the case $q \mid k$ later. As has been explained in [11, 7., p. 924-925], Burgess's bound for short character sums [1] implies that for each integer $r \geq 2$, we have

$$T(x;\beta,\rho,u_i,a_0,\mathfrak{d}) \ll_{\epsilon,r} x^{\frac{1}{4}\left(1-\frac{1}{r}\right)} \cdot x^{\frac{1}{2}\left(\frac{r+1}{4r^2}+\epsilon\right)},$$

so that on taking $r = 2$, we obtain

$$T(x;\beta,\rho,u_i) \ll_\epsilon g_0 x^{\frac{1}{4}-\frac{1}{32}+\epsilon}. \tag{4.3}$$

It remains to do the case $q \mid k$. Certainly, this implies $q \mid md$. So (4.3) holds if $q \nmid md$. Recall that $(c) = \mathfrak{g}\mathfrak{q}$, hence we have (4.3) unless

$$p \mid \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha') \implies p^2 \mid mdF\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha') \tag{4.4}$$

for all primes p, where α' is defined as in (4.1). Define $A_\square(x;\rho,u_i)$ as the contribution to $A(x;\rho,u_i)$ from β satisfying (4.4). Then we get

$$A_\square(x;\rho,u_i) \leq |\{\alpha \in u_i\mathcal{D} : N_{M/\mathbb{Q}}(\alpha) \leq x,\ p \mid \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha') \implies p^2 \mid mdF\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha')\}|.$$

We decompose $\mathcal{O}_M$ as $\mathcal{O}_M = \mathbb{Z}[i] \oplus \mathbb{M}'$, where $\mathbb{M}' = \mathbb{Z}\zeta_8 \oplus \mathbb{Z}\zeta_8^3 = \mathbb{Z}[i] \cdot \zeta_8$ is a free $\mathbb{Z}$-module of rank 2. The linear map $\mathbb{M}' \to \mathbb{Z}[i]$ given by $\alpha \mapsto \alpha'$ is injective. Now suppose $\alpha \in u_i\mathcal{D}$ and $\mathrm{N}_{M/\mathbb{Q}}(\alpha) \leq x$. Then by Lemma 3.5, if we write $\alpha = a_1 + a_2 i + (a_3 + a_4 i)\zeta_8$, we have $a_j \ll x^{\frac{1}{4}}$ for $1 \leq j \leq 4$. Hence the norm $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\cdot)$ of $\alpha' = -2(a_3 + a_4 i)$ is $\ll x^{\frac{1}{2}}$, and so

$$A_\square(x;\rho,u_i) \ll x^{\frac{1}{2}} |\{\alpha' \in \mathbb{Z}[i] : \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha') \ll x^{\frac{1}{2}},\ p \mid \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha') \implies p^2 \mid mdF\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha')\}|.$$

Note that there are at most $\ll_\epsilon b^\epsilon$ elements $\alpha' \in \mathbb{Z}[i]$ such that $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha') = b$. This gives

$$A_\square(x;\rho,u_i) \ll_\epsilon x^{\frac{1}{2}+\epsilon} \sum_{\substack{b \ll x^{\frac{1}{2}};\\ p\mid b \implies p^2 \mid mdFb}} 1,$$

where b runs over the positive rational integers. We assume that $m \leq x$ because otherwise $A(x)$ is the empty sum. This shows that $md \ll x^2$ and we conclude that

$$A_\square(x;\rho,u_i) \ll_\epsilon x^{\frac{3}{4}+\epsilon}.$$

Let $A_0(x;\rho,u_i)$ be the contribution to $A(x;\rho,u_i)$ of the terms $\alpha = a+\beta$ not satisfying (4.4). Then we can split $A(x;\rho,u_i)$ as

$$A(x;\rho,u_i) = A_\square(x;\rho,u_i) + A_0(x;\rho,u_i).$$

To estimate $A_0(x;\rho,u_i)$ we can try to use our bound (4.3) for every relevant β, but for this we need g_0 to be small. Hence we make the further partition

$$A_0(x;\rho,u_i) = A_1(x;\rho,u_i) + A_2(x;\rho,u_i),$$

where β satisfies the additional constraint

$$\begin{aligned} g_0 &\le Z \text{ in the sum } A_1(x;\rho,u_i), \\ g_0 &> Z \text{ in the sum } A_2(x;\rho,u_i). \end{aligned}$$

Here Z is at our disposal, and we choose it later. We estimate $A_1(x;\rho,u_i)$ as in [10] by using (4.3) and summing over $\beta = b_1\zeta_8 + b_2\zeta_8^2 + b_3\zeta_8^3 \in \mathbb{M}$ satisfying $b_i \ll x^{\frac{1}{4}}$ for $1 \le i \le 3$ to obtain

$$A_1(x;\rho,u_i) \ll_\epsilon Zx^{1-\frac{1}{32}+\epsilon}.$$

To finish the proof of Proposition 3.7 it remains to estimate $A_2(x;\rho,u_i)$. Note that $g_0 \le \sqrt{g}$ and $g \le \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(c) \le \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha') \ll x^{\frac{1}{2}}$. Hence, similarly as for $A_\square(x;\rho,u_i)$, with $b = \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha')$, we have

$$A_2(x;\rho,u_i) \ll_\epsilon x^{\frac{1}{2}+\epsilon} \sum_{Z<g_0\ll x^{\frac{1}{4}}} \sum_{\substack{b\ll x^{\frac{1}{2}} \\ g_0^2 \mid b}} 1 \ll_\epsilon Z^{-1}x^{1+\epsilon}.$$

Picking $Z = x^{\frac{1}{64}}$ finishes the proof of Proposition 3.7.

5 Proof of Proposition 3.8

Let w and z be odd elements in $\mathcal{O}_M$. All quadratic and quartic residue symbols that follow are over M. By (2.2), we have

$$[wz] = \left(\frac{8\sigma(wz)\sigma\tau(wz)}{wz}\right)_4 = [w][z]\left(\frac{\sigma(w)}{z}\right)_4\left(\frac{\sigma\tau(w)}{z}\right)_4\left(\frac{\sigma(z)}{w}\right)_4\left(\frac{\sigma\tau(z)}{w}\right)_4.$$

By Lemma 3.1, we have, for some $\mu_1 \in \{\pm1,\pm i\}$ that depends only on the congruence classes of w and z modulo 16,

$$\left(\frac{\sigma(w)}{z}\right)_4\left(\frac{\sigma(z)}{w}\right)_4 = \mu_1\left(\frac{z}{\sigma(w)}\right)_4\left(\frac{\sigma(z)}{w}\right)_4 = \mu_1\left(\frac{z}{\sigma(w)}\right)_4\sigma\left(\frac{z}{\sigma(w)}\right)_4 = \mu_1\left(\frac{z}{\sigma(w)}\right)_2,$$

because $\sigma(i) = i$. Similarly, for some $\mu_2 \in \{\pm1,\pm i\}$ that depends only on the congruence classes of w and z modulo 16,

$$\left(\frac{\sigma\tau(w)}{z}\right)_4\left(\frac{\sigma\tau(z)}{w}\right)_4 = \mu_2\left(\frac{z}{\sigma\tau(w)}\right)_4\sigma\tau\left(\frac{z}{\sigma\tau(w)}\right)_4 = \mu_2,$$

because $\sigma\tau(i) = -i$. Hence we get, for $\mu_3 = \mu_1\mu_2$,

$$[wz] = \mu_3[w][z]\left(\frac{z}{\sigma(w)}\right)_2. \tag{5.1}$$

This twisted multiplicativity formula for the symbol $[\cdot]$ is what makes the estimate in Proposition 3.8 possible; it is analogous to [9, Lemma 20.1, p. 1021], [10, (3.8), p. 708], [17, Proposition 8, p. 1010], and [13, (4.1), p. 19].

Let χ be a Dirichlet character modulo 8, and let $\{a(\chi)_{\mathfrak{n}}\}_{\mathfrak{n}}$ be the sequence defined in (2.3). Let $\{\alpha_{\mathfrak{m}}\}_{\mathfrak{m}}$ and $\{\beta_{\mathfrak{n}}\}_{\mathfrak{n}}$ be any two bounded sequences of complex numbers. Since each ideal of $\mathcal{O}_M$ has 8 different generators in $\mathcal{D}$, we have

$$\sum_{\mathrm{N}(\mathfrak{m})\leq M}\sum_{\mathrm{N}(\mathfrak{n})\leq N}\alpha_{\mathfrak{m}}\beta_{\mathfrak{n}}a(\chi)_{\mathfrak{mn}} = \frac{1}{8^2}\sum_{w\in\mathcal{D}(M)}\sum_{z\in\mathcal{D}(N)}\alpha_w\beta_z([wz]_\chi + [\varepsilon wz]_\chi).$$

Here $\varepsilon = 1+\sqrt{2}$, $\alpha_w := \alpha_{(w)}$ and $\beta_z := \beta_{(z)}$. Note that for any odd element $\alpha \in \mathcal{O}_M$, we have $[\alpha]_\chi = \mu_4 \cdot [\alpha]$ for some $\mu_4 \in \{\pm 1, \pm i\}$ that depends only on the congruence class of α modulo 8 (and so also modulo 16). Also note that (5.1) implies that $[\varepsilon wz] = \mu_5[wz]$ for some $\mu_5 \in \{\pm 1, \pm i\}$ that depends only on the congruence class of wz modulo 16. Hence, by restricting w and z to congruence classes modulo 16, we may break up the sum above into $2\cdot 16^2$ sums of the shape

$$\mu_6 \sum_{\substack{w\in\mathcal{D}(M)\\ w\equiv\omega \bmod 16}}\sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv\zeta \bmod 16}}\alpha_w\beta_z[wz],$$

where $\mu_6 \in \{\pm 1, \pm i\}$ depends only on the congruence classes ω and ζ modulo 16. Again by (5.1), we can replace α_w and β_z by $\alpha_w[w]$ and $\beta_z[z]$ to arrive at the sum

$$\mu_7 \sum_{\substack{w\in\mathcal{D}(M)\\ w\equiv\omega \bmod 16}}\sum_{\substack{z\in\mathcal{D}(N)\\ z\equiv\zeta \bmod 16}}\alpha_w\beta_z\left(\frac{z}{\sigma(w)}\right)_2,$$

where $\mu_7 \in \{\pm 1, \pm i\}$ depends only on ω and ζ. One can now apply Proposition 3.6 with $\gamma(w,z) = \left(\frac{z}{\sigma(w)}\right)_2$ (and $F = \mathbb{Q}(\zeta_8)$, $n = 4$, $\mathfrak{f} = (16)$). Indeed, property (P1) follows from Lemma 3.1, while property (P2) and the first part of property (P3) follow from basic properties of the quadratic residue symbol in $\mathbb{Q}(\zeta_8)$. For the second part of property (P3), we note that if $|\mathrm{N}(w)|$ is not a square in $\mathbb{Z}$, then the ideal generated by $\sigma(w)$ cannot be the square of an ideal in $\mathbb{Q}(\zeta_8)$, and the rest follows. This finishes the proof of Proposition 3.8.

References

[1] D. A. Burgess. On character sums and L-series. II. *Proc. Lond. Math. Soc. (3)*, 13:524–536, 1963.

[2] H. Cohn and J. C. Lagarias. On the existence of fields governing the 2-invariants of the classgroup of $\mathbf{Q}(\sqrt{dp})$ as p varies. *Math. Comp.*, 41(164):711–730, 1983.

[3] H. Cohn and J. C. Lagarias. Is there a density for the set of primes p such that the class number of $\mathbf{Q}(\sqrt{-p})$ is divisible by 16? In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, volume 34 of *Colloq. Math. Soc. János Bolyai*, pages 257–280. North-Holland, Amsterdam, 1984.

[4] C.-J. de la Vallée Poussin. *Mém. Couronnés Acad. Roy. Belgique*, 59:1–74, 1899.

[5] É. Fouvry and J. Klüners. Cohen-Lenstra heuristics of quadratic number fields. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 40–55. Springer, Berlin, 2006.

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

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

[8] É. Fouvry and J. Klüners. The parity of the period of the continued fraction of $\sqrt{d}$. *Proc. Lond. Math. Soc. (3)*, 101(2):337–391, 2010.

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

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

[11] J. B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin. Erratum to: The spin of prime ideals. *Invent. Math.*, 202(2):923–925, 2015.

[12] C. F. Gauss. *Disquisitiones arithmeticae.* Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[13] P. Koymans and D. Milovic. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-p})$. *ArXiv e-prints*, November 2016.

[14] S. Lang. *Algebraic Number Theory.* Springer-Verlag, New York, second edition, 1986.

[15] F. Lemmermeyer. *Reciprocity laws.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.

[16] P. A. Leonard and K. S. Williams. On the divisibility of the class numbers of $Q(\sqrt{-p})$ and $Q(\sqrt{-2p})$ by 16. *Canad. Math. Bull.*, 25(2):200–206, 1982.

[17] D. Milovic. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \mod 4$. *Geom. Funct. Anal.*, 27(4):973–1016, 2017.

[18] P. Morton. Density result for the 2-classgroups of imaginary quadratic fields. *J. Reine Angew. Math.*, 332:156–187, 1982.

[19] L. Rédei. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 171:55–60, 1934.

[20] A. Smith. Governing fields and statistics for 4-Selmer groups and 8-class groups. *ArXiv e-prints*, July 2016.

[21] A. Smith. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. *ArXiv e-prints*, February 2017.

[22] P. Stevenhagen. Ray class groups and governing fields. In *Théorie des nombres, Année 1988/89, Fasc. 1*, Publ. Math. Fac. Sci. Besançon, page 93. Univ. Franche-Comté, Besançon, 1989.

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

[24] R.-C. Vaughan. Sommes trigonométriques sur les nombres premiers. *C. R. Acad. Sci. Paris Sér. A-B*, 285(16):A981–A983, 1977.

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

[26] I. M. Vinogradov. *The method of trigonometrical sums in the theory of numbers.* Dover Publications, Inc., Mineola, NY, 2004. Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation.