ON THE 8-RANK OF NARROW CLASS GROUPS OF $\mathbb{Q}(\sqrt{-4pq})$, $\mathbb{Q}(\sqrt{-8pq})$, AND $\mathbb{Q}(\sqrt{8pq})$

DJORDJO MILOVIC

Abstract. Let $d \in \{-4, -8, 8\}$. We study the 8-part of the narrow class group in the thin families of quadratic number fields of the form $\mathbb{Q}(\sqrt{dpq})$, where $p \equiv q \equiv 1 \bmod 4$ are prime numbers, and we prove new lower bounds for the proportion of narrow class groups in these families that have an element of order 8. In the course of our proof, we prove a general double-oscillation estimate for the quadratic residue symbol in quadratic number fields.

1. Introduction

In [31], Stevenhagen studied the 2-part of narrow class groups in thin families of quadratic number fields parametrized by one prime number, namely families of the form $\{\mathbb{Q}(\sqrt{dp})\}_{p\equiv 1(4)}$, where $d \in \{-4, -8, 8\}$ and where p varies over prime numbers congruent to 1 modulo 4. In this paper, we aim to prove new results about the 2-part of narrow class groups in similar thin families of quadratic number fields, except this time parametrized by products of two distinct prime numbers. We consider quadratic fields of the form $\mathbb{Q}(\sqrt{dpq})$, where again $d \in \{-4, -8, 8\}$ and where now p and q vary over pairs of distinct prime numbers congruent to 1 modulo 4. One of the key features of [31] (and more generally [30]) is that the distribution of the 8-rank in one-parameter families as above can be deduced from the Čebotarev Density Theorem. The main novelty in the present setting is the introduction of double-oscillation estimates concerning certain families of Hecke characters to overcome the poor uniformity (in q) of the error terms in the Čebotarev Density Theorem when applied in families of number fields (parametrized by a prime q).

Let $d \in \{-4, -8, 8\}$, let $p \equiv q \equiv 1 \bmod 4$ be two distinct prime numbers, and consider the narrow class group $\mathrm{Cl}(dpq)$ of the quadratic number field of discriminant dpq. We recall that the narrow class group of a number field K is the quotient of the group of non-zero fractional ideals of K by the subgroup of principal ideals that can be generated by an element $\alpha \in K$ satisfying $\sigma(\alpha) > 0$ for every real embedding $\sigma : K \hookrightarrow \mathbb{R}$; the narrow class group is canonically isomorphic, via the Artin map, to the Galois group of the maximal abelian extension of K unramified at all finite primes. In particular, if K is totally complex, then the narrow and the usual class groups coincide.

Given any finite group G and an integer $k \geq 1$, we define the 2^k-rank of G to be $\mathrm{rk}_{2^k} G := \dim_{\mathbb{F}_2} \left(2^{k-1}G/2^k G\right)$. Gauss's genus theory [9] then implies that $\mathrm{rk}_2 \mathrm{Cl}(dpq) = 2$, i.e., that the 2-part of $\mathrm{Cl}(dpq)$ is a direct sum of two cyclic 2-groups. We wish to better understand of the size these cyclic 2-groups. Rédei's work [27] implies that $\mathrm{rk}_4 \mathrm{Cl}(dpq) = 2$ if and only if $p \equiv q \equiv 1 \bmod 8$ and p is a square modulo q. We note that Gerth [10, 11, 12] as well as Fouvry and Klüners [5, 6, 7],

Date: April 13, 2018.

building on the work of Heath-Brown [14, 15], developed robust techniques to study the 4-rank in families of many different types.

There are three main analytic results concerning the 8-rank in families of quadratic number fields. First, Stevenhagen [30] proved that if $d \neq 0$ is any integer, then there is a normal extension $M_d/\mathbb{Q}$ such that $\mathrm{rk}_8\mathrm{Cl}(dp)$ is determined by the Artin symbol of p in $M_d/\mathbb{Q}$; hence the density of the set of primes p for which $\mathrm{rk}_8\mathrm{Cl}(dp)$ is equal to a given value can be deduced from the Čebotarev Density Theorem applied to $M_d/\mathbb{Q}$. Note that the families studied by Stevenhagen are parametrized by a *single* prime. Next, Fouvry and Klüners [7] proved certain distribution results about the 8-rank in a special family parametrized by *arbitrarily many* primes $\not\equiv 3 \bmod 4$, but having 4-rank equal to 1. Finally, two recent works of Smith [28, 29] claim very strong results about the 8- and higher 2-power-ranks in the family of all *imaginary* quadratic fields. His methods, however, heavily rely on the fact that the average number of prime factors of a discriminant D grows as $\log\log D$ and are thus inapplicable to the *thin* families we study. We prove

Theorem 1. *Let p and q denote distinct prime numbers congruent to $1 \bmod 4$. Then for $d \in \{-4, -8, 8\}$, we have*

$$\liminf_{X\to\infty} \frac{\#\{pq \leq X : \mathrm{rk}_4\mathrm{Cl}(dpq) = 2, \mathrm{rk}_8\mathrm{Cl}(dpq) \geq 1\}}{\#\{pq \leq X : \mathrm{rk}_4\mathrm{Cl}(dpq) = 2\}} \geq \frac{c_d}{8},$$

where $c_{-4} = c_{-8} = 2$ and $c_8 = 1$.

The asymptotic formula for the denominator in the ratio above is

$$\#\{pq \leq X : p \equiv q \equiv 1 \bmod 4,\ \mathrm{rk}_4\mathrm{Cl}(dpq) = 2\} \sim \frac{1}{32}\frac{X\log\log X}{\log X} \tag{1}$$

as $X \to \infty$ (for any $d \in \{-4, -8, 8\}$). This formula is a slight variation of [10, Equation (2.12), p. 493], whose proof for our particular case can be found in [12]. The heuristic model of Cohen and Lenstra [1] predicts that the limit in the Main Theorem exists and is equal to $5/8$ in the cases $d = -4$ and $d = -8$ and $11/32$ in the case $d = 8$. See Section A for more details. We also note that the 16- and higher 2-power-ranks appear to be much harder to study from an analytic perspective, and there are only a few results in this direction [23, 24, 19, 20, 29]

The proof of the Theorem 1 exploits a new type of *lower* bound for the 8-rank. In [7], Fouvry and Klüners define a quantity λ_D conducive to analytic techniques which gives a good *upper* bound for the 8-rank of the narrow class group $\mathrm{Cl}(D)$ for a special class of positive discriminants D. This upper bound λ_D actually coincides with $\mathrm{rk}_8\mathrm{Cl}(D)$ when $\mathrm{rk}_4\mathrm{Cl}(D) = 1$. However, when $\mathrm{rk}_4\mathrm{Cl}(D) \geq 2$, the quantity λ_D is only an upper bound for $\mathrm{rk}_8\mathrm{Cl}(D)$ and hence cannot be used to deduce that $\mathrm{rk}_8\mathrm{Cl}(D) \geq 1$. Therefore, Theorem 1 cannot be readily deduced from the techniques in [7]. One might try to deduce Theorem 1 from [30] by first applying, for a fixed $d \in \{-4, -8, 8\}$ and each prime $q \equiv 1 \bmod 8$, the Čebotarev Density Theorem to the field extension $M_{dq}/\mathbb{Q}$ to get a density $\delta_{d,q}$ for the set $S_{d,q}$ of primes $p \equiv 1 \bmod 4$ for which $\mathrm{rk}_4\mathrm{Cl}(dpq) = 2$ and $\mathrm{rk}_8\mathrm{Cl}(dpq) \geq 1$, i.e.,

$$N_{d,q}(x) = \#\{p \in S_{d,q} : p \leq x\} = \delta_{d,q}\frac{x}{\log x} + E_{d,q}(x),$$

where $E_{d,q}(x) = o(x/\log x)$ as $x \to \infty$, and then patching together the contributions from different primes q to get the asymptotics for the sum $\sum_{q\leq X} N_q\left(X/q\right)$ as $X \to \infty$. Unfortunately, the fields M_{dq} are obtained via the existence theorem of

class field theory and hence not explicit enough in d and q for this approach to work. Smith [28], following Corsman [2], constructs the fields M_{dq} quite explicitly; however, the discriminants dpq with $\mathrm{rk}_4\mathrm{Cl}(dpq) = 2$ are not *generic* in the sense of Smith [28, Definition 2.4, p. 11] and hence not conducive to applying the Čebotarev Density Theorem. Perhaps more importantly, Smith assumes the Grand Riemann Hypothesis to overcome the very poor uniformity in q of the best known bounds for the error term $E_{d,q}(x)$.

To avoid assuming the Grand Riemann Hypothesis, we prove double-oscillation results in quadratic rings (such as $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{2}]$) that are reminiscent of [8, Proposition 21.3, p. 1027]. In our case, however, we need somewhat more precise estimates – the term $(MN)^\epsilon$ must be replaced by an arbitrary power of $\log(MN)$. A general approach to proving these types of double-oscillation results was already developed in [17], so, after making appropriate adjustments to work inside more general number rings instead of the rational integers, the heart of the proof of [8, Proposition 21.3, p. 1027] lies in achieving cancellation in characters sums as in [8, Lemma 21.1, p. 1025]. In Proposition 7 of this paper, we give a shorter and more natural proof of a generalization of this result.

Acknowledgements. I would like to thank Farrell Brumley, Étienne Fouvry, Carlo Pagano, Peter Stevenhagen, and the anonymous referee for their useful advice. This research was supported by an ALGANT Erasmus Mundus Scholarship and National Science Foundation agreement No. DMS-1128155.

2. Algebraic Criteria for the 8-rank

2.1. **Preliminaries.** Let K be a quadratic number field of discriminant D, $\mathcal{O}_K$ its maximal order, and Cl the narrow class group of $\mathcal{O}_K$. The *narrow Hilbert class field* H of K is the maximal abelian extension of K unramified at all finite primes. Hereafter, we will use the shorthand "unramified a.f.p." for "unramified at all finite primes". The Artin map induces a canonical isomorphism of groups

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

The above isomorphism allows us to deduce information about Cl by constructing and studying abelian unramified a.f.p. extensions of K.

The 2-torsion subgroup Cl[2] is generated by the classes of the ramified finite primes in $K/\mathbb{Q}$ (see for instance [30, Corollary 9.9, p. 80]), i.e.,

$$\mathrm{Cl}[2] = \langle [\mathfrak{p}] : \mathfrak{p} \text{ prime ideal of } \mathcal{O}_K \text{ such that } \mathfrak{p}|D \rangle . \tag{3}$$

We will use the two facts above in tandem via the following lemma; although it is a straightforward generalization of the argument in [30, p. 18-19], we have not been able to find the exact statement in the literature, and so we include a proof for the sake of completeness. Hereafter, C_n will denote a cyclic group of order n.

Lemma 1. *Let K be a quadratic number field. Suppose that L/K is an unramified a.f.p. C_{2^n}-extension for some $n \geq 1$. Then every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that is ramified in $K/\mathbb{Q}$ splits completely in L/K if and only if there exists an unramified a.f.p. $C_{2^{n+1}}$-extension L' of K containing L.*

Proof. As L/K is unramified a.f.p. and abelian, L must be contained in the narrow Hilbert class field H. A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ splits completely in L/K if and only if

$$\left(\frac{\mathfrak{p}}{L/K}\right) = 1 \in \mathrm{Gal}(L/K) \cong \mathrm{Cl}/\mathrm{Gal}(H/L).$$

Hence, by (3), every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that is ramified in $K/\mathbb{Q}$ splits completely in L/K if and only if $\mathrm{Cl}[2] \leq \mathrm{Gal}(H/L)$. Dually, in terms of the corresponding character groups, this holds if and only if

$$\mathrm{Cl}^\vee/\mathrm{Gal}(L/K)^\vee \cong \mathrm{Gal}(H/L)^\vee \twoheadrightarrow \mathrm{Cl}[2]^\vee \cong \mathrm{Cl}^\vee/\left(\mathrm{Cl}^\vee\right)^2,$$

i.e., if and only if $\mathrm{Gal}(L/K)^\vee \leq \left(\mathrm{Cl}^\vee\right)^2$. Now, as $\mathrm{Gal}(L/K) \cong C_{2^n}$, so also $\mathrm{Gal}(L/K)^\vee \cong C_{2^n}$, with a generator, say, χ. Thus $\mathrm{Gal}(L/K)^\vee \leq \left(\mathrm{Cl}^\vee\right)^2$ if and only if $\chi = \psi^2$ for some $\psi \in \mathrm{Cl}^\vee$, which holds if and only if there exists a group $A = \langle\psi\rangle \cong C_{2^{n+1}}$ with $\mathrm{Gal}(L/K)^\vee \leq A \leq \mathrm{Cl}^\vee$. Dually, this holds if and only if there exists a $C_{2^{n+1}}$-extension L'/K with $L \subset L' \subset H$. □

We will also make use of the following lemma from Galois theory (see [21, Chapter VI, Exercise 4, p.321]).

Lemma 2. *Let F be a field of characteristic different from 2, let $E = F(\sqrt{d})$, where $d \in F^\times \setminus (F^\times)^2$, and let $L = E(\sqrt{x})$, where $x \in E^\times \setminus (E^\times)^2$. Let $N = \mathrm{N}_{E/F}(x)$. Then $N \in d \cdot (F^\times)^2$ if and only if L/F is normal with $\mathrm{Gal}(L/F) \cong C_4$, the cyclic group of order 4.*

2.2. **Special two-parameter families.** Let $d \in \{-4, -8, 8\}$, and let p and q be odd primes congruent to 1 modulo 4. Let $K = \mathbb{Q}(\sqrt{dpq})$, and let H denote its narrow Hilbert class field. Let $d_0 = d/4$, so that the maximal order of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{d_0 pq}]$. We are ultimately interested in the average value of $\mathrm{rk}_8\mathrm{Cl}(dpq)$ of $\mathcal{O}_K$ as p and q range among prime numbers satisfying $pq \leq X$, for a real parameter X going to infinity.

Let $\mathrm{Cl} = \mathrm{Cl}(dpq)$. Gauss's genus theory implies that $\mathrm{rk}_2\mathrm{Cl} = 2$ and that the genus field, the maximal abelian extension of $\mathbb{Q}$ contained in H, is

$$G = H^{\mathrm{Cl}^2} = \mathbb{Q}(\sqrt{d}, \sqrt{p}, \sqrt{q}).$$

The three quadratic subfields $G_1 = K(\sqrt{d})$, $G_2 = K(\sqrt{p})$, and $G_3 = K(\sqrt{q})$ of G correspond to the three proper subgroups of $\mathrm{Cl}/\mathrm{Cl}^2$. The three ramified primes $\mathfrak{t}$, $\mathfrak{p}$, and $\mathfrak{q}$ of $\mathcal{O}_K$ that lie above 2, p, and q, respectively, generate the 2-torsion subgroup $\mathrm{Cl}[2]$ and will play a prominent role in the subsequent discussions. Clearly $\mathrm{rk}_4\mathrm{Cl} \leq \mathrm{rk}_2\mathrm{Cl} = 2$, and in fact the 4-rank of Cl is the largest it could be exactly when p and q satisfy

$$p \equiv q \equiv 1 \bmod 8, \tag{4}$$

and

$$\left(\frac{p}{q}\right) = 1. \tag{5}$$

Proposition 1. *Let $d \in \{-4, -8, 8\}$, and let p and q be odd prime numbers congruent to 1 modulo 4. Let $\mathrm{Cl} = \mathrm{Cl}(dpq)$ denote the narrow class group of the quadratic number field $\mathbb{Q}(\sqrt{dpq})$. Then $\mathrm{rk}_4\mathrm{Cl} = 2$ if and only if p and q satisfy (4) and (5).*

Proof. The extension $G_i/\mathbb{Q}$ is a V_4-extension for $i = 1, 2, 3$, so the splitting behavior of $\mathfrak{t}$, $\mathfrak{p}$, and $\mathfrak{q}$ in G_i/K is determined by the splitting behavior of 2, p, and q, respectively, in quadratic subfields of G_i. Conditions (4) and (5) imply that $\mathfrak{t}$, $\mathfrak{p}$, and $\mathfrak{q}$ all split in G_i/K for $i = 1, 2, 3$. For instance, by (4), the prime p splits in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, and so $\mathfrak{p}$ splits in G_1. Now Lemma 1 implies that p and q satisfy (4) and (5) if and only if there exists an unramified a.f.p. C_4-extension L_i/K containing G_i for $i = 1, 2, 3$. As $\mathrm{rk}_2\mathrm{Cl} = 2$, the result follows from applying Galois theory to the isomorphism (2). □

From now on, suppose p and q satisfy (4) and (5). Although Proposition 1 demonstrates the existence of at least three distinct unramified a.f.p. C_4-extensions of K, one for each G_i, it may be difficult to construct these extensions explicitly from d, p, and q. In one case, however, we can do exactly this.

By (4), both p and q split in the principal ideal domain $\mathbb{Z}[\sqrt{d_0}]$, so there exist primes $w, z \in \mathbb{Z}[\sqrt{d_0}]$ such that $\mathrm{N}(w) = p$ and $\mathrm{N}(z) = q$. If $d = -4$, then, again by (4), we have

$$w, z \equiv \pm 1 \equiv \square \bmod 4\mathbb{Z}[\sqrt{-1}].$$

If $d = -8$ or $d = 8$, then we can replace w by $-w$ and/or z by $-z$ if necessary to ensure that

$$w, z \equiv 1 \text{ or } 3 + 2\sqrt{d_0} \equiv \square \bmod 4\mathbb{Z}[\sqrt{d_0}].$$

In any case, we can choose primes w and z in $\mathbb{Z}[\sqrt{d_0}]$ such that

$$\mathrm{N}(w) = p, \quad \mathrm{N}(z) = q, \quad \text{and} \quad w, z \equiv \square \bmod 4\mathbb{Z}[\sqrt{d_0}]. \tag{6}$$

Define $\alpha \in \mathbb{Z}[\sqrt{d_0}]$ and $x, y \in \mathbb{Z}$ by the equation

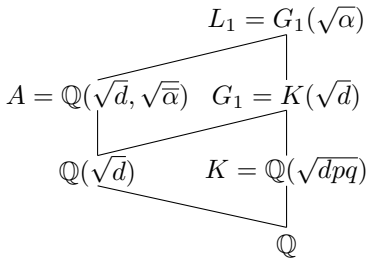
$$\alpha = wz = x + y\sqrt{d_0} \in \mathbb{Q}(\sqrt{d}) \subset G_1. \tag{7}$$

Then α satisfies the condition

$$\alpha \equiv \square \bmod 4\mathbb{Z}[\sqrt{d_0}], \tag{8}$$

and p, q, x, and y satisfy the relation $pq = x^2 - d_0y^2$. For an element a in $\mathbb{Q}(\sqrt{d})$, we will denote the conjugate of a in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ (or G_1/K) by $\overline{a}$, so that $\overline{\alpha} = \overline{w}\overline{z} = x - y\sqrt{d_0}$. Let $L_1 = G_1(\sqrt{\alpha}) = K(\sqrt{d}, \sqrt{\alpha})$. Note that $\sqrt{\overline{\alpha}} = \pm\sqrt{dpq}/(\sqrt{d}\sqrt{\alpha}) \in L_1$.

Proposition 2. *Let $\alpha \in \mathbb{Q}(\sqrt{d})$ be given by (7), and let L_1 be as above. Then L_1/K is an unramified a.f.p. C_4-extension.*



Proof. Since $\mathrm{N}_{G_1/K}(\alpha) = pq = d \cdot \left(\sqrt{dpq}/d\right)^2 \in d \cdot (K^\times)^2$, we see that L_1/K is a C_4-extension, by Lemma 2. The only primes that can ramify in L_1/K are $\mathfrak{t}$, $\mathfrak{p}$, and $\mathfrak{q}$. We will show that $\mathfrak{p}$ is unramified in L_1/K, and by symmetry this will imply that $\mathfrak{q}$ is also unramified in L_1/K. As w is a prime of degree one over p, it is coprime to $\overline{w}$. As p and q are distinct primes, w is also coprime to $\overline{z}$, and hence also to $\overline{\alpha}$.

Therefore w does not ramify in $A = \mathbb{Q}(\sqrt{d}, \sqrt{\overline{\alpha}})$, and so the ramification index of p in $L_1/\mathbb{Q}$ is at most 2. But p already ramifies in $K/\mathbb{Q}$, and hence $\mathfrak{p}$ must be unramified in L_1/K. Finally, to see that L_1/K is unramified over $\mathfrak{t}$, we may pass to the completion with respect to $\mathfrak{t}$ and show that $\mathbb{Q}_2(\sqrt{d}, \sqrt{\alpha})/\mathbb{Q}_2(\sqrt{d})$ is unramified. This is the case if and only if α is a square modulo 4 in the corresponding ring of integers $\mathbb{Z}_2[\sqrt{d_0}]$, and this is indeed ensured by condition (8). □

Now that we constructed L_1/K explicitly, we can apply Lemma 1 to determine when L_1 is contained in an unramified a.f.p. C_8-extension M_1/K. We must determine when $\mathfrak{t}$, $\mathfrak{p}$, and $\mathfrak{q}$ all split completely in L_1. For the prime $\mathfrak{t}$, this can once again be determined locally. Indeed, $\mathfrak{t}$ splits completely in L_1/K if and only if the extension of local fields $\mathbb{Q}_2(\sqrt{d}, \sqrt{\alpha})/\mathbb{Q}_2(\sqrt{d})$ is trivial. This occurs if and only if α is a square in $\mathbb{Q}_2(\sqrt{d})$, which happens if and only if α is a square modulo $\mathfrak{t}^5$, where by abuse of notation $\mathfrak{t}$ is now the maximal ideal in the discrete valuation ring $\mathbb{Z}_2[\sqrt{d_0}]$. Explicitly, this means that

$$\alpha \equiv \square \bmod \mathfrak{t}^5 \equiv \begin{cases} \pm 1 \bmod 4(1+\sqrt{-1})\mathbb{Z}_2[\sqrt{-1}] & \text{if } d = -4, \\ 1 \text{ or } 7 + 2\sqrt{-2} \bmod 4\sqrt{-2}\mathbb{Z}_2[\sqrt{-2}] & \text{if } d = -8, \\ 1 \text{ or } 3 + 2\sqrt{2} \bmod 4\sqrt{2}\mathbb{Z}_2[\sqrt{2}] & \text{if } d = 8. \end{cases} \tag{9}$$

For primes $\mathfrak{p}$ and $\mathfrak{q}$, the splitting criterion is somewhat different. We may again use the auxiliary extension $A = \mathbb{Q}(\sqrt{d}, \sqrt{\overline{\alpha}})$ from proof of Proposition 2. We have $p = w\overline{w}$ with w dividing α, so $\mathfrak{p}$ splits completely in L_1/K if and only if w splits in $A/\mathbb{Q}(\sqrt{d})$. We use a quadratic residue symbol in $\mathbb{Q}(\sqrt{d})$ to detect this, i.e., w splits in $A/\mathbb{Q}(\sqrt{d})$ if and only if

$$\left(\frac{\overline{\alpha}}{(w)}\right) = 1. \tag{10}$$

Similarly, the prime $\mathfrak{q}$ splits completely in L_1/K if and only if

$$\left(\frac{\overline{\alpha}}{(z)}\right) = 1. \tag{11}$$

We will now explore the link between the quadratic residue symbols $\left(\frac{\overline{\alpha}}{(w)}\right)$ and $\left(\frac{\overline{\alpha}}{(z)}\right)$. As w and z are primes of degree one over p and q, respectively, we find that

$$\left(\frac{\overline{\alpha}}{(w)}\right)\left(\frac{\overline{\alpha}}{(z)}\right) = \left(\frac{x - y\sqrt{d_0}}{(x + y\sqrt{d_0})}\right) = \left(\frac{2x}{(x + y\sqrt{d_0})}\right) = \left(\frac{2x}{pq}\right),$$

where the last symbol is simply a Jacobi symbol. Using the fact that $pq = x^2 - d_0y^2 \equiv 1 \bmod 8$, we find that

$$\left(\frac{2x}{pq}\right) = \left(\frac{|x|}{pq}\right) = \left(\frac{pq}{|x|}\right) = \left(\frac{x^2 - d_0y^2}{|x|}\right) = \left(\frac{-d_0}{|x|}\right).$$

We now make a distinction among the cases $d = -4$, $d = -8$, and $d = 8$. First suppose $d = -4$. Then $\left(\frac{-d_0}{|x|}\right) = \left(\frac{1}{|x|}\right) = 1$, and so

$$\left(\frac{\overline{\alpha}}{(w)}\right) = \left(\frac{\overline{\alpha}}{(z)}\right). \tag{12}$$

In other words, if $d = -4$, then $\mathfrak{p}$ splits completely in L_1/K if and only if $\mathfrak{q}$ does. Therefore, if $d = -4$, to ensure that L_1 is contained in an unramified a.f.p. C_8-extension M_1/K, we only need to verify that (9) and (10) are satisfied. Next

suppose $d = -8$. Then $\left(\frac{-d_0}{|x|}\right) = \left(\frac{2}{|x|}\right)$, and so

$$\left(\frac{\overline{\alpha}}{(w)}\right) = \left(\frac{\overline{\alpha}}{(z)}\right) \iff |x| \equiv 1, 7 \bmod 8 \iff x \equiv 1, 7 \bmod 8,$$

and this is guaranteed by (9). Again we conclude that L_1 is contained in an unramified a.f.p. C_8-extension M_1/K provided that (9) and (10) are satisfied. Finally, suppose $d = 8$. Then $\left(\frac{-d_0}{|x|}\right) = \left(\frac{-2}{|x|}\right)$, and so

$$\left(\frac{\overline{\alpha}}{(w)}\right) = \left(\frac{\overline{\alpha}}{(z)}\right) \iff |x| \equiv 1, 3 \bmod 8.$$

Thus if $|x| \equiv 5, 7 \bmod 8$, there is no chance that both (10) and (11) are satisfied and so L_1 is *not* contained in an unramified a.f.p. C_8-extension M_1/K. Looking back at (9), we see that $\mathfrak{t}$ splits in L_1/K if and only if x satisfies

$$x \equiv 1, 3 \bmod 8.$$

Hence, assuming that (9) holds, we find that $\left(\frac{\overline{\alpha}}{(w)}\right) = \left(\frac{\overline{\alpha}}{(z)}\right)$ if and only if

$$x > 0. \tag{13}$$

As $x^2 - 2y^2 = pq$, we deduce that $|x| > |y\sqrt{2}|$, so that

$$x > 0 \iff \alpha, \overline{\alpha} > 0.$$

In other words, the field L_1 cannot be contained in an unramified a.f.p. C_8-extension M_1/K unless L_1 is totally real, i.e., unless L_1/K is unramified also at the infinite places. We summarize the results of this section in the following proposition.

Proposition 3. *Let $d \in \{-4, -8, 8\}$, and let p and q be prime numbers satisfying* (4) *and* (5). *Let w and z be primes in $\mathbb{Z}[\sqrt{d_0}]$ satisfying* (6). *Let α and x be defined as in* (7). *Suppose α satisfies* (9). *Furthermore, if $d = 8$, also suppose x satisfies* (13). *Then there is an unramified a.f.p. C_8-extension of $\mathbb{Q}(\sqrt{dpq})$ containing $\mathbb{Q}(\sqrt{d}, \sqrt{pq})$ if and only if*

$$\left(\frac{\overline{\alpha}}{(w)}\right) = 1.$$

Consequently, under the assumptions above, if the equality above holds, then

$$\mathrm{rk}_8 \mathrm{Cl}(dpq) \geq 1.$$

2.3. **The splitting condition for $\mathfrak{t}$.** We now delve a bit deeper into the meaning of condition (9). Let w and z be primes in $\mathbb{Z}[\sqrt{d_0}]$ satisfying (6), and let $\mathfrak{t}$ be the prime ideal of $\mathbb{Z}[\sqrt{d_0}]$ lying above 2. Let t be a generator of $\mathfrak{t}$ defined by

$$t = \begin{cases} 1 + i & \text{if } d = -4 \\ \sqrt{2} & \text{if } d = 8. \end{cases} \tag{14}$$

In [31, proof of Theorem 1, p. 5], Stevenhagen proved that

$$\left(\frac{t}{(w)}\right) = \begin{cases} 1 & \text{if } w \equiv \square \bmod \mathfrak{t}^5 \\ -1 & \text{otherwise,} \end{cases} \tag{15}$$

and likewise for z. If we define

$$\chi_{\mathfrak{t}}(\mathfrak{a}) = \left(\frac{t}{\mathfrak{a}}\right) \tag{16}$$

for odd prime ideals $\mathfrak{a}$ in $\mathbb{Z}[\sqrt{d_0}]$ and extend multiplicatively to the group $\mathcal{I}(\mathfrak{t})$ of fractional ideals of $\mathbb{Z}[\sqrt{d_0}]$ coprime to $\mathfrak{t}$, then $\chi_{\mathfrak{t}}$ is a quadratic Hecke character on $\mathbb{Z}[\sqrt{d_0}]$. The significance of (15) is twofold: first, the variables p and q, which are inextricably linked in the definition of α, are now separated; and second, condition (9) can now be written in terms of the quadratic Hecke character $\chi_{\mathfrak{t}}$ on $\mathbb{Z}[\sqrt{d_0}]$, i.e.,

$$\alpha \equiv \square \bmod \mathfrak{t}^5 \Longleftrightarrow \chi_{\mathfrak{t}}((w))\chi_{\mathfrak{t}}((z)) = 1. \tag{17}$$

2.4. **Positivity condition on x.** The variables p and q are also inextricably linked in the definition of variable x appearing in (7). However, the positivity condition (13) on x can be unfolded via a theorem of Fouvry and Klüners [6, Proposition 6, p.2063]. We have

$$x > 0 \Longleftrightarrow [2, pq]_4 = [pq, 2]_4,$$

where $[\cdot, \cdot]_4$ is the symbol defined in [6, p. 2061], i.e.,

$$[2, pq]_4 = [2, p]_4[2, q]_4,$$

where

$$[2, p]_4 = \begin{cases} 1 & \text{if 2 is a fourth power modulo } p \\ -1 & \text{if 2 is a square, but not a fourth power modulo } p \\ 0 & \text{otherwise} \end{cases}$$

and similarly for $[2, q]_4$, and

$$[pq, 2]_4 = \begin{cases} 1 & \text{if } pq \equiv 1 \bmod 16 \\ -1 & \text{if } pq \equiv 9 \bmod 16 \\ 0 & \text{otherwise.} \end{cases}$$

When $p \equiv q \equiv 1 \bmod 8$, then

$$[2, pq]_4 = [2, p]_4[2, q]_4 = \chi_{\mathfrak{t}}((w))\chi_{\mathfrak{t}}((z)),$$

where w, z, and $\chi_{\mathfrak{t}}$ are as in Section 2.3. Provided (17) is satisfied, we deduce from the equations and definitions above that

$$x > 0 \Longleftrightarrow pq \equiv 1 \bmod 16. \tag{18}$$

3. Strategy for the Proof of the Main Theorem

As before, let $d \in \{-4, -8, 8\}$. The ultimate goal is to prove, in the set of fundamental discriminants $D = dpq$ satisfying $\mathrm{rk}_4\mathrm{Cl}(D) = 2$, a lower bound for the density of those D that also satisfy $\mathrm{rk}_8\mathrm{Cl}(D) \geq 1$. Suppose p and q are prime numbers satisfying (4). Let w and z be primes in $\mathbb{Z}[\sqrt{d_0}]$ satisfying (6), and define α and x as in (7). Set $\mathfrak{p} = (w)$ and $\mathfrak{q} = (z)$. If $d = 8$, suppose that $x > 0$. We define the symbol $\varepsilon(p, q)$ by

$$\varepsilon(p, q) = \left(\frac{\overline{\alpha}}{(w)}\right) = \left(\frac{\overline{\alpha}}{(z)}\right). \tag{19}$$

Recall from (18) that the positivity condition on x can be detected via congruence conditions on p and q modulo 16. Given that $p \equiv q \equiv 1 \bmod 8$, there are four choices for (p, q) mod 16. When $d < 0$, the positivity condition on x is irrelevant, so all four of the choices are valid; however, when $d = 8$, exactly two of the choices correspond to the condition (18). The splitting condition at the prime $\mathfrak{t}$ lying above

2 can be detected via the Hecke character $\chi_{\mathfrak{t}}$ as in (17). If $\chi_{\mathfrak{t}}(\mathfrak{p}) = s_1$ and $\chi_{\mathfrak{t}}(\mathfrak{q}) = s_2$ with $s_1, s_2 \in \{\pm 1\}$, then $\alpha \equiv \square \bmod \mathfrak{t}^5$ if and only if $s_1 s_2 = 1$.

In light of Proposition 3, the asymptotic formula (1), and the remarks above, Theorem 1 is a consequence of the following theorem.

Theorem 2. *Let d be -4, -8, or 8. Given primes p and q satisfying (4), let x and α be defined as in (7). Let $r_1, r_2 \in \{1, 9\}$ and, in case $d = 8$, suppose that $r_1 r_2 \equiv 1 \bmod 16$. Let $s_1, s_2 \in \{\pm 1\}$ and suppose that $s_1 s_2 = 1$. Then, as $X \to \infty$, we have*

$$\sum_{\substack{pq \le X,\ p<q \\ (p,q) \equiv (r_1,r_2) \bmod 16 \\ (\chi_{\mathfrak{t}}(\mathfrak{p}), \chi_{\mathfrak{t}}(\mathfrak{q})) = (s_1,s_2) \\ p \equiv \square \bmod q \\ \varepsilon(p,q)=1}} \sum 1 \sim \frac{1}{1024} \frac{X \log\log X}{\log X}.$$

Theorem 2 can be interpreted as follows. Classical theory of the distribution of prime numbers (see for instance [26, Section 7.4, p.228]) gives the count of positive integers that are a product of two primes in fixed congruence classes modulo 16, i.e., we have the asymptotic formula

$$\sum_{\substack{pq \le X,\ p<q \\ (p,q) \equiv (r_1,r_2) \bmod 16}} \sum 1 \sim \frac{1}{64} \frac{X \log\log X}{\log X} \tag{20}$$

as $X \to \infty$. The conditions $\chi_{\mathfrak{t}}(\mathfrak{p}) = s_1$ and $\chi_{\mathfrak{t}}(\mathfrak{q}) = s_2$ can likewise be inserted without any trouble because $\chi_{\mathfrak{t}}$ is a multiplicative character of a fixed conductor not depending on p or q. Hence, we have

$$\sum_{\substack{pq \le X,\ p<q \\ (p,q) \equiv (r_1,r_2) \bmod 16 \\ (\chi_{\mathfrak{t}}(\mathfrak{p}), \chi_{\mathfrak{t}}(\mathfrak{q})) = (s_1,s_2)}} \sum 1 \sim \frac{1}{256} \frac{X \log\log X}{\log X} \tag{21}$$

as $X \to \infty$. Each of the remaining two conditions under the summation in Theorem 2 can then be viewed as an event that occurs with probability one-half. Moreover, these two events are independent. To make this argument rigorous, we make use of the following formulas. Given a mathematical statement P, we define the indicator function of P to be

$$\mathbf{1}(P) := \begin{cases} 1 & \text{if } P \text{ is true} \\ 0 & \text{if } P \text{ is false.} \end{cases}$$

For distinct odd primes p and q, set $\chi_p(q) := \left(\frac{p}{q}\right)$. Then we have

$$\mathbf{1}(p \equiv \square \bmod q) = \frac{1}{2}\left(1 + \chi_p(q)\right) \tag{22}$$

Now we wish to generalize the character $\chi_{\mathfrak{t}}$ to a function χ_2 defined on all rational primes in a way that $\chi_2(p) = \chi_{\mathfrak{t}}(\mathfrak{p})$ for a prime $p \equiv 1 \bmod 8$. We set

$$\chi_2(p) = \frac{1}{\#\{\mathfrak{p}|p\}} \sum_{\mathfrak{p}|p} \chi_{\mathfrak{t}}(\mathfrak{p}),$$

where the sum is over all prime ideals $\mathfrak{p}$ in $\mathbb{Z}[\sqrt{d_0}]$ lying above p. With t defined as in (14), p a prime congruent to 1 modulo 8, and $\mathfrak{p}_1$ and $\mathfrak{p}_2$ the two primes in

$\mathbb{Z}[\sqrt{d_0}]$ lying above p, we have

$$\chi_{\mathfrak{t}}(\mathfrak{p}_1)\chi_{\mathfrak{t}}(\mathfrak{p}_2) = \left(\frac{t}{\mathfrak{p}_1}\right)\left(\frac{t}{\mathfrak{p}_2}\right) = \left(\frac{\mathrm{N}(t)}{\mathfrak{p}_1}\right) = \left(\frac{\mathrm{N}(t)}{p}\right) = 1,$$

so that $\chi_{\mathfrak{t}}(\mathfrak{p}_1) = \chi_{\mathfrak{t}}(\mathfrak{p}_2)$. Thus indeed $\chi_2(p) = \chi_{\mathfrak{t}}(\mathfrak{p})$ whenever $p \equiv 1 \bmod 8$.

Given primes p and q, an ordered pair of integers $\boldsymbol{r} = (r_1, r_2) \in \{1,9\} \times \{1,9\}$, and an ordered pair of integers $\boldsymbol{s} = (s_1, s_2) \in \{\pm 1\} \times \{\pm 1\}$, set

$$\boldsymbol{c}(p, q; \boldsymbol{r}, \boldsymbol{s}) := \mathbf{1}\left((p, q) \equiv \boldsymbol{r} \bmod 16 \text{ and } (\chi_2(p), \chi_2(q)) = \boldsymbol{s}\right).$$

Now let p and q be distinct primes, let $\boldsymbol{r}$ and $\boldsymbol{s}$ be as above, and suppose that $s_1 s_2 = 1$, and if $d = 8$, also that $r_1 r_2 \equiv 1 \bmod 16$. Then we have

$$\begin{aligned}\mathbf{1}((p, q) \equiv \boldsymbol{r} \bmod 16,\ (\chi_2(p), \chi_2(q)) = \boldsymbol{s},\ &\text{and } \varepsilon(p, q) = 1) \\ &= \boldsymbol{c}(p, q; \boldsymbol{r}, \boldsymbol{s}) \cdot \frac{1}{2}(1 + \varepsilon(p, q)).\end{aligned}$$

Finally, given a vector $\boldsymbol{e} = (e_1, e_2) \in \mathbb{F}_2^2$ and p, q, $\boldsymbol{r}$, and $\boldsymbol{s}$ as above, define

$$f(p, q) = f(p, q; \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{e}) := \boldsymbol{c}(p, q; \boldsymbol{r}, \boldsymbol{s})\chi_p(q)^{e_1}\varepsilon(p, q)^{e_2}. \tag{23}$$

Then, putting together the formulas above, we deduce that

$$\sum_{\substack{pq \le X,\ p<q \\ (p,q) \equiv \boldsymbol{r} \bmod 16 \\ (\chi_2(p), \chi_2(q)) = \boldsymbol{s} \\ p \equiv \square \bmod q \\ \varepsilon(p,q) = 1}} \sum 1 = \frac{1}{4} \sum_{\boldsymbol{e} \in \mathbb{F}_2^2} \sum_{\substack{pq \le X \\ p<q}} \sum f(p, q; \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{e})$$

whenever $\boldsymbol{s}$ satisfies $s_1 s_2 = 1$ and, if $d = 8$, $\boldsymbol{r}$ satisfies $r_1 r_2 \equiv 1 \bmod 16$. If $\boldsymbol{e} = (0, 0)$, then, as we noted above in (21), we have

$$\sum_{pq \le X,\ p<q} \sum f(p, q; \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{e}) \sim \frac{1}{256} \frac{X \log\log X}{\log X}$$

as $X \to \infty$. Hence Theorem 2 follows from the following oscillation statement.

Theorem 3. *Let $\boldsymbol{r} = (r_1, r_2) \in \{1,9\} \times \{1,9\}$ be such that $r_1 r_2 \equiv 1 \bmod 16$ if $d = 8$, let $\boldsymbol{s} = (s_1, s_2) \in \{\pm 1\} \times \{\pm 1\}$ be such that $s_1 s_2 = 1$, let $\boldsymbol{e} \in \mathbb{F}_2^2$, and let $f(p, q; \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{e})$ be defined as in (23). If $\boldsymbol{e} \neq (0, 0)$, then*

$$\sum_{pq \le X,\ p<q} \sum f(p, q; \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{e}) = o\left(\frac{X \log\log X}{\log X}\right)$$

as $X \to \infty$.

The rest of the paper is devoted to proving Theorem 3.

3.1. **Summing under a hyperbola.** We now describe how to handle sums of the form

$$S(X; f) := \sum_{pq \le X,\ p<q} \sum f(p, q), \tag{24}$$

where $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{C}$ is supported on pairs of prime numbers. The goal is to give good upper bounds for $S(X; f)$ when f oscillates. Let Y be a positive real number. Then

$$S(X; f) = A(X, Y; f) + B(X, Y; f), \tag{25}$$

where

$$A(X,Y;f) := \sum_{\substack{pq\le X,\ p<q\\ p\le Y}}\sum f(p,q), \tag{26}$$

and

$$B(X,Y;f) := \sum_{\substack{pq\le X\\ q>p>Y}}\sum f(p,q). \tag{27}$$

Usually Y is chosen small enough compared to X so that the sum $A(X,Y;f)$ can be handled using the Siegel-Walfisz theorem and variations thereof. Bounding the sum $B(X,Y;f)$ then usually proceeds by proving a double-oscillation theorem for f, and this type of theorem is generally useful only when Y is not too small. We make these techniques precise in the following proposition.

Proposition 4. *Let $X > 1$ be a real number, let $f : \mathbb{Z}\times\mathbb{Z}\to\mathbb{C}$ be a function satisfying $\|f\|_\infty \le 1$, and let $S(X;f)$ be defined as in (24). Let Y be a real number satisfying $1 < Y < X^{\frac{1}{4}}$. Suppose that there exist positive real numbers δ_1, δ_2, and δ_3 satisfying $\delta_3 < \delta_2$ such that*

$$A_p(X;f) := \sum_{q\le X} f(p,q) \ll XY^{-\delta_1} \tag{A}$$

for all $p \le Y$, where the implied constant is absolute, and such that

$$\mathcal{B}(M,N;f,\Delta) := \sum_{\substack{M<p\le M+\Delta M\\ N<q\le N+\Delta N}}\sum f(p,q) \ll \Delta^{-\delta_2}\left(M^{-\delta_3}+N^{-\delta_3}\right)\Delta^2 MN, \tag{B}$$

for all $M, N > 1$ and $\Delta \in (0,1)$ satisfying $\Delta M > M^{\frac{1}{2}}$, $\Delta N > N^{\frac{1}{2}}$, where the implied constant is absolute. Then there exists a positive real number δ in $(0,1)$ such that

$$S(X;f) \ll Y^{-\delta}X\log X,$$

where the implied constant is absolute. Moreover, we can take

$$\delta = \min\left(\frac{\delta_1}{2}, \frac{\delta_3}{2\delta_2}, \frac{\delta_3}{2}\right).$$

Proof. With $A(X,Y;f)$ defined as in (26), using hypothesis (A), we deduce that

$$\begin{aligned} A(X,Y;f) &= \sum_{p\le Y}\left(A_p(X/p;f) - A_p(p;f)\right)\\ &\ll \sum_{p\le Y}\left(Xp^{-1}Y^{-\delta_1} + pY^{-\delta_1}\right)\\ &\ll Y^{-\delta_1}X\log\log Y + Y^{2-\delta_1}\\ &\ll XY^{-\delta_1/2}. \end{aligned} \tag{28}$$

Let $\Delta = Y^{-\frac{\delta_3}{2\delta_2}}$. For each $k \ge 0$, set $M_k = N_k = Y(1+\Delta)^k$. Let $\mathcal{R}(X)$ be the region in $\mathbb{R}^2$ defined by

$$\mathcal{R}(X) = \left\{(x,y)\in\mathbb{R}^2 : x \ge Y, xy \le X(1+\Delta)^{-2}, x(1+\Delta)\le y\right\},$$

and let $\Sigma(X)$ be the subset of $\mathbb{Z}^2_{\ge 0}$ defined by

$$\Sigma(X) = \left\{(j,k)\in\mathbb{Z}^2_{\ge 0} : (M_j,N_k)\in\mathcal{R}(X)\right\}.$$

If $(j,k) \in \Sigma(X)$, then the box $[M_j, M_{j+1}] \times [N_k, N_{k+1}]$ is completely contained in the region

$$\mathcal{T}(X) = \left\{(x,y) \in \mathbb{R}^2 : x \geq Y, xy \leq X, x \leq y\right\}.$$

Let $B(X,Y;f)$ be the sum defined in (27). Then we can partition $B(X,Y;f)$ as

$$B(X,Y;f) = \sum_{(j,k)\in\Sigma(X)} \sum \mathcal{B}(M_j, N_k; f, \Delta) + R(X,Y;f,\Delta). \tag{29}$$

As $\|f\|_\infty \leq 1$, we give a trivial upper bound for $R(X,Y;f,\Delta)$ by counting lattice points in the region $\mathcal{T}(X) \setminus \mathcal{R}(X)$, i.e.,

$$|R(X,Y;f,\Delta)| \leq \#\left(\mathbb{Z}^2 \cap (\mathcal{T}(X) \setminus \mathcal{R}(X))\right).$$

The right-hand side above can be approximated by the area of the region $\mathcal{T}(X) \setminus \mathcal{R}(X)$, with an error term bounded by the sum of the lengths of the projections of $\mathcal{T}(X) \setminus \mathcal{R}(X)$ to the axes (this is known as the Lipschitz principle; see [3] and [4]). Thus we have

(30)

$$\begin{aligned} R(X,Y;f,\Delta) &\ll \int_0^{X^{\frac{1}{2}}} \Delta x dx + \int_Y^{X^{\frac{1}{2}}} \frac{\left(X - X/(1+\Delta)^2\right)}{x} dx + X^{\frac{1}{2}} + XY^{-1} + 1 \\ &\ll \Delta X + X\frac{2\Delta+\Delta^2}{(1+\Delta)^2} \log\left(\frac{X^{\frac{1}{2}}}{Y}\right) + X^{\frac{1}{2}} + XY^{-1} + 1 \\ &\ll \Delta X + \Delta X \log X + XY^{-1} \\ &\ll Y^{-\frac{\delta_3}{2\delta_2}} X \log X + Y^{-1}X. \end{aligned}$$

As $\delta_3 < \delta_2$ and $M_j, N_k \geq Y$, we have $\Delta M_j > M_j^{\frac{1}{2}}, \Delta N_k > N_k^{\frac{1}{2}}$. Thus we can use hypothesis (B) to give the bound

$$\begin{aligned} \sum_{(j,k)\in\Sigma(X)} \sum \mathcal{B}(M_j, N_k; f, \Delta) &\ll \Delta^{-\delta_2} Y^{-\delta_3} \sum_{(j,k)\in\Sigma(X)} \sum \Delta^2 M_j N_k \\ &\ll Y^{-\frac{\delta_3}{2}} \cdot \mathrm{Area}\mathcal{T}(X) \\ &\ll Y^{-\frac{\delta_3}{2}} X \log X. \end{aligned} \tag{31}$$

Combining (28), (30), and (31), we deduce the proposition. □

To apply Proposition 4, we will prove the following two propositions. In the following, define $f(p,q;\boldsymbol{r},\boldsymbol{s},\boldsymbol{e})$ as in Theorem 3, and suppose $\boldsymbol{e} \neq (0,0)$.

Proposition 5. *Let $f(p,q) = f(p,q;\boldsymbol{r},\boldsymbol{s},\boldsymbol{e})$. Then there is a constant $c > 0$ such that for all $p \leq (\log X)^{100}$, we have*

$$A_p(X;f) = \sum_{q \leq X} f(p,q) \ll X \exp\left(-c(\log X)^{\frac{1}{4}}\right),$$

where the implied constant is absolute (but ineffective).

Proposition 6. *Let $f(p,q) = f(p,q;\boldsymbol{r},\boldsymbol{s},\boldsymbol{e})$. Then, for all $M, N > 1$ and $\Delta \in (0,1)$ satisfying $\Delta M, \Delta N > 1$, we have*

$$\mathcal{B}(M,N;f,\Delta) = \sum_{\substack{M<p\leq M+\Delta M \\ N<q\leq N+\Delta N}} \sum f(p,q) \ll \Delta^{-\frac{11}{12}} \left(M^{-\frac{1}{12}} + N^{-\frac{1}{12}}\right) \Delta^2 MN,$$

where the implied constant is absolute.

Hence, assuming Propositions 5 and 6, we can apply Proposition 4 with $Y = (\log X)^{100}$, $\delta_1 = 1$, $\delta_2 = \frac{11}{12}$, and $\delta_3 = \frac{1}{12}$ to obtain Theorem 3. Our goal is now to prove Propositions 5 and 6.

4. Preliminaries on Quadratic Characters in Quadratic Fields

In this section, we prove some properties of quadratic residue symbols in quadratic number fields. The most important among them is Proposition 7 below, which is a generalization of [8, Lemma 21.1, p. 1025]. We have made an effort to make our proof more conceptually clear. Throughout this section, let L denote the quadratic number field of discriminant D, and let $\mathcal{O}_L = \mathbb{Z}[(D+\sqrt{D})/2]$ denote its maximal order.

4.1. **Primitivity.** We say that an ideal $\mathfrak{a}$ in $\mathcal{O}_L$ is *primitive* if $\gcd(\mathfrak{a}, \overline{\mathfrak{a}}) = 1$. Furthermore, we say that an element $w \in \mathcal{O}_L$ is *primitive* if the principal ideal generated by w is primitive. If $\mathfrak{a}$ is primitive, then all prime ideals dividing $\mathfrak{a}$ are unramified of degree one, and so the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_L$ induces an isomorphism

$$\mathbb{Z}/(\mathrm{N}(\mathfrak{a})) \xrightarrow{\sim} \mathcal{O}_L/\mathfrak{a}. \tag{32}$$

We call an ideal $\mathfrak{a}$ (resp. element w) in $\mathcal{O}_L$ *odd* if $\mathrm{N}(\mathfrak{a})$ (resp. $\mathrm{N}(w)$) is an odd integer.

Remark. For instance, in $\mathbb{Z}[\sqrt{-1}]$, the principal ideal (5) is odd but not primitive. Indeed, note that $\mathrm{N}(5) = 25$, but $\mathbb{Z}[\sqrt{-1}]/(5) \cong \mathbb{Z}[\sqrt{-1}]/(2+\sqrt{-1}) \times \mathbb{Z}[\sqrt{-1}]/(2-\sqrt{-1}) \cong \mathbb{Z}/(5) \times \mathbb{Z}/(5) \ncong \mathbb{Z}/(25)$.

If $\mathfrak{a}$ is primitive and odd, then for every rational integer n we have the equality of quadratic residue symbols

$$\left(\frac{n}{\mathrm{N}(\mathfrak{a})}\right) = \left(\frac{n}{\mathfrak{a}}\right), \tag{33}$$

where the symbol on the left is the usual Jacobi symbol while the symbol on the right is the quadratic residue symbol in $\mathcal{O}_L$. By (32) and (33), we deduce that

$$\sum_{z \in \mathcal{O}_L/\mathfrak{a}} \left(\frac{z}{\mathfrak{a}}\right) = \sum_{n \in \mathbb{Z}/(\mathrm{N}(\mathfrak{a}))} \left(\frac{n}{\mathrm{N}(\mathfrak{a})}\right). \tag{34}$$

Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_L$. If either of $\mathfrak{a}$ and $\mathfrak{b}$ is not primitive, then their product $\mathfrak{ab}$ is not primitive. Even if $\mathfrak{a}$ and $\mathfrak{b}$ are both primitive, we will now see that their product $\mathfrak{ab}$ is *not* necessarily primitive.

Lemma 3. *Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are primitive. Let $\mathfrak{r} = \gcd(\mathfrak{a}, \overline{\mathfrak{b}})$ and $r = \mathrm{N}(\mathfrak{r})$. Then $\mathfrak{ab}/(r)$ is primitive. In particular, $\mathfrak{ab}$ is primitive if and only if $\gcd(\mathfrak{a}, \overline{\mathfrak{b}}) = (1)$.*

Proof. Write $\mathfrak{a} = \mathfrak{r}\mathfrak{a}_1$ and $\mathfrak{b} = \overline{\mathfrak{r}}\mathfrak{b}_1$ with $\gcd(\mathfrak{a}_1, \overline{\mathfrak{b}}_1) = (1)$. The claim then is that $\mathfrak{a}_1\mathfrak{b}_1$ is primitive. As $\mathfrak{a}$ is primitive, we have $\gcd(\mathfrak{a}_1, \overline{\mathfrak{a}}_1) = (1)$ and hence $\gcd(\mathfrak{a}_1, \overline{\mathfrak{a}_1\mathfrak{b}_1}) = (1)$. Similarly, as $\mathfrak{b}$ is primitive, we deduce that $\gcd(\mathfrak{b}_1, \overline{\mathfrak{a}_1\mathfrak{b}_1}) = (1)$, and thus the claim is proved. □

Given two primitive ideals $\mathfrak{a}$ and $\mathfrak{b}$ and r as above, we now show that we can obtain a primitive ideal by dividing $\mathfrak{ab}$ by an ideal of norm r (as opposed to r^2).

As before, we set $\mathfrak{r} = \gcd(\mathfrak{a}, \overline{\mathfrak{b}})$ and we write $\mathfrak{r} = \mathfrak{r}_a\mathfrak{r}_b$, where

$$\mathfrak{r}_a = \prod_{\substack{\mathfrak{p}^k \| \mathfrak{r} \\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) < \mathrm{ord}_{\mathfrak{p}}(\overline{\mathfrak{b}})}} \mathfrak{p}^k, \qquad \text{and} \qquad \mathfrak{r}_b = \prod_{\substack{\mathfrak{p}^k \| \mathfrak{r} \\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \geq \mathrm{ord}_{\mathfrak{p}}(\overline{\mathfrak{b}})}} \mathfrak{p}^k.$$

We set $\mathfrak{c} = \mathfrak{r}_a\overline{\mathfrak{r}_b}$. Then clearly $\mathrm{N}(\mathfrak{c}) = \mathrm{N}(\mathfrak{r}) = r$. Moreover, by construction

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

so by Lemma 3, we conclude $\mathfrak{a}\mathfrak{b}/\mathfrak{c}$ is primitive. As $\gcd(\mathfrak{r}_a, \mathfrak{r}_b) = (1)$, we see that $\mathfrak{c}$ is also primitive. Finally, we claim that $\gcd(\mathfrak{c}, \mathfrak{a}\mathfrak{b}/\mathfrak{c}) = (1)$. Indeed, suppose that $\mathfrak{p}$ divides $\mathfrak{c}$. First, if $\mathfrak{p}$ divides $\mathfrak{r}_a$, then $\mathfrak{p}$ doesn't divide $\mathfrak{a}/\mathfrak{r}_a$ by construction and $\mathfrak{p}$ doesn't divide $\mathfrak{b}/\overline{\mathfrak{r}_b}$ because $\mathfrak{b}$ is primitive. Similarly, if $\mathfrak{p}$ divides $\overline{\mathfrak{r}_b}$, then $\mathfrak{p}$ doesn't divide $\mathfrak{b}/\overline{\mathfrak{r}_b}$ by construction and $\mathfrak{p}$ doesn't divide $\mathfrak{a}/\mathfrak{r}_a$ because $\mathfrak{a}$ is primitive. This proves the claim. Now the Chinese Remainder Theorem and (32) imply that

$$\mathcal{O}_L/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_L/(\mathfrak{a}\mathfrak{b}/\mathfrak{c}) \times \mathcal{O}_L/\mathfrak{c} \cong \mathbb{Z}/(Y/r) \times \mathbb{Z}/(r), \tag{35}$$

where $Y = \mathrm{N}(\mathfrak{a}\mathfrak{b})$.

4.2. **Cancellation in quadratic character sums.** The rough idea behind proving that the symbol $\varepsilon(p, q)$ defined in (19) oscillates as p and q vary in a box where neither p nor q is too small is to give meaning to $\varepsilon(m, n)$ for all integers m and n, then to prove that the bilinear sum

$$\sum_m \sum_n a_m b_n \varepsilon(m, n)$$

oscillates for any bounded sequences $\{a_m\}_m$ and $\{b_n\}_n$, and finally to apply this result to sequences $\{a_m\}_m$ and $\{a_n\}_n$ supported on the primes. The following definition generalizes the symbol $\varepsilon(p, q)$ in a way that will allow us to apply this method.

Let $w, z \in \mathcal{O}_L$ and suppose that w is odd. We define the quadratic multiplicative character $\chi_w : \mathcal{O}_L \to \{-1, 0, 1\}$ by setting

$$\chi_w(z) := \left(\frac{z}{(w)}\right),$$

and we define the multiplier factor $\mathrm{m}(w)$ for odd elements $w \in \mathcal{O}_L$ by setting $\mathrm{m}(w) := \chi_w(\overline{w})$. We note that $\chi_w(z) \neq 0$ if and only if $\gcd((z), (w)) = (1)$, and so in particular Lemma 3 implies that $\mathrm{m}(w)$ is supported on primitive elements w.

Remark. Suppose $w \in \mathcal{O}_L$ generates an odd prime of degree 1, so that $\mathrm{N}(w) = p$ for some rational prime p. Then

$$\chi_w(z)\chi_w(\overline{z}) = \left(\frac{\mathrm{N}(z)}{(w)}\right) = \left(\frac{\mathrm{N}(z)}{p}\right), \tag{36}$$

where the symbol on the far right is the usual Jacobi symbol.

Remark. In the particular case when w and z are primes in $\mathbb{Z}[\sqrt{d_0}]$ (with $d_0 \in \{-1, -2, 2\}$) lying above rational primes p and q, respectively, satisfying (4), (5), (6), (9), and, if $d = 8$, also (13), then $\varepsilon(p, q)$ as defined in (19) can be written as

$$\varepsilon(p, q) = \mathrm{m}(w)\chi_w(\overline{z}). \tag{37}$$

Remark. The Dirichlet symbol defined in [8, Equation (19.11), p. 1019] is simply equal to $\mathrm{m}(w)\chi_w(\overline{z})$ in the special case that $L = \mathbb{Q}(\sqrt{-1})$.

The following proposition provides all of the cancellation that we need for Proposition 6.

Proposition 7. *Let $w_1, w_2 \in \mathcal{O}_L$ be odd and primitive. Let $\mathfrak{r} = \gcd((w_1), (\overline{w}_2))$, $r = \mathrm{N}(r)$, $Y = \mathrm{N}(w_1 w_2)$. Then*

$$\left| \sum_{z \in \mathcal{O}_L/(Y)} \chi_{w_1}(z)\chi_{w_2}(z) \right| = \begin{cases} Y\varphi(r)\varphi(Y/r) & \text{if } Y \text{ and } r \text{ are squares} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We have

$$\sum_{z \in \mathcal{O}_L/(Y)} \chi_{w_1}(z)\chi_{w_2}(z) = \sum_{z \in \mathcal{O}_L/(Y)} \left(\frac{z}{(w_1 w_2)}\right) = Y \sum_{z \in \mathcal{O}_L/(w_1 w_2)} \left(\frac{z}{(w_1 w_2)}\right).$$

By (35), we have $\mathcal{O}_L/(w_1 w_2) \cong \mathcal{O}_L/\mathfrak{c}_1 \times \mathcal{O}_L/\mathfrak{c}_2$, where $\mathfrak{c}_1$ and $\mathfrak{c}_2$ are coprime primitive ideals of norm Y/r and r, respectively, satisfying $(w_1 w_2) = \mathfrak{c}_1\mathfrak{c}_2$. Hence

$$\sum_{z \in \mathcal{O}_L/(w_1 w_2)} \left(\frac{z}{(w_1 w_2)}\right) = \sum_{\substack{z_1 \bmod \mathfrak{c}_1 \\ z_2 \bmod \mathfrak{c}_2}} \sum \left(\frac{z'}{\mathfrak{c}_1\mathfrak{c}_2}\right),$$

where $z' = z'(z_1, z_2)$ is the unique congruence class modulo $\mathfrak{c}_1\mathfrak{c}_2$ such that $z' \equiv z_1 \bmod \mathfrak{c}_1$ and $z' \equiv z_2 \bmod \mathfrak{c}_2$. With these choices, we have

$$\left(\frac{z'}{\mathfrak{c}_1\mathfrak{c}_2}\right) = \left(\frac{z'}{\mathfrak{c}_1}\right)\left(\frac{z'}{\mathfrak{c}_2}\right) = \left(\frac{z_1}{\mathfrak{c}_1}\right)\left(\frac{z_2}{\mathfrak{c}_2}\right).$$

Then, by (34), we have

$$\sum_{z_1 \bmod \mathfrak{c}_1} \left(\frac{z_1}{\mathfrak{c}_1}\right) \sum_{z_2 \bmod \mathfrak{c}_2} \left(\frac{z_2}{\mathfrak{c}_2}\right) = \sum_{c_1 \in \mathbb{Z}/(Y/r)} \left(\frac{c_1}{Y/r}\right) \sum_{c_2 \in \mathbb{Z}/(r)} \left(\frac{c_2}{r}\right),$$

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

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

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

4.3. **A family of Hecke characters for $\mathbb{Z}[\sqrt{d_0}]$.** We now return to the case that $d \in \{-4, -8, 8\}$, and we set $d_0 = d/4$, as before. The function χ_w is a character on $\left(\mathbb{Z}[\sqrt{d_0}]/(w)\right)^\times$. We now show that this character can be completed into a Hecke character ψ_w for $\mathbb{Q}(\sqrt{d})$ in the case that w is a prime of degree 1 in $\mathbb{Z}[\sqrt{d_0}]$ satisfying $\mathrm{N}(w) = p \equiv 1 \bmod 8$. We must define a homomorphism ψ_w on the group $\mathcal{I}(w)$ of fractional ideals of $\mathbb{Z}[\sqrt{d_0}]$ coprime to (w), i.e.,

$$\psi_w : \mathcal{I}(w) \to S^1 = \{s \in \mathbb{C} : |s| = 1\},$$

such that there exists a continuous function

$$\chi_{w,\infty} : F^\times \to S^1$$

satisfying $\chi_w(u)\chi_{w,\infty}(u) = \psi_w((u)) = 1$ for all units $u \in \mathbb{Z}[\sqrt{d_0}]^\times$; here

$$F^\times = \begin{cases} \mathbb{C}^\times & \text{if } d = -4 \text{ or } -8, \\ \mathbb{R}^\times \times \mathbb{R}^\times & \text{if } d_0 = 8. \end{cases}$$

4.3.1. *The cases $d = -4$ and $d = -8$.* For the case $d = -8$, note that χ_w is trivial on $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$ because $p \equiv 1 \bmod 4$ (i.e., $\left(\frac{-1}{p}\right) = 1$). For the case $d = -4$, suppose $w = a + b\sqrt{-1}$ with $a, b \in \mathbb{Z}$, a odd, and $b = 2^k b'$ with b' odd. As $\gcd(b, p) = 1$, we can write $\sqrt{-1} \equiv -a/b \bmod w$. As $p = a^2 + b^2 \equiv 1 \bmod 8$, we have

$$\begin{aligned} \chi_w(\sqrt{-1}) &= \left(\frac{\sqrt{-1}}{(w)}\right) = \left(\frac{-a/b}{(w)}\right) = \left(\frac{-ab}{(w)}\right) \\ &= \left(\frac{-ab}{p}\right) = \left(\frac{|a|}{p}\right)\left(\frac{|b'|}{p}\right) \\ &= \left(\frac{p}{|a|}\right)\left(\frac{p}{|b'|}\right) = 1 \cdot 1 = 1, \end{aligned}$$

where the symbols from the second line onwards are usual Jacobi symbols. Hence χ_w is trivial on $\mathbb{Z}[\sqrt{-1}]^\times$. Therefore, in case $d \in \{-4, -8\}$, we can extend χ_w to a character on ideals in $\mathbb{Z}[\sqrt{d_0}]$ by setting $\chi_w(\mathfrak{a}) := \chi_w(z)$, where z is any generator of $\mathfrak{a}$. Now it suffices to take $\chi_{w,\infty}$ to be identically 1 on all of $\mathbb{C}^\times$. Then setting $\psi_w(\mathfrak{a}) := \chi_w(\mathfrak{a})$ defines is a character on $\mathcal{I}(w)$. Moreover, by (37), if p and q are primes satisfying (4) and (5), and w and z are primes in $\mathbb{Z}[\sqrt{d_0}]$ satisfying (6) and (9), then we have $\varepsilon(p, q) = \mathrm{m}(w)\psi_w((\overline{z}))$.

4.3.2. *The case $d = 8$.* Suppose $w = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. Then, as $p \equiv 1 \bmod 8$, b must be even. The unit group $\mathbb{Z}[\sqrt{2}]^\times$ is generated by -1 and $\varepsilon = 1 + \sqrt{2}$. We have $\chi_w(-1) = \left(\frac{-1}{p}\right) = 1$. If we write $b = 2^k b'$ with b' odd, we have

$$\begin{aligned} \chi_w(\varepsilon) &= \left(\frac{1+\sqrt{2}}{(w)}\right) = \left(\frac{1 - a/b}{(w)}\right) \\ &= \left(\frac{1-a/b}{p}\right) = \left(\frac{b^2 - ab}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{a-b}{p}\right) \\ &= \left(\frac{p}{|b'|}\right)\left(\frac{p}{|a-b|}\right) = 1 \cdot \left(\frac{p - (a^2 - b^2)}{|a-b|}\right) = \left(\frac{-1}{|a-b|}\right), \end{aligned} \tag{38}$$

where again the symbols from the second line onwards are usual Jacobi symbols. Every other generator for the ideal (w) of norm p is of the form $\pm\varepsilon^{2k}w$, where k is an integer. As $\varepsilon^2(a + b\sqrt{2}) = (3a + 4b) + (2a + 3b)\sqrt{2}$ and $(3a + 4b) - (2a + 3b) = a + b \equiv a - b \bmod 4$, the last line of (38) implies that $\chi_w(\varepsilon) = \chi_{\varepsilon^2 w}(\varepsilon)$. Moreover, again by the last line of (38), we have $\chi_{-w}(\varepsilon) = \left(\frac{-1}{|-a+b|}\right) = \left(\frac{-1}{|a-b|}\right) = \chi_w(\varepsilon)$. Thus we cannot always choose a generator w of a prime ideal lying above p satisfying both $\mathrm{N}(w) = p$ and $\chi_w(\varepsilon) = 1$. In fact, we have

$$\chi_w(\varepsilon) = \begin{cases} 1 & \text{if } |a - b| \equiv 1 \bmod 4, \\ -1 & \text{otherwise.} \end{cases}$$

We will define a different Hecke character ψ_w modulo $(w)\infty_1\infty_2$ in each of the cases above; here ∞_1 and ∞_2 are the two embeddings $\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{R}$. If $\chi_w(\varepsilon) = 1$, then χ_w is already a character on fractional ideals in $\mathbb{Z}[\sqrt{2}]$ and we simply define ψ_w :

$\mathcal{I}(w) \to S^1$ by setting $\psi_w(\mathfrak{a}) := \chi_w(z)$, where z is any generator of $\mathfrak{a}$. In this case, we again take $\chi_{w,\infty}$ to be identically 1 on all of $\mathbb{R}^\times \times \mathbb{R}^\times$. If $\chi_w(\varepsilon) = -1$, we take $\chi_{w,\infty}(z) = \mathrm{sign}(\mathrm{N}(z))$, and define $\psi_w(\mathfrak{a}) = \chi_w(z)\chi_{w,\infty}(z)$, where z is any generator of $\mathfrak{a}$. The homomorphism ψ_w is well-defined because $\chi_w(\varepsilon)\chi_{w,\infty}(\varepsilon) = -1 \cdot -1 = 1$ and $\chi_w(-1)\chi_{w,\infty}(-1) = 1 \cdot 1 = 1$.

We note that in both cases, if $z \equiv 1 \bmod {}^\times(w)\infty_1\infty_2$, so that $z, \overline{z} > 0$, then $\psi_w((z)) = 1 = \mathrm{sign}(z)$. Furthermore, similarly as in the cases $d = -4$ and $d = -8$, if p and q are primes satisfying (4) and (5) and w and z are primes in $\mathbb{Z}[\sqrt{2}]$ satisfying (6), (9), (13), then we have $\varepsilon(p,q) = \mathrm{m}(w)\psi_w((\overline{z}))$.

Finally, we remark that if w and z in $\mathbb{Z}[\sqrt{d_0}]$ (*any* $d_0 \in \{-1,-2,2\}$) satisfying (6), (9), and also (13) if $d_0 = 2$, then so do w and $\overline{z}$. Hence

$$\varepsilon(p,q) = \mathrm{m}(w)\psi_w(\mathfrak{q}), \tag{39}$$

where $\mathfrak{q}$ is any prime ideal in $\mathbb{Z}[\sqrt{d_0}]$ lying above q.

5. Proof of Proposition 5

In this section, we exploit the arithmetic of $\mathbb{Q}(\sqrt{d})$ ($d \in \{-4,-8,8\}$) to prove that $\varepsilon(p,q)$ oscillates when q varies over a range much bigger than the size of p. The main tool is the theory of Hecke L-functions. Let us first recall the sum from Proposition 5. We let

$$A_p(X;f) = \sum_{q \le X} f(p,q;\boldsymbol{r},\boldsymbol{s},\boldsymbol{e}),$$

where $\boldsymbol{r} = (r_1,r_2) \in \{1,9\} \times \{1,9\}$, $r_1r_2 \equiv 1 \bmod 16$ if $d = 8$, $\boldsymbol{s} = (s_1,s_2) \in \{\pm 1\} \times \{\pm 1\}$, $s_1s_2 = 1$, $\boldsymbol{e} \in \mathbb{F}_2^2$, $\boldsymbol{e} \neq (0,0)$, and

$$f(p,q;\boldsymbol{r},\boldsymbol{s},\boldsymbol{e}) = \begin{cases} \chi_p(q)^{e_1}\varepsilon(p,q)^{e_2} & \text{if } (p,q) \equiv \boldsymbol{r} \bmod 16 \text{ and } (\chi_2(p),\chi_2(q)) = \boldsymbol{s} \\ 0 & \text{otherwise.} \end{cases}$$

Hence $A_p(X;f)$ vanishes unless $p \equiv r_1 \bmod 16$ and $\chi_2(p) = s_1$. So let p be a prime number satisfying $p \equiv r_1 \bmod 16$ and $\chi_2(p) = s_1$, let $w \in \mathbb{Z}[\sqrt{d_0}]$ be a prime satisfying (6), and let ψ_w be the Hecke character on $\mathbb{Q}(\sqrt{d})$ defined in Section 4.3. By (39), we have

$$f(p,q;\boldsymbol{r},\boldsymbol{s},\boldsymbol{e}) = \begin{cases} \left(\frac{p}{\mathfrak{q}}\right)^{e_1} (\mathrm{m}(w)\psi_w(\mathfrak{q}))^{e_2} & \text{if } q \equiv r_2 \bmod 16 \text{ and } \chi_2(q) = s_2 \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathfrak{q}$ is a prime ideal in $\mathbb{Z}[\sqrt{d_0}]$ dividing q. To use the theory of L-functions for the number field $\mathbb{Q}(\sqrt{d})$, we now define a function on *all* ideals $\mathfrak{q}$ in $\mathbb{Z}[\sqrt{d_0}]$. Let

$$f_1(\mathfrak{q};w,\boldsymbol{e}) := \left(\frac{p}{\mathfrak{q}}\right)^{e_1} \psi_w(\mathfrak{q})^{e_2}.$$

We can detect the congruence condition $q \equiv r_2 \bmod 16$ via Dirichlet characters modulo 16 and the condition $\chi_2(q) = s_2$ via the formula

$$\frac{1}{2}\left(1 + s_2\chi_2(q)\right) = \begin{cases} 1 & \text{if } \chi_2(q) = s_2 \\ 0 & \text{otherwise.} \end{cases}$$

Then, with $c_p = 32 \cdot \mathrm{m}(w)^{e_2}$, we have

$$\begin{aligned} c_p \cdot A_p(X; f) &= \sum_{\substack{\chi_{16} \bmod 16 \\ e_3 \in \mathbb{F}_2}} \sum \sum_{\substack{\mathfrak{q} \text{ split} \\ \mathrm{N}(\mathfrak{q}) \leq X}} \chi_{16}(r_2 \mathrm{N}(\mathfrak{q}))(s_2 \chi_{\mathfrak{t}}(\mathfrak{q}))^{e_3} f_1(\mathfrak{q}; w, \boldsymbol{e}) \\ &= \sum_{\substack{\chi_{16} \bmod 16 \\ e_3 \in \mathbb{F}_2}} \sum \sum_{\substack{\mathfrak{q} \\ \mathrm{N}(\mathfrak{q}) \leq X}} \chi_{16}(r_2 \mathrm{N}(\mathfrak{q}))(s_2 \chi_{\mathfrak{t}}(\mathfrak{q}))^{e_3} f_1(\mathfrak{q}; w, \boldsymbol{e}) \\ &\quad - \sum_{\substack{\chi_{16} \bmod 16 \\ e_3 \in \mathbb{F}_2}} \sum \sum_{\substack{\mathfrak{q} \text{ inert} \\ \mathrm{N}(\mathfrak{q}) \leq X}} \chi_{16}(r_2 \mathrm{N}(\mathfrak{q}))(s_2 \chi_{\mathfrak{t}}(\mathfrak{q}))^{e_3} f_1(\mathfrak{q}; w, \boldsymbol{e}), \end{aligned}$$

where the outer sums are over Dirichlet characters χ_{16} modulo 16 and elements $e_3 \in \mathbb{F}_2$. But if a prime ideal $\mathfrak{q} = (q)$ in $\mathbb{Z}[\sqrt{d_0}]$ is inert, then $\mathrm{N}(\mathfrak{q}) = q^2$, so

$$\sum_{\substack{\mathfrak{q} \text{ inert} \\ \mathrm{N}(\mathfrak{q}) \leq X}} 1 \ll X^{\frac{1}{2}}.$$

Hence, to prove Proposition 5, it remains to show, for each Dirichlet character χ_{16} and element $e_3 \in \mathbb{F}_2$, that there exists a constant $c > 0$ such that

$$\sum_{\mathrm{N}(\mathfrak{q}) \leq X} \chi_{16}(\mathrm{N}(\mathfrak{q})) \chi_{\mathfrak{t}}(\mathfrak{q})^{e_3} f_1(\mathfrak{q}; w, \boldsymbol{e}) \ll X \exp\left(c\sqrt{\log X}\right)$$

for all $p = \mathrm{N}(w) \leq (\log X)^{100}$. We now apply the theory of Hecke L-functions to obtain this bound. Define the Hecke character ψ for $\mathbb{Z}[\sqrt{d_0}]$ by setting

$$\psi(\mathfrak{q}) = \chi_{16}(\mathrm{N}(\mathfrak{q})) \chi_{\mathfrak{t}}(\mathfrak{q})^{e_3} f_1(\mathfrak{q}; w, \boldsymbol{e}).$$

We claim that the function $\mathfrak{q} \mapsto \psi(\mathfrak{q})$ is a non-trivial Hecke character for $\mathbb{Z}[\sqrt{d_0}]$ of conductor $\mathfrak{f}$ satisfying $\mathrm{N}(\mathfrak{f}) \ll p^2$, where the implied constant is absolute. First, note that $\mathfrak{q} \mapsto \chi_{16}(\mathrm{N}(\mathfrak{q})) \chi_{\mathfrak{t}}(\mathfrak{q})^{e_3}$ is a Hecke character of conductor dividing a power of 2. If $e_1 = 1$ and $e_2 = 0$, then the claim follows because $\mathfrak{q} \mapsto \left(\frac{p}{\mathfrak{q}}\right)$ is a non-trivial Hecke character of conductor (p). If $e_1 = 0$ and $e_2 = 1$, then the claim follows because $\mathfrak{q} \mapsto \psi_w(\mathfrak{q})$ is a non-trivial Hecke character of conductor (w), as shown in Section 4.3. Finally, if $e_1 = e_2 = 1$, then by (36), we have

$$\left(\frac{p}{\mathfrak{q}}\right) \psi_w(\mathfrak{q}) = \psi_w(\overline{\mathfrak{q}}) = \psi_{\overline{w}}(\mathfrak{q}),$$

so that $\mathfrak{q} \mapsto \left(\frac{p}{\mathfrak{q}}\right) \psi_w(\mathfrak{q})$ is a non-trivial Hecke character of conductor $(\overline{w})$.

Now that we have established the claim, we use a version of the Siegel-Walfisz Theorem for Hecke L-functions. As usual, we define the Hecke L-function

$$L(s, \psi) = \sum_{\mathfrak{a}} \psi(\mathfrak{a}) \mathrm{N}(\mathfrak{a})^{-s} \quad (\Re(s) > 1),$$

where the sum is over all non-zero ideals $\mathfrak{a} \subset \mathbb{Z}[\sqrt{d_0}]$. By [25, Theorem 3.3.1, p. 93], $L(s, \psi)$ has a meromorphic continuation to $\mathbb{C}$ and satisfies a functional equation as well as other standard properties of L-functions. As ψ is not the trivial character, the order of the pole at $s = 1$ of $L(s, \psi)$ is 0. Hence [13, Main Theorem, p. 418]

(with, say, $\varepsilon = \frac{1}{800}$) implies that there is an absolute constant $c > 0$ such that for all $p \leq (\log X)^{100}$, we have

$$\sum_{\mathrm{N}(\mathfrak{q})} \psi(\mathfrak{q}) \ll X \exp\left(-c(\log X)^{\frac{1}{4}}\right).$$

This completes the proof of Proposition 5.

Remark. The range of p for which the above bound holds could be extended to $\exp\left(c'\sqrt{\log X}\right)$ for some small $c' > 0$ instead of a power of $\log X$ if we were certain that $L(s, \psi)$ has no Siegel zeros. Although this is conjectured to be true in any case, we can only show it in the cases when $d \in \{-4, -8\}$ and $e_2 = 1$. In all cases $d \in \{-4, -8, 8\}$, when $e_2 = 1$, the theta series

$$\Theta(z, \psi) = \sum_{\mathfrak{a}} \psi(\mathfrak{a}) \exp(2\pi i \mathrm{N}(\mathfrak{a}))$$

is a holomorphic modular form of weight 1 and level $4p$ (see [25, Theorem 4.8.2, p. 183]). Now a theorem of Hoffstein and Ramakrishnan [18, Theorem C, p.299] implies that the associated L-function $L(s, \psi)$ has no Siegel zero whenever $\Theta(z, \psi)$ is a cusp form. If $d = -4$ or $d = -8$, then this is indeed the case. Otherwise, if $d = 8$, unfortunately $\Theta(z, \psi)$ is *not* a cusp form.

6. Proof of Proposition 6

In this section we finish the proof of Proposition 6 and hence also of Theorem 1. We will use power-saving upper bounds for very general bilinear sums that were obtained in [8] for $d = -4$ and [24] for $d = 8$. We first prove an estimate that holds in general quadratic fields.

6.1. **Double-oscillation estimates for $\chi_w(z)$.** Let L be the quadratic number field of discriminant D, and let $\mathcal{O}_L$ be its ring of integers, as before. For a subset $S \subset \mathbb{R}^2$ and an element $w = a + b\sqrt{D} \in L$ with $a, b \in \mathbb{Q}$, we will write $w \in S$ if and only if $(a, b) \in S$. If $D > 0$, we define a region $\mathcal{R}_k \subset \mathbb{R}^2$ for each integer $k \geq 1$ by setting

$$\mathcal{R}_k := \left\{(x, y) \in \mathbb{R}^2 : \ x > 0, |y| \leq D^{-\frac{1}{2}} \frac{\varepsilon_D^k - 1}{\varepsilon_D^k + 1} x\right\}.$$

where ε_D is the fundamental unit of norm $+1$, i.e., the smallest element of $\mathcal{O}_L \hookrightarrow \mathbb{R}$ satisfying $\varepsilon_D > 1$ and $\mathrm{N}(\varepsilon_D) = 1$. Then $\mathcal{R}_k$ looks like a cone emanating from the origin. Moreover, the set of $\alpha \in \mathcal{O}_L \cap \mathcal{R}_k$ is exactly the set of totally positive $\alpha \in \mathcal{O}_L$ satisfying $\varepsilon_D^{-k} \leq \overline{\alpha}/\alpha \leq \varepsilon_D^k$. Hence every principal ideal of $\mathcal{O}_L$ that can be generated by a totally positive element has exactly one generator in $\mathcal{R}_1$ (see for instance [22, Chapter 6]). If $D < 0$, we simply set $\mathcal{R}_k = \mathbb{R}^2$. Finally, given positive real numbers X and Δ, we set

$$\mathcal{R}_k(X; \Delta) := \left\{(x, y) \in \mathcal{R}_k : \ X \leq \mathrm{N}(x + y\sqrt{D}) < X(1 + \Delta)\right\}.$$

We note that there are constants $c_1 = c_1(D, k) > 0$ and $c_2 = c_2(D, k) > 0$ such that the 2-dimensional volume of $\mathcal{R}_k(X; \Delta)$ is bounded by $c_2 \Delta X$ and such that the sum of the 1-dimensional volumes of the projections of $\mathcal{R}_k(X; \Delta)$ on the coordinate axes is bounded by $c_1 X^{\frac{1}{2}}$.

We now define the general bilinear sum of interest. Given two sequences of complex numbers $\alpha = \{\alpha_w\}$ and $\beta = \{\beta_z\}$ indexed by elements of $\mathcal{O}_L$, and real numbers $W, Z > 0$, we set

$$B(W, Z; \alpha, \beta) := \sum_{w \in \mathcal{R}_1(W;\Delta)}^{*} \sum_{z \in \mathcal{R}_1(Z;\Delta)}^{*} \alpha_w \beta_z \chi_w(z),$$

where $*$ restricts the sums to primitive elements. We will prove

Proposition 8. *There exists a real number $C > 0$ such that: for all real numbers $W, Z > 1$, for all real numbers $\Delta \in (0, 1)$ satisfying $\Delta W > W^{\frac{1}{2}}$, $\Delta Z \geq Z^{\frac{1}{2}}$, and for all sequences of complex numbers $\alpha = \{\alpha_w\}$ and $\beta = \{\beta_z\}$ satisfying $|\alpha_w|, |\beta_z| \leq 1$ and supported on w and z such that the principal ideals (w) and (z) each have at most f prime ideal factors in $\mathcal{O}_L$, we have*

$$|B(W, Z; \alpha, \beta)| \leq C \cdot 2^{40f} \Delta^{-\frac{11}{12}} \left(W^{-\frac{1}{12}} + Z^{-\frac{1}{12}} \right) \Delta^2 WZ \log(W + Z).$$

Proof. Fix an integer $k \geq 1$. The implied constants in the $\ll$ symbols that follow may depend on k in some cases, but we suppress this dependence since we will ultimately take $k = 3$. By Hölder's inequality (with $\frac{2k-1}{2k} + \frac{1}{2k} = 1$), we have

$$|B(W, Z; \alpha, \beta)|^{4k} \leq \left(\sum_{w}^{*} |\alpha_w|^{\frac{2k}{2k-1}} \right)^{4k-2} \cdot \left(\sum_{w}^{*} \left| \sum_{z}^{*} \beta_z \chi_w(z) \right|^{2k} \right)^2, \tag{40}$$

where the sums over w and z are implicitly restricted to $w \in \mathcal{R}_1(W, \Delta)$ and $z \in \mathcal{R}_1(Z, \Delta)$, each having at most f prime ideal factors. By the Lipschitz principle (see [3]), since $|\alpha_w| \leq 1$, and since $1 \leq W^{\frac{1}{2}} \leq \Delta W$, the first factor on the right-hand side of (40) is

$$\ll (\Delta W)^{4k-2}. \tag{41}$$

We expand the inner sum in the second factor on the right-hand side of (40) to get

$$\left| \sum_{z}^{*} \beta_z \chi_w(z) \right|^{2k} = \sum_{z} \beta'_z \chi_w(z),$$

where

$$\beta'_z = \sum_{\substack{z = z_1 \cdots z_{2k} \\ z_1, \ldots, z_{2k} \in \mathcal{R}_1(Z, \Delta) \\ z_1, \ldots, z_{2k} \text{ primitive}}} \beta_{z_1} \overline{\beta_{z_2}} \cdots \beta_{z_{2k-1}} \overline{\beta_{z_{2k}}}.$$

We now determine the support of β'_z. If $z = z_1 \cdots z_{2k}$ with $z_i \in \mathcal{R}_1(Z, \Delta)$ for $1 \leq i \leq 2k$, then $Z^{2k} \leq \mathrm{N}(z) \leq Z^{2k}(1 + \Delta)^{2k}$ and $z \in \mathcal{R}_{2k}$. Hence $\beta'_z = 0$ unless $z \in \mathcal{R}_{2k}(Z^{2k}, \Delta')$, where $\Delta' = (1 + \Delta)^{2k} - 1$, and unless the principal ideal (z) has at most $2kf$ prime ideal factors. We now apply the Cauchy-Schwarz inequality to the second factor on the right-hand side of (40) to get

$$\left(\sum_{z} \beta'_z \sum_{w}^{*} \chi_w(z) \right)^2 \ll \left(\sum_{z} |\beta'_z|^2 \right) \cdot \sum_{z} \left| \sum_{w}^{*} \chi_w(z) \right|^2, \tag{42}$$

where the summations over z are implicitly restricted to $z \in \mathcal{R}_{2k}(Z^{2k}, \Delta')$. Since β'_z is supported on z that are a product of $2k$ numbers $z_i \in \mathcal{R}_1(Z, \Delta)$, each of which has at most f prime ideal factors, and since each principal ideal has at most

g generators in $\mathcal{R}_1(Z,\Delta)$, where $g=1$ if $D>0$, $g=4$ if $D=-4$, $g=6$ if $D=-3$, and $g=2$ otherwise, we deduce by prime ideal factorization that

$$|\beta_z'| \le (2k)! \cdot \binom{2kfg}{f}^{2k} \le (2k)! \cdot 2^{24k^2 f}.$$

Hence the first factor on the right-hand side of (42) is

$$\ll 2^{48k^2 f} \Delta' Z^{2k} \ll 2^{48k^2 f} \Delta Z^{2k}, \tag{43}$$

since $\Delta' = (1+\Delta)^{2k} - 1 \le 2^{2k}\Delta$. We expand the square in the second factor on the right-hand side of (42) and rearrange the sums to get

$$\sideset{}{^*}\sum_{w_1} \sideset{}{^*}\sum_{w_2} \sum_{z \in \mathcal{R}_{2k}(Z^{2k},\Delta')} \chi_{w_1}(z)\chi_{w_2}(z). \tag{44}$$

For each pair of primitive w_1 and w_2, set $Y = \mathrm{N}(w_1 w_2)$ and $r = \mathrm{N}(\gcd((w_1),(\overline{w}_2)))$. Using the Lipschitz principle of Davenport [3] and Proposition 7, we estimate the inner sum by

$$\sum_{z \in \mathcal{R}_{2k}(Z^{2k},\Delta')} \chi_{w_1}(z)\chi_{w_2}(z) \ll \begin{cases} \Delta Z^{2k} + YZ^k + Y^2 & \text{if } Y \text{ and } r \text{ are squares} \\ YZ^k + Y^2 & \text{otherwise.} \end{cases}$$

Hence (44) is

$$\ll \sum_{\substack{W < m_1, m_2 \le (1+\Delta)W \\ m_1 m_2 \text{ square}}} \sum 4^f \left(\Delta Z^{2k} + W^2 Z^k + W^4\right) + (\Delta W)^2 \left(W^2 Z^k + W^4\right). \tag{45}$$

The factor 4^f appears because the summations over w_i are implicitly restricted to w_i with at most f prime ideal factors; the number of such $w \in \mathcal{R}_1(W)$ satisfying $\mathrm{N}(w) = m$ for a given m is at most 2^f. Combining (41), (43), and (45), we deduce that $|B(W,Z;\alpha,\beta)|^{4k}$ is less than some absolute constant $C>0$ times

$$2^{50k^2 f} \Delta^{4k+1} \left(W^{4k-1} Z^{4k} \log W + W^{4k+2} Z^{3k} + W^{4k+4}\right),$$

which implies that $B(W,Z;\alpha,\beta) \ll$

$$2^{13kf} \Delta^{1+\frac{1}{4k}} \left(W^{-\frac{1}{4k}} + W^{\frac{1}{2k}} Z^{-\frac{1}{4}} + W^{\frac{1}{k}} Z^{-1}\right) WZ \log W.$$

Note that $W^{-\frac{1}{4k}} > W^{\frac{1}{2k}} Z^{-\frac{1}{4}}$ whenever $Z > W^{\frac{k}{3}}$ and that $W^{-\frac{1}{4k}} > W^{\frac{1}{k}} Z^{-1}$ whenever $Z > W^{\frac{5}{4k}}$. Choosing $k=3$, we get that

$$B(W,Z;\alpha,\beta) \ll 2^{40f} \Delta^{\frac{13}{12}} W^{\frac{11}{12}} Z \log W \tag{46}$$

whenever $Z > W$. We now exploit the symmetry of the quadratic residue symbol. Indeed, by the law of quadratic reciprocity, we have

$$\chi_w(z) = \delta(w,z)\chi_z(w),$$

where $\delta(w,z)$ depends only on the congruence classes of w and z modulo 8. Hence

$$B(W,Z;\alpha,\beta) = \sum_{\omega \bmod 8} \sum_{\zeta \bmod 8} B(W,Z;\alpha(\omega),\beta(\zeta)),$$

where $\alpha(\omega)_w = \alpha_w \cdot \mathbf{1}(w \equiv \omega \bmod 8)$ and $\beta(\zeta)_z = \beta_z \cdot \mathbf{1}(z \equiv \zeta \bmod 8)$. But now $B(W, Z; \alpha(\omega), \beta(\zeta)) = \delta(\omega, \zeta) \cdot B(Z, W; \beta(\zeta), \alpha(\omega))$, so

$$\begin{aligned} |B(W, Z; \alpha, \beta)| &\leq 64^2 \cdot \max_{\omega, \zeta \bmod 8} |B(W, Z; \alpha(\omega), \beta(\zeta))| \\ &= 64^2 \cdot \max_{\omega, \zeta \bmod 8} |B(Z, W; \beta(\zeta), \alpha(\omega))| \\ &\ll 2^{40f} \Delta^{\frac{13}{12}} Z^{\frac{11}{12}} W \log Z \end{aligned} \tag{47}$$

whenever $W > Z$. Combining (46) and (47), we get the desired result. □

6.2. **From Proposition 8 Proposition 6.** We will now prove Proposition 6 from Proposition 8 by making appropriate choices for the sequences $\{\alpha_w\}$ and $\{\beta_z\}$. First recall the sum from Proposition 6. We defined

$$\mathcal{B}(M, N; f, \Delta) = \sum_{\substack{M < p \leq M + \Delta M \\ N < q \leq N + \Delta N}} \sum f(p, q; \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{e})$$

where $\boldsymbol{r} = (r_1, r_2) \in \{1, 9\} \times \{1, 9\}$, $r_1 r_2 \equiv 1 \bmod 16$ if $d = 8$, $\boldsymbol{s} = (s_1, s_2) \in \{\pm 1\} \times \{\pm 1\}$, $s_1 s_2 = 1$, $\boldsymbol{e} \in \mathbb{F}_2^2$, $\boldsymbol{e} \neq (0, 0)$, and

$$f(p, q; \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{e}) = \begin{cases} \chi_p(q)^{e_1} \varepsilon(p, q)^{e_2} & \text{if } (p, q) \equiv \boldsymbol{r} \bmod 16 \text{ and } (\chi_2(p), \chi_2(q)) = \boldsymbol{s} \\ 0 & \text{otherwise.} \end{cases}$$

For $w, z \in \mathbb{Z}[\sqrt{d_0}]$, we set

$$\begin{aligned} \alpha_{f,w} = \mathbf{1}(&w \text{ is a prime in } \mathbb{Z}[\sqrt{d_0}]) \cdot \mathbf{1}(\mathrm{N}(w) \equiv \delta_1 \bmod 16) \\ &\cdot \mathbf{1}(w \equiv \square \bmod 4\mathbb{Z}[\sqrt{d_0}]) \cdot \mathbf{1}(\chi_2(\mathrm{N}(w)) = s_1) \end{aligned}$$

and

$$\begin{aligned} \beta_{f,z} = \mathbf{1}(&z \text{ is a prime in } \mathbb{Z}[\sqrt{d_0}]) \cdot \mathbf{1}(\mathrm{N}(z) \equiv \delta_2 \bmod 16) \\ &\cdot \mathbf{1}(z \equiv \square \bmod 4\mathbb{Z}[\sqrt{d_0}]) \cdot \mathbf{1}(\chi_2(\mathrm{N}(z)) = s_2) \end{aligned}$$

Since there are exactly two primes in $\mathbb{Z}[\sqrt{d_0}]$ lying above each rational prime congruent to 1 modulo 8, we have, by (37), that

$$\mathcal{B}(M, N; f, \Delta) = \frac{1}{2g} \sideset{}{^*}\sum_{w \in \mathcal{R}_1(M)} \sideset{}{^*}\sum_{z \in \mathcal{R}_1(N)} \alpha_{f,w} \beta_{f,z} \left(\frac{\mathrm{N}(w)}{\mathrm{N}(z)}\right)^{e_1} (\mathrm{m}(w) \chi_w(\overline{z}))^{e_2},$$

where $g = 4$ if $d_0 = -1$, $g = 2$ if $d_0 = -2$, and $g = 1$ if $d_0 = 2$.

If $e_2 = 0$, then Proposition 6 is a statement about double oscillation of the usual Jacobi symbol $\left(\frac{p}{q}\right)$, and the claim follows from very strong bounds due to Heath-Brown (see [16]). If $e_2 = 1$, then we apply Proposition 8. Indeed, if $e_1 = 0$ and $e_2 = 1$, we can apply Proposition 8 directly to obtain the desired result (absorb $\mathrm{m}(w)$ into $\alpha_{f,w}$ and note that $\mathcal{R}_1(N)$ is invariant under $z \mapsto \overline{z}$). If $e_1 = 1$ and $e_2 = 1$, then by (36), we have

$$\left(\frac{\mathrm{N}(w)}{\mathrm{N}(z)}\right) \chi_w(\overline{z}) = \chi_w(z)$$

whenever (w) and (z) are degree-one primes in $\mathbb{Z}[\sqrt{d_0}]$ satisfying $\mathrm{N}(w) \equiv \mathrm{N}(z) \equiv 1 \bmod 8$. Once again, the desired result follows directly from Proposition 8 (again absorb $\mathrm{m}(w)$ into $\alpha_{f,w}$). This finishes the proof of Proposition 6.

References

[1] H. Cohen and H. W. Lenstra. Heuristics on class groups of number fields. In *Number Theory*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer-Verlag, New York, 1984.

[2] J. Corsman. *Redei symbols and governing fields*. ProQuest LLC, Ann Arbor, MI, 2007. Thesis (Ph.D.)–McMaster University (Canada).

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

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

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

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

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

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

[9] 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.

[10] F. Gerth, III. The 4-class ranks of quadratic fields. *Invent. Math.*, 77(3):489–515, 1984.

[11] F. Gerth, III. Extension of conjectures of Cohen and Lenstra. *Exposition. Math.*, 5(2):181–184, 1987.

[12] F. Gerth, III and S. W. Graham. Application of a character sum estimate to a 2-class number density. *J. Number Theory*, 19(2):239–247, 1984.

[13] L. J. Goldstein. A generalization of the Siegel-Walfisz theorem. *Trans. Amer. Math. Soc.*, 149:417–429, 1970.

[14] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. *Invent. Math.*, 111(1):171–195, 1993.

[15] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[16] D. R. Heath-Brown. A mean value estimate for real character sums. *Acta Arith.*, 72(3):235–275, 1995.

[17] H. Heilbronn. On the averages of some arithmetical functions of two variables. *Mathematika*, 5:1–7, 1958.

[18] J. Hoffstein and D. Ramakrishnan. Siegel zeros and cusp forms. *Internat. Math. Res. Notices*, (6):279–308, 1995.

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

[20] Peter Koymans and Djordjo Milovic. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \bmod 4$. *International Mathematics Research Notices*, page rny010, 2018.

[21] S. Lang. *Algebra*. Springer-Verlag, New York, 2002.

[22] D. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[23] D. Milovic. The infinitude of $\mathbb{Q}(\sqrt{-p})$ with class number divisible by 16. *Acta Arith.*, 178(3):201–233, 2017.

[24] 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.

[25] T. Miyake. *Modular forms*. Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.

[26] H. L. Montgomery and R. C. Vaughan. *Multiplicative Number Theory: I. Classical Theory*. Cambridge University Press, Cambridge, 2006.

[27] 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.

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

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

[30] P. Stevenhagen. Ray class groups and governing fields. *Publ. Math. Fac. Sci. Besançon*, 1989.
[31] P. Stevenhagen. Divisibility by 2-powers of certain quadratic class numbers. *J. Number Theory*, 43:1–19, 1993.

Appendix A. Heuristics

We briefly discuss the conjectural limit of the ratio in Theorem 1 and the limitations of our methods towards a proof of such a conjecture. Let G be a finite abelian group, and let $\#\mathrm{Aut}(G)$ be the number of automorphims of G. Cohen and Lenstra [1] developed a heuristic model for the average structure of class groups of quadratic number fields. Their model is based on the assumption that G occurs as the class group of an imaginary (resp. a real) quadratic field with probability proportional to the inverse of $\#\mathrm{Aut}(G)$ (resp. $\#G \cdot \#\mathrm{Aut}(G)$). Although they stated their model only for the prime-to-2 part of the class group, Gerth [11] extended the model to the 2-part of the class group by stating that it is $\mathrm{Cl}(D)^2$ instead of $\mathrm{Cl}(D)$ that behaves like a random group in the sense of [1].

Under these assumptions, we can compute a conjectural density for the ratio

$$\frac{\#\{pq \leq X : rk_4\mathrm{Cl}(dpq) = 2, \mathrm{rk}_8\mathrm{Cl}(dpq) \geq 1\}}{\#\{pq \leq X : \mathrm{rk}_4\mathrm{Cl}(dpq) = 2\}}$$

from the Main Theorem. Given that $\mathrm{rk}_4\mathrm{Cl}(D) = 2$, the 2-part of $\mathrm{Cl}(D)^2$ must be of the form $\mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ for some $n \geq m \geq 1$. In this notation $\mathrm{rk}_8\mathrm{Cl}(D) \geq 1$ precisely when $n \geq 2$. An elementary computation yields

$$\#\mathrm{Aut}(\mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}) = \begin{cases} 3 \cdot 2^{4m-3} & \text{if } m = n \\ 2^{3m+n-2} & \text{if } m < n. \end{cases}$$

Suppose now that $d = -4$, so that we're in the imaginary case. The total weight of all groups of the form $\mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ is

$$\sum_{m \geq 1} \frac{1}{3 \cdot 2^{4m-3}} + \sum_{m \geq 1} \sum_{n \geq m+1} \frac{1}{2^{3m+n-2}} = \frac{4}{9}.$$

The case when $\mathrm{rk}_8\mathrm{Cl}(D) = 0$, i.e. $m = n = 1$, has weight $1/6$. The probability of the complement is thus $(4/9 - 1/6)/(4/9) = 5/8$ and we are led to conjecture

Conjecture 1. *Let $d = -4$. Then*

$$\lim_{X \to \infty} \frac{\#\{pq \leq X : rk_4\mathrm{Cl}(dpq) = 2, \mathrm{rk}_8\mathrm{Cl}(dpq) \geq 1\}}{\#\{pq \leq X : \mathrm{rk}_4\mathrm{Cl}(dpq) = 2\}} = \frac{5}{8}$$

as $X \to \infty$.

Similarly, in the real case, when $d = 8$, the total weight is

$$\sum_{m \geq 1} \frac{1}{3 \cdot 2^{6m-3}} + \sum_{m \geq 1} \sum_{n \geq m+1} \frac{1}{2^{4m+2n-2}} = \frac{4}{63},$$

while the weight of the case $m = n = 1$ is $1/24$. The probability of the complement is then $(4/63 - 1/24)(4/63) = 11/32$, so that we conjecture

Conjecture 2. *Let $d = 8$. Then*

$$\lim_{X \to \infty} \frac{\#\{pq \leq X : rk_4\mathrm{Cl}(dpq) = 2, \mathrm{rk}_8\mathrm{Cl}(dpq) \geq 1\}}{\#\{pq \leq X : \mathrm{rk}_4\mathrm{Cl}(dpq) = 2\}} = \frac{11}{32}$$

as $X \to \infty$.

Both Conjectures 1 and 2 closely match numerical data generated in Sage.

There is another way to obtain the same conjectures that more closely matches our strategy of proof of Theorem 1. For the sake of simplicity, we focus on the

case $d = -4$. As we saw in Proposition 3, the existence of an unramified a.f.p. C_8-extension of $\mathbb{Q}(\sqrt{-4pq})$ containing $\mathbb{Q}(\sqrt{-4}, \sqrt{pq})$ is contingent upon two events. The first is

Event A: condition (17) holds, the splitting condition at 2,

and the second is

Event B: condition (10) holds, the splitting condition at p.

We already saw in (12) that the splitting condition at q is automatically satisfied if it is satisfied at p. Both Events A and B are determined by the values of certain quadratic residue symbols depending on p and q. Assuming these symbols take values $+1$ and -1 equally often and independently of each other, the probability that both Events A and B occur is $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. This is exactly how we prove Theorem 2.

When $\mathrm{rk}_4\mathrm{Cl}(-4pq) = 2$, there also exists an unramified a.f.p. C_4-extension L' (resp. L'') of $\mathbb{Q}(\sqrt{-4pq})$ that contains $\mathbb{Q}(\sqrt{-4p}, \sqrt{q})$ (resp. $\mathbb{Q}(\sqrt{p}, \sqrt{-4q})$). For L' (resp. L'')to be contained in an unramified a.f.p. C_8-extension of $\mathbb{Q}(\sqrt{-4pq})$, there are again two events that must occur. One of them once again concerns the splitting condition at 2, say Event A' (resp. Event A''). The other event, say Event B' (resp. B''), concerns the splitting condition at q (resp. p). We can once again expect Events A', A'', B', and B'' to be determined by values of certain quadratic residue symbols, except this time in $\mathbb{Z}[\sqrt{-4p}]$ or $\mathbb{Z}[\sqrt{-4q}]$. And we can again conjecture that each of there symbols takes the values $+1$ and -1 equally often. However, these events are *not* independent. If both $\mathbb{Q}(\sqrt{-4}, \sqrt{pq})$ and $\mathbb{Q}(\sqrt{-4p}, \sqrt{q})$ are contained in (distinct) unramified a.f.p. C_8-extensions of $\mathbb{Q}(\sqrt{-4pq})$, then so is $\mathbb{Q}(\sqrt{p}, \sqrt{-4q})$. One can check that out of the events A, A', and A'', either exactly one or all three events occur, and similarly for B, B', and B''. Hence, using the principle of inclusion-exclusion, we may conjecture that $\mathrm{rk}_8\mathrm{Cl}(D)$ is at least 1 with probability

$$\mathbb{P}(A\&B) + \mathbb{P}(A'\&B') + \mathbb{P}(A''\&B'') - 2\mathbb{P}(A\&A'\&A''\&B\&B'\&B'') = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} - 2 \cdot \frac{1}{16} = \frac{5}{8}.$$

Thus the discrepancy between our lower bound of $1/4$ from the Main Theorem and the conjectural limit $5/8$ comes from not taking into account unramified a.f.p. C_8-extensions of $\mathbb{Q}(\sqrt{-4pq})$ containing $\mathbb{Q}(\sqrt{-4p}, \sqrt{q})$ or $\mathbb{Q}(\sqrt{p}, \sqrt{-4q})$.

The main obstacle in extending the ideas of this paper to handle Events B' and B'' is that $\mathbb{Z}[\sqrt{-4p}]$ and $\mathbb{Z}[\sqrt{-4q}]$ are no longer principal ideal domains, and in fact $\mathrm{Cl}(-4p)$ or $\mathrm{Cl}(-4q)$ (or both) may have non-trivial odd torsion. Thus it is difficult to control (in a uniform way as p and q vary) the size of the analogues of α from (7), and a genuinely new idea would be required to apply similar analytic techniques. Theorem 2 already achieves a new lower bound for the 8-rank, so we leave the task of sharpening this lower bound for a future project.

University College London, London WC1E 6BT, United Kingdom