COMPOSITIO MATHEMATICA

Spins of prime ideals and the negative Pell equation $x^2 - 2py^2 = -1$

P. Koymans and D. Z. Milovic

Compositio Math. **155** (2019), 100–125.

doi:10.1112/S0010437X18007601

Compositio Math. 155 (2019) 100–125
doi:10.1112/S0010437X18007601

Spins of prime ideals and the negative Pell equation $x^2 - 2py^2 = -1$

P. Koymans and D. Z. Milovic

Abstract

Let $p \equiv 1 \bmod 4$ be a prime number. We use a number field variant of Vinogradov's method to prove density results about the following four arithmetic invariants: (i) 16-rank of the class group $\mathrm{Cl}(-4p)$ of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-4p})$; (ii) 8-rank of the ordinary class group $\mathrm{Cl}(8p)$ of the real quadratic field $\mathbb{Q}(\sqrt{8p})$; (iii) the solvability of the negative Pell equation $x^2 - 2py^2 = -1$ over the integers; (iv) 2-part of the Tate–Šafarevič group $Ш(E_p)$ of the congruent number elliptic curve $E_p : y^2 = x^3 - p^2x$. Our results are conditional on a standard conjecture about short character sums.

1. Introduction

In [FIMR13], Friedlander, Iwaniec, Mazur, and Rubin associated a quantity $\mathrm{spin}(\mathfrak{a}) \in \{0, \pm 1\}$ to each principal ideal $\mathfrak{a}$ in the ring of integers of a totally real number field K of degree $n \geqslant 3$ with a *cyclic* Galois group over $\mathbb{Q}$. Assuming a standard conjecture about short character sums, they proved that $\mathrm{spin}(\mathfrak{p})$ oscillates as $\mathfrak{p}$ varies over principal prime ideals. The conjecture is unconditional in the low-degree case when $n = 3$, and precisely in this setting their result has arithmetic applications to the distribution of 2-Selmer groups of quadratic twists of certain elliptic curves.

In this paper, we will associate a similar 'spin' to ideals in the ring of integers $\mathcal{O}_M$ of the totally complex number field

$$M = \mathbb{Q}(\zeta_8, \sqrt{1+i}),$$

where ζ_8 is a primitive 8th root of unity and $i = \zeta_8^2$. The essential part of our spin will come from symbols of the type

$$[\alpha]_r = \left(\frac{r(\alpha)}{\alpha}\right), \tag{1.1}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the quadratic residue symbol in M and $r \in \mathrm{Gal}(M/\mathbb{Q})$ is a fixed automorphism of order 4. Following the basic strategy of [FIMR13], we will also prove that the spin of prime ideals in $\mathcal{O}_M$ oscillates. Unfortunately, the field M is of degree 8 over $\mathbb{Q}$, and we are forced to assume the $n = 8$ case of [FIMR13, Conjecture C_n, p. 738]. Our result has applications to the arithmetic statistics of: (i) the 16-rank of the class group of $\mathbb{Q}(\sqrt{-p})$, (ii) the 8-rank of the *ordinary* class group of the *real* quadratic field $\mathbb{Q}(\sqrt{2p})$, (iii) the negative Pell equation $x^2 - 2py^2 = -1$, and (iv) the congruent number elliptic curve $y^2 = x^3 - p^2x$.

Received 9 February 2018, accepted in final form 21 September 2018, published online 23 November 2018.
2010 Mathematics Subject Classification 11R29, 11R45, 11N45, 11P21 (primary).
Keywords: class groups, negative Pell equation, sieve theory.
The second author is supported by ERC grant agreement No. 670239.

There are two main innovations that separate the present work from [FIMR13]. First, we have the aforementioned arithmetic applications. Second, the Galois group of $M/\mathbb{Q}$ is dihedral of order 8, and hence is not cyclic, and this seemingly technical difference causes the original arguments in [FIMR13] to break down. Fortunately, a lattice point counting argument offers a fix, which also substantially simplifies the proof in [FIMR13].

Before stating our main results, we define the aforementioned spin $s_{\mathfrak{a}}$ of non-zero ideals $\mathfrak{a} \subset \mathcal{O}_M$. One can check that $M/\mathbb{Q}$ is a totally complex dihedral extension of degree 8, that $\mathcal{O}_M$ is a principal ideal domain, and that ζ_8 generates the torsion subgroup of the unit group $\mathcal{O}_M^\times$. We fix a subgroup $V \leqslant \mathcal{O}_M^\times$ of rank 3 such that $\mathcal{O}_M^\times = \langle \zeta_8 \rangle \times V$ and fix a set of coset representatives $\mu_1, \dots, \mu_8$ for V^2 in V. We define a rational integer F as in (3.1); although F is an absolute constant, it is far too large to write out its decimal expansion. Suppose that

$$\psi : (\mathcal{O}_M/F\mathcal{O}_M)^\times \to \mathbb{C} \tag{1.2}$$

is a map such that $\psi(\alpha \bmod F) = \psi(\alpha\beta^2 \bmod F)$ for all $\alpha \in \mathcal{O}_M$ coprime to F and all $\beta \in \mathcal{O}_M^\times$. Fix once and for all an element of order 4 in $\mathrm{Gal}(M/\mathbb{Q})$, denote it by r, and define $[\cdot]_r$ as in (1.1). Finally, let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_M$. If $(\mathfrak{a}, F) \neq 1$, define $s_{\mathfrak{a}} = 0$. Otherwise, choose any generator α for $\mathfrak{a}$ and define

$$s_{\mathfrak{a}} = \frac{1}{64} \sum_{i=1}^{8} \sum_{j=1}^{8} \psi(\mu_i \zeta_8^j \alpha \bmod F) \cdot [\mu_i \zeta_8^j \alpha]_r. \tag{1.3}$$

The right-hand side above is independent of the choice of a generator α for $\mathfrak{a}$, as can be seen from (6.7) with $\sigma = r$. Compare the definition of $s_{\mathfrak{a}}$ with the definition of spin($\mathfrak{a}$) in [FIMR13, (3.4), p. 706]. The most important difference is that r does *not* generate the Galois group $\mathrm{Gal}(M/\mathbb{Q})$, whereas in [FIMR13], the automorphism σ does generate $\mathrm{Gal}(K/\mathbb{Q})$. An application of the geometry of numbers bridges this gap while simplifying the proof of Friedlander *et al.* [FIMR13, pp. 731–733]. Another difference is the extra averaging over generators of $\mathfrak{a}$ in the definition of $s_{\mathfrak{a}}$ above, necessary because, unlike in [FIMR13], we cannot make simplifying assumptions about the field over which we work.

We now state our main theorem and its consequences, all conditional on Conjecture 1, a standard conjecture about short character sums whose statement we postpone until § 3.3.

Theorem 1. *Assume that Conjecture 1 holds with $\delta > 0$. Then there is a constant $\delta' > 0$ depending only on δ such that for all $X > 1$, we have*

$$\sum_{\mathrm{N}(\mathfrak{p}) \leqslant X} s_{\mathfrak{p}} \ll X^{1-\delta'},$$

where the sum is taken over prime ideals $\mathfrak{p} \subset \mathcal{O}_M$ of norm at most X and the implied constant depends only on ψ. Moreover, one can take $\delta' = \delta/400$.

Let $\mathrm{Cl}(D)$, $\mathrm{Cl}^+(D)$, $h(D)$, and $h^+(D)$ denote the class group, the narrow class group, the class number, and the narrow class number, respectively, of the quadratic field of discriminant D. For a finite abelian group G and an integer $k \geqslant 1$, we define the 2^k-rank of G to be $\mathrm{rk}_{2^k} G = \dim_{\mathbb{F}_2}(2^{k-1}G/2^kG)$. A lot is known about the 8-rank of $\mathrm{Cl}^+(dp)$ for d fixed and p varying among the prime numbers (see [Ste89] and [Smi16]). We will prove some long-standing conjectures about the 16-rank of $\mathrm{Cl}(-4p)$ and the 8-rank of $\mathrm{Cl}(8p)$ (see for instance [CL84] and in particular their density conjecture $D_j(d)$ on p. 263).

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

Theorem 2. *Assume that Conjecture 1 holds with $\delta > 0$ and let δ' be as in Theorem 1. Let $r \in \{0, 8\}$. For all $X \geqslant 41$, we have*

$$\frac{\#\{p \leqslant X : h(-4p) \equiv r \bmod 16\}}{\#\{p \leqslant X : h(-4p) \equiv 0 \bmod 8\}} = \frac{1}{2} + O(X^{-\delta'}),$$

where the implied constant is absolute.

Theorem 3. *Assume that Conjecture 1 holds with $\delta > 0$ and let δ' be as in Theorem 1. Let $r \in \{0, 4\}$. Then for all $X \geqslant 113$, we have*

$$\frac{\#\{p \leqslant X : p \equiv 1 \bmod 4, h(8p) \equiv r \bmod 8\}}{\#\{p \leqslant X : p \equiv 1 \bmod 4, h^+(8p) \equiv 0 \bmod 8\}} = \frac{1}{2} + O(X^{-\delta'}),$$

where the implied constant is absolute.

Density results about the 2-parts of the narrow and ordinary class groups of $\mathbb{Q}(\sqrt{8p})$ have implications for the arithmetic statistics of the solvability of the negative Pell equation

$$x^2 - 2py^2 = -1, \tag{1.4}$$

with $x, y \in \mathbb{Z}$. For each $X \geqslant 3$, let

$$\delta^-(X) = \frac{\#\{p \text{ prime} : p \leqslant X, (1.4) \text{ is solvable over } \mathbb{Z}\}}{\#\{p \text{ prime} : p \leqslant X\}}.$$

Stevenhagen conjectured in [Ste93b] that $\lim_{X\to\infty} \delta^-(X)$ exists and is equal to $1/3$. We prove the following theorem.

Theorem 4. *Assume that Conjecture 1 holds. Let $\delta^-(X)$ be defined as above. Then*

$$\frac{5}{16} \leqslant \liminf_{X\to\infty} \delta^-(X) \leqslant \limsup_{X\to\infty} \delta^-(X) \leqslant \frac{11}{32}.$$

In particular, $|\delta^-(X) - 1/3| \leqslant 1/48 + o(X)$ as $X \to \infty$, so the bounds above are within 2.08% of Stevenhagen's conjecture.

Finally, we state an application of Theorem 1 to the distribution of the Tate–Šafarevič groups $Ш(E_p)$ of the congruent number elliptic curves

$$E_p : y^2 = x^3 - p^2 x.$$

Theorem 5. *Assume that Conjecture 1 holds. Then*

$$\liminf_{X\to\infty} \frac{\#\{p \leqslant X : (\mathbb{Z}/4\mathbb{Z})^2 \hookrightarrow Ш(E_p)\}}{\#\{p \leqslant X\}} \geqslant \frac{1}{16}.$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

2. Discussion of results

2.1 16-rank of class groups

Aside from two recent results due to the authors [Mil17b, KM18], density results about the 16-rank of class groups in one-prime-parameter families $\{\mathbb{Q}(\sqrt{dp})\}_p$ (d fixed and p varying) have remained elusive despite a large body of work on algebraic criteria for the 16-rank in such families [Kap77, Ori78, KW82, LW82, KW84, Yam84, KWH86, Ste93a, BH13]. This gap between algebraic and analytic understanding of the 16-rank can be largely attributed to the absence of appropriate governing fields and the subsequent inability to apply the Čebotarev density theorem. More precisely, for a finite extension of number fields E/F, let $\mathrm{Art}_{E/F}$ denote the corresponding Artin map. Cohn and Lagarias [CL83, CL84] conjectured that, for each integer $k \geqslant 1$ and each integer $d \not\equiv 2 \bmod 4$, the map

$$f_{d,k} : p \mapsto \mathrm{rk}_{2^k}\mathrm{Cl}^+(dp)$$

is *Frobenian*, in the sense of Serre [Ser12]. In other words, they conjectured that there exists a normal field extension $M_{d,k}/\mathbb{Q}$ for which there is a class function

$$\phi : \mathrm{Gal}(M_{d,k}/\mathbb{Q}) \to \mathbb{Z}_{\geqslant 0},$$

satisfying

$$f_{d,k}(p) = \phi(\mathrm{Art}_{M_{d,k}/\mathbb{Q}}(p))$$

for all primes p unramified in $M_{d,k}/\mathbb{Q}$; such a field $M_{d,k}$ is called a *governing field* for $\{\mathrm{rk}_{2^k}\mathrm{Cl}^+(dp)\}_p$. For $k \leqslant 3$, Stevenhagen [Ste89] proved these conjectures for all $d \not\equiv 2 \bmod 4$. Perhaps the simplest case is $d = -4$, where one can take $M_{-4,3}$ to be the field $M = \mathbb{Q}(\zeta_8, \sqrt{1+i})$ as above and where $h(-4p) \equiv 0 \bmod 8$ if and only if p splits completely in M. Hence, by the Čebotarev density theorem, the density of primes p such that $h(-4p) \equiv 0 \bmod 8$ is equal to $1/[M : \mathbb{Q}] = 1/8$.

Cohn and Lagarias [CL84] ruled out some obvious candidates for $M_{-4,4}$, i.e., the governing field for the 16-rank of $\mathrm{Cl}(-4p)$, and to this day no governing fields for the 16-rank in *any* family have been found. Nevertheless, we are able to show, in Theorem 2, that the density of primes p such that $h(-4p) \equiv 0 \bmod 16$ exists and is equal to $1/16$. It is proved unconditionally in [Mil17a] that there are infinitely many primes p such that $h(-4p) \equiv 0 \bmod 16$, but that result implies nothing about the density as in Theorem 1.

The key innovation that allows us to go beyond the 8-rank is to use Vinogradov's method [Vin47, Vin54] for studying the distribution of prime numbers instead of the heretofore used Čebotarev density theorem (as in [Smi16], for instance). Moreover, the current state-of-the-art bounds for the error term in the Čebotarev density theorem are essentially of size $X\exp(-\sqrt{\log X})$, far worse than the power-saving bound $X^{1-\delta'}$ in Theorem 2. In fact, obtaining such a power-saving error term in the Čebotarev density theorem would be tantamount to proving a zero-free region for the associated Artin L-functions of the form $\Re(s) > 1 - \delta'$, and this is well out of reach of current methods in analytic number theory. Nonetheless, the power-saving bound $X^{1-\delta'}$ does *not* prove the non-existence of a governing field – it merely suggests that one is unlikely to exist. We summarize this discussion with the following immediate corollary of Theorem 2.

Corollary 6. *Assume Conjecture 1 with $\delta > 0$, and let δ' be as in Theorem 1. At least one of the following two statements is true:*

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

– *a governing field for* $\mathrm{rk}_{16}\mathrm{Cl}(-4p)$ *does* not *exist;*
– *there exists a normal extension* $L/\mathbb{Q}$ *and two distinct unions of conjugacy classes in* $\mathrm{Gal}(L/\mathbb{Q})$*, say* S_1 *and* S_2*, such that for all* $X > 0$*, we have*

$$\#\{p \leqslant X : (p, L/\mathbb{Q}) \subset S_1\} - \#\{p \leqslant X : (p, L/\mathbb{Q}) \subset S_2\} \ll X^{1-\delta'},$$

where the implied constant is absolute. Here $(p, L/\mathbb{Q})$ *denotes the Artin conjugacy class of* p *in* $\mathrm{Gal}(L/\mathbb{Q})$.

2.2 Real quadratic fields and the negative Pell equation

In the case $d < 0$, the narrow class group $\mathrm{Cl}^+(dp)$ is the same as the ordinary class group $\mathrm{Cl}(dp)$. If $d > 0$, however, then $\mathrm{Cl}^+(dp)$ and $\mathrm{Cl}(dp)$ may be different; in fact, $\mathrm{Cl}^+(dp) = \mathrm{Cl}(dp)$ if and only if the fundamental unit ε_{dp} of $\mathbb{Q}(\sqrt{dp})$ has norm -1. While Cohn and Lagarias stated their conjecture on the existence of governing fields only for narrow class groups, one can ask what happens for ordinary class groups. As mentioned before, Stevenhagen proved the conjecture of Cohn and Lagarias for the 8-rank of narrow class groups of both imaginary and real quadratic fields. Theorem 3 is the first density result for the 8-rank of the *ordinary* class group in a family of *real* quadratic fields. Again the power-saving error term suggests that there is no governing field for $\mathrm{rk}_8\mathrm{Cl}(8p)$ in the family $\{\mathrm{Cl}(8p)\}_{p\equiv 1 \bmod 4}$. To place Theorem 3 in context, we note that the 2-part of $\mathrm{Cl}^+(8p)$ is cyclic, and, for $p \equiv 1 \bmod 4$, one has (for instance, see [Ste93a]):

– $h^+(8p) = h(8p) \equiv 2 \bmod 4 \Leftrightarrow p$ splits completely in $\mathbb{Q}(i)$ but not in $\mathbb{Q}(\zeta_8)$;
– $h^+(8p) \equiv h(8p) + 2 \equiv 0 \bmod 4 \Leftrightarrow p$ splits completely in $\mathbb{Q}(\zeta_8)$ but not in $\mathbb{Q}(\zeta_8, \sqrt[4]{2})$;
– $h^+(8p) = h(8p) \equiv 4 \bmod 8 \Leftrightarrow p$ splits completely in $\mathbb{Q}(\zeta_8, \sqrt[4]{2})$ but not in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$;
– $h^+(8p) \equiv 0 \bmod 8 \Leftrightarrow p$ splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$.

Hence, Theorem 3 in conjunction with the Čebotarev density theorem implies that

$$\lim_{X\to\infty} \frac{\#\{p \text{ prime} : p \leqslant X, p \equiv 1 \bmod 4, h(8p) \equiv 4 \bmod 8\}}{\#\{p \text{ prime} : p \leqslant X, p \equiv 1 \bmod 4\}} = \frac{3}{16}$$

and

$$\lim_{X\to\infty} \frac{\#\{p \text{ prime} : p \leqslant X, p \equiv 1 \bmod 4, h(8p) \equiv 0 \bmod 8\}}{\#\{p \text{ prime} : p \leqslant X, p \equiv 1 \bmod 4\}} = \frac{1}{16}.$$

The 2-torsion subgroup $\mathrm{Cl}^+(8p)[2]$ is generated by the classes of the ramified ideals $\mathfrak{t}$ and $\mathfrak{p}$ lying above 2 and p, respectively. Since the 2-part of $\mathrm{Cl}^+(8p)$ is cyclic, we have $\#\mathrm{Cl}^+(8p)[2] = 2$, so exactly one of the three ideals $\mathfrak{t}$, $\mathfrak{p}$, and $\mathfrak{tp}$ is in the trivial class in $\mathrm{Cl}^+(8p)$, while the remaining two are both in the non-trivial class in $\mathrm{Cl}^+(8p)[2]$. Moreover, (1.4) has a solution over the integers if and only if $\mathbb{Z}[\sqrt{2p}]$ has a unit of norm -1, which occurs if and only if the ideal $\mathfrak{tp} = (\sqrt{2p})$ can be generated by a totally positive element in $\mathbb{Z}[\sqrt{2p}]$, i.e., if and only if $\mathfrak{tp}$ is in the trivial class in $\mathrm{Cl}^+(8p)$. Stevenhagen conjectured in [Ste93b] that as p varies over all prime numbers, each of $\mathfrak{t}$, $\mathfrak{p}$, and $\mathfrak{tp}$ is in the trivial class in $\mathrm{Cl}^+(8p)$ equally often, which is why we expect $\lim_{X\to\infty} \delta^-(X)$ to exist and be equal to $1/3$ ($\delta^-(X)$ is defined following (1.4)).

Since $\mathbb{Z}[\sqrt{2p}]$ has a unit of norm -1 if and only if the narrow class group $\mathrm{Cl}^+(8p)$ coincides with the ordinary class group $\mathrm{Cl}(8p)$, we can obtain successively better upper and lower bounds for the proportion of primes p for which (1.4) is solvable over $\mathbb{Z}$ by comparing $h^+(8p)$ and $h(8p)$ modulo successively higher powers of 2. Note that (1.4) has no solutions (even over $\mathbb{Q}$) whenever

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

$p \equiv 3 \bmod 4$, since in that case -1 is not a quadratic residue modulo p. From this, the list of splitting criteria above, and the Čebotarev density theorem, one immediately deduces that

$$\frac{5}{16} \leqslant \liminf_{X\to\infty} \delta^-(X) \leqslant \limsup_{X\to\infty} \delta^-(X) \leqslant \frac{3}{8}. \tag{2.1}$$

Hence $|\delta^-(X) - 1/3| \leqslant 1/24 + o(X)$ as $X \to \infty$, i.e., at worst, the bounds above are within 4.17% of Stevenhagen's conjecture. Theorem 4 hence cuts the possible discrepancy from Stevenhagen's conjecture in half. Although the problem of improving (2.1) may have been first explicitly stated in 1993 in [Ste93b, p. 127], in essence it has been open since the 1930s, when Rédei [Red34], Reichardt [Rei34], and Scholz [Sch35] supplied the algebraic criteria sufficient to deduce (2.1).

2.3 Other results on 2-parts of class groups of number fields

Finally, we would like to contrast our results concerning one-prime-parameter families with results on 2-parts of class groups in families parametrized by arbitrarily many primes. The first significant achievement for families with arbitrary discriminants was made by Fouvry and Klüners [FK07], who translated Rédei's theory on 4-ranks of class groups to sums of characters conducive to analytic techniques and then successfully dealt with these sums, basing some of their work on the techniques developed by Heath-Brown in [Hea93, Hea94]. Fouvry and Klüners subsequently developed their methods in various settings [FK10a, FK10b, FK10c, FK11], most notably obtaining impressive upper and lower bounds for the solvability of the negative Pell equation $x^2 - dy^2 = -1$ for general squarefree integers $d > 0$. When specialized to the one-prime-parameter family $d = 2p$ with p prime, their results are as strong as the bounds in (2.1), so Theorem 4 can be viewed as the next natural step in the line of work initiated by Fouvry and Klüners.

A recent paper of Smith [Smi17] (see also [Smi16]) features ground-breaking distribution theorems about 2^k-ranks of class groups of imaginary quadratic fields for *all* $k \geqslant 3$. The very deep methods that underlie these theorems require the number of prime parameters on average to go to infinity and hence are unlikely to yield results in the direction of Theorems 2, 3, or 4; from the standpoint of analytic number theory, Theorem 2 is a result about the distribution of prime numbers, while the main analytic techniques underlying the results of [Smi17] are consequences of a very careful study of the anatomy of the prime divisors of highly composite integers.

3. Preliminaries

3.1 The governing field for the 8-rank of Cl$(-4p)$

As in § 1, let $M = \mathbb{Q}(\zeta_8, \sqrt{1+i})$ be the (minimal) governing field for the 8-rank in the family $\{\mathbb{Q}(\sqrt{-4p})\}_{p\equiv 1 \bmod 4}$. Using a computer algebra package such as Sage, one can readily check that:

(P1) the ring of integers of every subfield of M (including M itself) is a principal ideal domain;

(P2) the discriminant Δ_M of $M/\mathbb{Q}$ is equal to 2^{22}, and 2 is totally ramified in $M/\mathbb{Q}$; and

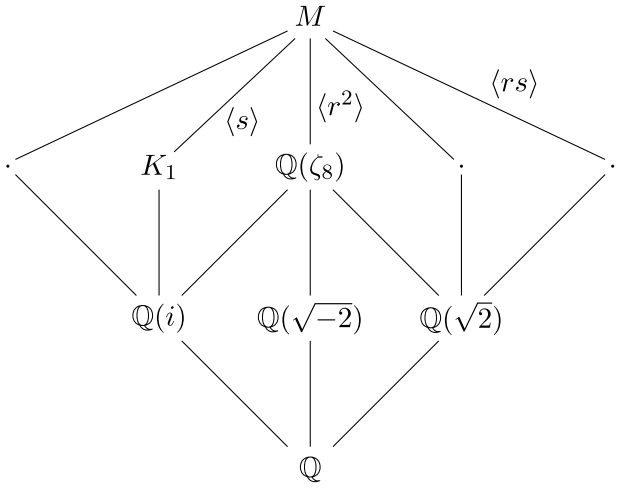
(P3) the torsion subgroup of the group of units in $\mathcal{O}_M$ is $\langle \zeta_8 \rangle$.

Recall that $\mathrm{rk}_8\mathrm{Cl}(-4p) = 1$ if and only if p splits completely in $M/\mathbb{Q}$, that is, if and only if p is odd and every prime ideal $\mathfrak{p}$ in $\mathcal{O}_M$ lying over p is of degree 1.

As noted in § 1, $M/\mathbb{Q}$ is a normal extension with Galois group isomorphic to the dihedral group D_8 of order 8. We fix an automorphism $r \in \mathrm{Gal}(M/\mathbb{Q})$ such that r generates the order 4 subgroup $\mathrm{Gal}(M/\mathbb{Q}(\sqrt{-2}))$, and we let $s \in \mathrm{Gal}(M/\mathbb{Q})$ be the non-trivial automorphism fixing the subfield $K_1 = \mathbb{Q}(i, \sqrt{1+i})$. Then $D_8 \cong \mathrm{Gal}(M/\mathbb{Q}) \cong \langle r, s \rangle$, with r of order 4, s of order 2,

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

and $sr = r^3 s$. Hereinafter, we refer to the following field diagram.



By the Čebotarëv density theorem, for each $\rho \in (\mathcal{O}_M/(\Delta_M))^\times$, we can choose an inverse $\rho' \in \mathcal{O}_M$ such that $\rho'\mathcal{O}_M$ is a prime of degree one. Fix a set of such ρ' and call it $\mathcal{R}$. Define F to be the rational integer

$$F = \Delta_M \cdot \prod_{\rho \in (\mathcal{O}_M/(\Delta_M))^\times} \mathrm{N}_{M/\mathbb{Q}}(\rho'). \tag{3.1}$$

This is not really analogous to F on [FIMR13, p. 723], but we denote it by the same letter because it will play an analogous role later on in the estimation of certain congruence sums.

3.2 Quadratic reciprocity

Let L be a number field and let $\mathcal{O}_L$ be its ring of integers. We say that an ideal $\mathfrak{a}$ in $\mathcal{O}_L$ is *odd* if $\mathrm{N}(\mathfrak{a})$ is odd; similarly, an element α in $\mathcal{O}_L$ is called *odd* if the principal ideal generated by α is odd. If $\mathfrak{p}$ is an odd prime ideal in $\mathcal{O}_L$, and α is an element in $\mathcal{O}_L$, then one defines

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_L = \begin{cases} 0 & \text{if } \alpha \in \mathfrak{p}, \\ 1 & \text{if } \alpha \notin \mathfrak{p} \text{ and } \alpha \text{ is a square modulo } \mathfrak{p}, \\ -1 & \text{otherwise.} \end{cases}$$

If $\mathfrak{b}$ is an odd ideal in $\mathcal{O}_L$, one defines

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_L = \prod_{\mathfrak{p}^{k_\mathfrak{p}} \| \mathfrak{b}} \left(\frac{\alpha}{\mathfrak{p}}\right)_L^{k_\mathfrak{p}}.$$

If $\alpha, \beta \in \mathcal{O}_L$ with β odd, we define

$$\left(\frac{\alpha}{\beta}\right)_L = \left(\frac{\alpha}{\beta\mathcal{O}_L}\right)_L.$$

A weak (but sufficient to us) version of the law of quadratic reciprocity for number fields can be stated as follows (see for instance [FIMR13, Lemma 2.1, p. 703]).

Lemma 3.1. *Suppose L is a totally complex number field, and let $\alpha, \beta \in \mathcal{O}_L$ be odd. Then*

$$\left(\frac{\alpha}{\beta}\right)_L = \varepsilon \cdot \left(\frac{\beta}{\alpha}\right)_L,$$

where $\varepsilon \in \{\pm 1\}$ depends only on the congruence classes of α and β modulo $8\mathcal{O}_L$. □

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

When α is not odd, the following supplement to the law of quadratic reciprocity will suffice for our purposes (see [FIMR13, Proposition 2.2, p. 703]).

Lemma 3.2. *Let L be a totally complex number field, and let $\alpha \in \mathcal{O}_L$ be non-zero. Then $\left(\frac{\alpha}{\beta}\right)_L$ depends only on the congruence class of β modulo $8\alpha\mathcal{O}_L$.* □

3.3 Short character sums

Here we state the conjecture that we assume in the proof of Theorem 1. It stipulates power-savings in short character (modulo q) sums of length $q^{1/8}$ and is essentially the same as the case $n = 8$ of Conjecture C_n in [FIMR13, p. 738].

Conjecture 1. There exist absolute constants $\delta > 0$ and $C > 0$ such that if χ is a non-principal real-valued Dirichlet character modulo a squarefree integer $q > 2$ and $N < q^{1/8}$, then

$$\left| \sum_{M \leqslant n \leqslant M+N} \chi(n) \right| \leqslant C q^{1/8-\delta}$$

for all integers M.

We feel that Conjecture 1 is of a genuinely different nature than the arithmetic applications that follow. It is the oscillation of spins over the set of *prime* ideals that yields the various arithmetic applications. In the sieving methods we use, proving oscillation of spins over prime ideals requires us to first prove oscillation over the set of *all* ideals. There we encounter character sums in the number field M that one wishes to relate to character sums in $\mathbb{Q}$, where oscillation of character sums is better understood. In passing from M to $\mathbb{Q}$, one suffers from the fact that, in some fixed integral basis for $\mathcal{O}_M$, a nicely chosen element of norm X generally has coordinates of size $X^{1/8}$. Conductors of characters in question have size similar to the norm, while the length of character sums in question is essentially limited by the size of the coordinates. We also remark that thanks to the work of Burgess [Bur62, Bur63], Conjecture 1 is known to be true when $1/8$ is replaced with any real number $\theta > 1/4$, in which case the exponent δ and the constant C depend on θ.

Instead of directly appealing to Conjecture 1, we will instead need a corollary of Conjecture 1 for arithmetic progressions. For q odd and squarefree, let χ_q be the real Dirichlet character $\left(\frac{\cdot}{q}\right)$. Following [FIMR15, 7, pp. 924–925] we will prove the following corollary.

Corollary 7. *Assume Conjecture 1. Then there exist absolute constants $\delta > 0$ and $C > 0$ such that for all odd squarefree integers $q > 1$, all integers $N < q^{1/8}$, all integers M, l, and k satisfying $q \nmid k$ we have*

$$\left| \sum_{\substack{M \leqslant n \leqslant M+N \\ n \equiv l \bmod k}} \chi_q(n) \right| \leqslant C q^{1/8-\delta}.$$

Proof. Write $n = km + l$. Then we have

$$\chi_q(n) = \chi_{(q,k)}(l)\chi_{q/(q,k)}(k)\chi_{q/(q,k)}(m + r),$$

where r satisfies $kr \equiv l \bmod q/(q,k)$. It follows that

$$\left| \sum_{\substack{M \leqslant n \leqslant M+N \\ n \equiv l \bmod k}} \chi_q(n) \right| \leqslant \left| \sum_{M' \leqslant m \leqslant M' + (N/k)} \chi_{q/(q,k)}(m) \right|,$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

where $M' = (M-l)k^{-1} + r$. By our assumption $q \nmid k$, we see that $q/(q,k)$ is an odd squarefree integer greater than one. Hence $\chi_{q/(q,k)}$ is a non-principal real-valued Dirichlet character. Now apply Conjecture 1. □

3.4 Vinogradov's method, after Friedlander, Iwaniec, Mazur, and Rubin

Vinogradov's method [Vin47, Vin54] has been substantially simplified by Vaughan [Vau77], and Friedlander *et al.* [FIMR13, § 5, pp. 717–722] gave a nice generalization to number fields. Morally speaking, power-saving estimates in sums over primes follow from power-saving estimates in linear congruence sums (sums of type I) and general bilinear sums (sums of type II). Precisely, by [FIMR13, Proposition 5.2, p. 722] with $\vartheta = \delta/4$ and $\theta = 1/48$, Theorem 1 is a direct consequence of the following two propositions.

Proposition 3.3. *Assume Conjecture 1 holds with $\delta > 0$. Then for all $\epsilon > 0$, we have*

$$\sum_{\mathrm{N}(\mathfrak{a}) \leqslant x,\ \mathfrak{m} \mid \mathfrak{a}} s_{\mathfrak{a}} \ll_{\epsilon} x^{1-\delta/4+\epsilon}$$

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

Proposition 3.4. *For each $\epsilon > 0$, there exists a constant $c_{\epsilon} > 0$ such that*

$$\sum_{\mathrm{N}(\mathfrak{a}) \leqslant M} \sum_{\mathrm{N}(\mathfrak{b}) \leqslant N} v_{\mathfrak{a}} w_{\mathfrak{b}} s_{\mathfrak{a}\mathfrak{b}} \ll_{\epsilon} (M+N)^{1/48} (MN)^{47/48+\epsilon}$$

uniformly for all $M, N \geqslant 2$ and all sequences of complex numbers $\{v_{\mathfrak{a}}\}$ and $\{w_{\mathfrak{b}}\}$ satisfying $|v_{\mathfrak{a}}|, |w_{\mathfrak{a}}| \leqslant c_{\epsilon} \mathrm{N}(\mathfrak{a})^{\epsilon}$.

Note that Proposition 3.4 is *unconditional* – it is only for the sums of type I featuring in Proposition 3.3 that we have to assume Conjecture 1. The proof of Proposition 3.4 is rather standard at this point; similar results in slightly different settings can be found in [FI98, FIMR13, Mil17b, Mil18, KM18], among others. The substantially more difficult proof of Proposition 3.3 requires us to make a genuine improvement to the argument of Friedlander *et al.* [FIMR13, § 6].

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

In the definition of $s_{\mathfrak{a}}$ in (1.3), we chose a generator α for the ideal $\mathfrak{a}$. As we will see in the proofs of Propositions 3.3 and 3.4, when summing over multiple ideals $\mathfrak{a}$, it will be useful to work with a compatible set of generators. Here we present a suitable set of such generators, given by a standard fundamental domain for the action of $\mathcal{O}_M^{\times}$ on $\mathcal{O}_M$.

Recall that $\mathcal{O}_M^{\times} = \langle \zeta_8 \rangle \times V$, where V is free of rank 3. The group V acts on $\mathcal{O}_M$ by multiplication, i.e., there is an action

$$\Psi : V \times \mathcal{O}_M \to \mathcal{O}_M$$

given by $\Psi(\mu, \alpha) = \mu\alpha$. Up to units of finite order, the orbits of Ψ correspond to ideals in $\mathcal{O}_M$.

Fix an integral basis for $\mathcal{O}_M$, say $\eta = \{\eta_1, \dots, \eta_8\}$. If $\alpha = a_1\eta_1 + \cdots + a_8\eta_8 \in \mathcal{O}_M$ with $a_i \in \mathbb{Z}$, we call a_i the coordinates of α in the basis η. The ideal in $\mathcal{O}_M$ generated by α is also generated by $\mu\alpha$ for any unit $\mu \in V$. As V is infinite, one can choose μ so that the coordinates of $\mu\alpha$ in the integral basis η are arbitrarily large. The following classical result ensures that one can choose μ so that the coordinates of $\mu\alpha$ are reasonably small.

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

LEMMA 3.5. *There exists a subset $\mathcal{D}$ of $\mathcal{O}_M$ such that:*

(i) *$\mathcal{D}$ is a fundamental domain for the action Ψ, i.e., for all $\alpha \in \mathcal{O}_M$, there exists a unique $\mu \in V$ such that $\mu\alpha \in \mathcal{D}$; and*

(ii) *every non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_M$ has exactly 8 generators in $\mathcal{D}$; if α is one such generator, then all such generators are of the form $\zeta_8^j\alpha$, where $j \in \{1, \dots, 8\}$; and*

(iii) *there exists a constant $C = C(\eta) > 0$ such that for all $\alpha \in \mathcal{D}$, the coordinates a_i of α in the basis η satisfy $|a_i| \leqslant C \cdot \mathrm{N}(\alpha)^{1/8}$.*

For a proof, see [KM18], based on [Lan86, Lemma 1, p. 131]. We are now ready to prove Propositions 3.3 and 3.4, thereby proving Theorem 1.

4. Proof of Theorem 1

As mentioned in § 3.4, thanks to [FIMR13, Proposition 5.2, p. 722], Theorem 1 reduces to proving the appropriate estimates for sums of type I and sums of type II.

4.1 Sums of type I

In this section, we prove Proposition 3.3. Define F as in (3.1). We recall that we fixed a rank 3 subgroup V of $\mathcal{O}_M$ and a set of representatives $\mu_1, \dots, \mu_8$ for V/V^2. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_M$ coprime with F. Recall the definition of $s_{\mathfrak{a}}$ in (1.3). After using Lemma 3.5 to transform a sum over ideals in $\mathcal{O}_M$ to a sum over elements in the fundamental domain $\mathcal{D}$, our goal becomes to bound the following sum

$$A(x) = \frac{1}{64} \sum_{\substack{\mathrm{N}(\mathfrak{a}) \leqslant x \\ (\mathfrak{a}, F) = 1, \mathfrak{m} | \mathfrak{a}}} \sum_{i=1}^{8} \sum_{j=1}^{8} [\mu_i \zeta_8^j \alpha] = \frac{1}{64} \sum_{i=1}^{8} \sum_{\substack{\alpha \in \mathcal{D}; \mathrm{N}(\alpha) \leqslant x \\ (\alpha, F) = 1, \mathfrak{m} | \alpha}} [\mu_i \alpha],$$

where, for convenience of notation, we have set $[\beta] = \psi(\beta \bmod F)[\beta]_r$ for $\beta \in \mathcal{O}_M$. The rough strategy of our proof will be the same as the strategy in [FIMR13, § 6], although we will have to make the appropriate adjustments in numerous places. We can simplify several steps thanks to the special properties of the field M as described in § 3.1. At some point, however, the strategy of [FIMR13, § 6] will no longer suffice, and we will need a new ingredient.

By making changes of variables $\alpha \mapsto \mu_i^{-1}\alpha$, we rewrite the sum above as

$$A(x) = \frac{1}{64} \sum_{i=1}^{8} \sum_{\substack{\alpha \in \mu_i \mathcal{D}; \mathrm{N}(\alpha) \leqslant x \\ (\alpha, F) = 1, \mathfrak{m} | \alpha}} [\alpha]$$

and after splitting the sum into congruence classes modulo F, we get

$$A(x) = \frac{1}{64} \sum_{i=1}^{8} \sum_{\substack{\rho \bmod F; \\ (\rho, F) = 1}} \psi(\rho) A(x; \rho, \mu_i),$$

where

$$A(x; \rho, \mu_i) = \sum_{\substack{\alpha \in \mu_i \mathcal{D}; \mathrm{N}(\alpha) \leqslant x \\ \alpha \equiv \rho \bmod F \\ \alpha \equiv 0 \bmod \mathfrak{m}}} [\alpha]_r.$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

Our goal is to estimate $A(x;\rho,\mu_i)$ for each congruence class $\rho \bmod F$, $(\rho,F)=1$ and unit μ_i. As a $\mathbb{Z}$-module, the ring $\mathcal{O}_M$ decomposes as $\mathcal{O}_M = \mathbb{Z}\oplus\mathbb{M}$, where $\mathbb{M}$ is a free $\mathbb{Z}$-module of rank 7, so that we can write

$$\mathbb{M} = \omega_2\mathbb{Z} + \cdots + \omega_8\mathbb{Z}$$

for some $\omega_2,\dots,\omega_8 \in \mathcal{O}_M$. This means that α can be written uniquely as

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

so the four summation conditions above are equivalent to

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

Part 3 of Lemma 3.5 implies that the conjugates of β, say $\beta^{(i)}$ for $1\leqslant i\leqslant 8$, satisfy $|\beta^{(i)}|\ll x^{1/8}$ for any embedding $M\hookrightarrow\mathbb{C}$. Because our field M and the integral basis $\{1,\omega_2,\dots,\omega_8\}$ is fixed, the implied constant is absolute.

Perhaps the main step of [FIMR13, § 6] is a trick on p. 725, which we use to rewrite $[\alpha]_r = \left(\frac{r(\alpha)}{\alpha}\right)$ as

$$\left(\frac{r(\alpha)}{\alpha}\right) = \left(\frac{r(a+\beta)}{a+\beta}\right) = \left(\frac{r(\beta)-\beta}{a+\beta}\right).$$

Morally speaking, this allows us to fix β and vary a, thereby creating a genuine character sum in which the variable of summation does not depend on the conductor of the character. If $\beta = r(\beta)$, then β does not contribute to the sum. So we can and will assume $\beta\neq r(\beta)$. By property (P1) in § 3.1, we can write

$$r(\beta)-\beta = \eta^2 c_0 c$$

with $c_0,c,\eta\in\mathcal{O}_M$, $c_0\mid F$ squarefree, $\eta\mid F^\infty$, and $(c,F)=1$. Then

$$\left(\frac{r(\beta)-\beta}{a+\beta}\right) = \left(\frac{\eta^2c_0c}{a+\beta}\right) = \left(\frac{c_0c}{a+\beta}\right) = \left(\frac{c_0}{a+\beta}\right)\left(\frac{c}{a+\beta}\right).$$

By Lemma 3.2, the factor $\left(\frac{c_0}{a+\beta}\right)$ depends only on the congruence class of $a+\beta$ modulo $8c_0$, and, as c_0 is squarefree and divides F, it depends only on ρ.

Next we claim that

$$\left(\frac{c}{a+\beta}\right) = \varepsilon_1\cdot\left(\frac{a+\beta}{c}\right),$$

where $\varepsilon_1\in\{\pm1\}$ depends only on ρ and β. Indeed, ρ determines the congruence class of $a+\beta$ modulo 8 and c depends only on β, so an application of Lemma 3.1 proves the claim. Combining everything gives

$$\left(\frac{r(\alpha)}{\alpha}\right) = \varepsilon_2\cdot\left(\frac{a+\beta}{c}\right),$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

where $\varepsilon_2 = \varepsilon_2(\rho, \beta) \in \{\pm 1\}$ depends only on ρ and β. Having rewritten $\left(\frac{r(\alpha)}{\alpha}\right)$ in a desirable form, we can now split $A(x; \rho, \mu_i)$ as follows

$$\begin{aligned} A(x;\rho,\mu_i) &= \sum_{\substack{\alpha\in\mu_i\mathcal{D};\mathrm{N}(\alpha)\leqslant x\\ \alpha\equiv\rho \bmod F\\ \alpha\equiv 0 \bmod \mathfrak{m}}} \left(\frac{r(\alpha)}{\alpha}\right) = \sum_{\substack{a+\beta\in\mu_i\mathcal{D};\mathrm{N}(a+\beta)\leqslant x\\ a+\beta\equiv\rho \bmod F\\ a+\beta\equiv 0 \bmod \mathfrak{m}}} \left(\frac{r(a+\beta)}{a+\beta}\right) \\ &= \sum_{\beta\in\mathbb{M}} \sum_{\substack{a\in\mathbb{Z};\\ a+\beta\in\mu_i\mathcal{D},\mathrm{N}(a+\beta)\leqslant x\\ a+\beta\equiv\rho \bmod F\\ a+\beta\equiv 0 \bmod \mathfrak{m}}} \left(\frac{r(a+\beta)}{a+\beta}\right) = \sum_{\beta\in\mathbb{M}} \sum_{\substack{a\in\mathbb{Z};\\ a+\beta\in\mu_i\mathcal{D};\mathrm{N}(a+\beta)\leqslant x\\ a+\beta\equiv\rho \bmod F\\ a+\beta\equiv 0 \bmod \mathfrak{m}}} \varepsilon_2(\rho,\beta)\left(\frac{a+\beta}{c}\right) \\ &\leqslant \sum_{\beta\in\mathbb{M}} |T(x;\beta,\rho,\mu_i)|, \end{aligned}$$

where $T(x; \beta, \rho, \mu_i)$ is defined as

$$T(x;\beta,\rho,\mu_i) = \sum_{\substack{a\in\mathbb{Z};\\ a+\beta\in\mu_i\mathcal{D},\mathrm{N}(a+\beta)\leqslant x\\ a+\beta\equiv\rho \bmod F\\ a+\beta\equiv 0 \bmod \mathfrak{m}}} \left(\frac{a+\beta}{c}\right).$$

From now on we treat β as fixed and estimate $T(x; \beta, \rho, \mu_i)$. Recall that c is odd and hence no ramified prime can divide the ideal $(c) = c\mathcal{O}_M$ by property (P2) in § 3.1. This implies that (c) can be factored as

$$(c) = \mathfrak{g}\mathfrak{q},$$

where, similarly as in [FIMR13, (6.21), p. 727], $\mathfrak{g}$ consists of all prime ideals dividing (c) that are of degree greater than one or unramified primes of degree one for which some conjugate is also a factor of (c). By construction $\mathfrak{q}$ consists of all the remaining primes dividing $c\mathcal{O}_M$. Then $q := N\mathfrak{q}$ is a squarefree integer and $g := N\mathfrak{g}$ is a squarefull number coprime with q. There exists a rational integer b with $b \equiv \beta \bmod \mathfrak{q}$ by an application of the Chinese remainder theorem. Again, as c depends on β and not on a, so also b is a rational integer that depends on β and not on a. We get

$$\left(\frac{a+\beta}{c}\right) = \left(\frac{a+\beta}{\mathfrak{g}}\right)\left(\frac{a+\beta}{\mathfrak{q}}\right) = \left(\frac{a+\beta}{\mathfrak{g}}\right)\left(\frac{a+b}{\mathfrak{q}}\right).$$

Define g_0 as the radical of g, i.e.,

$$g_0 = \prod_{p\mid g} p.$$

Note that the quadratic residue symbol $\left(\frac{\alpha}{\mathfrak{g}}\right)$ is periodic in α modulo $\mathfrak{g}^* = \prod_{\mathfrak{p}\mid\mathfrak{g}} \mathfrak{p}$. Since $\mathfrak{g}^*$ divides g_0, we conclude that the symbol $\left(\frac{a+\beta}{\mathfrak{g}}\right)$ is periodic of period g_0 as a function of $a \in \mathbb{Z}$. We split $T(x; \beta, \rho, \mu_i)$ into congruence classes modulo g_0, giving

$$|T(x;\beta,\rho,\mu_i)| \leqslant \sum_{a_0 \bmod g_0} |T(x;\beta,\rho,\mu_i,a_0)|, \tag{4.1}$$

where

$$T(x;\beta,\rho,\mu_i,a_0) = \sum_{\substack{a\in\mathbb{Z};\\ a+\beta\in\mu_i\mathcal{D},\mathrm{N}(a+\beta)\leqslant x\\ a+\beta\equiv\rho \bmod F\\ a+\beta\equiv 0 \bmod \mathfrak{m}\\ a\equiv a_0 \bmod g_0}} \left(\frac{a+b}{\mathfrak{q}}\right).$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

Note that $a+\beta \in \mu_i \mathcal{D}$ implies that $a \ll x^{1/8}$, where the implied constant depends only on one of the eight units μ_i. The condition $\mathrm{N}(a+\beta) \leqslant x$ for fixed β and x is a polynomial inequality of degree 8 in a. So the summation variable $a \in \mathbb{Z}$ runs over a collection of at most 8 intervals whose endpoints depend on β and x. But from $a \ll x^{1/8}$ we see that for the length L of each such interval we have $L \ll x^{1/8}$.

Furthermore, the congruences $a+\beta \equiv \rho \bmod F$, $a+\beta \equiv 0 \bmod \mathfrak{m}$ and $a \equiv a_0 \bmod g_0$ mean that a runs over a certain arithmetic progression of modulus k, which divides $g_0 m F$, where $m := \mathrm{N}\mathfrak{m}$. Hence, we see that the inner sum in (4.1) can be rewritten as at most 8 sums, each of which runs over an arithmetic progression of modulus k in a single segment of length $\ll x^{1/8}$.

As $q = \mathrm{N}(\mathfrak{q})$ is squarefree, $\left(\frac{\cdot}{\mathfrak{q}}\right)$ is the real primitive Dirichlet character of modulus q, and hence we have at most 8 incomplete character sums of length $\ll x^{1/8}$ and modulus $q \ll x$. When the modulus q of the Dirichlet character divides the modulus k of the arithmetic progression, one can not expect to get cancellation. For now we assume that $q \nmid k$, and we will deal with the case $q \mid k$ later on. Corollary 7 implies that

$$T(x; \beta, \rho, \mu_i, a_0) \ll x^{1/8-\delta},$$

and hence that

$$T(x; \beta, \rho, \mu_i) \ll g_0 x^{1/8-\delta}. \tag{4.2}$$

Just as in [FIMR13], the implied constant above does not depend on β because Conjecture 1, and so also Corollary 7, encompasses all incomplete character sums of length $\ll x^{1/8}$, regardless of the endpoints of the interval being summed over.

We still need to deal with the case $q \mid k$. Certainly, this implies $q \mid m$. So (4.2) holds if $q \nmid m$. Hence, by the definition of (c) and the factorization $(c) = \mathfrak{g}\mathfrak{q}$, we have (4.2) unless

$$p \mid \mathrm{N}(\alpha - r(\alpha)) \implies p^2 \mid mF\mathrm{N}(\alpha - r(\alpha)). \tag{4.3}$$

We write $A_{\square}(x; \rho, \mu_i)$ for the contribution to $A(x; \rho, \mu_i)$ with (4.3). We have

$$A_{\square}(x; \rho, \mu_i) \leqslant |\{\alpha \in \mu_i \mathcal{D} : N\alpha \leqslant x,\ p \mid \mathrm{N}(\alpha - r(\alpha)) \implies p^2 \mid mF\mathrm{N}(\alpha - r(\alpha))\}|.$$

Decompose $\mathcal{O}_M$ as

$$\mathcal{O}_M = \mathbb{Z}[\sqrt{-2}] \oplus \mathbb{M}',$$

where $\mathbb{M}'$ is a free $\mathbb{Z}$-module of rank 6. Then we get an injective map $\mathbb{M}' \to \mathcal{O}_M$ given by $\alpha \mapsto \alpha - r(\alpha)$. Since $\alpha \in \mu_i \mathcal{D}$ and $\mathrm{N}(\alpha) \leqslant x$, we know that all the conjugates $|\alpha^{(k)}|$ are $\ll x^{1/8}$. If we write

$$\alpha = a + b\sqrt{-2} + m'$$

with $a, b \in \mathbb{Z}$, and $m' \in \mathbb{M}'$, then it follows that $|a|, |b| \leqslant y$ and furthermore all the conjugates of $\gamma = \alpha - r(\alpha)$ satisfy $|\gamma^{(k)}| \leqslant y$ for some $y \asymp x^{1/8}$. Therefore, we have

$$A_{\square}(x; \rho, \mu_i) \leqslant y^2 |\{\gamma \in \mathcal{O}_M : |\gamma^{(k)}| \leqslant y,\ p \mid \mathrm{N}(\gamma) \implies p^2 \mid mF\mathrm{N}(\gamma)\}|.$$

Since it is easier to count ideals than integers, we replace γ by the principal ideal it generates. We remark that an ideal $\mathfrak{b}$ with $\mathrm{N}\mathfrak{b} \leqslant y^8$ has $\ll (\log y)^8$ generators satisfying $|\gamma^{(k)}| \leqslant y$ for all k. Hence

$$A_{\square}(x; \rho, \mu_i) \ll x^{1/4} (\log x)^8 |\{\mathfrak{b} \subseteq \mathcal{O}_M : \mathrm{N}\mathfrak{b} \leqslant y^8,\ p \mid \mathrm{N}\mathfrak{b} \implies p^2 \mid mF\mathrm{N}\mathfrak{b}\}|.$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

Now we can use the multiplicative structure of the ideals in $\mathcal{O}_M$, giving the bound

$$A_\square(x;\rho,\mu_i) \ll x^{1/4}(\log x)^8 \sum_{\substack{b\leqslant y^8 \\ p|b \Longrightarrow p^2|mFb}} \tau(b),$$

where b runs over the positive rational integers and $\tau(b)$ counts the number of ideals in M with norm b. Then we have $\tau(b) \ll b^\epsilon$. Note that we can assume $m \leqslant x$ because otherwise $A(x)$ is the empty sum. Hence, recalling that $y \asymp x^{1/8}$, we conclude that

$$A_\square(x;\rho,\mu_i) \ll x^{3/4+\epsilon},$$

where the implied constant depends only on ϵ.

Define $A_0(x;\rho,\mu_i)$ to be the contribution of $A(x;\rho,\mu_i)$ of the terms $\alpha = a+\beta$ not satisfying (4.3). We have

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

To estimate $A_0(x;\rho,\mu_i)$ we can use (4.2) for every relevant β. Unfortunately, the bound (4.2) is only good when g_0 is small. So we make the further partition

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

where the components run over $\alpha = a+\beta$ with β satisfying

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

Here Z is at our disposal and we choose it later. It is here that we must improve on the bounds of [FIMR13]. In their proof they define three sums

$$\begin{aligned} g_0 &\leqslant Z \quad \text{in the sum } A_1(x;\rho,\mu_i), \\ g_0 &> Z, g \leqslant Y \quad \text{in the sum } A_2(x;\rho,\mu_i), \\ g_0 &> Z, g > Y \quad \text{in the sum } A_3(x;\rho,\mu_i), \end{aligned}$$

with $Z \leqslant Y$ at their disposal. Following the proof in [FIMR13] would give

$$A_0(x;\rho,\mu_i) \ll x^\epsilon(Zx^{1-\delta} + Y^{-1/2}x^{1+1/4} + Z^{-1}\log Y x + Y^{5/2}x^{1/4}),$$

and it is easily seen that there is no choice of $Z \leqslant Y$ that makes $A_0(x;\rho,\mu_i) \ll x^{1-\theta_1}$ for some $\theta_1 > 0$. Our proof is conceptually simpler and provides sharper bounds.

We estimate $A_1(x;\rho,\mu_i)$ as in [FIMR13] by using (4.2) and summing over $\beta \in \mathbb{M}$ satisfying $|\beta^{(1)}|,\dots,|\beta^{(8)}| \ll x^{1/8}$ to obtain

$$A_1(x;\rho,\mu_i) \ll Zx^{1-\delta}.$$

Our next goal is to estimate $A_2(x;\rho,\mu_i)$. We keep the condition $\alpha - r(\alpha) \equiv 0 \bmod \mathfrak{g}$, giving

$$|A_2(x;\rho,\mu_i)| \leqslant y^2 \sum_{\substack{\mathfrak{g} \\ g_0 > Z}} E_\mathfrak{g}(y), \tag{4.4}$$

where $y \asymp x^{1/8}$ and

$$E_\mathfrak{g}(y) := |\{\gamma \in \mathbb{M}'' : \gamma \equiv 0 \bmod \mathfrak{g}, |\gamma^{(k)}| \leqslant y \text{ for all } k\}|.$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

Here $\mathbb{M}''$ is by definition the image of $\mathbb{M}'$ under the map $\beta \mapsto \beta - r(\beta)$. Let $\eta_3, \dots, \eta_8$ be a $\mathbb{Z}$-basis of $\mathbb{M}''$. We view $\mathbb{M}'' \subseteq \mathbb{R}^6$ via $a_3\eta_3 + \cdots + a_8\eta_8 \mapsto (a_3, \dots, a_8)$. In this way, we identify $\mathbb{M}''$ with $\mathbb{Z}^6$, so $\mathbb{M}''$ becomes a lattice in $\mathbb{R}^6$. Furthermore, define $\Lambda_{\mathfrak{g}}$ as

$$\Lambda_{\mathfrak{g}} := \{\gamma \in \mathbb{M}'' : \gamma \equiv 0 \bmod \mathfrak{g}\}.$$

Then it is easily seen that $\Lambda_{\mathfrak{g}}$ is a sublattice of $\mathbb{M}''$.

We further define

$$S_x = \{(a_3, \dots, a_8) \in \mathbb{R}^6 : |a_i| \leqslant c_1 x^{1/8}\},$$

where the constant $c_1 > 0$ is taken large enough such that

$$E_{\mathfrak{g}}(y) \leqslant |S_x \cap \Lambda_{\mathfrak{g}}|. \tag{4.5}$$

Note that $S_x = x^{1/8} S_1$, which implies that $\mathrm{Vol}(S_x) = x^{3/4}\mathrm{Vol}(S_1)$. Because S_1 is a 6-dimensional hypercube, it has 12 sides. Hence, there exist an absolute constant L and functions $\varphi_1, \dots, \varphi_{12} : [0,1]^5 \to \mathbb{R}^6$ satisfying a Lipschitz condition

$$|\varphi_i(a) - \varphi_i(b)| \leqslant L|a - b|$$

for $a, b \in [0,1]^5$, $i = 1, \dots, 12$ such that the boundary of S_1, denoted by ∂S_1, is covered by the images of the φ_i. Then $x^{1/8}\varphi_1, \dots, x^{1/8}\varphi_{12}$ are Lipschitz functions for $\partial S_x = \partial x^{1/8} S_1 = x^{1/8}\partial S_1$. Hence, we can choose $x^{1/8}L$ as the Lipschitz constant for S_x.

We now apply [Wid10, Theorem 5.4], which gives

$$\left| |S_x \cap \Lambda_{\mathfrak{g}}| - \frac{\mathrm{Vol}(S_x)}{\det \Lambda_{\mathfrak{g}}} \right| \ll_L \max_{0 \leqslant i < 6} \frac{x^{i/8}}{\lambda_{\mathfrak{g},1} \cdot \ldots \cdot \lambda_{\mathfrak{g},i}}, \tag{4.6}$$

where $\lambda_{\mathfrak{g},1}, \dots, \lambda_{\mathfrak{g},6}$ are the successive minima of $\Lambda_{\mathfrak{g}}$ and $\ll_L$ means that the implied constant may depend on L. Our next goal is to give a lower bound for $\lambda_{\mathfrak{g},1}$.

So let $\gamma \in \Lambda_{\mathfrak{g}}$ be non-zero. Then $\mathfrak{g} \mid \gamma$ and hence $g \mid \mathrm{N}(\gamma)$. Write $\gamma = (a_3, \dots, a_8)$. We fix some small $\epsilon > 0$. If $a_3, \dots, a_8 \leqslant c_2 g^{1/8-\epsilon}$ for some sufficiently small absolute constant $c_2 > 0$, we obtain $\mathrm{N}(\gamma) < g$. Since $g \mid \mathrm{N}(\gamma)$, we conclude that $\mathrm{N}(\gamma) = 0$, contradiction. Hence there is an i with $a_i > c_2 g^{1/8-\epsilon}$. This implies that the length of γ satisfies $\|\gamma\| \gg g^{1/8-\epsilon}$ and therefore

$$\lambda_{\mathfrak{g},1} \gg g^{1/8-\epsilon}. \tag{4.7}$$

By Minkowski's second theorem and (4.7) we find that

$$\det \Lambda_{\mathfrak{g}} \gg g^{3/4-6\epsilon}. \tag{4.8}$$

Combining (4.6)–(4.8) gives

$$|S_x \cap \Lambda_{\mathfrak{g}}| \ll \frac{x^{3/4}}{g^{3/4-6\epsilon}} + \frac{x^{5/8}}{g^{5/8-5\epsilon}} \ll \frac{x^{3/4}}{g^{3/4-6\epsilon}}. \tag{4.9}$$

Plugging (4.5) and (4.9) back into (4.4) gives

$$|A_2(x; \rho, \mu_i)| \leqslant y^2 \sum_{\substack{\mathfrak{g} \\ g_0 > Z}} E_{\mathfrak{g}}(y) \leqslant y^2 \sum_{\substack{\mathfrak{g} \\ g_0 > Z}} |S_x \cap \Lambda_{\mathfrak{g}}| \ll \sum_{\substack{\mathfrak{g} \\ g_0 > Z}} \frac{x}{g^{3/4-6\epsilon}}.$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

We rewrite the last sum as

$$\sum_{\substack{\mathfrak{g} \\ g_0 > Z}} \frac{x}{g^{3/4-6\epsilon}} = x \sum_{\substack{g \leqslant x \\ g \text{ squarefull} \\ g_0 > Z}} \frac{\tau(g)}{g^{3/4-6\epsilon}} \ll x^{1+\epsilon'} \sum_{\substack{g \leqslant x \\ g \text{ squarefull} \\ g_0 > Z}} \frac{1}{g^{3/4-6\epsilon}}$$
$$= x^{1+\epsilon'} \sum_{\substack{g \leqslant x \\ g \text{ squarefull} \\ g_0 > Z}} g^{-1/4+6\epsilon} \frac{1}{g^{1/2}} \leqslant x^{1+\epsilon'} Z^{-1/2+3\epsilon} \sum_{\substack{g \leqslant x \\ g \text{ squarefull} \\ g_0 > Z}} \frac{1}{g^{1/2}}$$
$$\leqslant x^{1+\epsilon'} Z^{-1/2+3\epsilon} \sum_{\substack{g \leqslant x \\ g \text{ squarefull}}} \frac{1}{g^{1/2}} \ll x^{1+\epsilon'} Z^{-1/2+3\epsilon} \log x.$$

By picking $Z = X^{\delta/2}$, ϵ and ϵ' sufficiently small, we get the desired result with $\theta_1 = \delta/4$.

5. Sums of type II

Our goal in this section is to prove Proposition 3.4, thereby completing the proof of Theorem 1. A power-saving bound for the bilinear sum in Proposition 3.4 is possible because the symbol

$$[\alpha]_r = \left(\frac{r(\alpha)}{\alpha}\right)$$

is *not* multiplicative in α but instead satisfies the following elegant identity, analogous to [FIMR13, (3.8), p. 708]. Let α and β be odd elements in $\mathcal{O}_M$. Then

$$[\alpha\beta]_r = \left(\frac{r(\alpha\beta)}{\alpha\beta}\right) = [\alpha]_r[\beta]_r \left(\frac{r(\alpha)}{\beta}\right)\left(\frac{r(\beta)}{\alpha}\right) = \varepsilon_3 \cdot [\alpha]_r[\beta]_r \gamma(\alpha,\beta), \tag{5.1}$$

where

$$\gamma(\alpha,\beta) = \left(\frac{\beta}{r(\alpha)r^3(\alpha)}\right), \tag{5.2}$$

and $\varepsilon_3 \in \{\pm 1\}$ depends only on the congruence classes of α and β modulo 8 (see Lemma 3.1). We remark here that the natural one-line proof of (5.1) should be contrasted with the rather involved proofs of [FI98, Lemma 20.1, p. 1021] and [Mil17b, Proposition 8, p. 31]. It would be very interesting to find a common source of these identities, if it exists.

With $\mu_1, \ldots, \mu_8$ and $[\cdot] = \psi(\cdot \bmod F)[\cdot]_r$ is as in the beginning of § 4.1, we see that the bilinear sum from Proposition 3.4 is equal to

$$\frac{1}{64} \sum_{\zeta \in \langle \zeta_8 \rangle} \sum_{i=1}^{8} B(M, N; \zeta, i),$$

where

$$B(M, N; \zeta, i) = \sum_{\alpha \in \mathcal{D}(M)} \sum_{\beta \in \mathcal{D}(N)} v_\alpha w_\beta [\zeta \mu_i \alpha\beta]. \tag{5.3}$$

Here $\mathcal{D}(X) = \{x \in \mathcal{D} : \mathrm{N}(x) \leqslant X\}$; v_α (respectively w_β) depends only on the ideal generated by α (respectively β); and, the double sum over α and β is assumed to be supported on α and β such that $(\alpha\beta, F) = 1$.

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

The condition $(\alpha\beta, F) = 1$ is equivalent to the two conditions $(\alpha, F) = 1$ and $(\beta, F) = 1$. Hence we can decompose the sum (5.3) into $(\#(\mathcal{O}_M/F\mathcal{O}_M)^\times)^2$ sums $B(M, N; \zeta, i, \rho_1, \rho_2)$ where we further restrict the support of α and β to fixed invertible congruence classes modulo F, i.e.,

$$\alpha \equiv \rho_1 \bmod F \quad \text{and} \quad \beta \equiv \rho_2 \bmod F. \tag{5.4}$$

Hence, with $\varepsilon_4 = \psi(\zeta\mu_i\rho_1\rho_2 \bmod F)$ fixed for fixed ζ, μ_i, ρ_1, and ρ_2, we have

$$B(M, N; \zeta, i, \rho_1, \rho_2) = \varepsilon_4 \sum_{\alpha \in \mathcal{D}(M)} \sum_{\beta \in \mathcal{D}(N)} v_\alpha w_\beta [\zeta\mu_i\alpha\beta]_r, \tag{5.5}$$

where we again note that the support of α and β is restricted to (5.4). To prove Proposition 3.4, it suffices to prove the desired estimate for each of the

$$64 \cdot (\#(\mathcal{O}_M/F\mathcal{O}_M)^\times)^2$$

sums $B(M, N; \zeta, i, \rho_1, \rho_2)$. To this end, we now take advantage of the special non-multiplicativity of the spin symbol $[\cdot]_r$. By (5.1), we can unfold $[\zeta\mu_i\alpha\beta]_r$ into the product

$$[\zeta\mu_i\alpha\beta]_r = \varepsilon_5 [\alpha\beta]_r [\zeta\mu_i]_r \gamma(\zeta\mu_i, \alpha\beta).$$

The factor $\varepsilon_5 \in \{\pm 1\}$ depends only on the congruence classes $\zeta\mu_i \bmod 8$ and $\alpha\beta \bmod 8$, the factor $[\zeta\mu_i]_r$ does not depend on α and β in any way, and the factor

$$\gamma(\zeta\mu_i, \alpha\beta) = \left(\frac{\zeta\mu_i}{r(\alpha\beta)r^3(\alpha\beta)}\right)$$

is determined by the congruence class $r(\alpha\beta)r^3(\alpha\beta) \bmod 8$, by Lemma 3.2. As 8 divides F, all of these congruence classes are determined by ζ, μ_i, ρ_1 and ρ_2. Hence

$$B(M, N; \zeta, i, \rho_1, \rho_2) = \varepsilon_6 \cdot \sum_{\alpha \in \mathcal{D}(M)} \sum_{\beta \in \mathcal{D}(N)} v_\alpha w_\beta [\alpha\beta]_r, \tag{5.6}$$

where $\varepsilon_6 = \varepsilon_6(\zeta, \mu_i, \rho_1, \rho_2)$ depends only on ζ, μ_i, ρ_1, and ρ_2 but not on α and β. Next, using (5.1) again, we get

$$B(M, N; \zeta, i, \rho_1, \rho_2) = \varepsilon_7 \cdot \sum_{\alpha \in \mathcal{D}(M)} \sum_{\beta \in \mathcal{D}(N)} v'_\alpha w'_\beta \gamma(\alpha, \beta), \tag{5.7}$$

where ε_7 depends only on ζ, μ_i, ρ_1, and ρ_2, and

$$v'_\alpha = v_\alpha \cdot [\alpha]_r \quad \text{and} \quad w'_\beta = w_\beta \cdot [\beta]_r.$$

The sum in (5.7) has exactly the same shape as [KM18, (3.2), p. 11]. Moreover, the function γ satisfies the properties (P1)–(P3) on [KM18, p. 11]; indeed, (P1) follows by Lemma 3.1, and (P2) is clear. For (P3), suppose that $r(\alpha)r^3(\alpha)\mathcal{O}_M = \mathfrak{a}^2$ for some odd ideal $\mathfrak{a} \subset \mathcal{O}_M$. Then, as $r(\alpha)r^3(\alpha)$ is fixed by r^2 and is thus an odd element of $\mathbb{Q}(\zeta_8)$, we have

$$r(\alpha)r^3(\alpha)\mathbb{Z}[\zeta_8] = \mathfrak{a}'^2$$

for some odd ideal $\mathfrak{a}' \subset \mathbb{Z}[\zeta_8]$. Taking norms to $\mathbb{Q}$, we get that

$$\mathrm{N}_{M/\mathbb{Q}}(\alpha) = \mathrm{N}_{M/\mathbb{Q}}(r(\alpha)) = \mathrm{N}_{\mathbb{Q}(\zeta_8)/\mathbb{Q}}(r(\alpha)r^3(\alpha)) = \mathrm{N}_{\mathbb{Q}(\zeta_8)/\mathbb{Q}}(\mathfrak{a}')^2.$$

Hence, if $\mathrm{N}_{M/\mathbb{Q}}(\alpha)$ is not a square, we see that $r(\alpha)r^3(\alpha)$ does not generate the square of an ideal in $\mathcal{O}_M$, and so

$$\sum_{\xi \bmod \mathrm{N}(\alpha)\mathcal{O}_M} \gamma(\alpha, \xi) = \mathrm{N}(\alpha)^6 \cdot \sum_{\xi \bmod r(\alpha)r^3(\alpha)} \left(\frac{\xi}{r(\alpha)r^3(\alpha)}\right) = \mathrm{N}(\alpha)^6 \cdot 0 = 0,$$

which proves (P3). Proposition 3.4 now follows by [KM18, Proposition 3.6, p. 11].

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

6. Proof of Theorem 2

We will now deduce Theorem 2 from Theorem 1 by choosing the factor ψ in the definition of $s_{\mathfrak{a}}$ appropriately. First note that Theorem 2 is equivalent to the statement that

$$\sum_{p \leqslant X} a_p \ll X^{1-\delta'},$$

where

$$a_p = \begin{cases} 1 & \text{if } h(-4p) \equiv 0 \bmod 16, \\ -1 & \text{if } h(-4p) \equiv 8 \bmod 16, \\ 0 & \text{otherwise.} \end{cases} \tag{6.1}$$

We will use an algebraic criterion for the 16-rank due to Bruin and Hemenway [BH13]. Let p be a prime number such that $h(-4p) \equiv 0 \bmod 8$, i.e., such that p splits completely in $M/\mathbb{Q}$. As in § 3.1, set $K_1 = \mathbb{Q}(i, \sqrt{1+i})$. Let ρ be a prime in $\mathcal{O}_{K_1}$ dividing p, and let δ_p be an element of $\mathcal{O}_{K_1}$ such that $\mathrm{N}_{K_1/\mathbb{Q}(i)}(\delta_p) = p$ and such that $\delta_p \notin \rho\mathcal{O}_{K_1}$. Bruin and Hemenway proved that

$$h(-4p) \equiv 0 \bmod 16 \iff \left(\frac{\delta_p \cdot \sqrt{1+i}}{\rho}\right)_{K_1} = 1. \tag{6.2}$$

We will now interpret this symbol as a quadratic residue symbol in M. Recall the definition of r and s and the field diagram in § 3.1.

Let π be a prime in $\mathcal{O}_M$ dividing p such that

$$p = \prod_{\sigma \in \mathrm{Gal}(M/\mathbb{Q})} \sigma(\pi). \tag{6.3}$$

We define elements ρ and δ_p in $\mathcal{O}_{K_1}$ by setting $\rho = \pi \cdot s(\pi)$ and

$$\delta_p = r(\pi)r^2(\pi) \cdot sr(\pi)sr^2(\pi).$$

Note that $\mathrm{N}_{K_1/\mathbb{Q}(i)}(\delta_p) = \delta_p \cdot r^2(\delta_p) = p$ and $\delta_p \notin \rho\mathcal{O}_{K_1}$, so that ρ and δ_p satisfy the assumptions implicit in criterion (6.2). Next, note that since p splits completely in $M/\mathbb{Q}$, the inclusion $\mathcal{O}_{K_1} \hookrightarrow \mathcal{O}_M$ induces an isomorphism of finite fields of order p

$$\mathcal{O}_{K_1}/\rho\mathcal{O}_{K_1} \cong \mathcal{O}_M/\pi\mathcal{O}_M.$$

Hence

$$\left(\frac{\delta_p \cdot \sqrt{1+i}}{\rho}\right)_{K_1} = \left(\frac{\delta_p \cdot \sqrt{1+i}}{\pi}\right)_M,$$

and so

$$h(-4p) \equiv 0 \bmod 16 \iff \left(\frac{r(\pi)r^2(\pi) \cdot sr(\pi)sr^2(\pi) \cdot \sqrt{1+i}}{\pi}\right)_M = 1. \tag{6.4}$$

The above quadratic residue symbol factors into five quadratic residue symbols, the first four of which are of the form $\left(\frac{\sigma(\pi)}{\pi}\right)_M$ with σ in $\{r, r^2, sr, sr^2\}$, and the last one of which is $\left(\frac{\sqrt{1+i}}{\pi}\right)_M$. For $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$, we set

$$[\alpha]_\sigma = \left(\frac{\sigma(\alpha)}{\alpha}\right)_M.$$

We will now show that when σ is an element of order 2, the spin symbol $[\alpha]_\sigma$ can be absorbed into the factor ψ. One part of what follows is an adaptation of the treatment of such spins in [FIMR13, § 12, pp. 745–749].

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

Proposition 6.1. *Let $\alpha \in \mathcal{O}_M$ be such that $(\alpha, F) = 1$, and let σ be an element of order 2 in $\mathrm{Gal}(M/\mathbb{Q})$ such that $(\alpha, \sigma(\alpha)) = 1$. Then $[\alpha]_\sigma$ depends only on σ and on the congruence class of α modulo F.*

The proof of our claim proceeds in two steps. The first step will be to reduce to the case $\alpha \equiv 1 \bmod 8$. The second step will be to use the ideas from Section 12 of [FIMR13]. Recall the definitions of $\mathcal{R}$ and F in § 3.1.

Proof. As $(\alpha, F) = 1$, we also have $(\alpha, \Delta_M) = 1$. Let $\rho' \in \mathcal{R}$ be such that $\alpha\rho' \equiv 1 \bmod \Delta_M$ and in particular, by property (P2) from the beginning of § 3.1, such that $\alpha\rho' \equiv 1 \bmod 8$. We emphasize two important facts. First, note that ρ' depends only on $\alpha \bmod \Delta_M$ and hence only on $\alpha \bmod F$. Second, as $\mathrm{N}(\rho')$ divides F and (ρ') is a prime of degree 1, we have

$$(\sigma(\rho'), \alpha) = (\sigma(\alpha), \rho') = (\rho', \sigma(\rho')) = 1.$$

Hence, each of the four factors on the right-hand side of

$$\left(\frac{\sigma(\alpha\rho')}{\alpha\rho'}\right)_M = \left(\frac{\sigma(\alpha)}{\alpha}\right)_M \left(\frac{\sigma(\rho')}{\alpha}\right)_M \left(\frac{\sigma(\alpha)}{\rho'}\right)_M \left(\frac{\sigma(\rho')}{\rho'}\right)_M$$

is non-zero. Using Lemma 3.1 and the assumption that σ is an involution, we get

$$\left(\frac{\sigma(\rho')}{\alpha}\right)_M = \varepsilon_8 \cdot \left(\frac{\alpha}{\sigma(\rho')}\right)_M = \varepsilon_8 \cdot \left(\frac{\sigma(\alpha)}{\rho'}\right)_M,$$

where $\varepsilon_8 \in \{\pm 1\}$ depends only on σ and the congruence classes of $\sigma(\rho')$ and α modulo 8, both of which depend only on σ and $\alpha \bmod F$. Furthermore, $\left(\frac{\sigma(\rho')}{\rho'}\right)_M \in \{\pm 1\}$ also depends only on σ and $\alpha \bmod F$. This gives

$$\left(\frac{\sigma(\alpha\rho')}{\alpha\rho'}\right)_M = \varepsilon_9 \cdot \left(\frac{\sigma(\alpha)}{\alpha}\right)_M \left(\frac{\sigma(\alpha)^2}{\rho'}\right)_M = \varepsilon_9 \cdot \left(\frac{\sigma(\alpha)}{\alpha}\right)_M, \tag{6.5}$$

where $\varepsilon_9 \in \{\pm 1\}$ depends only on σ and $\alpha \bmod F$. So from now on we may assume that $\alpha \equiv 1 \bmod 8$.

In the interest of not being repetitive, we now refer to the argument used to prove [FIMR13, Proposition 12.1, p. 745]. Define L to be the subfield of M fixed by $\langle\sigma\rangle$. In our case, the discriminant ideal $\mathrm{Disc}(M/L)$ is even, and in fact divides a power of $2\mathcal{O}_L$. Although the proof of [FIMR13, Proposition 12.1, p. 745] relies on $\mathfrak{D}$ being odd in an essential way, we will overcome this by using the fact that $\mathcal{O}_L$ is a principal ideal domain.

Similarly as in [FIMR13, (12.4), p. 747], one can deduce that

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)_M = \varepsilon_{10} \left(\frac{-\gamma^2}{\beta}\right)_L,$$

where $\varepsilon_{10} \in \{\pm 1\}$ depends only on σ and $\alpha \bmod 8$, and where γ and β are defined via

$$\beta = \tfrac{1}{2}(\alpha + \sigma(\alpha)) \equiv 1 \bmod 4, \quad \gamma = \tfrac{1}{2}(\alpha - \sigma(\alpha)) \equiv 0 \bmod 4.$$

Defining the submodule $\mathcal{M}$ of $\mathcal{O}_M$ in the same way as on [FIMR13, p. 747], i.e., $\mathcal{M} = \mathcal{O}_L + ((1+\alpha)/2)\mathcal{O}_L$, we arrive at the identity

$$\gamma^2 \mathcal{O}_L = \mathrm{Disc}(\mathcal{M}) = \mathfrak{a}^2 \,\mathrm{Disc}(M/L),$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

where $\mathfrak{a}$ is an ideal in $\mathcal{O}_L$ such that $\mathcal{O}_M/\mathcal{M} \cong \mathcal{O}_L/\mathfrak{a}$. Since $\mathcal{O}_L$ is a principal ideal domain (see (P1) in § 3.1), we obtain the equation

$$\gamma^2 = u \cdot a^2 \cdot D,$$

where now $D \in \mathcal{O}_L$ is some generator of the discriminant $\mathrm{Disc}(M/L)$, $a \in \mathcal{O}_L$ is some generator of the ideal $\mathfrak{a}$, and $u \in \mathcal{O}_L^\times$. Then we have

$$\left(\frac{-\gamma^2}{\beta}\right)_L = \left(\frac{-uD}{\beta}\right)_L,$$

which, by Lemma 3.2, depends only on the congruence class $\beta \bmod 8D$. One can check that $16D$ divides Δ_M for any involution $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$, and so $\beta \bmod 8D$ is completely determined by σ and the congruence class $\alpha \bmod \Delta_M$. Hence, whenever $\alpha \equiv 1 \bmod 8$, the symbol $[w]_\sigma$ only depends on σ and $\alpha \bmod \Delta_M$. In conjunction with (6.5), this completes the proof of our proposition. □

If ρ is an invertible class modulo F and $\sigma \in \{r^2, sr, sr^2\}$, we define

$$\psi_\sigma(\rho) = [\alpha]_\sigma,$$

where α is any element of $\mathcal{O}_M$ such that $\alpha \equiv \rho \bmod F$ and such that $(\alpha, \sigma(\alpha)) = 1$; this is well-defined by Proposition 6.1. Moreover, define

$$\psi_M(\rho) = \left(\frac{\sqrt{1+i}}{\alpha}\right)_M,$$

where α is any element of $\mathcal{O}_M$ such that $\alpha \equiv \rho \bmod F$; this is well-defined by Lemma 3.2. We then define

$$\psi_0(\rho) = \psi_{r^2}(\rho)\psi_{sr}(\rho)\psi_{sr^2}(\rho)\psi_M(\rho). \tag{6.6}$$

We now check that $\psi_0(\alpha \bmod F) = \psi_0(\alpha\beta^2 \bmod F)$ for all $\alpha \in \mathcal{O}_M$ coprime to F and all $\beta \in \mathcal{O}_M^\times$. Indeed, it is clear that $\psi_M(\alpha\beta^2 \bmod F) = \psi_M(\alpha \bmod F)$, and, for any $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$, we have

$$\left(\frac{\sigma(\alpha\beta^2)}{\alpha\beta^2}\right) = \left(\frac{\sigma(\alpha\beta^2)}{\alpha}\right) = \left(\frac{\sigma(\alpha)}{\alpha}\right)\left(\frac{\sigma(\beta)^2}{\alpha}\right) = \left(\frac{\sigma(\alpha)}{\alpha}\right). \tag{6.7}$$

From (6.4), we now deduce the following criterion for the 16-rank of $\mathrm{Cl}(-4p)$, valid for all but finitely many primes p.

PROPOSITION 6.2. *Let p be a rational prime such that p splits completely in $M/\mathbb{Q}$ and such that $(p, F) = 1$. Let π be any prime in $\mathcal{O}_M$ dividing p. Then*

$$h(-4p) \equiv 0 \bmod 16 \iff \psi_0(\pi \bmod F) \cdot [\pi]_r = 1.$$

Let a_p be defined as (6.1). With ψ_0 as in (6.6), we set $\psi = \psi_0$ and define $s_\mathfrak{a}$ as in (1.3). If $(p, F) = 1$, p splits completely in $M/\mathbb{Q}$, and $\mathfrak{p}$ is any prime ideal in $\mathcal{O}_M$ lying above p, then Proposition 6.2 implies that

$$a_p = s_\mathfrak{p}. \tag{6.8}$$

Since there are only finitely many primes dividing F, and since each unramified degree 1 prime ideal $\mathfrak{p}$ in $\mathcal{O}_M$ has 8 conjugates, we have

$$\sum_{p \leqslant X} a_p = \sum_{\substack{p \leqslant X \\ p \nmid F}} a_p + O(1) = \frac{1}{8} \sum_{\substack{\mathrm{N}(\mathfrak{p}) = p \leqslant X \\ p \nmid F}} s_\mathfrak{p} + O(1) = \frac{1}{8} \sum_{\mathrm{N}(\mathfrak{p}) = p \leqslant X} s_\mathfrak{p} + O(1).$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

The number of prime ideals in $\mathcal{O}_M$ of degree at least 2 and of norm $\leqslant X$ is

$$\leqslant 4 \sum_{p \leqslant X^{1/2}} 1 \ll X^{1/2},$$

so we have

$$\sum_{p \leqslant X} a_p = \frac{1}{8} \sum_{\mathrm{N}(\mathfrak{p}) \leqslant X} s_{\mathfrak{p}} + O(X^{1/2}).$$

Theorem 1 in conjunction with (6.8) now gives the desired estimate.

7. Proof of Theorem 3

To deduce Theorem 3 from Theorem 1, we will make a different choice for ψ. Similarly as in the proof of Theorem 2, we define

$$b_p = \begin{cases} 1 & \text{if } h^+(8p) \equiv h(8p) \equiv 0 \bmod 8, \\ -1 & \text{if } h^+(8p) + 4 \equiv h(8p) \equiv 4 \bmod 8, \\ 0 & \text{otherwise,} \end{cases} \tag{7.1}$$

and note that Theorem 3 is equivalent to the estimate

$$\sum_{p \leqslant X} b_p \ll X^{1-\delta'}.$$

Throughout, we fix a primitive 16th root of unity ζ_{16} and we set $\zeta_8 = \zeta_{16}^2$, $i = \zeta_8^2$, $\sqrt{-2} = \zeta_8 + \zeta_8^3$, and $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$. As stated in the discussion prior to the statement of Theorem 3, for a prime number $p \equiv 1 \bmod 4$, we have $h^+(8p) \equiv 0 \bmod 8$ if and only if p splits completely in the number field

$$M' = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2}).$$

Since $1 + i = \zeta_8\sqrt{2}$, we have $M = \mathbb{Q}(\zeta_8, \sqrt{1+i}) = \mathbb{Q}(\zeta_8, \zeta_{16}\sqrt[4]{2})$, and so $M \subset M'$ is a quadratic extension, generated by $\sqrt{\zeta_8}$. We now use a criterion of Kaplan and Williams [KW84, p. 26]. Suppose that $p \equiv 1 \bmod 8$, i.e., that $h^+(8p) \equiv 0 \bmod 4$. Then we can write

$$p = a^2 + b^2 = c^2 + 2d^2, \tag{7.2}$$

with $a, b, c, d \in \mathbb{Z}$. After possibly interchanging a and b, we can guarantee that a is odd. Replacing a by $-a$ and c by $-c$ is necessary, we can then ensure that

$$a \equiv c \equiv 1 \bmod 4. \tag{7.3}$$

Assume now that $h^+(8p) \equiv 0 \bmod 8$, i.e., that p splits completely in $M'/\mathbb{Q}$; this forces the congruence conditions [KW84, p. 23]

$$a \equiv c \equiv 1 \bmod 8, \quad b \equiv 0 \bmod 8, \quad d \equiv 0 \bmod 4.$$

With b_p defined as in (7.1), and with α and β as on [KW84, p. 26], we have

$$b_p = \alpha\beta = (-1)^{(a-1+b+2d+h(-4p))/8}.$$

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

As $M \subset M'$, it must be that $h(-4p) \equiv 0 \bmod 8$, so that with a_p as in the statement of Theorem 2, we get

$$b_p = (-1)^{(a-1+b+2d)/8} a_p. \tag{7.4}$$

In light of (6.8), it remains to express the factor $(-1)^{(a-1+b+2d)/8}$ in terms of a generator ϖ for an ideal in $\mathcal{O}_M$ lying above p. The main difficulty here lies in the sensitivity of the formula (7.4) to the conditions (7.3). Note that

$$(-1)^{(a-1+b)/8} = \begin{cases} 1 & \text{if } a+b-1 \equiv 0 \bmod 16, \\ -1 & \text{if } a+b-1 \equiv 8 \bmod 16, \end{cases}$$

and

$$(-1)^{d/4} = \begin{cases} 1 & \text{if } d \equiv 0 \bmod 8, \\ -1 & \text{if } d \equiv 4 \bmod 8. \end{cases}$$

The only units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1, so if $\mathrm{N}_{M/\mathbb{Q}(\sqrt{-2})}(\varpi) = c' + d'\sqrt{-2}$, we must have either $(c', d') = (c, d)$ or $(c', d') = (-c, -d)$. Note that $d \equiv 0 \bmod 8$ if and only if $-d \equiv 0 \bmod 8$, and also $d \equiv 4 \bmod 8$ if and only if $-d \equiv 4 \bmod 8$. Hence, the factor $(-1)^{d/4}$ in (7.4) is always equal to $(-1)^{d'/4}$.

The situation for $\mathbb{Z}[i]$ is slightly more complicated. Suppose $\mathrm{N}_{M/\mathbb{Q}(i)}(\varpi) = a' + b'i$. Define $e(\varpi) \in \{\pm 1\}$ by the equation

$$a' + b' \equiv e(\varpi) \bmod 4.$$

Since $p = a'^2 + b'^2 \equiv 1 \bmod 8$, one of a' and b' must be congruent to 0 mod 4, and the other is then congruent to $e(\varpi)$ mod 4. If $e(\varpi) = 1$, then either (a', b') or (b', a') satisfies the same conditions as (a, b) in (7.2) and (7.3), and so $(-1)^{(a-1+b)/8} = (-1)^{(a'+b'-1)/8}$. If $e(\varpi) = -1$, then either $(-a', -b')$ or $(-b', -a')$ satisfies the same conditions as (a, b) in (7.2) and (7.3), and so $(-1)^{(a-1+b)/8} = (-1)^{(-a'-b'-1)/8} = (-1)^{(a'+b'+1)/8}$. In any case, $(-1)^{(a-1+b)/8} = (-1)^{(a'+b'-e(\varpi))/8}$, so that

$$b_p = (-1)^{(a'+b'-e(\varpi)+2d')/8} a_p. \tag{7.5}$$

Note that the formula (7.5) holds regardless of the congruence classes of a', b', and d'. In other words, we have managed to remove the dependence of the formula for b_p on conditions of the shape (7.3).

Now let α be *any* odd element in $\mathcal{O}_M$, not necessarily an element of norm p. We define $a'', b'', c'', d'' \in \mathbb{Z}$, and $e(\alpha) \in \{\pm 1\}$ via equations

$$\mathrm{N}_{M/\mathbb{Q}(i)}(\alpha) = a'' + b''i, \quad \mathrm{N}_{M/\mathbb{Q}(\sqrt{-2})}(\alpha) = c'' + d''\sqrt{-2}, \quad a'' + b'' = e(\alpha) \bmod 4. \tag{7.6}$$

Let ρ be an invertible congruence class modulo F. Define

$$\psi_t(\rho) = \frac{1}{2}\left(\exp\left(\frac{\pi i}{8}(a'' + b'' - e(\alpha))\right) + \exp\left(-\frac{\pi i}{8}(a'' + b'' - e(\alpha))\right)\right)\exp\left(\frac{\pi i}{4}d''\right), \tag{7.7}$$

where α is any element of $\mathcal{O}_M$ such that $\alpha \equiv \rho \bmod F$ and a'', b'', d'', and $e(\alpha)$ are defined via the equations (7.6); this is well-defined since F is divisible by 16 and $\exp(2\pi i) = 1$. Finally, we define

$$\psi_{M'}(\rho) = \left(\frac{\zeta_8}{\alpha}\right)_M, \tag{7.8}$$

where α is any element of $\mathcal{O}_M$ such that $\alpha \equiv \rho \bmod F$; this is well-defined by Lemma 3.2.

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

Suppose $\alpha \in \mathcal{O}_M$ is coprime to F, and suppose $\beta \in \mathcal{O}_M^\times$. Again, it is clear that

$$\psi_{M'}(\alpha\beta^2 \bmod F) = \psi_{M'}(\alpha \bmod F).$$

Furthermore, because $\mathrm{N}_{M/\mathbb{Q}(i)}(\beta^2) = \mathrm{N}_{M/\mathbb{Q}(i)}(\beta)^2 \in \{\pm 1\}$ and $\mathrm{N}_{M/\mathbb{Q}(\sqrt{-2})}(\beta^2) = \mathrm{N}_{M/\mathbb{Q}(\sqrt{-2})}(\beta)^2 = 1$, and because of the symmetry in (7.7) with respect to the transformation $(a'' + b'' - e(\alpha)) \mapsto -(a'' + b'' - e(\alpha))$, we also have $\psi_t(\alpha\beta^2 \bmod F) = \psi_t(\alpha \bmod F)$.

Finally, with ψ_0 defined as in (6.6), we define two functions ψ_1, ψ_2 on $(\mathcal{O}_M/F\mathcal{O}_M)^\times$ by setting

$$\psi_1(\rho) = \psi_0(\rho)\psi_t(\rho) \tag{7.9}$$

and

$$\psi_2(\rho) = \psi_0(\rho)\psi_t(\rho)\psi_{M'}(\rho). \tag{7.10}$$

Now suppose p splits completely in $M/\mathbb{Q}$ and let ϖ be any prime in $\mathcal{O}_M$ of norm p. Since $M' = M(\sqrt{\zeta_8})$, we have

$$\frac{1}{2}\left(1 + \left(\frac{\zeta_8}{\varpi}\right)_M\right) = \begin{cases} 1 & \text{if } p \text{ splits completely in } M'/\mathbb{Q}, \\ 0 & \text{otherwise,} \end{cases}$$

so this can be detected by $\psi_{M'}$ for p coprime to F. With a'', b'', and d'' defined as in (7.6) with $\alpha = \varpi$, we always have $a'' + b'' - e(\varpi) \equiv 0 \bmod 8$; as $\exp(\pi i) = \exp(-\pi i)$, we have

$$\psi_t(\varpi) = \exp\left(\frac{\pi i}{8}(a'' + b'' - e(\varpi) + 2d'')\right) = (-1)^{(a''+b''-e(\varpi)+2d'')/8}.$$

Hence, from (7.5) and Proposition 6.2, supposing also that $(p, F) = 1$, we obtain

$$b_p = \tfrac{1}{2}(\psi_1(\varpi \bmod F) + \psi_2(\varpi \bmod F))[\varpi]_r. \tag{7.11}$$

Now, with ψ_1 and ψ_2 as in (7.9) and (7.10), respectively, we set $\psi = \psi_1$ (respectively $\psi = \psi_2$) and define $s_{1,\mathfrak{a}}$ (respectively $s_{2,\mathfrak{a}}$) as in (1.3). If $(p, F) = 1$, p splits completely in $M/\mathbb{Q}$, and $\mathfrak{p}$ is any prime ideal in $\mathcal{O}_M$ lying above p, then (7.11) implies that

$$b_p = \tfrac{1}{2}(s_{1,\mathfrak{p}} + s_{2,\mathfrak{p}}). \tag{7.12}$$

By the same argument as at the end of § 6, Theorem 1 applied to the sequences $\{s_{1,\mathfrak{a}}\}_{\mathfrak{a}}$ and $\{s_{2,\mathfrak{a}}\}_{\mathfrak{a}}$ proves Theorem 3.

8. Proof of Theorem 5

We start by recalling a criterion due to Bruin and Hemenway [BH13, Theorem B, p. 66]. Suppose p is a prime number that splits completely in $M/\mathbb{Q}$ and let ϖ be a prime in $\mathcal{O}_M$ of absolute norm p. Then

$$\left(\frac{\zeta_8 \cdot r(\varpi)r^2(\varpi)sr(\varpi)sr^2(\varpi) \cdot \sqrt{1+i}}{\varpi}\right)_M = -1 \Longrightarrow (\mathbb{Z}/4\mathbb{Z})^2 \hookrightarrow Ш(E_p)$$

(the right-hand side implies that $p \in W(3)\backslash W(2)$, where $W(e)$ is defined in [BH13, p. 65]; see also [BH13, Corollary 2.2, p. 67]). The above product differs from the product in (6.4) only by

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press

the factor $\left(\frac{\zeta_8}{\varpi}\right)_M$. We thus define $\psi : (\mathcal{O}_M/F\mathcal{O}_M)^\times \to \mathbb{C}$ by

$$\psi(\rho) = \psi_0(\rho)\psi_{M'}(\rho),$$

where ψ_0 is as in (6.6) and $\psi_{M'}$ is as in (7.8). Theorem 1 applied to the sequence $\{s_{\mathfrak{a}}\}_{\mathfrak{a}}$, defined as in (1.3) with ψ as above, now gives the desired result.

Acknowledgements

The authors would like to thank Jan-Hendrik Evertse, Étienne Fouvry, Zev Klagsbrun, Carlo Pagano, and Peter Stevenhagen for useful discussions related to this work. The first author is a doctoral student at Leiden University. The second author was also supported by an ALGANT Erasmus Mundus Scholarship and the National Science Foundation agreement No. DMS-1128155 for part of this research.

References

BH13 N. Bruin and B. Hemenway, *On congruent primes and class numbers of imaginary quadratic fields*, Acta Arith. **159** (2013), 63–87.

Bur62 D. A. Burgess, *On character sums and primitive roots*, Proc. Lond. Math. Soc. (3) **12** (1962), 179–192.

Bur63 D. A. Burgess, *On character sums and L-series. II*, Proc. Lond. Math. Soc. (3) **13** (1963), 524–536.

CL83 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** (1983), 711–730.

CL84 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*, Colloq. Math. Soc. János Bolyai, vol. 34 (North-Holland, Amsterdam, 1984), 257–280.

FK07 É. Fouvry and J. Klüners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), 455–513.

FK10a É. Fouvry and J. Klüners, *On the negative Pell equation*, Ann. of Math. (2) **172** (2010), 2035–2104.

FK10b É. Fouvry and J. Klüners, *On the Spiegelungssatz for the 4-rank*, Algebra Number Theory **4** (2010), 493–508.

FK10c É. Fouvry and J. Klüners, *The parity of the period of the continued fraction of* $\sqrt{d}$, Proc. Lond. Math. Soc. (3) **101** (2010), 337–391.

FK11 É. Fouvry and J. Klüners, *Weighted distribution of the 4-rank of class groups and applications*, Int. Math. Res. Not. IMRN **11** (2011), 3618–3656.

FIMR13 J. B. Friedlander, H. Iwaniec, B. Mazur and K. Rubin, *The spin of prime ideals*, Invent. Math. **193** (2013), 697–749.

FIMR15 J. B. Friedlander, H. Iwaniec, B. Mazur and K. Rubin, *Erratum to: The spin of prime ideals*, Invent. Math. **202** (2015), 923–925.

FI98 J. Friedlander and H. Iwaniec, *The polynomial* $X^2 + Y^4$ *captures its primes*, Ann. of Math. (2) **148** (1998), 945–1040.

Hea93 D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), 171–195.

Hea94 D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), 331–370; with an appendix by P. Monsky.

Kap77 P. Kaplan, *Cycles d'ordre au moins 16 dans le 2-groupe des classes d'idéaux de certains corps quadratiques*, Bull. Soc. Math. France Mém. **49–50** (1977), 113–124; utilisation des calculateurs en mathématiques pures (Conf., Limoges, 1975).

KW82 P. Kaplan and K. S. Williams, *On the class numbers of* $\mathbb{Q}(\sqrt{\pm 2p})$ *modulo 16, for* $p \equiv 1 \pmod 8$ *a prime*, Acta Arith. **40** (1981/82), 289–296.

KW84 P. Kaplan and K. S. Williams, *On the strict class number of* $\mathbb{Q}(\sqrt{2p})$ *modulo 16,* $p \equiv 1 \pmod 8$ *prime*, Osaka J. Math. **21** (1984), 23–29.

KWH86 P. Kaplan, K. S. Williams and K. Hardy, *Divisibilité par 16 du nombre des classes au sens strict des corps quadratiques réels dont le deux-groupe des classes est cyclique*, Osaka J. Math. **23** (1986), 479–489.

KM18 P. Koymans and D. Milovic, *On the 16-rank of class groups of* $\mathbb{Q}(\sqrt{-2p})$ *for primes* $p \equiv 1 \bmod 4$, Int. Math. Res. Not. IMRN (2018), rny010.

Lan86 S. Lang, *Algebraic number theory*, second edition (Springer, New York, 1986).

LW82 P. A. Leonard and K. S. Williams, *On the divisibility of the class numbers of* $\mathbb{Q}(\sqrt{-p})$ *and* $\mathbb{Q}(\sqrt{-2p})$ *by 16*, Canad. Math. Bull. **25** (1982), 200–206.

Mil17a D. Milovic, *The infinitude of* $\mathbb{Q}(\sqrt{-p})$ *with class number divisible by 16*, Acta Arith. **178** (2017), 201–233.

Mil17b D. Milovic, *On the 16-rank of class groups of* $\mathbb{Q}(\sqrt{-8p})$ *for* $p \equiv -1 \bmod 4$, Geom. Funct. Anal. **27** (2017), 973–1016.

Mil18 D. Milovic, *On the* 8*-rank of narrow class groups of* $\mathbb{Q}(\sqrt{-4pq})$, $\mathbb{Q}(\sqrt{-8pq})$ *and* $\mathbb{Q}(\sqrt{8pq})$, Int. J. Number Theory **14** (2018), 2165–2193.

Ori78 B. Oriat, *Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques* $Q(\sqrt{2p})$ *et* $Q(\sqrt{-2})$, J. Math. Soc. Japan **30** (1978), 279–285.

Red34 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** (1934), 55–60.

Rei34 H. Reichardt, *Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. **170** (1934), 75–82.

Sch35 A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. **39** (1935), 95–111.

Ser12 J.-P. Serre, *Lectures on* $N_X(p)$, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11 (CRC Press, Boca Raton, FL, 2012).

Smi16 A. Smith, *Governing fields and statistics for 4-Selmer groups and 8-class groups*, Preprint (2016), arXiv:1607.07860.

Smi17 A. Smith, 2^∞*-Selmer groups,* 2^∞*-class groups, and Goldfeld's conjecture*, Preprint (2017), arXiv:1702.02325.

Ste89 P. Stevenhagen, *Ray class groups and governing fields*, in *Théorie des nombres, Année 1988/89, Fasc. 1*, Publications Mathématiques de la Faculté des Sciences de Besançon (Université de Franche-Comté, Faculté des Sciences, Besançon, 1989).

Ste93a P. Stevenhagen, *Divisibility by 2-powers of certain quadratic class numbers*, J. Number Theory **43** (1993), 1–19.

Ste93b P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Experiment. Math. **2** (1993), 121–136.

Vau77 R.-C. Vaughan, *Sommes trigonométriques sur les nombres premiers*, C. R. Acad. Sci. Paris Sér. A-B **983** (1977), A981–A983.

Vin47 I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Trav. Inst. Math. Stekloff **23** (1947).

Vin54 I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers* (Dover Publications, Mineola, NY, 2004); translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, reprint of the 1954 translation.

Wid10 M. Widmer, *Counting primitive points of bounded height*, Trans. Am. Math. Soc. **362** (2010), 4793–4829.

Yam84 Y. Yamamoto, *Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic*, Osaka J. Math. **21** (1984), 1–22.

P. Koymans p.h.koymans@math.leidenuniv.nl
Mathematisch Instituut, Universiteit Leiden, Niels Bohrweg 1,
2333 CA Leiden, The Netherlands

D. Z. Milovic djordjo.milovic@ucl.ac.uk
Department of Mathematics, University College London, Gower Street,
London WC1E 6BT, UK

https://doi.org/10.1112/S0010437X18007601 Published online by Cambridge University Press