ACTA ARITHMETICA
202.1 (2022)

On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-3p})$ for primes p congruent to 1 modulo 4

by

Margherita Piccolo (Düsseldorf)

1. Introduction. The study of the 2-parts of the class groups of quadratic number fields is an active area of research. We recall that, for $k \in \mathbb{N}$, the 2^k-rank of a finite abelian group G is the dimension of the $\mathbb{F}_2$-vector space $2^{k-1}G/2^kG$. Milovic [M17] studied the density for the 16-rank in certain particular thin families of quadratic number fields. Koymans and Milovic [KM19a], [KM19b] proved density results for the 16-rank in families of imaginary quadratic number fields of the form $\mathbb{Q}(\sqrt{-p})$ for primes p and $\mathbb{Q}(\sqrt{-2p})$ for primes p congruent to 1 modulo 4.

These results are in line with Gerth's conjecture [G87], which extends a conjecture of Cohen and Lenstra [CL84] to include the 2-part. It is expected that the group $2\,\mathrm{Cl}(K)[2^\infty]$ satisfies the Cohen–Lenstra heuristic, where K varies over imaginary quadratic number fields and $\mathrm{Cl}(K)[2^\infty]$ denotes the 2-part of the class group $\mathrm{Cl}(K)$. More recently, Smith [S] proved Gerth's conjecture and gave a new powerful method to study the 2-part of class groups, but it is uncertain whether this new method is applicable to *thin* families that we are about to consider.

Our aim is to continue the work of Koymans and Milovic, by proving results for the 16-rank of the class groups of *thin* families of imaginary quadratic number fields. The first natural case to consider is $\mathbb{Q}(\sqrt{-3p})$, in accordance with the title of the article. For technical reasons, we restrict ourselves to primes p congruent to 1 modulo 4, so that only two primes divide the discriminant. In this situation, we find that the 2-part of the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-3p}))$ is non-trivial and cyclic, by Gauss genus theory.

2020 *Mathematics Subject Classification*: Primary 11N45, 11R29; Secondary 11R44, 11N36.
Key words and phrases: class groups, asymptotic results, sieve methods.
Received 22 April 2020; revised 13 April 2021.
Published online 3 December 2021.

DOI: 10.4064/aa200422-9-6

Our approach to $\mathbb{Q}(\sqrt{-3p})$ extends to families $K_{p,q} := \mathbb{Q}(\sqrt{-qp})$ with fixed $q \in Q := \{3, 7, 11, 19, 43, 67, 163\}$ and p varying over all primes congruent to 1 modulo 4. The elements in Q are the complete list of primes q congruent to 3 modulo 4 such that the field $\mathbb{Q}(\sqrt{-1}, \sqrt{q})$ is a principal ideal domain (see [U86]). These conditions are useful in the technical considerations of the analytic part of our work.

Our main result is the following.

THEOREM 1.1. *Let $q \in \{3, 7, 11, 19, 43, 67, 163\}$ be fixed. For primes p, let $h(-qp)$ denote the class number of the imaginary quadratic number field $K_{p,q} = \mathbb{Q}(\sqrt{-qp})$. For each prime p congruent to 1 modulo 4, set*

$$e_p = \begin{cases} 1 & \textit{if } 16 \mid h(-qp), \\ -1 & \textit{if } 8 \mid h(-qp) \textit{ but } 16 \nmid h(-qp), \\ 0 & \textit{otherwise.} \end{cases}$$

Then

$$\sum_{\substack{p \le x \\ p \equiv 1 \bmod 4}} e_p \ll x^{1-1/3200} \qquad \textit{for } x > 0.$$

In the theorem, $\ll$ denotes the Vinogradov symbol for $O(\ )$.

We will see in §3.3 that the numbers e_p are not always zero and so our result shows that the sequence e_p oscillates as p varies. Indeed, if 8 divides the class number, 16 divides it approximately half of the time.

COROLLARY 1.2. *Let $q \in \{3, 7, 11, 19, 43, 67, 163\}$. Then the limit*

$$\delta(16) := \lim_{x\to\infty} \frac{\#\{p \le x : p \equiv 1 \bmod 4,\ 16 \mid h(-pq)\}}{\#\{p \le x : p \equiv 1 \bmod 4\}}$$

exists and $\delta(16) = 1/8$.

The main tool we use is the generalized version of Vinogradov's method in the setting of number fields, given by Friedlander et al. [FIMR13], similarly to the works of Koymans and Milovic [KM19a], [KM19b]. Moreover, as in [KM19a], our results are unconditional, in contrast to the work of Friedlander et al. [FIMR13], which uses a conjecture on short character sums.

The key ingredient of our argument is a sequence, defined in §3.5, that encodes when 16 divides the class number of $K_{p,q}$. We carry out careful estimation of the so-called sums of type I and sums of type II that are needed to use Vinogradov's method.

2. Prerequisites

2.1. Hilbert symbols and nth power residue symbol. Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. Let n be a natural number and denote by μ_n the group of nth roots of unity in $\mathbb{C}$. Let $K_\mathfrak{p}$ be the completion of K with respect to a finite prime $\mathfrak{p}$ of K. We assume that $K_{\mathfrak{p}}^{\times}$ contains a primitive nth root of unity. Then $L_{\mathfrak{p}} := K_{\mathfrak{p}}(\sqrt[n]{K_{\mathfrak{p}}^{\times}})$ is the maximal abelian extension of exponent n of $K_{\mathfrak{p}}$, by Kummer theory.

We employ the notation of [N99, Chapter V, §3]. The nth Hilbert symbol is the non-degenerate bilinear pairing

$$\left(\frac{\ ,\ }{\mathfrak{p}}\right)_{K,n} : K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^n \times K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^n \to \mu_n, \qquad (a,b) \mapsto \frac{\sigma_a(\sqrt[n]{b})}{\sqrt[n]{b}},$$

where σ_a is the corresponding element of a in $\mathrm{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}})$, given by the isomorphism $K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^n \cong \mathrm{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}})$ of class field theory. We recall basic properties of this symbol; see [N99, Chapter V, §3, Proposition 3.2].

PROPOSITION 2.1. *For all $a, a', b, b' \in K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^n$, the nth Hilbert symbol has the following properties:*

(i) $\left(\frac{aa',b}{\mathfrak{p}}\right)_{K,n} = \left(\frac{a,b}{\mathfrak{p}}\right)_{K,n}\left(\frac{a',b}{\mathfrak{p}}\right)_{K,n}$,
(ii) $\left(\frac{a,bb'}{\mathfrak{p}}\right)_{K,n} = \left(\frac{a,b}{\mathfrak{p}}\right)_{K,n}\left(\frac{a,b'}{\mathfrak{p}}\right)_{K,n}$,
(iii) $\left(\frac{a,b}{\mathfrak{p}}\right)_{K,n} = 1 \Leftrightarrow a$ *lies in the image of the norm map of the extension* $K_{\mathfrak{p}}(\sqrt[n]{b})/K_{\mathfrak{p}}$,
(iv) $\left(\frac{a,b}{\mathfrak{p}}\right)_{K,n} = \left(\frac{b,a}{\mathfrak{p}}\right)_{K,n}^{-1}$,
(v) $\left(\frac{a,1-a}{\mathfrak{p}}\right)_{K,n} = 1$ *and* $\left(\frac{a,-a}{\mathfrak{p}}\right)_{K,n} = 1$,
(vi) *if* $\left(\frac{a,b}{\mathfrak{p}}\right)_{K,n} = 1$ *for all* $b \in K_{\mathfrak{p}}^{\times}$, *then* $a \in K_{\mathfrak{p}}^{\times n}$.

Let $\mathfrak{p}$ be a finite prime of K that does not divide n and let a be an invertible element of the valuation ring of $K_{\mathfrak{p}}$. Denote by N the norm of the prime ideal $\mathfrak{p}$ i.e. $N := \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$. The nth power residue symbol $\left(\frac{a}{\mathfrak{p}}\right)_{K,n} \in \mu_n$ is defined by the congruence

$$\left(\frac{a}{\mathfrak{p}}\right)_{K,n} \equiv a^{\frac{N-1}{n}} \bmod \mathfrak{p}. \tag{2.1}$$

For every odd ideal $\mathfrak{b}$ of $\mathcal{O}_K$ (i.e. coprime to 2) that is coprime to n, and every element $a \in \mathcal{O}_K$ coprime to $\mathfrak{b}$, i.e. $\gcd((a), \mathfrak{b}) = (1)$, we define the nth power residue symbol by

$$\left(\frac{a}{\mathfrak{b}}\right)_{K,n} := \prod_{\mathfrak{p}|\mathfrak{b}} \left(\frac{a}{\mathfrak{p}}\right)_{K,n}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})} \tag{2.2}$$

and we set $\left(\frac{a}{\mathfrak{b}}\right)_{K,n} = 0$ if a is not coprime to $\mathfrak{b}$.

For $b \in \mathcal{O}_K$, we define

$$\left(\frac{a}{b}\right)_{K,n} := \left(\frac{a}{b\,\mathcal{O}_K}\right)_{K,n}. \tag{2.3}$$

For $K = \mathbb{Q}$ we omit the subscript K.

2.2. Quartic reciprocity. The quadratic and the quartic residue symbols will be the ones that we will use the most. Since we will work in the field $M_q := \mathbb{Q}(\sqrt{-1}, \sqrt{q})$, for $q \in Q$ where $Q = \{3, 7, 11, 19, 43, 67, 163\}$, we will state a weak version of the quartic reciprocity law in this setting.

Lemma 2.2. *Let $a, b \in \mathcal{O}_{M_q}$ with b odd. If we fix a, then $\left(\frac{a}{b}\right)_{M_q,4}$ depends only on the congruence class of b modulo $32a\mathcal{O}_{M_q}$. Moreover, if a is odd, then*

$$\left(\frac{a}{b}\right)_{M_q,4} = \mu \cdot \left(\frac{b}{a}\right)_{M_q,4},$$

where $\mu \in \{\pm 1, \pm i\}$ depends only on the congruence classes of a and b modulo $32\mathcal{O}_{M_q}$.

Proof. First, let us focus on the second part of the lemma and fix $a \in \mathcal{O}_{M_q}$. If a and b are not coprime to each other, then on both sides of the identity we have 0. Now, suppose that they are coprime to each other and that $q \neq 7$. Using [N99, Chapter VI, §8, Theorem 8.3], we get

$$\left(\frac{a}{b}\right)_{M_q,4} = \left(\frac{b}{a}\right)_{M_q,4} \cdot \left(\frac{a, b}{\mathfrak{I}}\right)_{M_q,4},$$

where $\mathfrak{I}$ denotes the ideal $(1+i)$ of M_q. Note that the infinite places do not contribute in this product, since the field M_q is totally complex.

We prove that $\left(\frac{a,b}{\mathfrak{I}}\right)_{M_q,4}$ depends only on a and b modulo 32. If $a \equiv 1 \bmod 32$, where $a \in \mathcal{O}_{(M_q)_\mathfrak{I}}$, then a is a fourth power in $(M_q)_\mathfrak{I}$ by Hensel's lemma. So we deduce that $\left(\frac{a,b}{\mathfrak{I}}\right)_{M_q,4} = 1$ applying Proposition 2.1(iii). If b is congruent to 1 modulo 32, then we get the same result using Proposition 2.1(iii, iv). If neither a nor b is congruent to 1 modulo 32, let a' and b' be different from a and b respectively and such that $a \equiv a' \bmod 32$ and $b \equiv b' \bmod 32$. Then $a = \gamma a'$ and $b = \tilde{\gamma} b'$ with $\gamma, \tilde{\gamma}$ congruent to 1 modulo 32. Using Proposition 2.1(i, ii), we get

$$\begin{aligned}\left(\frac{a, b}{\mathfrak{I}}\right)_{M_q,4} &= \left(\frac{\gamma a', \tilde{\gamma} b'}{\mathfrak{I}}\right)_{M_q,4} = \left(\frac{\gamma, \tilde{\gamma} b'}{\mathfrak{I}}\right)_{M_q,4} \left(\frac{a', \tilde{\gamma}}{\mathfrak{I}}\right)_{M_q,4} \left(\frac{a', b'}{\mathfrak{I}}\right)_{M_q,4} \\ &= \left(\frac{a', b'}{\mathfrak{I}}\right)_{M_q,4}.\end{aligned}$$

In the case of $q = 7$, we have two different prime ideals $\mathfrak{I}_1$ and $\mathfrak{I}_2$, in M_7 above 2. So we have

$$\left(\frac{a}{b}\right)_{M_7,4} = \left(\frac{b}{a}\right)_{M_7,4} \left(\frac{a, b}{\mathfrak{I}_1}\right)_{M_7,4} \left(\frac{a, b}{\mathfrak{I}_2}\right)_{M_7,4}.$$

Nonetheless, we can use the same argument as before, taking into account that we have two different prime ideals above 2 instead of just one.

Now, let us prove that $(a/b)_{M_q,4}$ depends only on the congruence class of b modulo $32a\mathcal{O}_{M_q}$. Using [N99, Chapter VI, §8, Theorem 8.3], we obtain

$$\left(\frac{a}{b}\right)_{M_q,4} = \prod_{\mathfrak{p}\notin S(a)} \left(\frac{b,a}{\mathfrak{p}}\right)_{M_q,4} = \prod_{\mathfrak{p}\in S(a)} \left(\frac{a,b}{\mathfrak{p}}\right)_{M_q,4},$$

where $S(a) := \{\mathfrak{p} : \mathfrak{p} \mid n\cdot\infty \text{ or } \mathrm{ord}_{\mathfrak{p}}(a) \neq 0\}$.

As for the prime ideal $\mathfrak{I}$, we already saw that $\left(\frac{a,b}{\mathfrak{I}}\right)_{M_q,4}$ depends only on b modulo 32 (and the same holds for $\mathfrak{I}_1$ and $\mathfrak{I}_2$ in the case of $q = 7$). If $\mathfrak{p} \in S(a)$ is odd, we have

$$\left(\frac{a,b}{\mathfrak{p}}\right)_{M_q,4} = \left(\frac{b}{\mathfrak{p}}\right)_{M_q,4}^{\mathrm{ord}_{\mathfrak{p}}(a)}.$$

Hence the value of these symbols depends only on b modulo a. Therefore the total symbol depends only on b modulo $32a$. ■

2.3. Field lowering. For the reader's convenience, we state three lemmas that we will use in the proof of Theorem 1.1, reducing the quartic residue symbol in a quartic number field to a quadratic residue symbol in a quadratic number field. These lemmas are stated and proved in [KM19a, §3.2].

LEMMA 2.3. *Let K be a number field and let $\mathfrak{p}$ be an odd prime ideal of $\mathcal{O}_K$. Suppose that L is a quadratic extension of K such that L contains $\mathbb{Q}(\sqrt{-1})$ and $\mathfrak{p}$ splits in L. Denote by ψ the non-trivial element in* $\mathrm{Gal}(L/K)$*. Then if ψ fixes $\mathbb{Q}(\sqrt{-1})$, for all $\alpha \in \mathcal{O}_K$ we have*

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

and if ψ does not fix $\mathbb{Q}(\sqrt{-1})$, for all $\alpha \in \mathcal{O}_K$ with $\mathfrak{p} \nmid \alpha$ we have

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

LEMMA 2.4. *Let K be a number field and let $\mathfrak{p}$ be an odd prime ideal of $\mathcal{O}_K$ of degree 1 lying above p. Suppose that L is a quadratic extension of K such that L contains i and $\mathfrak{p}$ stays inert in L. For all $\alpha \in \mathcal{O}_K$ we have*

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

LEMMA 2.5. *Let K be a number field and let L be a quadratic extension of K. Denote by ψ the non-trivial element in* $\mathrm{Gal}(L/K)$*. Suppose that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ that does not ramify in L and further suppose that $\beta \in \mathcal{O}_L$ satisfies $\beta \equiv \psi(\beta) \bmod \mathfrak{p}\mathcal{O}_L$. Then there is $\beta' \in \mathcal{O}_K$ such that $\beta' \equiv \beta \bmod \mathfrak{p}\mathcal{O}_L$.*

3. The 2-part of the class group. Let $k \geq 1$ be an integer. The 2^k-rank of a finite abelian group G, denoted by $\mathrm{rk}_{2^k} G$, is the dimension of the $\mathbb{F}_2$-vector space $2^{k-1}G/2^kG$. If the 2-Sylow subgroup of G is cyclic, we have $\mathrm{rk}_{2^k} G \in \{0,1\}$ and $\mathrm{rk}_{2^k} G = 1$ if and only if $2^k \mid \#G$. We will study the necessary and sufficient conditions for $2^k \mid h(-qp)$ for $k \in \{1,2,3,4\}$. Moreover, for each $k \geq 1$ and any fixed $q \in Q$ where $Q = \{3,7,11,19,43,67,163\}$, we define a density $\delta(2^k)$ as

$$\delta(2^k) := \lim_{x\to\infty} \frac{\#\{p \leq x : p \equiv 1 \bmod 4,\ 2^k \mid \# \mathrm{Cl}(K_{p,q})\}}{\#\{p \leq x : p \equiv 1 \bmod 4\}},$$

if the limit exists.

3.1. The 2-rank. The discriminant $D_{K_{p,q}}$ of the extension $K_{p,q} = \mathbb{Q}(\sqrt{-qp})$ is equal to $-qp$, where $q \in Q$ and p is a prime congruent to 1 modulo 4. Then, by Gauss genus theory, we have $|\mathrm{Cl}(K_{p,q})[2]| = 2$ and so $\delta(2) = 1$. In particular, it follows that the 2-Sylow subgroup $\mathrm{Cl}(K_{p,q})[2^\infty]$ of the class group is cyclic, as it is an abelian 2-group with just one non-trivial element of order 2. We describe it as

$$\mathrm{Cl}(K_{p,q})[2] = \langle [\mathfrak{t}], [\mathfrak{p}] \rangle,$$

where $\mathfrak{t}$ is the prime ideal above q and $\mathfrak{p}$ is the prime ideal above p in $K_{p,q}$.

3.2. The 4-rank. For the 4-rank of the class group of $K_{p,q}$, we look for an element of order 4. We have $\mathrm{rk}_4 \mathrm{Cl}(K_{p,q}) = 1$ if and only if the map

$$\varphi : \mathrm{Cl}(K_{p,q})[2] \to \mathrm{Cl}(K_{p,q})/2\,\mathrm{Cl}(K_{p,q})$$

is the zero map. By class field theory, the genus field H_2 is the field $K_{p,q}(\sqrt{-q})$ and we have

$$\mathrm{Cl}(K_{p,q})/2\,\mathrm{Cl}(K_{p,q}) \cong \mathrm{Gal}(H_2/K_{p,q}).$$

So the map φ is trivial if and only if the Artin symbol corresponding to $\mathfrak{p}$, the prime ideal above p (or analogously the one corresponding to $\mathfrak{t}$), is trivial. It is equivalent to say that $\mathfrak{p}$ (or analogously $\mathfrak{t}$) splits completely in $K_{p,q} \subset H_2$. This is the same as asking that p splits completely in $\mathbb{Q}(\sqrt{-q})$ (or analogously that q splits completely in $\mathbb{Q}(\sqrt{p})$). Then we have

$$4 \mid h(-qp) \iff \left(\frac{-q}{p}\right) = 1 \iff \left(\frac{p}{q}\right) = 1.$$

So, the 4-rank is 1 if and only if p splits completely in $\mathbb{Q}(\sqrt{-1}, \sqrt{-q})$. Using the Chebotarev Density Theorem, we obtain $\delta(4) = 1/2$.

3.3. The 8-rank. We have an element of order 8 in the class group if and only if the map

$$\psi : \mathrm{Cl}(K_{p,q})[2] \to \mathrm{Cl}(K_{p,q})/4\,\mathrm{Cl}(K_{p,q})$$

is the zero map. Again, by class field theory, we have an extension H_4 of $K_{p,q}$, called the 4-Hilbert class field, that is contained in the Hilbert class field $H(K_{p,q})$. The field H_4 is such that $\mathrm{Gal}(H_4/K_{p,q}) \cong \mathrm{Cl}(K_{p,q})/4\,\mathrm{Cl}(K_{p,q})$. The map ψ is trivial if and only if the Artin symbol of $\mathfrak{p}$ (resp. of $\mathfrak{t}$) of the extension $K_{p,q} \subset H_4$ is trivial, which corresponds to asking that $\mathfrak{p}$ (resp. $\mathfrak{t}$) splits completely in H_4. We choose to work with the prime q, but it is symmetric to the prime p.

Since q ramifies in $\mathbb{Q}(\sqrt{-q})$, it is equivalent to ask that $(\sqrt{-q})$ splits completely in the extension $\mathbb{Q}(\sqrt{-q}) \subset H_4$. Let $F := \mathbb{Q}(\sqrt{-q})$. We have

$$\begin{tikzcd}
& H_4 \arrow[d, dash] & \\
& H_2 = \mathbb{Q}(\sqrt{-q}, \sqrt{p}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
F = \mathbb{Q}(\sqrt{-q}) \arrow[dr, dash] & K_{p,q} = \mathbb{Q}(\sqrt{-qp}) \arrow[d, dash] & \mathbb{Q}(\sqrt{p}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

The extension $F \subset H_4$ is abelian of order 4 and exponent 2. The only primes that ramify are the ones over p, say $\mathfrak{p}_1$ and $\mathfrak{p}_2$; they are tamely ramified of ramification index 2. The conductor of this extension is p. Let $\mathrm{Cl}_p(F)$ be the ray class group with respect to the conductor p. Recall that we have an exact sequence of finite abelian groups

$$0 \to (\mathcal{O}_F/p\,\mathcal{O}_F)^\times/\mathrm{Im}(\mathcal{O}_F^\times) \to \mathrm{Cl}_p(F) \to \mathrm{Cl}(F) \to 0,$$

and since $\mathrm{Cl}(F) = 1$, we have the isomorphism

$$(\mathcal{O}_F/p\,\mathcal{O}_F)^\times/\mathrm{Im}(\mathcal{O}_F^\times) \cong \mathrm{Cl}_p(F).$$

Note that $(\mathcal{O}_F/p\,\mathcal{O}_F)^\times \cong (\mathcal{O}_F/\mathfrak{p}_1\,\mathcal{O}_F)^\times \times (\mathcal{O}_F/\mathfrak{p}_2\,\mathcal{O}_F)^\times$, and for $i \in \{1,2\}$, each factor $(\mathcal{O}_F/\mathfrak{p}_i\,\mathcal{O}_F)^\times$ is isomorphic to $\mathbb{F}_p^\times$. The Artin map ensures the existence of a surjection

$$\mathrm{Cl}_p(F) \twoheadrightarrow \mathrm{Gal}(H_4/F) \cong C_2 \times C_2,$$

which sends a prime ideal of $\mathrm{Cl}_p(F)$ onto its Artin symbol. Then, if we quotient by $2\,\mathrm{Cl}_p(F)$, we get the isomorphisms

$$(\mathbb{F}_p^\times \times \mathbb{F}_p^\times)/\square \cong \mathrm{Cl}_p(F)/2\,\mathrm{Cl}_p(F) \cong \mathrm{Gal}(H_4/F) \cong C_2 \times C_2. \tag{3.1}$$

In order to see that $(\sqrt{-q})$ splits completely in H_4, we want its Artin symbol to be trivial. Hence, considering (3.1), we need $\sqrt{-q}$ to be a square modulo p. Therefore, if p is a prime congruent to 1 modulo 4 and such that

$(-q/p) = 1$, we have the following condition:

$$8 \mid h(-qp) \iff \left(\frac{-q}{p}\right)_4 = 1, \tag{3.2}$$

where the quartic symbol is for $K = \mathbb{Q}$.

Note that (3.2) is equivalent to p splitting completely in $\mathbb{Q}(\sqrt{-1}, \sqrt[4]{-q})$. Indeed if we consider the extensions

$$\begin{tikzcd} \mathbb{Q}(\sqrt{-1}, \sqrt[4]{-q}) \arrow[d, dash] \\ \mathbb{Q}(\sqrt{-1}, \sqrt{-q}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

we see that p splits completely in $\mathbb{Q}(\sqrt{-1}, \sqrt{-q})$, since $(-q/p) = 1$. If $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\sqrt{-1}, \sqrt{-q})$ above p, then $\mathfrak{p}$ splits completely in $\mathbb{Q}(\sqrt{-1}, \sqrt[4]{-q})$ if and only if p splits completely in $\mathbb{Q}(\sqrt{-1}, \sqrt[4]{-q})$ if and only if $(-q/p)_4 = 1$.

We know that $\mathbb{Q}(\sqrt{-1}, \sqrt{-q})$ is a principal ideal domain and so if π is a generator of a prime ideal $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{-1}, \sqrt{-q})$ above p, since $\mathfrak{p}$ has degree 1, we have

$$\left(\frac{-q}{p}\right)_{\mathbb{Q},4} = \left(\frac{-q}{\pi}\right)_{\mathbb{Q}(\sqrt{-1},\sqrt{-q}),4}.$$

Using again the Chebotarev Density Theorem, we obtain $\delta(8) = 1/4$.

3.4. The 16-rank. The criterion for the divisibility of $h(-qp)$ by 16 is due to Leonard and Williams [LW85, Theorem 2]. Let p be a prime number congruent to 1 modulo 4, such that $\left(\frac{-q}{p}\right) = 1$ and $\left(\frac{-q}{p}\right)_4 = 1$. There exist positive integers u and v satisfying $p = u^2 - qv^2$. We will show that we can always find a solution with $u \equiv 1 \bmod 4$. Then

$$16 \mid h(-qp) \iff \\ \left(\frac{u}{p}\right)_4 = \left(\frac{2}{u}\right), \quad \text{where } u \equiv 1 \bmod 4 \text{ and } p = u^2 - qv^2, \text{ with } u, v \in \mathbb{Z}.$$

We note that the first quartic symbol has both entries depending on p, since u has to satisfy the relation $p = u^2 - qv^2$. Hence, we cannot interpret this condition as the splitting behaviour of p in some normal extension of $\mathbb{Q}$ and thus we cannot directly apply the Chebotarev Density Theorem, as we did before. Instead, we will follow Koymans and Milovic's idea using Vinogradov's method.

Note that u and v are not uniquely determined. Let us see how we can compute these integers. It is natural to work in the field $\mathbb{Q}(\sqrt{q})$. We observe that p splits completely in $M_q = \mathbb{Q}(\sqrt{-1}, \sqrt{q})$, since $(-q/p) = 1$. We already know that M_q is a principal ideal domain. Let ζ_{12} be a 12th root of unity and $i = \sqrt{-1}$ be a fourth root of unity. We see that $\mathcal{O}_{M_q}^{\times} = \langle \nu_q \rangle \times \langle \varepsilon_q \rangle$, where

$$\nu_q = \begin{cases} \zeta_{12} & \text{if } q = 3, \\ i & \text{otherwise,} \end{cases}$$

and

$$\begin{aligned} \varepsilon_3 &= \zeta_{12} - 1, \\ \varepsilon_7 &= \tfrac{1}{2}(1-i)(\sqrt{7}+3), \\ \varepsilon_{11} &= \tfrac{1}{2}(1-i)(\sqrt{11}+3), \\ \varepsilon_{19} &= \tfrac{1}{2}(1+i)(3\sqrt{19}+13), \\ \varepsilon_{43} &= \tfrac{1}{2}(1+i)(9\sqrt{43}-59), \\ \varepsilon_{67} &= \tfrac{1}{2}(1+i)(27\sqrt{67}-221), \\ \varepsilon_{163} &= \tfrac{1}{2}(1-i)(627\sqrt{163}+8005). \end{aligned} \tag{3.3}$$

Note that $M_q/\mathbb{Q}$ is a normal extension with Galois group isomorphic to the Klein four group, say $\{1, \sigma, \tau, \sigma\tau\}$, where σ fixes $\mathbb{Q}(\sqrt{q})$ and τ fixes $\mathbb{Q}(\sqrt{-1})$.

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{-1}, \sqrt{q}) \arrow[dl, dash, "\langle\tau\rangle"'] \arrow[d, dash, "\langle\tau\sigma\rangle"] \arrow[dr, dash, "\langle\sigma\rangle"] & \\ \mathbb{Q}(\sqrt{-1}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{-q}) \arrow[d, dash] & \mathbb{Q}(\sqrt{q}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

We consider $\pi \in M_q$ such that π generates one of the prime ideals $\mathfrak{p}$ in $\mathcal{O}_{M_q}$ above p. Then there exist $u, v \in \mathbb{Z}$ such that $u + \sqrt{q}\, v = \mathrm{N}_{M_q/\mathbb{Q}(\sqrt{q})}(\pi)$ and so we get

$$\pm p = \mathrm{N}_{M_q/\mathbb{Q}}(\pi) = (u + \sqrt{q}\, v)(u - \sqrt{q}\, v) = u^2 - qv^2.$$

Looking at this equation modulo 4, we have

$$p = u^2 - qv^2, \tag{3.4}$$

as wanted. Thus we can choose

$$u = \frac{\pi\sigma(\pi) + \tau(\pi)\tau(\sigma(\pi))}{2} \quad \text{and} \quad v = \frac{\pi\sigma(\pi) - \tau(\pi)\tau(\sigma(\pi))}{2\sqrt{q}}.$$

We now check that $u > 0$ and that we can always find $u \equiv 1 \bmod 4$. In fact, if u_0 and v_0 are a solution of (3.4), then also $u + \sqrt{q}\, v = (u_0 + \sqrt{q}\, v_0)(\sigma(\varepsilon_q)\varepsilon_q)^k$, for $k \in \mathbb{N}$, is a solution. Indeed,

$$\mathrm{N}_{M/\mathbb{Q}(\sqrt{q})}(\pi) = \mathrm{N}_{M/\mathbb{Q}(\sqrt{q})}(\varepsilon_q \pi) = \sigma(\varepsilon_q)\varepsilon_q(u_0 + \sqrt{q}\, v_0).$$

The map that describes the transformation of a given solution (u, v) for the equation (3.4), by the multiplication with $\sigma(\varepsilon_q)\varepsilon_q$ modulo 4, is the following:

$$\begin{aligned}
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, && \\
&(u, v) \mapsto (2u - 3v, 2v - u) && \text{if } q = 3, 11, 19, 163, \\
&(u, v) \mapsto (v, 3u) && \text{if } q = 7, \\
&(u, v) \mapsto (2u + 3v, u + 2v) && \text{if } q = 43, 67.
\end{aligned} \tag{3.5}$$

The possibilities for u and v are $u = 0, 2$ and $v = 1, 3$, or $u = 1, 3$ and $v = 0, 2$ modulo 4 and so, looking at the orbits of the above map, we note that they are of length 4 and that we always find exactly one u in each orbit that satisfies $u \equiv 1 \bmod 4$.

3.5. Encoding the 16-rank of $\mathrm{Cl}(K_{p,q})$ **into sequences** $\{a_{\mathfrak{n},q}\}_{\mathfrak{n}}$**.** Let q be a fixed prime in the set Q and let n_q be equal to $2q$. We define, for any $\alpha \in \mathbb{Z}[\sqrt{q}]$,

$$\mathtt{u}(\alpha) = \tfrac{1}{2}(\alpha + \tau(\alpha)).$$

Note that for every $w \in \mathcal{O}_{M_q} \setminus \{0\}$ the inequality $\mathtt{u}(w\sigma(w)) > 0$ holds. We define, for any element $w \in \mathcal{O}_{M_q}$ coprime to n_q,

$$[w] := \left(\frac{\mathtt{u}(w\sigma(w))}{w}\right)_{M_q,4} \left(\frac{2}{\mathtt{u}(w\sigma(w))}\right)_{\mathbb{Q},2}. \tag{3.6}$$

Hence $16 \mid h(-qp)$ if and only if $[w] = 1$, where w is any element of $\mathcal{O}_{M_q}$ such that $N_{M_q/\mathbb{Q}}(w) = p$ and $\mathtt{u}(w\sigma(w)) \equiv 1 \bmod 4$. We note that

$$\begin{aligned}
\left(\frac{\mathtt{u}(w\sigma(w))}{w}\right)_{M_q,4} &= \left(\frac{(w\sigma(w) + \tau(w\sigma(w)))/2}{w}\right)_{M_q,4} \\
&= \left(\frac{\tau(w\sigma(w))}{w}\right)_{M_q,4} \left(\frac{8}{w}\right)_{M_q,4}.
\end{aligned} \tag{3.7}$$

Let ε_q be as in (3.3). Then

$$\begin{aligned}
\left(\frac{\mathrm{u}(\varepsilon^4 w\sigma(\varepsilon_q^4 w))}{\varepsilon_q^4 w}\right)_{M_q,4} &= \left(\frac{\mathrm{u}(\varepsilon_q^4 w\sigma(\varepsilon_q^4 w))}{w}\right)_{M_q,4} \\
&= \left(\frac{\tau(\varepsilon_q^4 w\sigma(\varepsilon_q^4 w))}{w}\right)_{M_q,4} \left(\frac{8}{w}\right)_{M_q,4} \\
&= \left(\frac{\mathrm{u}(w\sigma(w))}{w}\right)_{M_q,4}.
\end{aligned}$$

The equality

$$\left(\frac{2}{\mathtt{u}(\varepsilon_q^4 w\sigma(\varepsilon_q^4 w))}\right)_{\mathbb{Q},2} = \left(\frac{2}{\mathtt{u}(w\sigma(w))}\right)_{\mathbb{Q},2}$$

is given by $2\mathtt{u}(\varepsilon_q^4 w\sigma(\varepsilon_q^4 w)) \equiv 2\mathtt{u}(w\sigma(w)) \bmod 16$. In fact, $2\mathtt{u}(\varepsilon_q^4 w\sigma(\varepsilon_q^4 w)) = (\varepsilon_q\sigma(\varepsilon_q))^4 w\sigma(w) + \tau(\varepsilon_q\sigma(\varepsilon_q))^4\tau(w\sigma(w))$ and a straightforward computation (with $w\sigma(w) = u + \sqrt{q}\, v$) shows that

$$\begin{aligned}
2\mathtt{u}(\varepsilon_3^4 w\sigma(\varepsilon_3^4 w)) &= 194\, u - 336\, v,\\
2\mathtt{u}(\varepsilon_7^4 w\sigma(\varepsilon_7^4 w)) &= 64514\, u + 170688\, v,\\
2\mathtt{u}(\varepsilon_{11}^4 w\sigma(\varepsilon_{11}^4 w)) &= 158402\, u + 525360\, v,\\
2\mathtt{u}(\varepsilon_{19}^4 w\sigma(\varepsilon_{19}^4 w)) &= 13362897602\, u + 58247520240\, v,\\
2\mathtt{u}(\varepsilon_{43}^4 w\sigma(\varepsilon_{43}^4 w)) &= 2351987525322434\, u - 15423013607227056\, v,\\
2\mathtt{u}(\varepsilon_{67}^4 w\sigma(\varepsilon_{67}^4 w)) &= 910528910165841333314\, u - 7453000338695970346 08\, v,\\
2\mathtt{u}(\varepsilon_{163}^4 w\sigma(\varepsilon_{163}^4 w)) &= 26978058980591390850645997786080 2\, u\\
&\quad + 344432799856116564026009656135704 0\, v.
\end{aligned}$$

Hence we have proved that

$$[w] = [\varepsilon_q^4 w].$$

Note that

$$[w] = [\nu_q w].$$

Indeed, for $q = 3$, we see that $\zeta_{12}\sigma(\zeta_{12}) = 1$ and hence $\tau(\zeta_{12}\sigma(\zeta_{12})) = 1$. Then $\mathtt{u}(\zeta_{12}w\,\sigma(\zeta_{12}w)) = \mathtt{u}(w\sigma(w))$. For the other values of q, note that $i\sigma(i) = 1$ and so $\tau(i\sigma(i)) = 1$. Thus $\mathtt{u}(iw\,\sigma(iw)) = \mathtt{u}(w\sigma(w))$.

For $w \in \mathcal{O}_{M_q}$ such that $N_{M_q/\mathbb{Q}}(w) = p$, we define

$$s(w) = \begin{cases} 1 & \text{if } \mathtt{u}(w\sigma(w)) \equiv 1 \bmod 4,\\ 0 & \text{otherwise.}\end{cases}$$

Then

$$\sum_{i=0}^{3} s(\varepsilon_q^i w) = 1$$

with ε_q as in (3.3), by looking at the orbits of the map (3.5). Thus it is clear that

$$\sum_{i=0}^{3} s(\varepsilon_q^i w) = \sum_{i=0}^{3} s(\varepsilon_q^{i+k} w),$$

where $k \in \mathbb{N}$.

Having determined the action of the units $\mathcal{O}_{M_q}^\times$ on this sum and on $[\,\cdot\,]$, we see that the quantity $\sum_{i=0}^{3} s(\varepsilon_q^i w)[\varepsilon_q^i w]$ does not depend on the choice of the generator w but only on the prime ideal $\mathfrak{p}$ above p. We have proved the following.

PROPOSITION 3.1. *Let p be a prime congruent to 1 modulo 4 and such that $(-q/p) = 1$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{M_q}$, lying above p, with generator w. Then*

$$\sum_{i=0}^{3} s(\varepsilon_q^i w)[\varepsilon_q^i w]\frac{1}{2}\left(1+\left(\frac{-q}{\varepsilon_q^i w}\right)_{M_q,4}\right) = \begin{cases} 1 & \textit{if } 16 \mid h(-qp), \\ -1 & \textit{if } 8 \mid h(-qp) \textit{ but } 16 \nmid h(-qp), \\ 0 & \textit{otherwise.} \end{cases}$$

We define the sequence $\{a_{\mathfrak{n},q}\}_{\mathfrak{n}}$, indexed by ideals of $\mathcal{O}_{M_q}$, in the following way:

$$a_{\mathfrak{n},q} := \begin{cases} 0 & \text{if } (\mathfrak{n}, n_q) = 1, \\ \sum_{i=0}^{3} s(\varepsilon_q^i w)[\varepsilon_q^i w]\frac{1}{2}\left(1+\left(\frac{-q}{\varepsilon_q^i w}\right)_{M_q,4}\right) & \text{otherwise,} \end{cases} \tag{3.8}$$

where w is any generator of the ideal $\mathfrak{n}$ coprime to n_q.

4. Vinogradov's method, after Friedlander, Iwaniec, Mazur and Rubin. The version of Vinogradov's method that we are going to use is the one introduced by Friedlander et al. [FIMR13]. In order to use this powerful machinery, we need to verify that the sequence $(a_{\mathfrak{n},q})$ defined in (3.8) satisfies the hypothesis of [FIMR13, Proposition 5.2]. In other words, it remains to prove analogues of Propositions 3.7 and 3.8 of [KM19a] for our sequences $(a_{\mathfrak{n},q})$ with $q \in Q$ fixed and the field M_q, where $Q = \{3, 7, 11, 19, 43, 67, 163\}$. In the literature, the sums that will appear are called sums of type I and sums of type II respectively.

Once we have proved it, we will have

$$\sum_{\mathrm{N}\mathfrak{n} \le x} a_{\mathfrak{n},q}\Lambda(\mathfrak{n}) \ll_\theta x^{1-\theta} \quad \text{for } x > 0,$$

for all $\theta < 1/(49 \cdot 64) = 1/3136$. This implies Theorem 1.1.

4.1. Sums of type I. In this section, we will adapt the proof of [KM19a, Proposition 3.7] to our sequence $(a_{\mathfrak{n},q})$ and the field M_q for q fixed.

Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_{M_q}$ coprime to n_q. We want to bound the sum

$$\begin{aligned} A(x) = A(x, \mathfrak{m}) &:= \sum_{\substack{\mathrm{N}(\mathfrak{n}) \le x \\ (\mathfrak{n}, n_q)=1,\, \mathfrak{m} \mid \mathfrak{n}}} a_{\mathfrak{n},q} \\ &= \sum_{\substack{\mathrm{N}(\mathfrak{n}) \le x \\ (\mathfrak{n}, n_q)=1,\, \mathfrak{m} \mid \mathfrak{n}}} \left(\sum_{i=0}^{3} s(\varepsilon_q^i \alpha)[\varepsilon_q^i \alpha]\frac{1}{2}\left(1+\left(\frac{-q}{\varepsilon_q^i \alpha}\right)_{M_q,4}\right)\right), \end{aligned}$$

where α is a generator of $\mathfrak{n}$. We consider the integral basis $\{1, \eta_1^{(q)}, \eta_2^{(q)}, \eta_3^{(q)}\}$ (e.g. for $q = 3$ we consider $\{1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3\}$) and a fundamental domain $\mathcal{D}_q$ as described in [KM19a, Lemma 3.5] with $F = M_q$ and $n = 4$.

In the case $q = 3$, the torsion group of $\mathcal{O}_{M_3}^\times$, has twelve elements and then every ideal $\mathfrak{n}$ has exactly twelve generators $\alpha \in \mathcal{D}_3$. For the other cases, the torsion part of the unit group $\mathcal{O}_{M_q}^\times$ has four elements and so every ideal $\mathfrak{n}$ has exactly four generators $\alpha \in \mathcal{D}_q$. We recall that $s(\alpha)$ depends only on the congruence class of α modulo 4. Observe that

$$\begin{aligned}[\alpha] &= \left(\frac{\mathtt{u}(\alpha\sigma(\alpha))}{\alpha}\right)_{M_q,4}\left(\frac{2}{\mathtt{u}(\alpha\sigma(\alpha))}\right)_{\mathbb{Q},2} \\ &= \left(\frac{\tau(\alpha)}{\alpha}\right)_{M_q,4}\left(\frac{\tau(\sigma(\alpha))}{\alpha}\right)_{M_q,4}\left(\frac{8}{\alpha}\right)_{M_q,4}\left(\frac{2}{\mathtt{u}(\alpha\sigma(\alpha))}\right)_{\mathbb{Q},2}.\end{aligned}$$

The symbol $\left(\frac{2}{\mathtt{u}(\alpha\sigma(\alpha))}\right)_{\mathbb{Q},2}$ depends only on the congruence class of α modulo 8 and, by Lemma 2.2, the symbol $(8/\alpha)_{M_q,4}$ depends only on the congruence class of α modulo 2^8. We set $F_q = q \cdot 2^8$ and we split the sum $A(x)$ into congruence classes modulo F_q.

Using Lemma 2.2, the symbol $(-q/\alpha)_{M_q,4}$ depends only on α modulo $32q$ and so we find that

$$A(x) = \frac{1}{12}\sum_{i=0}^{3}\sum_{\substack{\rho \bmod F_3 \\ (\rho,F_3)=1}} \frac{1}{2}\,\mu(\rho\varepsilon_3^i)A(x;\rho,\varepsilon_3^i)\left(1 + \left(\frac{-3}{\varepsilon_3^i\alpha}\right)_{M_3,4}\right) \qquad \text{for } q = 3,$$

and

$$A(x) = \frac{1}{4}\sum_{i=0}^{3}\sum_{\substack{\rho \bmod F_q \\ (\rho,F_q)=1}} \frac{1}{2}\,\mu(\rho,\varepsilon_q^i)A(x;\rho,\varepsilon_q^i)\left(1 + \left(\frac{-q}{\varepsilon_q^i\alpha}\right)_{M_q,4}\right) \qquad \text{otherwise},$$

where $\mu(\rho, \varepsilon_q^i) \in \{\pm 1, \pm i\}$ depends only on ρ and ε_q^i and with

$$A(x;\rho,\varepsilon_q^i) := \sum_{\substack{\alpha\in\varepsilon_q^i\mathcal{D}_q,\, \mathrm{N}(\alpha)\le x \\ \alpha\equiv\rho \bmod F_q \\ \alpha\equiv 0 \bmod \mathfrak{m}}} \left(\frac{\tau(\alpha)}{\alpha}\right)_{M_q,4}\left(\frac{\tau(\sigma(\alpha))}{\alpha}\right)_{M_q,4}.$$

Since $(-q/\alpha)_{M_q,4} \in \{0, \pm 1, \pm i\}$, we obtain

$$\left|1 + \left(\frac{-q}{\alpha}\right)_{M_q,4}\right| \le 2.$$

Hence we have the bound

$$|A(x)| \leq \frac{1}{4} \sum_{i=0}^{3} \sum_{\substack{\rho \bmod F_q \\ (\rho, F_q)=1}} |A(x; \rho, \varepsilon_q^i)|$$

for every $q \in Q$.

For each ε_q^i and congruence class $\rho \bmod F_q$ with $(\rho, F_q) = 1$, we estimate $A(x; \rho, \varepsilon_q^i)$ separately. We consider the free $\mathbb{Z}$-module

$$\mathbb{M} = \mathbb{Z}\eta_1^{(q)} \oplus \mathbb{Z}\eta_2^{(q)} \oplus \mathbb{Z}\eta_3^{(q)}$$

of rank 3 and so we write the decomposition $\mathcal{O}_{M_q} = \mathbb{Z} \oplus \mathbb{M}$ viewing $\mathcal{O}_{M_q}$ as a free $\mathbb{Z}$-module of rank 4. We write α uniquely as

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

so our summation conditions become

$$a+\beta \in \varepsilon_q^i \mathcal{D}_q, \quad N(a+\beta) \leq x, \quad a+\beta \equiv \rho \bmod F_q, \quad a+\beta \equiv 0 \bmod \mathfrak{m}. \tag{4.1}$$

If $\tau(\alpha) = \alpha$ and $\tau(\sigma(\alpha)) = \alpha$, we get no contribution to $A(x; \rho, \varepsilon_q^i)$, so we can assume $\tau(\alpha) \neq \alpha$ and $\tau(\sigma(\alpha)) \neq \alpha$. Next we are going to interchange the upper entry and the lower entry of our quartic residue symbols. Since M_q is a principal ideal domain, let

$$\tau(\alpha) - \alpha = \eta^4 c_0 c \quad \text{and} \quad \tau(\sigma(\alpha)) - \alpha = \eta'^4 c_0' c'$$

with $c_0, c_0', c, c', \eta, \eta' \in \mathcal{O}_{M_q}$, $c_0, c_0' \mid F_q$ quadric-free, η, η' that divide some power of F_q and $(c, F_q) = (c', F_q) = 1$. We can ensure $c \in \mathbb{Z}[\sqrt{-1}]$ and $c' \in \mathbb{Z}\big[\frac{1+\sqrt{-q}}{2}\big]$. In fact, we can take

$$c = \frac{\tau(\alpha) - \alpha}{\sqrt{q}} = \frac{\tau(\beta) - \beta}{\sqrt{q}} \in \mathbb{Z}[\sqrt{-1}],$$
$$c' = \frac{\tau(\sigma(\alpha)) - \alpha}{i} = \frac{\tau(\sigma(\beta)) - \beta}{i} \in \mathbb{Z}\left[\frac{1+\sqrt{-q}}{2}\right].$$

Hence

$$\left(\frac{\tau(\alpha)}{\alpha}\right)_{M_q,4} = \left(\frac{a+\tau(\beta)}{\alpha}\right)_{M_q,4} = \left(\frac{\tau(\beta)-\beta}{\alpha}\right)_{M_q,4}$$
$$= \left(\frac{\eta^4 c_0 c}{\alpha}\right)_{M_q,4} = \left(\frac{c_0}{\alpha}\right)_{M_q,4} \left(\frac{c}{\alpha}\right)_{M_q,4}.$$

Since we are working with $\alpha \equiv \rho \bmod F_q$, $(\rho, F_q) = 1$ and c and c' depend only on β, we apply Lemma 2.2 to obtain

$$\left(\frac{\tau(\alpha)}{\alpha}\right)_{M_q,4} = \tilde{\mu} \cdot \left(\frac{a+\beta}{c\mathcal{O}_{M_q}}\right)_{M_q,4},$$

and the same for the other quadric symbol,

$$\left(\frac{\tau(\sigma(\alpha))}{\alpha}\right)_{M_q,4} = \tilde{\mu}' \cdot \left(\frac{a+\beta}{c'\mathcal{O}_{M_q}}\right)_{M_q,4},$$

with $\tilde{\mu}, \tilde{\mu}' \in \{\pm 1, \pm i\}$ that depend only on ρ and β. Hence

$$A(x;\rho,\varepsilon_q^i) \leq \sum_{\beta\in\mathbb{M}} |T(x;\beta,\rho,\varepsilon_q^i)|,$$

where

$$T(x;\beta,\rho,\varepsilon_q^i) := \sum_{\substack{a\in\mathbb{Z} \\ a+\beta \text{ sat. (4.1)}}} \left(\frac{a+\beta}{c\mathcal{O}_{M_q}}\right)_{M_q,4} \left(\frac{a+\beta}{c'\mathcal{O}_{M_q}}\right)_{M_q,4}.$$

In order to study $(a+\beta/c\mathcal{O}_{M_q})_{M_q,4}$, we want to replace β with a rational integer modulo $c\mathcal{O}_{M_q}$. However this is possible only for ideals of degree 1. For this reason, we factor $c\mathcal{O}_{M_q}$. Since we choose $c \in \mathbb{Z}[\sqrt{-1}]$, we can define the ideals $\mathfrak{g}$ and $\mathfrak{l} \in \mathbb{Z}[\sqrt{-1}]$ in a unique way such that

$$(c) = \mathfrak{g}\mathfrak{l}$$

with $l := \mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathfrak{l})$ a squarefree integer coprime to n_q and $g := \mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathfrak{g})$ a squarefull integer coprime to $n_q l$.

Note that c is coprime to $2q$. Hence, in the factorization of the ideal $\mathfrak{l}$, those prime ideals that divide $\mathfrak{l}$ in $\mathbb{Z}[\sqrt{-1}]$ do not ramify in the quadratic extension M_q. We can then apply Lemma 2.5 for any prime ideal dividing $\mathfrak{l}$ and, using the Chinese Remainder Theorem, we find $\beta' \in \mathbb{Z}[\sqrt{-1}]$ such that $\beta \equiv \beta' \bmod \mathfrak{l}\mathcal{O}_{M_q}$. We deduce that the upper entry of our quartic residue symbol is in $\mathbb{Z}[\sqrt{-1}]$.

If a prime ideal $\mathfrak{p}$ that divides $\mathfrak{l}$ splits in M_q, we apply Lemma 2.3 in order to reduce our quartic symbol to a quadratic one. If $\mathfrak{p}$ stays inert in M_q, then $\mathfrak{p}$ has degree 1. If we define $p := \mathfrak{p} \cap \mathbb{Z}$, we find that $p \equiv 1 \bmod 4$, since p splits in $\mathbb{Z}[\sqrt{-1}]$, and so $(p+1)/2$ is an odd number. Applying Lemma 2.4 and combining all these results, we have

$$\left(\frac{\alpha+\beta'}{\mathfrak{l}\mathcal{O}_{M_q}}\right)_{M_q,4} = \left(\frac{\alpha+\beta'}{\mathfrak{l}}\right)_{\mathbb{Q}(\sqrt{-1}),2}.$$

Using again the Chinese Remainder Theorem and the fact that l is squarefree, we find a rational integer b such that $\beta' \equiv b \bmod \mathfrak{l}$. Hence,

$$\left(\frac{a+\beta}{c\mathcal{O}_{M_q}}\right)_{M_q,4} = \left(\frac{a+\beta}{\mathfrak{g}\mathcal{O}_{M_q}}\right)_{M_q,4} \left(\frac{a+b}{\mathfrak{l}}\right)_{\mathbb{Q}(\sqrt{-1}),2}.$$

Note that b depends on β and not on a, because c depends only on β. We denote the product of all primes dividing g by $g_0 := \prod_{p|g} p$ and the product of all prime ideals dividing $\mathfrak{g}$ by $\mathfrak{g}^* := \prod_{\mathfrak{p}|\mathfrak{g}} \mathfrak{p}$. The quartic symbol $(\alpha/\mathfrak{g})_{M_q,4}$

is periodic in the upper entry modulo $\mathfrak{g}^*$, and so also modulo g_0, since $\mathfrak{g}^*$ divides g_0. Since our β is fixed, we can split $T(x;\beta,\rho,\varepsilon_q^i)$ into residue classes modulo g_0, and we obtain

$$|T(x;\beta,\rho,\varepsilon_q^i)| \leq \sum_{a_0 \bmod g_0} \Bigg| \sum_{\substack{a\in\mathbb{Z} \\ a+\beta \text{ sat. (4.1)} \\ a\equiv a_0 \bmod g_0}} \left(\frac{a+b}{\mathfrak{q}}\right)_{\mathbb{Q}(\sqrt{-1}),2} \left(\frac{a+\beta}{c'\mathcal{O}_{M_q}}\right)_{M_q,4} \Bigg|.$$

Now, we focus on the quartic symbol $((a+\beta)/c'\mathcal{O}_{M_q})_{M_q,4}$. We claim that it is the indicator function for $\gcd(a+\beta,c')$. Note that we have chosen $c' \in \mathbb{Z}\big[\frac{1+\sqrt{-q}}{2}\big]$ and that it is coprime to n_q. We factor the principal ideal $(c') \subset \mathbb{Z}\big[\frac{1+\sqrt{-q}}{2}\big]$ as $(c') = \prod_{i=1}^k \mathfrak{p}_i^{e_i}$ where the $\mathfrak{p}_i$'s are prime ideals of $\mathbb{Z}\big[\frac{1+\sqrt{-q}}{2}\big]$ that do not ramify in M_q, since we are sure that they do not divide the discriminant thanks to the coprimality condition with n_q. We can then use the definition of quartic residue symbol to get

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

To prove that our claim is true, we need to show that $((a+\beta)/\mathfrak{p}\mathcal{O}_{M_q})_{M_q,4} = 1$ whenever $\mathfrak{p} \nmid a+\beta$. Using Lemma 2.5, instead of β we can work with $\beta' \in \mathbb{Z}\big[\frac{1+\sqrt{-q}}{2}\big]$. Then we can apply Lemma 2.3 for the prime ideals $\mathfrak{p}$ that split in M_q. Otherwise, if $\mathfrak{p}$ stays inert in M_q, then $p := \mathfrak{p}\cap\mathbb{Z}$ has to split in $\mathbb{Q}(\sqrt{-q})$ but not completely in M_q. It follows that p is inert in $\mathbb{Q}(\sqrt{-1})$ and so $(p+1)/2$ is an even number. Then we find that $\mathfrak{p}$ has degree 1 and we conclude our argument by applying Lemma 2.4.

Hence we obtain

$$\left(\frac{a+\beta}{c'\mathcal{O}_{M_q}}\right)_{M_q,4} = \mathbb{1}_{\gcd(a+\beta,c')=(1)} = \sum_{\substack{\mathfrak{d}|c' \\ \mathfrak{d}|a+\beta}} \mu(\mathfrak{d}),$$

where $\mu(\mathfrak{n})$ is the Möbius function for an integral ideal $\mathfrak{n}$ defined by

$$\mu(\mathfrak{n}) = \begin{cases} (-1)^t & \text{if } \mathfrak{n} \text{ is the product of } t \text{ distinct prime ideals,} \\ 0 & \text{otherwise.} \end{cases}$$

We obtain

$$|T(x;\beta,\rho,\varepsilon_q^i)| \leq \sum_{a_0 \bmod g_0} \sum_{\substack{\mathfrak{d}|c' \\ \mathfrak{d} \text{ squarefree}}} |T(x;\beta,\rho,\varepsilon_q^i,a_0,\mathfrak{d})|$$

with

$$T(x;\beta,\rho,\varepsilon_q^i,a_0,\mathfrak{d}) := \sum_{\substack{a\in\mathbb{Z}\\ a+\beta \text{ sat. (4.1)}\\ a\equiv a_0 \bmod g_0\\ a+\beta\equiv 0 \bmod \mathfrak{d}}} \left(\frac{a+b}{\mathfrak{l}}\right)_{\mathbb{Q}(\sqrt{-1}),2}. \tag{4.2}$$

Now we can follow the steps of Koymans and Milovic [KM19a, §4, p. 17] where our $\mathfrak{l}$ corresponds to their $\mathfrak{q}$, our integral basis corresponds to the generically written basis $\{1,\eta_1^{(q)},\eta_2^{(q)},\eta_3^{(q)}\}$, and our units ε_q^i correspond to the units u_i.

4.2. Sums of type II. We now adapt the proof of [KM19a, Proposition 3.8] to our sequence $(a_{\mathfrak{n},q})$ and the field M_q, dealing with bilinear sums or sums of type II.

We consider w and z in $\mathcal{O}_{M_q}$ that are coprime to n_q. Recalling our definition of the symbol $[\cdot]$ in (3.6) and the observation of (3.7), we have

$$[wz] = \left(\frac{8\tau(wz)\tau\sigma(wz)}{wz}\right)_{M_q,4}\left(\frac{2}{\mathtt{u}(wz\sigma(wz))}\right)_{\mathbb{Q},2}.$$

We can then rewrite this equality as

$$[wz] = [w][z]Q_2(w,z)\left(\frac{\tau(w)}{z}\right)_{M_q,4}\left(\frac{\tau\sigma(w)}{z}\right)_{M_q,4}\left(\frac{\tau(z)}{w}\right)_{M_q,4}\left(\frac{\tau\sigma(z)}{w}\right)_{M_q,4},$$

where

$$Q_2(w,z) := \left(\frac{2}{\mathtt{u}(w\sigma(w))}\right)_{\mathbb{Q},2}\left(\frac{2}{\mathtt{u}(z\sigma(z))}\right)_{\mathbb{Q},2}\left(\frac{2}{\mathtt{u}(wz\sigma(wz))}\right)_{\mathbb{Q},2}.$$

We note that $Q_2(w,z)\in\{\pm1,\pm i\}$ depends only on the congruence classes of w and z modulo 8.

Now we want to simplify the quartic residue symbols. We use Lemma 2.2 to find some $\mu_1\in\{\pm1,\pm i\}$, which depends on the congruence classes of w and z modulo 32, such that

$$\begin{aligned}\left(\frac{\tau(w)}{z}\right)_{M_q,4}\left(\frac{\tau(z)}{w}\right)_{M_q,4} &= \mu_1\left(\frac{z}{\tau(w)}\right)_{M_q,4}\left(\frac{\tau(z)}{w}\right)_{M_q,4}\\ &= \mu_1\left(\frac{z}{\tau(w)}\right)_{M_q,4}\tau\left(\frac{z}{\tau(w)}\right)_{M_q,4}\\ &= \mu_1\left(\frac{z}{\tau(w)}\right)_{M_q,2},\end{aligned}$$

since $\tau(i)=i$. For the remaining symbols, we can find some $\mu_2\in\{\pm1,\pm i\}$, which depends on the congruence classes of w and z modulo 32, such that

$$\begin{aligned}\left(\frac{\tau\sigma(w)}{z}\right)_{M_q,4}\left(\frac{\tau\sigma(z)}{w}\right)_{M_q,4} &= \mu_2\left(\frac{z}{\tau\sigma(w)}\right)_{M_q,4}\tau\sigma\left(\frac{z}{\tau\sigma(w)}\right)_{M_q,4} \\ &= \mu_2\,\mathbb{1}_{\gcd(z,\tau\sigma(w))=(1)},\end{aligned}$$

since $\tau\sigma(i) = -i$. We can then define $\mu_3 := \mu_1\mu_2 Q_2(w,z) \in \{\pm 1, \pm i\}$ and get

$$[wz] = \mu_3[w][z]\left(\frac{z}{\tau(w)}\right)_{M_q,2}\mathbb{1}_{\gcd(z,\tau\sigma(w))=(1)}. \tag{4.3}$$

We consider two bounded sequences $\{\alpha_{\mathfrak{m}}\}_{\mathfrak{m}}$ and $\{\beta_{\mathfrak{n}}\}_{\mathfrak{n}}$ of complex numbers. Then

$$\begin{aligned}&\sum_{\mathrm{N}(\mathfrak{m})\leq M}\sum_{\mathrm{N}(\mathfrak{n})\leq N}\alpha_{\mathfrak{m}}\beta_{\mathfrak{n}}a_{\mathfrak{mn}} \\ &\quad= \frac{1}{12^2}\sum_{w\in\mathcal{D}_3(M)}\sum_{z\in\mathcal{D}_3(N)}\alpha_w\beta_z\left(\sum_{i=0}^{3}s(\varepsilon_3^i wz)[\varepsilon_3^i wz]\frac{1}{2}\left(1+\left(\frac{-3}{\varepsilon_3^i wz}\right)_{M_3,4}\right)\right)\end{aligned}$$

for $q=3$ and for the other $q \in Q\setminus\{3\}$ we have

$$\begin{aligned}&\sum_{\mathrm{N}(\mathfrak{m})\leq M}\sum_{\mathrm{N}(\mathfrak{n})\leq N}\alpha_{\mathfrak{m}}\beta_{\mathfrak{n}}a_{\mathfrak{mn}} \\ &\quad= \frac{1}{4^2}\sum_{w\in\mathcal{D}_q(M)}\sum_{z\in\mathcal{D}_q(N)}\alpha_w\beta_z\left(\sum_{i=0}^{3}s(\varepsilon_q^i wz)[\varepsilon_q^i wz]\frac{1}{2}\left(1+\left(\frac{-q}{\varepsilon_q^i wz}\right)_{M_q,4}\right)\right),\end{aligned}$$

using [KM19a, Lemma 3.5] with $F = M_q$ and $n=4$ that tells us that every ideal of $\mathcal{O}_{M_3}$ has twelve different generators in the fundamental domain $\mathcal{D}_3$ and $\mathcal{O}_{M_q}$ has four different generators for $q \in Q\setminus\{3\}$, and defining $\alpha_w := \alpha_{(w)}$ and $\beta_z := \beta_{(z)}$. We note that $s(\varepsilon_q^i wz)$ depends on the congruence class of wz modulo 4 and that $[\varepsilon_q^i wz] = \mu_4[wz]$ for some $\mu_4 \in \{\pm 1, \pm i\}$ depending on the congruence class modulo 32, by Lemma 2.2. What is more, the expression $\frac{1}{2}\big(\big(\frac{-q}{\varepsilon_q^i wz}\big)_{M_q,4}+1\big)$ takes values in the set $\{0, 1, (1+i)/2, (1-i)/2\}$. This implies that

$$\left|\frac{1}{2}\left(1+\left(\frac{-q}{\varepsilon_q^i wz}\right)_{M_q,4}\right)\right| \leq 1.$$

We focus on the congruence classes of w and z modulo $q\cdot 2^5$ and so we can bound the previous sums by a finite number of sums of the form

$$\mu_5\sum_{\substack{w\in\mathcal{D}_q(M)\\ w\equiv\omega \bmod q\cdot 2^5}}\sum_{\substack{z\in\mathcal{D}_q(N)\\ z\equiv\zeta \bmod q\cdot 2^5}}\alpha_w\beta_z[wz],$$

where μ_5 depends on the congruence classes ω and ζ modulo $q\cdot 2^5$.

We now use our simplification of the symbol $[wz]$ of (4.3) and we replace α_w and β_z with $\alpha_w[w]$ and $\beta_z[z]$. Then, if we consider $\mu_6 \in \{\pm 1, \pm i\}$ depending only on ω and ζ, we have

$$\mu_6 \sum_{\substack{w\in\mathcal{D}_q(M) \\ w\equiv\omega \bmod q\cdot 2^5}} \sum_{\substack{z\in\mathcal{D}_q(N) \\ z\equiv\zeta \bmod q\cdot 2^5}} \alpha_w\beta_z \left(\frac{z}{\tau(w)}\right)_{M_q,2} \mathbb{1}_{\gcd(z,\tau\sigma(w))=(1)}.$$

The last thing to do is to check that the function

$$\gamma(w,z) := \left(\frac{z}{\tau(w)}\right)_{M_q,2} \mathbb{1}_{\gcd(z,\tau\sigma(w))=(1)}$$

has properties (P1)–(P3) stated in [KM21, Lemma 4.1]. We can easily see that (P1) follows from Lemma 2.2, since we are working with congruence classes modulo $q\cdot 2^5$. Property (P2) is satisfied by the properties of the quadratic residue symbol in M_q given by Proposition 2.1 and Definitions 2.1–2.3 together with the fact that the indicator function of the gcd is completely multiplicative and $\mathbb{1}_{\gcd(z,\tau\sigma(w))=(1)} = \mathbb{1}_{\gcd(w,\tau\sigma(z))=(1)}$.

The first part of property (P3) is given again by the properties of the quadratic residue symbol in M_q and recalling that $\tau(w)$ divides the norm $\mathrm{N}_{M_q/\mathbb{Q}}(w)$. For the second part of (P3), we define the function

$$f(w) := \sum_{\xi \bmod \mathrm{N}_{M_q/\mathbb{Q}}(w)} \gamma(w,\xi) = \sum_{\xi \bmod \mathrm{N}_{M_q/\mathbb{Q}}(w)} \left(\frac{\xi}{\tau(w)}\right)_{M_q,2} \mathbb{1}_{\gcd(\xi,\tau\sigma(w))=(1)}.$$

If w and w' are two elements that generate ideals coprime to n_q and such that $\gcd(\mathrm{N}_{M_q/\mathbb{Q}}(w), \mathrm{N}_{M_q/\mathbb{Q}}(w')) = 1$, then $f(ww') = f(w)f(w')$. Hence, in order to prove property (P3), we just need to prove that $f(w) = 0$ for w that generates a prime ideal coprime to n_q of degree 1. We can surely find such an element that divides a generic w, because by assumption $\mathrm{N}_{M_q/\mathbb{Q}}(w)$ is not squarefull.

So let w be an element that generates a prime ideal coprime to n_q of degree 1. Then w, $\sigma(w)$, $\tau(w)$, and $\tau\sigma(w)$ are all coprime to each other. By the Chinese Remainder Theorem, using these coprimality relations, the function $f(w)$, apart from a non-zero factor, becomes

$$\sum_{\xi \bmod \tau(w\sigma(w))} \left(\frac{\xi}{\tau(w)}\right)_{M_q,2} \mathbb{1}_{\gcd(\xi,\tau\sigma(w))=(1)}$$
$$= \sum_{\xi \bmod \tau(w)} \left(\frac{\xi}{\tau(w)}\right)_{M_q,2} \sum_{\xi \bmod \tau\sigma(w)} \mathbb{1}_{\gcd(\xi,\tau\sigma(w))=(1)}.$$

We note that by [FIMR13, Lemma 3.6], the Dirichlet character given by the quadratic residue symbol is not principal. Hence we obtain the desired result by basic properties of cancellation of Dirichlet characters in a complete set of representatives.

This proves [KM19a, Proposition 3.8]. As we saw at the beginning of §4, we apply [FIMR13, Proposition 5.2] to obtain Theorem 1.1.

Acknowledgements. This research forms part of my Master Thesis at the University of Leiden under the supervision of P. Koymans and P. Stevenhagen. I am grateful to them for introducing me to the subject and for very useful discussions. Additionally, I wish to thank B. Klopsch for his numerous suggestions which have significantly improved the paper. I would also like to thank the referee for their detailed and thoughtful report, which has improved the exposition.

References

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, in: Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math. 1068, Springer, Berlin, 1984, 33–62.

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

[G87] F. Gerth, *Extension of conjectures of Cohen and Lenstra*, Exposition. Math. 5 (1987), 181–184.

[KM19a] 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. Notices 2019, 7406–7427.

[KM19b] P. Koymans and D. Milovic, *Spins of prime ideals and the negative Pell equation* $x^2 - 2py^2 = -1$, Compos. Math. 155 (2019), 100–125.

[KM21] P. Koymans and D. Milovic, *Joint distribution of spins*, Duke Math. J. 170 (2021), 1723–1755.

[LW85] P. A. Leonard and K. S. Williams, *On the divisibility of the class number of* $\mathbb{Q}(\sqrt{-pq})$ *by 16*, in: Number Theory (Winnipeg, Man., 1983), Rocky Mountain J. Math. 15 (1985), 491.

[M17] D. Milovic, *On the 16-rank of class group of* $\mathbb{Q}(\sqrt{-8p})$ *for* $p \equiv -1 \bmod 4$, Geom. Funct. Anal. 27 (2017), 973–1016.

[N99] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.

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

[U86] K. Uchida, *Imaginary abelian number fields of degrees* 2^m *with class number one*, in: Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, 151–170.

Margherita Piccolo
Heinrich-Heine-Universität, Düsseldorf
Universitätsstr. 1
40225 Düsseldorf, Germany
E-mail: margherita.piccolo@hhu.de