ON THE 16-RANK OF CLASS GROUPS OF $\mathbb{Q}(\sqrt{-3p})$ FOR PRIMES $p$ CONGRUENT TO 1 MODULO 4

MARGHERITA PICCOLO

Abstract. For fixed $q \in \{3, 7, 11, 19, 43, 67, 163\}$, we consider the density of primes $p$ congruent to 1 modulo 4 such that the class group of the number field $\mathbb{Q}(\sqrt{-qp})$ has order divisible by 16. We show that this density is equal to $1/8$, in line with a more general conjecture of Gerth. Vinogradov’s method is the key analytic tool for our work.

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 [8] studied the density for the 16-rank in certain particular thin families of quadratic number fields. Koymans and Milovic [4] [5] 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 [3], which extends a conjecture of Cohen and Lenstra [1] to include the 2-part. It is expected that the group $2 \text{Cl}(K)[2^\infty]$ satisfies the Cohen–Lenstra heuristic, where $K$ varies over imaginary quadratic number fields and $\text{Cl}(K)[2^\infty]$ denotes the 2-part of the class group $\text{Cl}(K)$. More recently, Smith [10] proved Gerth’s conjecture and he 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 to primes $p$ congruent to 1 modulo 4, so that only two primes divide the discriminant. In this situation, we obtain that the 2-part of the class group $\text{Cl}(\mathbb{Q}(\sqrt{-3p}))$ is non-trivial and cyclic, by Gauss genus theory. Moreover, our approach to $\mathbb{Q}(\sqrt{-3p})$, extends to families $K_{p,q} := \mathbb{Q}(\sqrt{-qp})$ with fixed $q \in \mathbb{Q} := \{3, 7, 11, 19, 43, 67, 163\}$ 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 [11]). 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

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

Then we have

$$\sum_{\substack{p \leq x \\ p \equiv 1 \mod 4}} e_p \ll x^{1 - \frac{1}{3200}} \quad \text{for } x > 0.$$ 

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

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

exists and $\delta(16) = \frac{1}{8}$.

The main tool we use is the generalized version of Vinogradov’s method in the setting of number fields, given by Friedlander et al. [2], similarly as in the works of Koymans and Milovic [11] [12]. Moreover, as in [3], our results are unconditional in contrast to the work of Friedlander et al. [2], 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 $n$-th 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 $\mu_n$ the group of $n$-th roots of unity in $\mathbb{C}$. Let $K_p$ be the completion of $K$ with respect to a finite prime $p$ of $K$. We assume that $K_p^{\times}$ contains a primitive $n$-th root of unity. Then $L_p := K_p(\sqrt[n]{K_p^{\times}})$ is the maximal abelian extension of exponent $n$ of $K_p$, by Kummer theory.

We employ the notation of [9, Chapter V, §3]. The $n$-th Hilbert symbol is the non-degenerate bilinear pairing

$$\left(\frac{\cdot}{p}\right)_{K,n} : K_p^{\times}/(K_p^{\times})^n \times K_p^{\times}/(K_p^{\times})^n \longrightarrow \mu_n$$

$$(a,b) \mapsto \frac{\sigma_a(a/b)}{a/b},$$

where $\sigma_a$ is the corresponding element of $a$ in $\text{Gal}(L_p/K_p)$, given by the isomorphism $K_p^{\times}/(K_p^{\times})^n \cong \text{Gal}(L_p/K_p)$ of class field theory. We recall basic properties of this symbol, see [9, Chapter V, §3, Proposition 3.2].
Proposition 2.1. For all \(a, a', b, b' \in K_p^\times / (K_p^\times)^n\), the \(n\)-th Hilbert symbol has the following properties:

(i) \(\left( \frac{aa'}{p} \right)_{K,n} = \left( \frac{a}{p} \right)_{K,n} \left( \frac{a'}{p} \right)_{K,n}\),

(ii) \(\left( \frac{ab'}{p} \right)_{K,n} = \left( \frac{a}{p} \right)_{K,n} \left( \frac{b}{p} \right)_{K,n}\),

(iii) \(\left( \frac{a}{p} \right)_{K,n} = 1 \iff a \text{ lies in the image of the norm map of the extension } K_p(\sqrt[n]{b})/K_p\),

(iv) \(\left( \frac{a}{p} \right)_{K,n} = \left( \frac{b}{p} \right)_{K,n}^{-1}\),

(v) \(\left( \frac{a-b}{p} \right)_{K,n} = 1 \text{ and } \left( \frac{a-b}{p} \right)_{K,n} = 1\),

(vi) if \(\left( \frac{a}{b} \right)_{K,n} = 1 \text{ for all } b \in K_p^\times\), then \(a \in K_p^\times\).

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

\[
\left( \frac{a}{b} \right)_{K,n} \equiv a^{N-1} \mod p.
\]

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

\[
\left( \frac{a}{b} \right)_{K,n} := \prod_{p^e \mid b} \left( a \right)^{\text{ord}_p(b)}
\]

and we set \(\left( \frac{a}{b} \right)_{K,n} = 0\) if \(a\) is not coprime to \(b\). For \(b \in \mathcal{O}_K\), we define

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

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 \(M_q := \mathbb{Q}(-1, \sqrt[q]{b})\), for \(q \in Q\) with \(Q = \{3, 7, 11, 19, 43, 67, 163\}\), 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 \( q \not= 7 \). Using [9, Chapter VI, §8, Theorem 8.3], we get
\[
\left( \frac{a}{b} \right)_{M_q,4} = \left( \frac{b}{a} \right)_{M_q,4} \cdot \left( \frac{a, b}{3} \right)_{M_q,4}
\]
where \( \mathcal{I} \) 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 \( \left( \frac{a \cdot b}{3} \right)_{M_q,4} \) depends only on \( a \) and \( b \) modulo 32. If \( a \equiv 1 \mod 32 \), where \( a \in \mathcal{O}(M_q) \), then \( a \) is a fourth power in \((M_q)\gamma\) by Hensel’s lemma. So we deduce that
\[
\left( \frac{a, b}{3} \right)_{M_q,4} = 1
\]
applying property \( (iii) \) of Proposition 2.1. If \( b \) is congruent to 1 modulo 32, then we get the same result using properties \( (iii) \) and \( (iv) \) of Proposition 2.1.

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 \( a \equiv a' \mod 32 \) and \( b \equiv b' \mod 32 \). Then \( a = \gamma a' \) and \( b = \gamma b' \) with \( \gamma, \tilde{\gamma} \) congruent to 1 modulo 32. Using properties \( (i) \) and \( (ii) \) of Proposition 2.1, we get
\[
\left( \frac{a, b}{3} \right)_{M_q,4} = \left( \frac{\gamma a', \tilde{\gamma} b'}{3} \right)_{M_q,4} = \left( \frac{\gamma, \tilde{\gamma}}{3} \right)_{M_q,4} \left( \frac{a', b'}{3} \right)_{M_q,4}
\]
In the case of \( q = 7 \), we have two different prime ideals \( \mathcal{I}_1 \) and \( \mathcal{I}_2 \), in \( M_7 \) above 2. So we have
\[
\left( \frac{a}{b} \right)_{M_7,4} = \left( \frac{b}{a} \right)_{M_7,4} \left( \frac{a, b}{\mathcal{I}_1} \right)_{M_7,4} \left( \frac{a, b}{\mathcal{I}_2} \right)_{M_7,4}
\]
Nonetheless, we can use the very same argument we used before, taking into account that we have two different prime ideals above 2 instead of just one.

Now, let us prove that \( (a/b)_{M_6,4} \) depends only on the congruence class of \( b \) modulo 32a\( \mathcal{O}_{M_6} \). Using [9, Chapter VI, §8, Theorem 8.3], we obtain
\[
\left( \frac{a}{b} \right)_{M_q,4} = \prod_{p \not\in S(a)} \left( \frac{b, a}{p} \right)_{M_q,4} = \prod_{p \in S(a)} \left( \frac{a, b}{p} \right)_{M_q,4},
\]
where \( S(a) := \{ p : p \mid n \cdot \infty \text{ or } \ord_p(a) \neq 0 \} \).

As for the prime ideal \( \mathcal{I} \), we already saw that \( \left( \frac{a, b}{3} \right)_{M_q,4} \) depends only on \( b \) modulo 32 (and the same holds for \( \mathcal{I}_1 \) and \( \mathcal{I}_2 \) in the case of \( q = 7 \)). If \( p \in S(a) \) is odd, we have
\[
\left( \frac{a, b}{p} \right)_{M_q,4} = \left( \frac{b}{p} \right)^{\ord_p(a)}_{M_q,4}.
\]
Hence the value of these symbols depends only on \( b \) modulo \( a \). Therefore the total symbol depends only on \( b \) modulo 32a. \( \square \)
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 [4, §3.2].

**Lemma 2.3.** Let $K$ be a number field and let $p$ 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 $p$ splits in $L$. Denote by $\psi$ the non-trivial element in $\text{Gal}(L/K)$. Then if $\psi$ fixes $\mathbb{Q}(\sqrt{-1})$, we have for all $\alpha \in \mathcal{O}_K$

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

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

$$\left( \frac{\alpha}{p \mathcal{O}_L} \right)_{L/A} = 1.$$

**Lemma 2.4.** Let $K$ be a number field and let $p$ 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 $p$ stays inert in $L$. We have for all $\alpha \in \mathcal{O}_K$

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

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

### 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 $\text{rk}_{2^k} G$, is the dimension of the $\mathbb{F}_2$-vector space $2^{k-1} G / 2^k G$. If the 2-Sylow subgroup of $G$ is cyclic, we have $\text{rk}_{2^k} G \in \{0, 1\}$ and $\text{rk}_{2^k} G = 1$ if and only if $2^k | \#G$. We will study the necessary and sufficient conditions such that $2^k \mid h(-qp)$ for $k \in \{1, 2, 3, 4\}$. Moreover, for each integer $k \geq 1$ and fixed $q \in Q$ with $Q = \{3, 7, 11, 19, 43, 67, 163\}$, we define a density $\delta(2^k)$ as

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

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 $p$ a prime congruent to 1 modulo 4. Then, by Gauss genus theory, we have that $| \text{Cl}(K_{p,q})[2] | = 2$ and so $\delta(2) = 1$. In particular, it follows that the 2-Sylow subgroup $\text{Cl}(K_{p,q})[2^\infty]$ 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

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

where $t$ is the prime ideal above $q$ and $p$ 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 that $\text{rk}_4 \text{Cl}(K_{p,q}) = 1$ if and only if the map
\[ \varphi : \text{Cl}(K_{p,q})[2] \rightarrow \text{Cl}(K_{p,q})/2 \text{Cl}(K_{p,q}) \]
is the zero map. By class field theory, the genus field $H_2$ is the field $K_{p,q}(\sqrt{-q})$ and we have
\[ \text{Cl}(K_{p,q})/2 \text{Cl}(K_{p,q}) \cong \text{Gal}(H_2/K_{p,q}). \]
So the map $\varphi$ is trivial if and only if the Artin symbol corresponding to $p$, the prime ideal above $p$, (or analogously the one corresponding to $t$) is trivial. It is equivalent to say that $p$ (or analogously $t$) 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
\[ 4 | h(-qp) \iff \left(\frac{-q}{p}\right) = 1 \iff \left(\frac{p}{q}\right) = 1. \]
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 $\delta(4) = \frac{1}{2}$.

3.3. The 8-rank. We have an element of order 8 in the class group if and only if the map
\[ \psi : \text{Cl}(K_{p,q})[2] \rightarrow \text{Cl}(K_{p,q})/4 \text{Cl}(K_{p,q}) \]
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 $\text{Gal}(H_4/K_{p,q}) \cong \text{Cl}(K_{p,q})/4 \text{Cl}(K_{p,q})$. The map $\psi$ is trivial if and only if the Artin symbol of $p$ (resp. of $t$) of the extension $K_{p,q} \subset H_4$ is trivial that corresponds to ask that $p$ (resp. $t$) 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 us call $F := \mathbb{Q}(\sqrt{-q})$. We have

\[ H_4 \quad \xrightarrow{\text{inclusion}} \quad H_2 = \mathbb{Q}(\sqrt{-q}, \sqrt{p}) \quad \xrightarrow{\text{inclusion}} \quad F = \mathbb{Q}(\sqrt{-q}) \quad \xrightarrow{\text{inclusion}} \quad K_{p,q} = \mathbb{Q}(\sqrt{-qp}) \quad \xrightarrow{\text{inclusion}} \quad \mathbb{Q}(\sqrt{p}) \quad \xrightarrow{\text{inclusion}} \quad \mathbb{Q} \]

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 $p_1$ and $p_2$, they are tamely ramified of ramification index 2. The conductor of this extension is $p$. Let $\text{Cl}_p(F)$ be the ray class group with respect to the conductor $p$. Recall that we have an exact sequence of finite abelian groups
\[ 0 \rightarrow (\mathcal{O}_F/p \mathcal{O}_F)^\times /\text{Im}(\mathcal{O}_F^\times) \rightarrow \text{Cl}_p(F) \rightarrow \text{Cl}(F) \rightarrow 0 \]
and, since $\text{Cl}(F) = 1$, we have the following isomorphism
\[ (\mathcal{O}_F/p \mathcal{O}_F)^\times /\text{Im}(\mathcal{O}_F^\times) \cong \text{Cl}_p(F). \]
Note that $(\mathcal{O}_F/p \mathcal{O}_F)^\times \cong (\mathcal{O}_F/p_1 \mathcal{O}_F)^\times \times (\mathcal{O}_F/p_2 \mathcal{O}_F)^\times$ and for $i \in \{1, 2\}$, each factor $(\mathcal{O}_F/p_i \mathcal{O}_F)^\times$ is isomorphic to $\mathbb{F}_p^\times$. The Artin map ensures us the existence of a surjection

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

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

$$\text{(3.1)} \quad (\mathbb{F}_p^\times \times \mathbb{F}_p^\times) / \mathfrak{a} \cong \text{Cl}_p(F) / 2 \text{Cl}_p(F) \cong \text{Gal}(H_4/F) \cong C_2 \times C_2.$$

In order to have that $(\sqrt{-q})$ splits completely in $H_4$, we want that its Artin symbol is trivial. Hence, considering (3.1), we need that $\sqrt{-q}$ is 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

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

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

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

$$\mathbb{Q}(\sqrt{-1}, \sqrt{-q}) \xrightarrow{\mathbb{Q}(\sqrt{-1}, \sqrt{-q})} \mathbb{Q}(\sqrt{-1}, \sqrt{-q}) \xrightarrow{\mathbb{Q}(\sqrt{-1}, \sqrt{-q})} \mathbb{Q}$$

we have 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 we have that $\mathfrak{p}$ splits completely in $\mathbb{Q}(\sqrt{-1}, \sqrt{-q})$ if and only if $p$ splits completely in $\mathbb{Q}(\sqrt{-1}, \sqrt{-q})$ 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 $\pi$ 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 that

$$\left(\frac{-q}{p}\right)_{\mathbb{Q}(\sqrt{-1}, \sqrt{-q})} = \left(\frac{-q}{\pi}\right)_{\mathbb{Q}(\sqrt{-1}, \sqrt{-q})}.$$
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 we have \( (-q/p) = 1 \). We already know that \( M_q \) is a principal ideal domain. Let \( \zeta_{12} \) be a 12-th root of unity and \( i = \sqrt{-1} \) be a fourth root of unity. We see that \( \mathcal{O}_{M_q}^{*} = \langle \nu_q \rangle \times \langle \varepsilon_q \rangle \), where

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

and

\[
\varepsilon_3 = \zeta_{12} - 1, \\
\varepsilon_7 = \frac{1}{2}(1 - i)(\sqrt{7} + 3), \\
\varepsilon_{11} = \frac{1}{2}(1 - i)(\sqrt{11} + 3), \\
\varepsilon_{19} = \frac{1}{2}(1 + i)(3\sqrt{19} + 13), \\
\varepsilon_{43} = \frac{1}{2}(1 + i)(9\sqrt{43} - 59), \\
\varepsilon_{67} = \frac{1}{2}(1 + i)(27\sqrt{67} - 221), \\
\varepsilon_{163} = \frac{1}{2}(1 - i)(627\sqrt{163} + 8005).
\]

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 \( \sigma \) fixes \( \mathbb{Q}(\sqrt{q}) \) and \( \tau \) fixes \( \mathbb{Q}(\sqrt{-1}) \).

\[
\begin{array}{c}
\mathbb{Q}(\sqrt{-1}, \sqrt{q}) \\
\mathcal{O}_{M_q}^{*} \\
\mathbb{Q}(\sqrt{-1}) \\
\mathbb{Q}(\sqrt{-q}) \\
\mathbb{Q}(\sqrt{q}) \\
\mathbb{Q}
\end{array}
\]

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

\[
\pm p = N_{M_q/\mathbb{Q}(\pi)} = (u + \sqrt{q}v)(u - \sqrt{q}v) = u^2 - qv^2.
\]

Looking at this equation mod 4, we have

\[
(3.4) \quad p = u^2 - qv^2,
\]

as wanted. Thus we can choose

\[
u = \frac{\pi \sigma(\pi) + \tau(\pi)\tau(\sigma(\pi))}{2\sqrt{q}} \quad \text{and} \quad v = \frac{\pi \sigma(\pi) - \tau(\pi)\tau(\sigma(\pi))}{2\sqrt{q}}.
\]
We now check that \( u > 0 \) and that we can always find \( u \equiv 1 \mod 4 \). In fact, if \( u_0 \) and \( v_0 \) are a solution of (3.3), then also \( u + \sqrt{q}v = (u_0 + \sqrt{q}v_0)(\varepsilon_q)\varepsilon_q^k \), for \( k \in \mathbb{N} \), is a solution. Indeed

\[
N_{M/\mathbb{Q}((\sqrt{q}))}(\pi) = N_{M/\mathbb{Q}((\sqrt{q}))}(\varepsilon_q \pi) = \varepsilon_q(u_0 + \sqrt{q}v_0).
\]

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

\[
(3.5) \quad Z/4Z \times Z/4Z \rightarrow Z/4Z \times Z/4Z,
\]

\[
(u, v) \mapsto (2u - 3v, 2v - u), \quad \text{if } q = 3, 11, 19, 163,
\]

\[
(u, v) \mapsto (v, 3u), \quad \text{if } q = 7,
\]

\[
(u, v) \mapsto (2u + 3v, u + 2v), \quad \text{if } q = 43, 67.
\]

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 afore defined map, we note that those are of length 4 and that we always find exactly one \( u \) in each orbit that satisfies \( u \equiv 1 \mod 4 \).

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

\[
u(\alpha) = \frac{1}{2}(\alpha + \tau(\alpha)).
\]

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

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

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 \( u(w\sigma(w)) \equiv 1 \mod 4 \). We note that

\[
(3.6) \quad \left( \frac{u(w\sigma(w))}{w} \right)_{M_q,4} = \left( \frac{(w\sigma(w) + \tau(w\sigma(w)))}{w} \right)_{M_q,4} = \left( \frac{\tau(w\sigma(w))}{w} \right)_{M_q,4} \left( \frac{8}{w} \right)_{M_q,4}.
\]

Let \( \varepsilon_q \) be as in (3.3). Then

\[
\left( \frac{u(\varepsilon_q^4w\sigma(\varepsilon_q^4w))}{\varepsilon_q^4w} \right)_{M_q,4} = \left( \frac{u(\varepsilon_q^4w\sigma(\varepsilon_q^4w))}{w} \right)_{M_q,4} = \left( \frac{\tau(\varepsilon_q^4w\sigma(\varepsilon_q^4w))}{w} \right)_{M_q,4} \left( \frac{8}{w} \right)_{M_q,4} = \left( \frac{u(w\sigma(w))}{w} \right)_{M_q,4}.
\]

The equality

\[
\left( \frac{2}{u(\varepsilon_q^4w\sigma(\varepsilon_q^4w))} \right)_{\mathbb{Q},2} = \left( \frac{2}{u(w\sigma(w))} \right)_{\mathbb{Q},2},
\]
is given by $2u(e_q^j w \sigma(e_q^j w)) \equiv 2u(w \sigma(w)) \mod 16$. In fact, we have that $2u(e_q^j w \sigma(e_q^j w)) = (e_q \sigma(e_q))^j w \sigma(w) + \tau(e_q \sigma(e_q))^j \tau(w \sigma(w))$ and a straightforward computation (with $w \sigma(w) = u + \sqrt{q} v$) shows that

\begin{align*}
2u(e_q^3 w \sigma(e_q^3 w)) &= 194 u - 336 v, \\
2u(e_q^7 w \sigma(e_q^7 w)) &= 64514 u + 170688 v, \\
2u(e_q^1 w \sigma(e_q^1 w)) &= 158402 u + 525360 v, \\
2u(e_q^{19} w \sigma(e_q^{19} w)) &= 13362897602 u + 58247520240 v, \\
2u(e_q^{43} w \sigma(e_q^{43} w)) &= 2351987525322434 u - 15423013607227056 v, \\
2u(e_q^{107} w \sigma(e_q^{107} w)) &= 91052891016584133314 u - 745300033869597034608 v, \\
2u(e_q^{163} w \sigma(e_q^{163} w)) &= 269780589805913908506459977860802 u \\
&\quad + 3444327998561165640260096561357040 v.
\end{align*}

Hence we proved that $[w] = [e_q^j w]$. 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 $u(\zeta_{12} w \sigma(\zeta_{12} w)) = u(w \sigma(w))$. For the other values of $q$, note that $i \sigma(i) = 1$ and so $\tau(i \sigma(i)) = 1$. Then $u(i w \sigma(i w)) = u(w \sigma(w))$.

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

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

Then

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

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

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

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

Having determined the action of the units $O_{M_q}^\times$, on this sum and on $[\cdot]$, we see that the quantity $\sum_{i=0}^{3} s(e_q^i w)[e_q^i w]$ does not depend on the choice of the generator $w$ but only on the prime ideal $p$ 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 $p$ be a prime ideal of $O_{M_q}$, lying above $p$, with generator $w$. Then

$$\sum_{i=0}^{3} s(e_q^i w)[e_q^i w] = \frac{1}{2} \left( 1 + \frac{-q}{e_q^i w} \right)_{M_q/4} = \begin{cases} 1 & \text{if } 16 \mid h(-qp), \\ -1 & \text{if } 8 \mid h(-qp) \text{ but } 16 \nmid h(-qp), \\ 0 & \text{otherwise.}\end{cases}$$
We define the sequence \( \{ a_{n,q} \} \), indexed by ideals of \( \mathcal{O}_{M_q} \), in the following way

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

where \( w \) is any generator of the ideal \( n \) 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. in [2]. In order to use this powerful machinery, we need to verify that the sequence \( \{ a_{n,q} \} \) defined in (3.8), satisfies the hypothesis of [2, Proposition 5.2]. In other words, it remains to prove analogues of Propositions 3.7 and 3.8 of [4] for our sequences \( \{ a_{n,q} \} \) 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 that

\[
\sum_{N(n) \leq x} a_{n,q} A(n) \ll \varepsilon x^{1-\varepsilon}, \quad \text{with } x > 0,
\]

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

4.1. Sums of type I. In this section, we will adapt the proof of [4, Proposition 3.7] for our sequence \( \{ a_{n,q} \} \) and the field \( M_q \) for \( q \) fixed.

Let \( m \) be an ideal of \( \mathcal{O}_{M_q} \) coprime with \( n_q \). We want to bound the following sum

\[
A(x) = A(x, m) := \sum_{N(n) \leq x} a_{n,q}
\]

\[
= \sum_{N(n) \leq x} \left( \sum_{(n, n_q) = 1, m|n} \left( \sum_{i=0}^{3} s(\varepsilon_q^i \alpha)[\varepsilon_q^i \alpha]^\frac{1}{2} \left( 1 + \left( \frac{-q}{\varepsilon_q^i \alpha} \right)_{M_q,4} \right) \right) \right),
\]

where \( \alpha \) is a generator of \( n \). 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 \( D_q \) as described in [4, Lemma 3.5] with \( F = M_q \) and \( n = 4 \).

In the case \( q = 3 \), the torsion group of \( \mathcal{O}_{M_q}^\times \) has twelve elements and then every ideal \( n \) 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 \( n \) has exactly four generators \( \alpha \in \mathcal{D}_q \). We recall that \( s(\alpha) \) depends only on the congruence class of \( \alpha \) modulo 4. See that

\[
[\alpha] = \left( \frac{u(\alpha \sigma(\alpha))}{\alpha} \right)_{M_q,4} \left( \frac{2}{\alpha u(\alpha \sigma(\alpha))} \right)_{\mathbb{Q},2}
\]

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

The symbol \( \left( \frac{2}{\alpha u(\alpha \sigma(\alpha))} \right)_{\mathbb{Q},2} \) depends only on the congruence class of \( \alpha \) modulo 8 and, by Lemma 2.2, the symbol \( \left( \frac{8}{\alpha} \right)_{M_q,4} \) depends only on the congruence class of \( \alpha \) 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 \(\alpha\) modulo \(32q\) and so we find that

\[
A(x) = \frac{1}{12} \sum_{i=0}^{3} \sum_{\rho \mod F_q \atop (\rho, F_q) = 1} \frac{1}{2} \mu(\rho, \varepsilon_q^i) A(x; \rho, \varepsilon_q^i) \left( 1 + \left( \frac{-3}{\varepsilon_q^i \alpha} \right)_{M_q,4} \right) \quad \text{for } q = 3,
\]

and

\[
A(x) = \frac{1}{4} \sum_{i=0}^{3} \sum_{\rho \mod F_q \atop (\rho, F_q) = 1} \frac{1}{2} \mu(\rho, \varepsilon_q^i) A(x; \rho, \varepsilon_q^i) \left( 1 + \left( \frac{-q}{\varepsilon_q^i \alpha} \right)_{M_q,4} \right) \quad \text{otherwise,}
\]

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

\[
A(x; \rho, \varepsilon_q^i) := \sum_{\alpha \in \varepsilon_q^i D_q, N(\alpha) \leq x \atop \alpha \equiv \rho \mod F_q \atop \alpha \equiv 0 \mod m} \left( \frac{\tau(\alpha)}{\alpha} \right)_{M_q,4} \left( \frac{\tau(\sigma(\alpha))}{\alpha} \right)_{M_q,4}.
\]

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

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

Hence we have the following bound

\[
|A(x)| \leq \frac{1}{4} \sum_{i=0}^{3} \sum_{\rho \mod F_q \atop (\rho, F_q) = 1} |A(x; \rho, \varepsilon_q^i)|
\]

for every \(q \in Q\).

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

\[
\mathbb{M} = \mathbb{Z} n_1^{(q)} \oplus \mathbb{Z} n_2^{(q)} \oplus \mathbb{Z} n_3^{(q)}
\]

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 four. We write \(\alpha\) uniquely as

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

so our summation conditions become

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

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

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

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

Hence we have
\[
\left( \frac{\tau(\alpha)}{\alpha} \right)_{M_q, A} = \left( \frac{a + \tau(\beta)}{\alpha} \right)_{M_q, A} = \left( \frac{\tau(\beta) - \beta}{\alpha} \right)_{M_q, A} = \left( \frac{\eta^4 c_0 c}{\alpha} \right)_{M_q, A} = \left( \frac{c_0}{\alpha} \right)_{M_q, A} \left( \frac{c}{\alpha} \right)_{M_q, A}.
\]

Since we are working with \( \alpha \equiv \rho \mod F_q \), \( (\rho, F_q) = 1 \) and \( c' \) depend only on \( \beta \), we apply Lemma 2.2 and we obtain
\[
\left( \frac{\tau(\alpha)}{\alpha} \right)_{M_q, A} = \tilde{\mu} \cdot \left( \frac{a + \beta}{c \mathcal{O}_{M_q}} \right)_{M_q, A},
\]
and the same for the other quadric symbol
\[
\left( \frac{\tau(\sigma(\alpha))}{\alpha} \right)_{M_q, A} = \tilde{\mu}' \cdot \left( \frac{a + \beta}{c' \mathcal{O}_{M_q}} \right)_{M_q, A},
\]
with \( \tilde{\mu}, \tilde{\mu}' \in \{ \pm 1, \pm i \} \) that depend only on \( \rho \) and \( \beta \). Hence
\[
A(x; \rho, \varepsilon_q^i) \leq \sum_{\beta \in \mathbb{M}} |T(x; \beta, \rho, \varepsilon_q^i)|,
\]
where
\[
T(x; \beta, \rho, \varepsilon_q^i) := \sum_{a \in \mathbb{Z} \atop a + \beta \text{ sat.} [14]} \left( \frac{a + \beta}{c \mathcal{O}_{M_q}} \right)_{M_q, A} \left( \frac{a + \beta}{c' \mathcal{O}_{M_q}} \right)_{M_q, A}.
\]

In order to study \( (\alpha + \beta/c \mathcal{O}_{M_q})_{M_q, A} \), we want to replace \( \beta \) 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 \( g \) and \( l \in \mathbb{Z}[\sqrt{-1}] \) in a unique way such that
\[
(c) = gl
\]
with \( l := N_{Q(\sqrt{-1})/Q}(l) \) a squarefree integer coprime with \( n_q \) and \( g := N_{Q(\sqrt{-1})/Q}(g) \) a squarefull integer coprime with \( n_q l \).

Note that \( c \) is coprime with \( 2q \). Hence, in the factorization of the ideal \( l \), all the prime ideals that divide \( l \) in \( \mathbb{Z}[\sqrt{-1}] \) do not ramify in the quadratic extension \( M_q \). We can then apply Lemma 2.3 for any prime ideal dividing \( l \) and, using the Chinese Remainder Theorem, we find \( \beta' \in \mathbb{Z}[\sqrt{-1}] \) such that \( \beta \equiv \beta' \mod \mathcal{O}_{M_q} \). We obtain that the upper entry of our quartic residue symbol is in \( \mathbb{Z}[\sqrt{-1}] \).

If a prime ideal \( p \) that divides \( l \) and splits in \( M_q \), we apply Lemma 2.3 in order to reduce our quartic symbol to a quadratic one. If \( p \) stays inert in \( M_q \), then we have that \( p \) has degree 1. If we define \( p := p \cap \mathbb{Z} \), we find that \( p \equiv 1 \mod 4 \), since \( p \) splits in \( \mathbb{Z}[\sqrt{-1}] \), and so \( (p + 1)/2 \) is an odd number. Applying Lemma 2.3 and combining all these results, we have
\[
\left( \frac{\alpha + \beta'}{l \mathcal{O}_{M_q}} \right)_{M_q, A} = \left( \frac{\alpha + \beta'}{l} \right)_{Q(\sqrt{-1}), 2}.
\]
Using again the Chinese Remainder Theorem and the fact that \( l \) is squarefree, we find a rational integer \( b \) such that \( \beta' \equiv b \mod l \). Hence, we have

\[
\left( \frac{a + \beta}{c \mathcal{O}_M} \right)_{M,q,4} = \left( \frac{a + \beta}{g \mathcal{O}_M} \right)_{M,q,4} \left( \frac{a + b}{l} \right)_{\mathbb{Q}(\sqrt{-1}), 2}.
\]

Note that \( b \) depends on \( \beta \) and not on \( a \), because \( c \) depends only on \( \beta \). We define the product of all the primes dividing \( g \) as \( g_0 := \prod_{p|g} p \) and the product of all the prime ideals dividing \( g \) as \( g^* := \prod_{p|g} \mathfrak{p} \). The quartic symbol \( (\alpha/g)_{M,q,4} \) is periodic in the upper entry modulo \( g^* \), and so also modulo \( g_0 \), since \( g^* \) divides it. Since our \( \beta \) is fixed, we can split \( T(x; \beta', \rho, \varepsilon_q') \) into residue classes modulo \( g_0 \), and we obtain

\[
| T(x; \beta, \rho, \varepsilon_q') | \leq \sum_{a_0 \mod g_0} \left| \sum_{a \in \mathbb{Z}, a \equiv a_0 \mod g_0, a + \beta \text{ sat. } \mathfrak{L}} \left( \frac{a + b}{q} \right)_{\mathbb{Q}(\sqrt{-1}), 2} \left( \frac{a + \beta}{c' \mathcal{O}_M} \right)_{M,q,4} \right|.
\]

Now, we focus on the quartic symbol \( \left( \frac{a + \beta}{c' \mathcal{O}_M} \right)_{M,q,4} \). We prove that it is the indicator function for \( \gcd(a + \beta, c') \). Note that we have chosen \( c' \in \mathbb{Z} \left[ \frac{1 + \sqrt{-q}}{2} \right] \) and that it is coprime with \( n_q \). We factor the principal ideal \( (c') \subset \mathbb{Z} \left[ \frac{1 + \sqrt{-q}}{2} \right] \) as \( (c') = \prod_{i=1}^k \mathfrak{p}_i^{e_i} \), where all the \( \mathfrak{p}_i \)'s are prime ideals of \( \mathbb{Z} \left[ \frac{1 + \sqrt{-q}}{2} \right] \) 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 that we gave and we have

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

To prove that our claim is true, we need to show that \( \left( \frac{(a + \beta)/\mathfrak{p} \mathcal{O}_M}{M,q,4} \right) = 1 \) whenever \( \mathfrak{p} \nmid a + \beta \). Using Lemma 2.3 instead of \( \beta \) we can work with \( \beta' \in \mathbb{Z} \left[ \frac{1 + \sqrt{-q}}{2} \right] \). Then we can apply Lemma 2.3 for the prime ideals \( \mathfrak{p} \) that split in \( M_q \). Instead, if \( \mathfrak{p} \) stays inert in \( M_q \), we have that \( p := \mathfrak{p} \cap \mathbb{Z} \) 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 with Lemma 2.4.

Hence we obtain

\[
\left( \frac{a + \beta}{c' \mathcal{O}_M} \right)_{M,q,4} = \mathbb{1}_{\gcd(a + \beta, c') = 1} = \sum_{\mathfrak{d}|c', \mathfrak{d}|a + \beta} \mu(\mathfrak{d}),
\]

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

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

We obtain

\[
| T(x; \beta, \rho, \varepsilon_q^i) | \leq \sum_{a_0 \mod g_0} \sum_{\mathfrak{d}|c', \mathfrak{d}\text{ squarefree}} | T(x; \beta, \rho, \varepsilon_q^i, a_0, \mathfrak{d}) |,
\]
with

$$T(x; \beta, \rho, \varepsilon_i^j, a_0, \varnothing) := \sum_{a \in \mathbb{Z} \atop a+\beta \text{ sat. } \mathfrak{l}} \left( \frac{a+b}{l} \right)_{\mathbb{Q}(\sqrt{-1})}^2.$$

From now on we can follow the steps of Koymans and Milovic in [11 §4, p. 17] where our \( l \) corresponds to \( q \), our integral basis correspond to the generically written basis \( \{1, \eta_1^{(q)}, \eta_2^{(q)}, \eta_3^{(q)}\} \) and our units \( \varepsilon_i^j \) correspond to the units as \( u_i \).

4.2. **Sums of type II.** In this section, we will adapt the proof of [11 Proposition 3.8] for our sequence \( (a_{n,q}) \) 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 with \( n_q \). Recalling our definition of the symbol \([ \cdot ]\) in (3.6) and the observation of (3.7), we have

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

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

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

We note that \( Q_2(w, z) \in \{\pm 1, \pm i\} \) depends only on the congruence class of \( w \) and \( z \) modulo 8.

Now we want to simplify the quartic residue symbols. We use Lemma 2.2 to find some \( \mu_1 \in \{\pm 1, \pm i\} \) that depends on the congruence classes of \( w \) and \( z \) modulo 32, such that we have

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

since \( \tau(i) = i \). For the remaining symbols, we can find some \( \mu_2 \in \{\pm 1, \pm i\} \) that depends on the congruence classes of \( w \) and \( z \) modulo 32, such that

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

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 we get

$$[wz] = \mu_3 [w][z] \left( \frac{z}{\tau(w)} \right)_{M_q,2} \mathbb{1}_{\gcd(z, \tau\sigma(w))=1}.$$
We consider \( \{\alpha_n\}_n \) and \( \{\beta_n\}_n \) two bounded sequences of complex numbers. Then
\[
\sum_{N(\alpha) \leq N} \sum_{N(\beta) \leq N} \alpha_n \beta_n a_{mn} =
\]
\[
\frac{1}{12^2} \sum_{w \in \mathcal{D}_q(M)} \sum_{z \in \mathcal{D}_q(N)} \alpha_w \beta_z \left( \sum_{i=0}^{3} s(\varepsilon_q^i w z) [\varepsilon_q^i w z] \frac{1}{2} \left( 1 + \left( \frac{-3}{\varepsilon_q^i w z} \right)_{M_{3,4}} \right) \right)
\]
for \( q = 3 \) and for the other \( q \in \mathbb{Q} \setminus \{3\} \) we have
\[
\sum_{N(\alpha) \leq N} \sum_{N(\beta) \leq N} \alpha_n \beta_n a_{mn} =
\]
\[
\frac{1}{4^2} \sum_{w \in \mathcal{D}_q(M)} \sum_{z \in \mathcal{D}_q(N)} \alpha_w \beta_z \left( \sum_{i=0}^{3} s(\varepsilon_q^i w z) [\varepsilon_q^i w z] \frac{1}{2} \left( 1 + \left( \frac{-q}{\varepsilon_q^i w z} \right)_{M_{q,4}} \right) \right).
\]

using \([4] \text{ Lemma 3.5}\) 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 \( q \in \mathbb{Q} \setminus \{3\} \) and defining \( \alpha_w := \alpha_w(w) \) and \( \beta_z := \beta_z(z) \). We note that \( s(\varepsilon_q^i w z) \) depends on the congruence class of \( w z \) modulo \( 4 \) and that \( [\varepsilon_q^i w z] = \mu_q[w z] \) for some \( \mu_q \in \{\pm 1, \pm i\} \) depending on the congruence class modulo \( 32 \), by Lemma \([4] \text{ Lemma 2.2}\). What is more, the expression \( \frac{1}{2} \left( \left( \frac{-q}{\varepsilon_q^i w z} \right)_{M_{q,4}} + 1 \right) \) takes values in the set \( \{0, 1, (1+i)/2, (1-i)/2\} \). This implies that
\[
\left| \frac{1}{2} \left( 1 + \left( \frac{-q}{\varepsilon_q^i w z} \right)_{M_{q,4}} \right) \right| \leq 1.
\]

We focus on the congruence classes of \( w \) and \( z \) modulo \( 4 \cdot 2^5 \) and so we can bound the previous sums by a finite number of sums of the form
\[
\mu_5 \sum_{w \in \mathcal{D}_q(M)} \sum_{z \in \mathcal{D}_q(N)} \alpha_w \beta_z [w z],
\]
where \( \mu_5 \) depends on the congruence classes \( \omega \) and \( \zeta \) modulo \( q \cdot 2^5 \).

We now use our simplification of the symbol \([w z]\) of \([4,3]\) and we replace \( \alpha_w \) and \( \beta_z \) with \( \alpha_w[w] \) and \( \beta_z[z] \). Then, if we consider \( \mu_6 \in \{\pm 1, \pm i\} \) depending only on \( \omega \) and \( \zeta \), we have
\[
\mu_6 \sum_{w \in \mathcal{D}_q(M)} \sum_{z \in \mathcal{D}_q(N)} \alpha_w \beta_z \left( \frac{z}{\tau(w)} \right)_{M_{q,2}} 1_{\gcd(z,\tau(w))=1}.
\]
The last thing to do is to check that the function
\[
\gamma(w, z) := \left( \frac{z}{\tau(w)} \right)_{M_{q,2}} 1_{\gcd(z,\tau(w))=1}
\]
satisfies the properties (P1), (P2) and (P3) stated in \([6] \text{ Lemma 4.1}\). We can easily see that (P1) follows from Lemma \([4] \text{ Lemma 2.2}\) 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 \([4] \text{ Definitions} 2.1, 2.2, 2.3\) and \([4] \text{ together} \).
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 \( N_{M_q/Q}(w) \). For the second part of (P3), we define the function

\[
f(w) := \sum_{\xi \mod N_{M_q/Q}(w)} \gamma(w, \xi) = \sum_{\xi \mod N_{M_q/Q}(w)} \left( \frac{\xi}{\tau(w)} \right)_{M_q, 2} \mathbb{1}_{\gcd(\xi, \tau \sigma(w)) = (1)}.
\]

If \( w \) and \( w' \) are two elements that generate ideals coprime to \( n_q \) and such that \( \gcd(N_{M_q/Q}(w), N_{M_q/Q}(w')) = 1 \), then we have that \( f(w w') = f(w) f(w') \). 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 are sure that we can find such an element that divides a generic \( w \), because we have by assumption that \( N_{M_q/Q}(w) \) is not squarefull.

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

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

We note that by [2, 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 [4, Proposition 3.8]. As we saw at the beginning of §4, we apply [2, Proposition 5.2] to obtain Theorem 1.1.

**Acknowledgements.** This research forms part of my Master Thesis at the University of Leiden with 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 like to thank the referee for their detailed and thoughtful report, which has improved the exposition of this paper.

**References**

[1] 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.

[2] J. B. Friedlander, H. Iwaniec, B. Mazur and K. Rubin, The spin of prime ideals, *Invent. Math.* 193 (2013), no. 3, 697–749.

[3] F. Gerth, Extension of conjectures of Cohen and Lenstra, *Exposition. Math.* 5 (1987), no. 2, 181–184.

[4] P. Koymans and D. Milovic, On the 16-rank of class groups of \( \mathbb{Q}(\sqrt{-2p}) \) for primes \( p \equiv 1 \mod 4 \), *Int. Math. Res. Not. IMRN* (2018), no. 23, 7406–7427.

[5] P. Koymans and D. Milovic, Spins of prime ideals and the negative Pell equation \( x^2 - 2py^2 = -1 \), *Compos. Math.* 155 (2019), no. 1, 100–125.

[6] P. Koymans and D. Milovic, *Joint distribution of spins*, preprint (2018): arXiv: 1809.09597.
[7] P. A. Leonard and K. S. Williams, On the divisibility of the class number of \( \mathbb{Q}(\sqrt{-pq}) \) by 16, Number theory (Winnipeg, Man., 1983), *Rocky Mountain J. Math.* 15 (1985), no. 2, 491.

[8] D. Milovic, On the 16-rank of class group of \( \mathbb{Q}(\sqrt{-8p}) \) for \( p \equiv -1 \text{ mod } 4 \), *Geom. Funct. Anal.* 27 (2017), no. 4, 973–1016.

[9] J. Neukirch, *Algebraic number theory*, Translated from the 1992 German original and with a note by Norbert Schappacher, Springer-Verlag, Berlin Heidelberg, 1999.

[10] A. Smith, \( 2^\infty \)-Selmer groups, \( 2^\infty \)-class groups, and Goldfeld’s conjecture, preprint (2017): arXiv: 1708.08509.

[11] K. Uchida, Imaginary abelian number fields of degree \( 2^m \) with class number one, *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)* (1986), 151–170, Nagoya Univ., Nagoya.

Margherita Piccolo: Mathematisches Institut, Heinrich-Heine-Universität, 40225 Düsseldorf, Germany

*Email address:* margherita.piccolo@hhu.de