THE INFINITUDE OF $Q(\sqrt{-p})$ WITH CLASS NUMBER DIVISIBLE BY 16

DJORDJO MILOVIC

Abstract. The density of primes $p$ such that the class number $h$ of $Q(\sqrt{-p})$ is divisible by $2^k$ is conjectured to be $2^{-k}$ for all positive integers $k$. The conjecture is true for $1 \leq k \leq 3$ but still open for $k \geq 4$. For primes $p$ of the form $p = a^2 + c^4$ with $c$ even, we describe the 8-Hilbert class field of $Q(\sqrt{-p})$ in terms of $a$ and $c$. We then adapt a theorem of Friedlander and Iwaniec to show that there are infinitely many primes $p$ for which $h$ is divisible by 16, and also infinitely many primes $p$ for which $h$ is divisible by 8 but not by 16.

1. Introduction

Let $p$ be a prime number, and let $C$ and $h$ be the class group and the class number of $Q(\sqrt{-p})$, respectively. Since the discriminant of this field is either $-p$ or $-4p$, Gauss’s genus theory implies that the 2-part of $C$ is cyclic, and so the structure of the 2-part of the class group is entirely determined by the highest power of 2 dividing $h$. More precisely, Gauss’s genus theory implies that

$$2|h \iff p \equiv 1 \mod 4.$$ 

The criterion

$$4|h \iff p \equiv 1 \mod 8$$

can be deduced easily from Rédei’s work on the 4-rank of quadratic number fields [13]. In [1], Barrucand and Cohn gave an explicit criterion for divisibility by 8 by successively extracting square roots of the class of order two. It states that

$$8|h \iff p = x^2 + 32y^2$$

for some integers $x$ and $y$.

This can be restated as

$$8|h \iff p \equiv 1 \mod 8 \text{ and } 1 + i \text{ is a square modulo } p$$

where $i$ is a square root of $-1$ modulo $p$ (see [1] (10), p.68]). In [13], Stevenhagen also obtained the criterion ([1], albeit by a more abstract argument using class field theory over the field $Q(i)$.

Given a subset $S$ of the prime numbers, and a real number $X \geq 2$, define

$$R(S, X) := \frac{\#\{p \leq X \text{ prime} : p \in S\}}{\#\{p \leq X \text{ prime}\}}.$$
If the limit \( \lim_{X \to \infty} R(S, X) \) exists, we denote it by \( \rho(S) \) and call it the natural density of \( S \). Let

\[ S(n) = \{ p \text{ prime} : n|h(-p) \} ; \]

here we write \( h(-p) \) for the class number of \( \mathbb{Q}(\sqrt{-p}) \) to emphasize its dependence on \( p \). From the above, it is clear that \( \rho(S(2)) = 1/2 \) and \( \rho(S(4)) = 1/4 \). From (1), we see that 8 divides \( h \) if and only if \( p \) splits completely in \( \mathbb{Q}(\zeta_8, \sqrt{1+i}) \), where \( \zeta_8 \) is a primitive 8th root of unity. Since this is a degree 8 extension of \( \mathbb{Q} \), Čebotarev’s density theorem implies that \( \rho(S(8)) = 1/8 \). For a discussion of these and similar density results, see [16, p.16-19].

The Cohen-Lenstra heuristics [2] can be adapted to this situation to predict the density of primes \( p \) such that \( 2^k \) divides \( h \) for \( k \geq 1 \). Cohen and Lenstra stipulate that an abelian group \( G \) occurs as the class group of an imaginary quadratic field with probability proportional to the inverse of the size of the automorphism group of \( G \). Under this assumption, the cyclic group of order \( 2^{k-1} \) would occur as the 2-part of the class group of an imaginary quadratic number field twice as often as the cyclic group of order \( 2^k \). As we just saw above, \( \rho(S(2^k)) = \frac{1}{2^k} \rho(S(2^{k-1})) \) for \( k \leq 3 \), so we are led to conjecture

**Conjecture 1.** For all \( k \geq 1 \), \( \lim_{X \to \infty} R(S(2^k), X) \) exists and is equal to \( 2^{-k} \).

While Conjecture 1 is true for \( k \leq 3 \), it has not been proven for any \( k \geq 4 \), and a proof along the lines of the arguments for \( k \leq 3 \) seems out of reach (see [16, p. 16]). Although several criteria for divisibility by 16 have been found already (see [9], [17], and [12]), none of them appear to be sufficient to produce even infinitely many primes \( p \) for which the class number of \( \mathbb{Q}(\sqrt{-p}) \) is divisible by 16. This is precisely our aim in this paper – we will show that there is an infinite number of primes \( p \) for which \( 16|h \) and also an infinite number of primes \( p \) for which \( 8|h \) but \( 16 \nmid h \). We also derive some consequences for the fundamental unit \( \varepsilon_p \) of the real quadratic number field \( \mathbb{Q}(\sqrt{p}) \).

We tackle the question of infinitude not by developing a new criterion for divisibility by 16 which handles all primes, but by focusing on a very special subset of primes. These are the primes of the form

\[ p = a^2 + c^4, \quad c \text{ even}. \]  

The main theorem that we prove gives a new and very explicit criterion for divisibility by 16 of class numbers of \( \mathbb{Q}(\sqrt{-p}) \) for \( p \) of the form (2).

**Theorem 1.** Suppose \( p \) is a prime of the form \( a^2 + c^4 \), where \( a \) and \( c \) are integers. Let \( h_{-4p} \) denote the class number of \( \mathbb{Q}(\sqrt{-p}) \).

(i) If \( a \equiv \pm 1 \mod 16 \) and \( c \equiv 0 \mod 4 \), then \( h_{-4p} \equiv 0 \mod 16 \).

(ii) If \( a \equiv \pm 3 \mod 16 \) and \( c \equiv 2 \mod 4 \), then \( h_{-4p} \equiv 0 \mod 16 \).

(iii) If \( a \equiv \pm 7 \mod 16 \) and \( c \equiv 0 \mod 4 \), then \( h_{-4p} \equiv 8 \mod 16 \).

(iv) If \( a \equiv \pm 5 \mod 16 \) and \( c \equiv 2 \mod 4 \), then \( h_{-4p} \equiv 8 \mod 16 \).
The infinitude of \( \mathbb{Q}(\sqrt{-p}) \) with class number divisible by 16

Once we prove Theorem 1, the infinitude of primes \( p \) of the form as in the statements (i) – (iv) of the theorem follows from the following generalization of a powerful theorem of Friedlander and Iwaniec (see [7, Theorem 1]):

**Proposition 1.** Let \( a_0 \in \{1, 3, 5, 7, 9, 11, 13, 15\} \) and \( c_0 \in \{0, 2\} \). Then, uniformly for \( X \geq 3 \), we have the equality

\[
\sum_{a \equiv a_0 \mod 16} \sum_{c \equiv c_0 \mod 4} \sum_{a^2 + c^4 \text{ prime}} 1 = \frac{\kappa}{2\pi} \frac{X^{3/4}}{\log X} \left( 1 + O\left( \frac{\log \log X}{\log X} \right) \right),
\]

where \( a \) and \( c \) run over all integers and

\[
\kappa = \int_0^1 (1 - t^4)^{1/2} dt \approx 0.874 \ldots
\]

In particular, there exist infinitely many primes of the form \( a^2 + c^4 \) with \( a \equiv a_0 \mod 16 \) and \( c \equiv c_0 \mod 4 \).

Theorem 1 and Proposition 1 immediately imply:

**Corollary 1.** For a prime \( p \), let \( h_{-4p} \) denote the class number of \( \mathbb{Q}(\sqrt{-p}) \). Then, for sufficiently large \( X \), we have

\[
\#\{p \leq X : h_{-4p} \equiv 0 \mod 16\} \geq \frac{X^{3/4}}{4\log X}
\]

and

\[
\#\{p \leq X : h_{-4p} \equiv 8 \mod 16\} \geq \frac{X^{3/4}}{4\log X}.
\]

The proof of Proposition 1 will take a significant portion of our paper. Although the ideas required to generalize [7, Theorem 1] in this way are not particularly deep, implementing them turns out to be quite complicated simply because the proof of [7, Theorem 1] itself is very difficult. One can thus view Sections 4-6 as a summary of the proof of [7, Theorem 1] in a slightly more general context.

Since primes of the form \( a^2 + c^4 \) with \( c \) even have density 0 in the set of all primes, our methods cannot be used to tackle Conjecture 1. Nonetheless, each of the cases (i) – (iv) in Theorem 1 occurs with the same density among all primes of this form, so the conjecture for \( k = 4 \) deduced from the Cohen-Lenstra heuristics above holds within the thin family of imaginary quadratic number fields \( \mathbb{Q}(\sqrt{-p}) \) where \( p \) is a prime of the form \( a^2 + c^4 \) with \( c \) even. This is yet another piece of evidence suggesting that Conjecture 1 is true for \( k = 4 \). However, we also note that Conjecture 1 for \( k = 4 \) does not imply Corollary [1] as knowledge of the behavior of the class numbers of \( \mathbb{Q}(\sqrt{-p}) \) over the set of all primes \( p \) does not necessarily give information about their behavior over a thin subset of all primes.

We now give a consequence of our results and a criterion for divisibility by 16 due to Williams [17]. Let \( p \equiv 1 \mod 8 \), and let \( \epsilon_p \) be a fundamental unit of the
real quadratic field $\mathbb{Q}(\sqrt{p})$, written in the form $\epsilon_p = T + U\sqrt{p}$, where $T$ and $U$ are integers. The criterion states that if $8|h$, then
\begin{equation}
 h \equiv T + p - 1 \mod 16,
\end{equation}
so that $16|h$ if and only if $T \equiv 1 - p \mod 16$. An immediate byproduct of Theorem 1 and criterion (4) is the following corollary.

**Corollary 2.** Suppose $p$ is a prime of the form $a^2 + c^4$, where $a$ is odd and $c$ is even. Let $\epsilon_p = T + U\sqrt{p}$ denote a fundamental unit of $\mathbb{Q}(\sqrt{p})$.

(i) If $a \equiv \pm 1 \mod 16$ and $c \equiv 0 \mod 4$, then $T \equiv 0 \mod 16$ and $U \equiv \pm 1 \mod 8$.

(ii) If $a \equiv \pm 3 \mod 16$ and $c \equiv 2 \mod 4$, then $T \equiv 8 \mod 16$ and $U \equiv \pm 5 \mod 8$.

(iii) If $a \equiv \pm 7 \mod 16$ and $c \equiv 0 \mod 4$, then $T \equiv 8 \mod 16$ and $U \equiv \pm 1 \mod 8$.

(iv) If $a \equiv \pm 5 \mod 16$ and $c \equiv 2 \mod 4$, then $T \equiv 0 \mod 16$ and $U \equiv \pm 5 \mod 8$.

This can be viewed as an extension of [10, Corollary 1.2(i), p.115-116] to primes of the form $p = a^2 + c^4$. Now Proposition 1 gives

**Corollary 3.** For a prime $p \equiv 1 \mod 8$, let $\epsilon_p = T + U\sqrt{p}$ denote the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Then, for sufficiently large $X$, we have
\begin{align*}
 \# \{p \leq X : p \equiv 1 \mod 8, \; T \equiv 0 \mod 16\} &\geq \frac{X^{3/4}}{4 \log X} \\
\# \{p \leq X : p \equiv 1 \mod 8, \; T \equiv 8 \mod 16\} &\geq \frac{X^{3/4}}{4 \log X}.
\end{align*}

The existence of infinitely many $p \equiv 1 \mod 8$ such that $T \equiv T_0 \mod 16$ for a fixed $T_0 \in \{0, 8\}$ is not at all trivial. Hence Corollary 2 sheds some new light on the fundamental unit $\epsilon_p$ of $\mathbb{Q}(\sqrt{p})$, one of the most mysterious quantities in number theory.

## 2. Hilbert class fields

Suppose $p \equiv 1 \mod 4$. Then there are two finite primes of $\mathbb{Q}$ which ramify in $\mathbb{Q}(\sqrt{-p})$, namely 2 and $p$. The prime $p = (\sqrt{-p})$ of $\mathbb{Q}(\sqrt{-p})$ lying above $p$ is principal, and so its ideal class in $\mathcal{C}$ is the identity. Genus theory then implies that the class of the prime ideal $t = (2, 1 + \sqrt{-p})$ of $\mathbb{Q}(\sqrt{-p})$ lying above 2 is the unique element of order two in $\mathcal{C}$. Assuming that $h$ is divisible by $2^n$ for some non-negative integer $n$, to check that it is divisible by $2^{n+1}$, it would suffice to check that the class of $t$ belongs to $\mathcal{C}^{2^n}$.

### 2.1. $2^n$-Hilbert class fields

Recall that the Hilbert class field $H$ of $K = \mathbb{Q}(\sqrt{-p})$ is the maximal unramified abelian extension of $\mathbb{Q}(\sqrt{-p})$. The Artin symbol induces a canonical isomorphism of groups
\begin{equation}
 \left( \frac{\cdot}{H/K} \right) : \mathcal{C} \longrightarrow \text{Gal}(H/\mathbb{Q}(\sqrt{-p})).
\end{equation}
Suppose for the moment that $2^n/h$ for some non-negative integer $n$. Then $C^{2^n}$ is a subgroup of $C$ of index $2^n$. We define the $2^n$-Hilbert class field $H_{2^n}$ to be the subfield of $H$ fixed by the the image of $C^{2^n}$ under the isomorphism $[5]$. Since the 2-primary part of $C$ is cyclic, it follows immediately that $H_{2^n}$ is the unique unramified, cyclic, degree-$2^n$ extension of $K$. Moreover, $[5]$ induces a canonical isomorphism of cyclic groups of order $2^n$

\[(6) \quad \left(\frac{.}{H_{2^n}/K}\right) : C/C^{2^n} \longrightarrow \text{Gal}(H_{2^n}/K).\]

Hence $t$ belongs to $C^{2^n}$ if and only if $t$ has trivial Artin symbol in $\text{Gal}(H_{2^n}/K)$. By class field theory, this is equivalent to $t$ splitting completely in $H_{2^n}$.

The main idea of the proof of Theorem 1 is to write down explicitly the $8$-Hilbert class field $H_8$ of $Q(\sqrt{p})$, and then to characterize those $p$ such that $t$ splits completely in $H_8$. We remark here that although Cohn and Cooke [3] have already written down $H_8$ in terms of the fundamental unit $\epsilon_p$ of the real quadratic number field $Q(\sqrt{p})$ and certain integer solutions $u$ and $v$ to $p = 2u^2 - v^2$, not enough is known about either $\epsilon_p$ or $u$ and $v$ to deduce anything about the distribution of primes $p$ such that $t$ splits completely in $H_8$.

2.2. Generating $2^n$-Hilbert class fields. We first state and prove some lemmas which will prove to be useful in our quest to explicitly generate $H_8$.

The $2$-Hilbert class field, also called the genus field of $Q(\sqrt{-p})$, is known to be $H_2 = Q(i, \sqrt{p})$. Hence every $2^n$-Hilbert class field of $Q(\sqrt{-p})$ contains $Q(i)$, and so we can study the splitting behavior of $t$ in $H_{2^n}$ by working over the quadratic subfield $Q(i)$ of $H_2$. With this in mind, we now state some well-known generalities about the completion of $Q(i)$ with respect to the prime ideal $(1+i)$ lying over $2$.

This completion is $Q_2(i)$, and its ring of integers $Z_2[i]$ is a discrete valuation ring with maximal ideal $m = 1 + i$. Let $U = (Z_2[i])^\times$ denote the group of units of $Z_2[i]$ and for each positive integer $k$, define $U^{(k)} = 1 + m^k$. Then there is a filtration

\[U = U^{(1)} \supset U^{(2)} \supset \cdots \supset U^{(k)} \supset \cdots.\]

For any $k \geq 3$, squaring gives an isomorphism $U^{(k)} \cong U^{(k+2)}$. Indeed, let $1 + m^{k+2}y \in U^{(k+2)}$. Hensel’s lemma implies that there exists $x \in m^{k-2}$ such that $x^2 + x = m^{k-2}y$. Then $(1 + 2x)^2 = 1 + m^{k+2}y$ and $1 + 2x \in U^{(k)}$. It is not hard to see that

\[U = \langle i \rangle \times U^{(3)} = \langle i \rangle \times \langle 2 + i \rangle \times U^{(4)},\]

so that $U^2 = (-1) \times U^{(5)}$. In other words, $u \in U$ is a square in $Q_2(i)$ if and only if $u \equiv \pm 1 \pmod{m^5}$. Moreover, if $\omega \equiv \pm 1 \pmod{m^4}$ (or if $\omega \equiv \pm 1 \pmod{m^4}$), then the minimal polynomial of $\sqrt{\omega}$ over $Z_2[i]$ reduces to $X^2 + X$ or $X^2 + X + 1$ (respectively $X^2 + 1$) modulo $m$. We collect these observations into the following lemma.

**Lemma 1.** Let $\omega$ be a unit in $Z_2[i]$. Then $Q_2(i, \sqrt{\omega})$ is unramified over $Q_2(i)$ if and only if $\omega \equiv \pm 1 \pmod{m^4}$. Moreover, $Q_2(i, \sqrt{\omega}) = Q_2(i)$, i.e. $\omega$ is a square in $Q(i)$ if and only if $\omega \equiv \pm 1 \pmod{m^5}$.
Next, we state two lemmas which we will use to check that the extensions of $\mathbb{Q}(\sqrt{-p})$ which we construct are normal and cyclic.

**Lemma 2.** Let $K$ be a field of characteristic different from 2, let $d$ be an element of $K$ which is not a square in $K$, and let $L = K(\sqrt{d})$. Let $a, b \in K$ such that $a + b\sqrt{d}$ is not a square in $L$ and let $M = L(\sqrt{a + b\sqrt{d}})$. Then $L/K$ is cyclic of degree 4 if and only if $a^2 - db^2 \in d \cdot K^2$.

**Proof.** See [11][Chapter VI, Exercise 4, p.321].

**Lemma 3.** Let $K$ be a field. Suppose $M/K$ is a cyclic extension of degree $2m$ and let $\sigma$ be a generator of $\text{Gal}(M/K)$. Let $L$ be the subfield of $M$ fixed by $\sigma^m$. Suppose $N/K$ is a Galois extension containing $M$ such that $N/L$ is cyclic of degree 4. Then $N/K$ is cyclic of degree $4m$.

**Proof.** Let $\sigma_1$ denote a lifts of $\sigma$ to $\text{Gal}(N/K)$. The order of $\sigma_1$ is at least $2m$ since the order of $\sigma$ is $2m$. As $\sigma^m$ fixes $L$, $\sigma_1^m$ is an element of $\text{Gal}(N/L)$ which is non-trivial on $M$ and hence has order 4. Thus the order of $\sigma_1$ is $4m$.

Finally, we arrive at the main lemma we will use to construct $2^n$-Hilbert class fields from $2^{n-1}$-Hilbert class fields. This result is inspired by a theorem of Reichardt [14][Satz, p.82]. His theorem proves the existence of generators $\sqrt{\omega}$ for $H_{2^n}$ over $H_{2^{n-1}}$ with $\omega \in H_{2^{n-1}}$ of a certain form. We prove sufficient conditions for an element $\omega$ of a similar form to give rise to a generator, so that we can actually construct $H_{2^n}$.

**Lemma 4.** Let $h$ be the class number of $\mathbb{Q}(\sqrt{-p})$, let $n \geq 2$, and suppose that $2^n$ divides $h$. Suppose $A_{2^{n-1}}$ is a degree $2^{n-1}$ extension of $\mathbb{Q}$ such that:

- $A_{2^{n-1}} \subset H_{2^{n-1}}$,  
- $A_{2^{n-1}}$ contains $\mathbb{Q}(i)$ and $(1 + i)$ is unramified in $A_{2^{n-1}}/\mathbb{Q}(i)$, and
- there is a prime element $\omega$ in $A_{2^{n-1}}$ such that:
  - $\omega$ lies above $p$ and its ramification and inertia indices over $p$ are equal to 1,
  - denoting the conjugate of $\omega$ over $A_{2^{n-2}} = A_{2^{n-1}} \cap H_{2^{n-2}}$ by $\omega'$, we have $H_{2^{n-1}} = H_{2^{n-2}}(\sqrt{\omega\omega'}) = A_{2^{n-1}}(\sqrt{\omega\omega'})$,
  - (U2): $(1 + i)$ remains unramified in $A_{2^n} = A_{2^{n-1}}(\sqrt{\omega})$, and
  - (N): $H_{2^{n-1}}(\sqrt{\omega})$ is normal over $\mathbb{Q}$.

Then $H_{2^n} = H_{2^{n-1}}(\sqrt{\omega})$.

**Proof.** Since the ramification index of $\omega$ over $p$ is 1, $\omega$ and $\omega'$ are coprime in $A_{2^{n-1}}$.

First we check that $\omega$ is not a square in $H_{2^{n-1}}$. Note that $H_{2^{n-1}}$ is normal over $A_{2^{n-2}}$, while $A_{2^n}$ is not normal over $A_{2^{n-2}}$ ($\sqrt{\omega'}$ is not an element of $A_{2^n}$). Hence $A_{2^n}$ cannot be a subfield of $H_{2^{n-1}}$ and so $\sqrt{\omega} \notin H_{2^{n-1}}$.

By assumption, $H_{2^{n-1}}(\sqrt{\omega})$ is normal over $\mathbb{Q}$, and hence also over $\mathbb{Q}(\sqrt{-p})$ and...
$H_{2n-2}$. Since $\omega$ and $\omega'$ are conjugates over $A_{2n-2}$, they are also conjugates over $H_{2n-2}$. As $H_{2n-1} = H_{2n-2}(\sqrt{\omega\omega'})$ and $\omega\omega' = \omega\omega' \cdot 1^2$, Lemma 3 implies that $H_{2n-1}(\sqrt{\omega})$ is a degree 4 cyclic extension of $H_{2n-2}$. Moreover, $H_{2n-1}$ is a degree $2^{n-1}$ cyclic extension of $Q(\sqrt{-p})$, so Lemma 3 implies that $H_{2n-1}(\sqrt{\omega})$ is a degree $2^n$ cyclic extension of $Q(\sqrt{-p})$.

It remains to show that $H_{2n-1}(\sqrt{\omega})/Q(\sqrt{-p})$ is unramified. We will establish this by showing that each of the ramification indices of the primes 2 and $p$ in $H_{2n-1}(\sqrt{\omega})$ is at most 2.

The prime 2 ramifies in $Q(i)$, but by assumption $(1+i)$ is unramified in $A_{2n}$. As $H_{2n-1}(\sqrt{\omega}) = A_{2n}(\sqrt{\omega\omega'})$ and $p \equiv 1 \mod 4$, Lemma 1 ensures that $(1+i)$ is unramified in $H_{2n-1}(\sqrt{\omega})$. Hence the ramification index of 2 in $H_{2n-1}(\sqrt{\omega})$ is 2.

Now note that $A_{2n}$ is a subfield of $H_{2n-1}(\sqrt{\omega})$ of index 2. The ramification index of the prime $\omega'$ over $p$ is 1. Since $\omega$ and $\omega'$ are coprime, $\omega'$ does not ramify in $A_{2n}$. Hence the ramification index of $p$ in $H_{2n-1}(\sqrt{\omega})$ is at most 2, and this completes the proof. □

2.3. Explicit constructions of $H_4$ and $H_8$. Recall from the discussion at the end of Section 2.1 that 4 divides $h$ if and only if the prime ideal $t$ lying over 2 splits in $H_2$, which happens if and only if $(1+i)$ splits in $H_2/Q(i)$. As $H_2$ is obtained from $Q(i)$ by adjoining a square root of $p$, Lemma 1 implies that this happens if and only if $p \equiv \pm 1 \mod 8$, which, for $p \equiv 1 \mod 4$, is true if and only if $p \equiv 1 \mod 8$. Thus we have recovered the criterion for divisibility by 4.

From now on, assume that 4 divides $h$, i.e. that $p \equiv 1 \mod 8$. We will now use Lemma 3 to construct the 4-Hilbert class field of $Q(\sqrt{-p})$.

A prime $p \equiv 1 \mod 4$ splits in $Q(i)$, so that there exists $\pi$ in $Z[i]$ such that $p = \pi\overline{\pi}$, here $\overline{\pi}$ denotes the conjugate of $\pi$ over $A_4 := Q$. If we write $\pi$ as $a + bi$ with $a$ and $b$ integers, then we see that $p = a^2 + b^2$. We choose $\pi$ so that $b$ is even.

As $p \equiv 1 \mod 8$, we see that $b$ is in fact divisible by 4. Hence

$$\pi = a + bi, \quad b \equiv 0 \mod 4.$$  \hspace{1cm} (7)

Now fix a square root of $\pi$ and denote it by $\sqrt{\pi}$. Recall that $H_2 = Q(i, \sqrt{p})$ is the 2-Hilbert class field of $Q(\sqrt{-p})$. We claim that the hypotheses of Lemma 3 for $n = 2$ are satisfied with $A_2 := Q(i)$ and $\omega = \pi$.

All of the hypotheses other than $(U_2)$ and $(N)$ are easy to check. Note that our choice of $\pi$ ensures that $\pi \equiv \pm 1 \mod 4$, so that $(U_2)$ follows from Lemma 4. To see that $(N)$ is satisfied, note that $H_2(\sqrt{\pi})$ is the splitting field (over $Q$) of the polynomial $f_4(X) := (X-\pi)(X-\overline{\pi})$. Indeed, $\pi\overline{\pi}$ is a square in $H_2$, so both square roots of $\overline{\pi}$ are also contained in $H_2(\sqrt{\pi})$. Hence we conclude by Lemma 4 that the 4-Hilbert class field is given by

$$H_4 = H_2(\sqrt{\pi}) = Q(i, \sqrt{p}, \sqrt{\pi})$$  \hspace{1cm} (8)

with $\pi$ as in (7).
Next, we find a criterion for divisibility by 8. Recall that $h$ is divisible by 8 if and only if it splits completely in $H_4$, i.e. if and only if $\pi$ is a square in $Q_2(i)$. By Lemma 1, this happens if and only if $\pi \equiv \pm 1 \pmod{m^5}$. In terms of $a$ and $b$ from (11), this means that

$$8|h \iff a + b \equiv \pm 1 \pmod{8}.$$ 

We remark that Fouvry and Klünners developed similar methods in [5], where they constructed an analogue of the 4-Hilbert class field to deduce a criterion for the 8-rank of class groups in a family of real quadratic number fields. From now on, suppose that $8|h$. Replacing $\pi$ by $-\pi$ if necessary, we assume that

$$\pi \equiv 1 \pmod{m^3}. \tag{9}$$

This means that $a + b \equiv 1 \pmod{8}$. Our choice of $\sqrt{\pi}$ above is only unique up to sign. By Hensel’s lemma, we can now fix this sign by imposing that

$$\sqrt{\pi} \equiv 1 \pmod{m^3}. \tag{10}$$

In order to explicitly generate $H_8$ from $H_4$ using Lemma 4, we are led to the problem of finding a prime element in $A_4 = Q(i, \sqrt{\pi})$ whose norm down to $Q(i)$ is $\pi$, up to units. This is the problem that we cannot solve explicitly enough in general to answer questions about infinitude or density.

However, for a very thin subset of primes, we can write down an element of $A_4$ of norm $-\pi$. These are primes $p$ of the form

$$p = a^2 + c^4, \quad c \text{ even}, \tag{11}$$

that is, primes $p$ of the form $a^2 + b^2$ with $b$ a perfect square divisible by 4.

Suppose that $p$ is a prime of the form (11). Set

$$\varpi_0 = c(1 + i) + \sqrt{\pi}. \tag{12}$$

Let $\sigma$ be a generator for $\text{Gal}(H_4/Q(\sqrt{-p}))$ and set $\varpi_2 = \sigma^2(\varpi_0)$. Then

$$\varpi_0 \cdot \varpi_2 = (c(1 + i) + \sqrt{\pi})(c(1 + i) - \sqrt{\pi}) = -\pi. \tag{13}$$

We can now prove the main result of this section.

**Proposition 2.** Let $p$ be a prime of the form (11), let $\pi$ be as in (9), let $\sqrt{\pi}$ be as in (10), and let $\varpi$ be as in (12). Let $\sqrt{\varpi}$ denote a square root of $\varpi$. Then $H_4(\sqrt{\varpi})$ is the 8-Hilbert class field of $Q(\sqrt{-p})$. 

The two cases above correspond to the residue class of \( c \) modulo 4. First recall that \( a + b \equiv 1 \pmod{8} \), i.e., \( a + c^2 \equiv 1 \pmod{m^6} \). In the first case, if \( c \equiv 0 \pmod{m^4} \), then \( c^2 \in m^6 \), so \( a-1 \in m^6 \) as well. Then \( \pi = a + c^2 i \equiv 1 \pmod{m^6} \), which means that \( \sqrt{\pi} \equiv 1 \pmod{m^4} \). Then
\[
\omega_0 = c(1+i) + \sqrt{\pi} \equiv 1 \pmod{m^4}.
\]
In the second case, \( c \equiv 2 \pmod{m^4} \), so that \( c^2 \equiv -m^4 \pmod{m^6} \). Then \( a-1+m^4 \in m^6 \), so that \( \pi = a + c^2 i \equiv 1 - m^4 - m^4 i \equiv 1 + m^4 (1-i) \equiv 1 + m^5 \pmod{m^6} \).

\[
H_8 = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi}, \sqrt{\alpha})
\]
\[
\mathcal{A}_4 = \mathbb{Q}(i, \sqrt{\pi}, \sqrt{\beta})
\]
\[
A_4 = \mathbb{Q}(i, \sqrt{\pi}, \sqrt{\alpha})
\]
\[
A_2 = \mathbb{Q}(i, \sqrt{\pi})
\]
\[
A_1 = \mathbb{Q}(i)
\]

We now prove hypothesis (\( U_2 \)). The assumption that \( \pi \equiv 1 \pmod{m^5} \) actually means that \( \pi \) is a square in \( \mathbb{Q}_2(i) \), i.e., that \( (1+i) \) splits in \( A_4 \). Hence it remains to show that \( \mathbb{Q}_2(i, \sqrt{\omega_0}) \) is unramified over \( \mathbb{Q}_2(i) \), and Lemma 1 implies that it is enough to prove that \( \omega_0 \equiv \pm 1 \pmod{m^4} \).

Recall from (10) that \( \sqrt{\pi} \equiv 1 \pmod{m^4} \). Thus \( \sqrt{\pi} \equiv 1 \) or \( 1 + m^3 \pmod{m^4} \). Squaring, we find that \( \pi \equiv 1 \) or \( 1 + m^5 \pmod{m^6} \), respectively.

Proof. We again use Lemma 3, but this time with \( n = 3 \), \( A_4 = \mathbb{Q}(i, \sqrt{\pi}) \) and \( \omega = \omega_0 \). All of the hypotheses except for (\( U_2 \)) and (\( N \)) immediately follow from the identity (13).

It remains to prove hypothesis (\( N \)). For \( 0 \leq m \leq 3 \), set \( \omega_m = \sigma^m(\omega) \), where \( \sigma \) is a generator for \( \text{Gal}(H_4/\mathbb{Q}(\sqrt{-p})) \). We claim that \( H_4(\sqrt{\omega_0}) \) is the splitting field of the polynomial
\[
f_8(X) = (X^2 - \omega_0)(X^2 - \omega_1)(X^2 - \omega_2)(X^2 - \omega_3).
\]
It is easy to see that \( \omega_0 \omega_2 = -\pi \) and \( \omega_1 \omega_3 = -\pi \) are squares in \( H_4 \). To prove (\( N \)), it now suffices to show that \( \omega_0 \omega_1 \) is a square in \( H_4 \). Write \( \sqrt{\pi} = d + ei \) with \( d = \frac{\sqrt{\pi} + \sqrt{\sigma(\pi)}}{2}, \ e = \frac{\sqrt{\pi} - \sqrt{\sigma(\pi)}}{2i} \in H_4 \).

One can now check that \( \omega_0 \omega_1 = (c + di - ei)^2 \), which proves hypothesis (\( N \)).
This means that $\sqrt{\pi} \equiv 1 + m^3 \pmod{m^4}$. Finally,
\[
\varpi_0 = \sqrt{\pi} + c(1 + i) \equiv 1 + m^3 + m^3 \equiv \pm 1 \pmod{m^4},
\]
which proves that $\mathbb{Q}_2(i, \sqrt{\varpi_0})$ is unramified over $\mathbb{Q}_2(i)$. \hfill $\square$

3. Proof of Theorem 1

The proof of Theorem 1 will proceed in much the same way as the last part of the proof of Proposition 2. Now, instead of showing that $\mathbb{Q}_2(i, \sqrt{\varpi_0})$ is unramified over $\mathbb{Q}_2(i)$, we must decide when this extension is trivial (i.e. when $t$ splits completely in $H_8$) and when it is unramified of degree 2 (i.e. when $t$ does not split completely in $H_8$). This is equivalent to determining when $\varpi_0$ is a square in $\mathbb{Q}_2(i)$.

We will distinguish between two cases as above. The first case is when $c \equiv 0 \pmod{4}$, i.e. $c \in \mathbb{m}^4$. Recall from above that then $a \equiv 1 \pmod{8}$ and $\sqrt{\pi} \equiv \pm 1 \pmod{m^4}$.

To check whether or not $\varpi_0$ is a square in $\mathbb{Q}_2(i)$, we must compute $\varpi_0$ modulo $m^5$. Since $c \equiv 0 \pmod{4}$, we deduce that $\varpi_0 \equiv \sqrt{\pi} \pmod{m^5}$. Thus, we must determine conditions on $a$ such that $\sqrt{\pi} \equiv \pm 1 \pmod{m^5}$, and for this, by Hensel’s lemma, it is necessary to determine $\pi$ modulo $m^7$. Hence, assuming $c \equiv 0 \pmod{4}$,
\[
16|h \iff \sqrt{\pi} \equiv \pm 1 \pmod{m^5} \iff \pi \equiv 1 \pmod{m^7} \iff a \equiv 1 \pmod{16}.
\]
This proves parts (i) and (iii) of Theorem 1.

We handle the second case similarly. Now $c \equiv 2 \pmod{4}$, $a \equiv 5 \pmod{8}$ and $\sqrt{\pi} \equiv 1 + m^3 \pmod{m^4}$. Then $\alpha \equiv 2m + \sqrt{\pi} \pmod{m^5}$ and so we must determine conditions on $a$ such that $\sqrt{\pi} \equiv \pm 1 - 2m \pmod{m^5}$. Under the current assumptions,
\[
16|h \iff \sqrt{\pi} \equiv \pm 1 - 2m \pmod{m^5} \iff \pi \equiv 1 + m^5 + m^6 \pmod{m^7} \iff a \equiv -3 \pmod{16}.
\]
Note that because of the choice $a$ we have actually shown the theorem for $a \equiv 1 \pmod{4}$. If $p = a^2 + c^4$ with $a \equiv 3 \pmod{4}$, then $p = (-a)^2 + c^4$ with $-a \equiv 1 \pmod{4}$, so that the other cases can be deduced immediately. This finishes the proof of Theorem 1.

4. Overview of the proof of Proposition 1

In [7], Friedlander and Iwaniec prove an asymptotic formula for the number of primes of the form $a^2 + c^4$, that is, primes of the form $a^2 + b^2$ where $b$ itself is a square. For a summary of their proof, see the exposition in [8, Chapter 21]. They use a new sieve that they developed to detect primes in relatively thin sequences [6]. This sieve has its roots in the work of Fouvry and Iwaniec [4], where they used similar sieve hypotheses to give an asymptotic formula for the number of primes of
the form \(a^2 + b^2\) where \(b\) is a prime.

The purpose of the following three sections is to demonstrate that the method of Friedlander and Iwaniec is robust enough to incorporate congruence conditions on \(a\) and \(c\). While we are convinced that Proposition 1 remains true when \(a\) and \(c\) satisfy reasonable congruence conditions modulo any positive integers \(q_1\) and \(q_2\), respectively, the technical obstacles necessary to insert the congruence condition for \(c\) are cumbersome. Hence we will restrict ourselves to the case \(q_2 = 4\).

The proof of Proposition 1 involves certain alterations in the way that the sieve [6] is used. For this reason, we first briefly recall the inputs and the output of the sieve.

4.1. Asymptotic sieve for primes. Suppose \((a_n) (n \in \mathbb{N})\) is a sequence of non-negative real numbers. Then the asymptotic sieve for primes developed in [6] yields an asymptotic formula for

\[ S(x) = \sum_{\substack{p \leq x \\text{prime}}} a_p \log p \]

provided that the sequence \((a_n)\) satisfies several hypotheses, all but two of which are not difficult to verify. To state them, we first need to fix some terminology. For \(d \geq 1\), let

\[ A_d(x) = \sum_{\substack{n \leq x \\text{mod } d}} a_n \]

and let \(A(x) = A_1(x)\). Moreover, let \(g\) be a multiplicative function, and define the error term \(r_d(x)\) by the equality

\[ A_d(x) := g(d)A(x) + r_d(x). \tag{14} \]

The hypotheses which are not difficult to verify are listed in equations (2.1)-(2.8) in [7]. We briefly recall them here. We assume the bounds

(H1) \[ A(x) \gg A(\sqrt{x})(\log x)^2 \]

and

(H2) \[ A(x) \gg x^{\frac{1}{3}} \left( \sum_{n \leq x} a_n^2 \right)^{\frac{1}{2}}. \]

We assume that the multiplicative function \(g\) satisfies

(H3) \[ 0 \leq g(p^2) \leq g(p) \leq 1, \]

(H4) \[ g(p) \ll p^{-1}, \]

and

(H5) \[ g(p^2) \ll p^{-2}. \]

We also assume that for all \(y \geq 2\),

(H6) \[ \sum_{p \leq y} g(p) = \log \log y + c + O((\log y)^{-10}), \]
where \( c \) is a constant depending only on \( g \); this is the linear sieve assumption. Finally, we assume the bound
\[
A_d(x) \ll d^{-1} \tau(d)^8 A(x)
\]
uniformly in \( d \leq x^{\frac{3}{4}} \); here \( \tau \) is the divisor function.

Now we state the two hypotheses which are more difficult to verify. The first is a classical sieve hypothesis; it is a condition on the average value of the error terms \( r_d(x) \). Let \( L = (\log x)^{244} \).

**Hypothesis (R).** There exists \( x_r > 0 \) and \( D = D(x) \) in the range
\[
x^{\frac{2}{3}} < D < x
\]
such that for all \( x \geq x_r \), we have
\[
\sum_{d \text{ cubefree} \atop d \leq DL^2} |r_d(t)| \leq A(x)L^{-2}
\]
uniformly in \( t \leq x \).

In our applications, \( D \) will be \( x^{3/4 - \varepsilon} \) for a sufficiently small \( \varepsilon \). This condition about remainders will be called condition (R).

The second is a complicated condition on bilinear forms in the elements of the sequence \((a_n)\) weighed by truncated sums of the Möbius function
\[
\beta(n,C) = \mu(n) \sum_{c|n, c \leq C} \mu(c).
\]
It is designed to make sure that the sequence \((a_n)\) is orthogonal to the Möbius function; this is crucial in overcoming the parity problem. We now state this hypothesis, named (B) for bilinear.

**Hypothesis (B).** Suppose (R) is satisfied for \( x_r \) and \( D = D(x) \). Then there exists \( x_b > x_r \) such that for every \( x > x_b \), there exist \( \delta, \Delta, \) and \( P \) satisfying
\[
2 \leq \delta \leq \Delta, \quad 2 \leq P \leq \Delta^{1/235} \log \log x,
\]
and such that for every \( C \) with
\[
1 \leq C \leq xD^{-1},
\]
and for every \( N \) with
\[
\Delta^{-1} \sqrt{D} < N < \delta^{-1} \sqrt{x},
\]
we have
\[
\sum_m \left| \sum_{N \leq n \leq 2N} \beta(n,C)a_{mn} \right| \leq A(x)(\log x)^{-226},
\]
where
\begin{equation}
\Pi = \prod_{p \leq P} p.
\end{equation}

Note that establishing condition (R) for a larger \( D \) decreases the range of \( C \) and \( N \) for which we have to verify condition (B).

The main result of [6] is

**Theorem 2.** Assuming hypotheses (H1)-(H7), (R), and (B), we have
\[ S(x) = H A(x) \left( 1 + O\left( \frac{\log \delta}{\log \Delta} \right) \right), \]
where \( H \) is the positive constant given by the convergent product
\[ H = \prod_{p} \left( 1 - g(p) \right) \left( 1 - \frac{1}{p} \right)^{-1}, \]
and the constant implied in the \( O \)-symbol depends on the function \( g \) and the constants implicit in (H1), (H2), and (H7).

### 4.2. Preparing the sieve for Proposition 1.

For our application, we will denote by \( v' \) the analogue of a quantity \( v \) from the proof of Friedlander and Iwaniec in [7].

We take \( (a'_{n}) \) to be the following sequence. Suppose \( q_1 \) and \( q_2 \) are positive integers and let \( q \) denote the least common multiple of \( q_1 \) and \( q_2 \). We say that a pair of congruence classes
\[ a_0 \text{ mod } q_1 \quad c_0 \text{ mod } q_2 \]

is **admissible** if for every pair congruence classes
\[ a_1 \text{ mod } q \quad c_1 \text{ mod } q \]
such that \( a_1 \equiv a_0 \text{ mod } q_1 \) and \( c_1 \equiv c_0 \text{ mod } q_2 \), the congruence class \( a_1^2 + c_1^2 \text{ mod } q \) is a unit modulo \( q \).

**Example.** Suppose that \( a_0 \in \{1, 3, 5, 7, 9, 11, 13, 15\} \) and \( c_0 \in \{0, 2\} \). Then the pair of congruence classes \( a_0 \text{ mod } 16 \) and \( c_0 \text{ mod } 4 \) is admissible.

**Example.** Suppose that \( a_0 = c_0 = 1 \). Then the pair of congruence classes \( a_0 \text{ mod } 3 \) and \( c_0 \text{ mod } 2 \) is **not** admissible. Indeed, \( 1 \equiv a_0 \equiv c_0 \text{ mod } 6 \) but \( 2 \equiv 1^2 + 1^4 \text{ mod } 6 \) is not invertible modulo 6. This does not mean, however, that there are no primes of the form \( a^2 + c^4 \) with \( a \equiv 1 \text{ mod } 3 \) and \( c \equiv 1 \text{ mod } 2 \); one such prime is \( 4^2 + 1^4 \).

Henceforth, suppose \( q_1 \) and \( q_2 \) are positive integers, let \( q \) be the least common multiple of \( q_1 \) and \( q_2 \), and suppose \( a_0 \text{ mod } q_1 \) and \( c_0 \text{ mod } q_2 \) is an admissible pair of congruence classes. We define
\begin{equation}
\sum_{a, b \in \mathbb{Z}} 3^f(b),
\end{equation}
where

\[(19)\quad Z'(b) := \sum_{\substack{c \in \mathbb{Z} \\mid \ c^2 = b \mod q_1 \ \text{and} \ c^2 = b \mod q_2}} 1.\]

Let \( g \) be the multiplicative function supported on cubefree integers defined in [7, Equation 3.16, p.961] as follows: let \( \chi_4 \) denote the character of conductor 4; for \( p \geq 3 \) set

\[ g(p) = 1 + \chi_4(p) \left( 1 - \frac{1}{p} \right) \]

and

\[ g(p^2) = 1 + (1 + \chi_4(p)) \left( 1 - \frac{1}{p} \right); \]

finally, set \( g(2) = \frac{1}{2} \) and \( g(4) = \frac{1}{4} \). For our extension, we define a multiplicative function \( g' \) by setting

\[ g'(n) = \begin{cases} g(n) & \text{if } (n, q) = 1 \\ 0 & \text{otherwise.} \end{cases} \]

Then, provided that (H1)-(H7), (R), and (B) are satisfied with \( \delta \) a large power of \( \log x \) and \( \Delta \) a small power of \( x \), the asymptotic formula given by the sieve (see Theorem 2) is

\[(20)\quad S'(x) := \sum_{\substack{p \leq x \\text{prime}}} a_p \log p = c(q_1, q_2) \frac{16\kappa}{\pi} x^{3/4} \left( 1 + O \left( \frac{\log \log x}{\log x} \right) \right)\]

where

\[ c(q_1, q_2) = \frac{1}{q_1 q_2} \prod_{p|q} (1 - g(p))^{-1} \]

and \( \kappa \) is the integral given in the statement of Proposition 1. Note that the sieve applied to the original sequence \( (a_n) \) from [7], with

\[(21)\quad a_n = \sum_{\substack{a, b \in \mathbb{Z} \\mid \ a^2 + b^2 = n}} Z(b),\]

where

\[(22)\quad Z(b) = \sum_{\substack{c \in \mathbb{Z} \\mid \ c^2 = b}} 1,\]

yields the asymptotic formula

\[ S(x) = \frac{16\kappa}{\pi} x^{3/4} \left( 1 + O \left( \frac{\log \log x}{\log x} \right) \right) \]

(see [2] Theorem 1, p.946). Thus \( c(q_1, q_2) \) can be interpreted as the density of primes of the form \( a^2 + c^4 \) such that \( a \equiv a_0 \mod q_1 \) and \( c \equiv c_0 \mod q_2 \) within the set of all primes of the form \( a^2 + c^4 \).

Remark. Throughout the following two sections, we regard \( q_1 \) and \( q_2 \) as fixed constants, and so the implied constants in every bound we give may depend on \( q_1 \) and \( q_2 \), even if this dependence is not explicitly stated. Thus, whenever we state “the implied constant is absolute,” the implied constant may actually depend on \( q_1 \) and
q_2$. In our application $q_1 = 16$ and $q_2 = 4$, so we are not concerned with uniformity of the above asymptotic formula with respect to $q_1$ and $q_2$.

It is obvious that our modified sequence $(a'_n)$ satisfies (H1)-(H7) for the same reasons as the original sequence $(a_n)$. We will prove that $(a'_n)$ above satisfies condition (R) for general $q_1$ and $q_2$. The congruence condition on $c$ is more difficult to insert into the proof of condition (B), so we prove condition (B) only for the special case where $q_2 = 4$ and $c_0 \in \{0, 2\}$.

5. Proof of condition (R)

Here we closely follow and refer to the arguments laid out in [7, Section 3, p.955-962]. Define

$$A'_d(x) := \sum_{n \leq x \mod d} a'_n$$

and

$$A'(x) := A'_1(x).$$

The goal is to check that the error terms $r'_d(x)$ defined by

$$r'_d(x) := A'_d(x) - g'(d)A'(x)$$

are small on average. To do this, we will prove an analogue of [7, Lemma 3.1, p.956], with $M_d(x)$ (representing the main term and defined in [7, p.955]) replaced by

$$M'_d(x) = \frac{1}{dq_1} \sum_{0 < a^2 + b^2 \leq x} 3'(b)\rho(b; d) \quad \text{if } (d, q_1) = 1$$

and $M'_d(x) = 0$ otherwise; here $\rho(b; d)$ is defined as in [7, p.955], i.e. it is the number of solutions $\alpha \mod d$ to

$$\alpha^2 + b^2 \equiv 0 \mod d.$$ 

We separate the case when $d$ is not coprime to $q$ because in this case $A'_d(x) = 0$. This follows because the pair of congruences $a_0 \mod q_1$ and $c_0 \mod q_2$ is admissible and hence $a'_n$ is supported on $n$ coprime to $q$. The lemma we wish to prove is now identical to [7, Lemma 3.1, p.956].

Lemma 5. For any $D \geq 1$, any $\varepsilon > 0$, and any $x \geq 2$, we have

$$\sum_{d \leq D} |A'_d(x) - M'_d(x)| \ll D^{1+\varepsilon},$$

where the implied constant depends only on $\varepsilon$.

This result is useful because it is easy to obtain an asymptotic formula for $M'_d(x)$ where the coefficient of the leading term is, up to a constant, a nice multiplicative function of $d$. In fact, let $h$ be the multiplicative function supported on cubefree integers defined in [7 (3.16), p.961] by

$$h(p^a)p = 1 + 2(1 + \chi_4(p)) \quad \text{and} \quad h(p^2)p^2 = p + 2(1 + \chi_4(p)),$$

where

$$h(p) = 1 + 2(1 + \chi_4(p)).$$
and define a multiplicative function $h'$ by setting

$$h'(n) = \begin{cases} h(n) & \text{if } (n, q) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then following the same argument as in the proof of [7, Lemma 3.4, p.961], we get

**Lemma 6.** For $d$ cubefree we have

$$M'_d(x) = g'(d) \frac{4\kappa x^{9/4}}{q_1 q_2} + O \left( h'(d) x^{9/16} \right),$$

where $\kappa$ is the integral given in the statement of Proposition 1 and the implied constant is absolute. $\square$

Combining Lemmas 5 and 6, we get, as in [7, Proposition 3.5, p.362],

**Proposition 3.** Let

$$a_0 \mod q_1 \quad c_0 \mod q_2$$

be an admissible pair of congruence classes, let $a'_n$ be defined as in (18), and let $r'_d(x)$ be defined as in (23). Then for every $\varepsilon > 0$ and every $D \geq 1$, there exists an $x_0 = x_0(\varepsilon) > 0$ and $C = C(\varepsilon) > 0$ such that for every $x \geq x_0$, we have

$$\sum_{d \leq D \text{ cubefree}} |r'_d(t)| \leq CD^{1/4} x^{9/16} + \varepsilon$$

uniformly for $t \leq x$.

Choosing $D = x^{5/4 - 8\varepsilon}$, we obtain hypothesis (R).

It remains to prove Lemma 5. We may assume that the sum is over $d \leq D$ with $(d, q) = 1$. For such $d$, we first approximate the sum $A'_d(x)$ by a smoothed sum

$$A'_d(f) = \sum_{n \equiv 0 \mod d} a'_n f(n),$$

where $f$ is a smooth function satisfying:

- $f$ is supported on $[0, x]$,
- $f(u) = 1$ for $0 < u \leq x - y$,
- $f^{(j)}(u) \ll y^{-j}$ for $x - y < u < x$,

where $y = D^{1/4} x^{13/16}$ and the implied constants depend only on $j$ (see [7, p.958]). Since $a'_n$ is supported on integers of the form $a^2 + c^4$, we trivially have

$$\sum_{d \leq D \atop (d, q) = 1} |A'_d(x) - A'_d(f)| \ll yx^{-1/4 + \varepsilon},$$

where the implied constant depends only on $\varepsilon$. With the above choice of $y$, it remains to prove Lemma 5 with $A'_d(x)$ replaced by $A'_d(f)$. Similarly as on [7, p.958], we write

$$A'_d(f) = \sum_b \sum_{\alpha \equiv 0 \mod d} \sum_{a \equiv \alpha \mod d} f(a^2 + b^2).$$

(26)
Since \((d, q) = 1\), so also \((d, q_1) = 1\), and the two conditions \(a \equiv \alpha \mod d\) and \(a \equiv a_0 \mod q_1\) can be combined into one condition \(a \equiv \alpha' \mod dq_1\). In fact, fixing an integer \(d\) that is an inverse of \(d\) modulo \(q_1\) and an integer \(q_1\) that is an inverse of \(q_1\) modulo \(d\), we can define \(\alpha'\) as

\[
\alpha' = aq_1q_1 + a_0d.
\]

We apply Poisson’s summation formula to the sum over \(a\) to obtain

\[
\sum_{a \equiv \alpha' \mod dq_1} f(a^2 + b^2) = \frac{1}{dq_1} \sum_k e\left(\frac{\alpha' k}{dq_1}\right) \int_{-\infty}^{\infty} f(t^2 + b^2)e\left(-\frac{tk}{dq_1}\right) dt.
\]

Here and henceforth, we use the standard notation

\[
e(t) := e^{2\pi it}.
\]

Substituting this into (26) we get

\[
A'_d(f) = \frac{2}{dq_1} \sum_b 3'(b) \sum_k \rho'(k, b; d) I(k, b; dq_1) dt,
\]

where

\[
\rho'(k, b; d) = \sum_{\alpha \equiv \alpha' \mod dq_1} e\left(\frac{\alpha' k}{dq_1}\right),
\]

and where

\[
I(k, b; dq_1) = \int_{0}^{\infty} f(t^2 + b^2) \cos(2\pi tk/dq_1) dt
\]

is defined exactly the same as on [7, p.959]. We define \(M'_d(f)\) to be the main term in this expansion, i.e. the term corresponding to \(k = 0\),

\[
M'_d(f) = \frac{2}{dq_1} \sum_b 3'(b) \rho(b; d) I(0, b; dq_1).
\]

Since \(I(0, b; dq_1) = I(0, b, q_1)\), the argument on page 959 shows that

\[
\sum_{d \leq D \atop (d,q) = 1} |M'_d(f) - M'_d(x)| \ll yx^{-\frac{1}{2}}(\log x)^2 \ll D^{-1}x^{\frac{1}{2} + \varepsilon},
\]

where the implied constants depend only on \(\varepsilon\). It remains to prove Lemma 5 with \(A'_d(f)\) in place of \(A'_d(x)\) and \(M'_d(f)\) in place of \(M'_d(x)\), i.e. to show that \(M'_d(f)\) is indeed (on average) the main term in the above Fourier expansion of \(A'_d(f)\).

Following the argument on [7, p.959-960], we see that it suffices to show an analogue of [7, Lemma 3.3, p.957] for \(\rho'(k, l; d)\).

**Lemma 7.** For any \(D, K, \) and \(L \geq 1\), for any complex numbers \(\xi(k, l)\), and for any \(\varepsilon > 0\), we have the inequality

\[
\sum_{d \leq D} \sum_{0 < k \leq K} \sum_{0 < l \leq L} |\xi(k, l)|^2 \rho'(k, l; d) \ll (D + \sqrt{DKL})(DKL)^{\varepsilon} ||\xi||
\]

where

\[
||\xi|| = \sum_{0 < k \leq K} \sum_{0 < l \leq L} |\xi(k, l)|^2,
\]
and the implied constant depends only on $\varepsilon$.

Recall the following inequality from [7] (3.6), p.957: for any complex numbers $\alpha_n$ and any $D, N \geq 1$, we have

\begin{equation}
\sum_{d \leq D} \sum_{\nu \equiv 1 \mod d} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu n}{d}\right) \right| \ll D^{\frac{1}{2}} (D + N)^{\frac{1}{2}} \|\alpha\|, \tag{27}
\end{equation}

where

$$\|\alpha\| := \left( \sum_{n} |\alpha_n|^2 \right)^{\frac{1}{2}},$$

and the implied constant is absolute. Lemma 7 can be proved in the same way as [7] Lemma 3.3, p.957 given the following analogue of inequality (27).

**Lemma 8.** Let $D, N \geq 1$ and let $\alpha_n$ be any complex numbers. For integers $d$ such that $(d, q_1) = 1$, let $\nu'$ be an integer in the unique residue class modulo $dq_1$ that reduces to $\nu$ modulo $d$ and $a_0$ modulo $q_1$. Then there exists an absolute constant $C = C(q_1)$ such that for all $D$ and $N$ sufficiently large, we have

\begin{equation}
\sum_{d \leq D} \sum_{\nu \equiv 1 \mod d} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu' n}{dq_1}\right) \right| \leq CD^{\frac{1}{2}} (D + N)^{\frac{1}{2}} \|\alpha\|. \tag{28}
\end{equation}

Inequality (28) is a consequence of a large sieve inequality applied to the rationals $\nu/d \mod 1$ with $\nu$ ranging over the roots of $\nu^2 + 1 \equiv 0 \mod d$ for $d$ in a range around $D$. The large sieve inequality can be applied because these rationals $\nu/d$ are well-spaced modulo 1 for $d$ in a certain range around $D$ (i.e. pairwise differences are uniformly bounded from below by about $1/D$ instead of $1/D^2$). This is a key ingredient in the work of [4]. In our analogue, however, it is not clear that $\nu'/dq_1$ are also well-spaced modulo 1 for $d$ in a similar range around $D$. Nonetheless, we can reduce Lemma 8 to inequality (27) as follows.

We first split the sum over $n$ into congruence classes modulo $q_1$ to get

$$\sum_{n_0 \mod q_1} \sum_{n \leq N} \alpha_n e\left(\frac{\nu' n}{dq_1}\right) = \sum_{n_0 \mod q_1} \sum_{m \leq (N-n_0)/q_1} \alpha_{m,n_0} e\left(\frac{\nu' m}{d}\right) e\left(\frac{\nu' n_0}{dq_1}\right),$$

where

$$\alpha_{m,n_0} = \alpha_{m+q_1,n_0}.$$

Since $e\left(\frac{\nu' n_0}{dq_1}\right)$ does not depends on $m$, the sum on the left-hand-side of (28) is

$$\leq \sum_{n_0 \mod q_1} \sum_{d \leq D} \sum_{\nu \equiv 1 \mod d} \left| \sum_{m \leq (N-n_0)/q_1} \alpha_{m,n_0} e\left(\frac{\nu' m}{d}\right) \right|.$$

Now $e\left(\frac{\nu' m}{d}\right) = e\left(\frac{\nu m}{d}\right)$ and

$$\sum_{m} |\alpha_{m,n_0}|^2 \leq \sum_{n} |\alpha_n|^2,$$
so that by (27) we get
\[ \sum_{d \leq D} \sum_{\nu \mod d} \sum_{n \leq N} \alpha_n e \left( \frac{\nu' n}{d^2q_1} \right) \ll q_1 D^{1/2} (D + N/q_1)^{1/2} \|\alpha\|. \]
This finishes the proof of \(8\) and thus also the proof of condition (R).

6. PROOF OF CONDITION (B)

Many of the upper bound estimates carried out in sections 4 and 5 of \cite{7} require no changes since \(0 \leq a'_n \leq a_n\) (compare (18) and (21)). In most cases, we now sum over fewer non-negative terms.

Recall that we established condition (R) with \(D = x^{\frac{3}{4} - 8\varepsilon}\). All of the refinements from \cite{7} Section 4, p.962-966 remain valid for our modified sequence \((a'_n)\). We briefly recall these refinements. First note that it is enough to prove the analogue of \cite{7} Proposition 4.1, p.963:

**Proposition 4.** Let \(c_0 \in \{0, 2\}\), let \(q_2 = 4\), and let
\[ a_0 \mod q_1 \quad c_0 \mod q_2 \]
be an admissible pair of congruence classes. Define \(\beta(n, C)\) as in (10), \(\Pi\) as in (11), and \(a'_n\) as in (13). Let \(x \geq 3\), \(\eta > 0\), and \(A > 0\). Let \(P\) be in the range
\[ (\log \log x)^2 \leq \log P \leq (\log x)(\log \log x)^{-2}. \]

Let
\[ B = 4A + 2^{20}. \]
Then there exists \(x_0 = x_0(\eta, A)\) such that for all \(x \geq x_0\), for all \(N\) with
\[ x^{\frac{3}{4} + \eta} < N < x^{\frac{3}{2} - B}, \]
and for all \(C\) with
\[ 1 \leq C \leq N^{1-\eta}, \]
we have
\[ \sum_m \left| \sum_{N \leq n \leq 2N} \beta(n, C) a_{mn} \right| \leq A'(x)(\log x)^{5-A}. \]

6.1. From Propositions 3 and 4 to Proposition 1. Before proving Proposition 4, we deduce Proposition 1 from Propositions 3 and 4. Let \(a_0 \in \{1, 3, 5, 7, 9, 11, 13, 15\}\), \(q_1 = 16\), \(c_0 \in \{0, 2\}\), and \(q_2 = 4\). Then
\[ a_0 \mod q_1 \quad c_0 \mod q_2 \]
is an admissible pair of congruences. We apply the asymptotic sieve for primes described in Section 4.1 to the sequence \((a'_n)\) defined in (13). Hypotheses (H1)-(H7) for \((a'_n)\) are verified in the same way as hypotheses (H1)-(H7) for the sequence \((a_n)\) defined in (21) (see comment at the end of Section 4.2).
Proposition 3 implies that \((a'_n)\) satisfies hypothesis (R) for \(\varepsilon = 1/8000\),

\[
D = x^{\frac{1}{10000}},
\]

which is indeed in the range \((15)\), and \(x_{r} = x_{r}(\varepsilon)\) large enough.

Applying Proposition 4 with the same \(D\) as in \((34)\), with \(P\) any number in the range \((15)\), with \(A = 5 + 2^{26}\), and with \(\eta = \frac{1}{100}\) establishes hypothesis (B) for the sequence \((a'_n)\) with \(\delta = (\log x)^{B'\varepsilon} = x^{\eta}, \Delta = x^{\eta}, \text{and } x_b = \max\{x_r, x_0(\eta, A)\}\).

We then obtain the asymptotic formula \((20)\) with

\[
c(q_1, q_2) = \frac{1}{32}
\]

which proves \((3)\).

6.2. Proof of Proposition 4. Suppose that we are in the setting of Proposition 4. Now take \(A' = 2A + 2^{20}\) (see [7, p.1018]) and define

\[
\varrho := (\log x)^{-A}
\]

and

\[
\theta := (\log x)^{-A'}
\]

as on [7, p.965]. We split the sum \((33)\) by using a smooth partition of unity. Let \(p\) be a smooth function supported on an interval

\[
N' < n \leq (1 + \theta)N'
\]

with \(N < N' < 2N\), and suppose that \(p\) is twice differentiable with

\[
p^{(j)} \ll (\theta N)^{-j}
\]

for \(j = 0, 1, 2\) (see [7, (4.14), p.965]). It then suffices to show Proposition 4 with \(\beta(n, C)\) replaced by a smoothed version

\[
(36) \quad \beta(n) = \beta(n, C) = p(n)\mu(n) \sum_{c|n, c \leq C} \mu(c)
\]

and the bound \(\leq A'(x)(\log x)^{B'\varepsilon - A}\) replaced by \(\leq C\varrho A'(x)(\log x)^{B}\) (see [7, (4.17), p.965]). Moreover, one can split the sum over \(m\) in \((33)\) into dyadic segments \(M \leq m \leq 2M\) with \(M\) satisfying

\[
(37) \quad \varrho x \leq MN \leq x.
\]

We remark that \((31)\) now implies that \(N \leq \varrho \theta(MN)^{\frac{1}{2}}\). Sums over the remaining dyadic segments are bounded trivially at an acceptable cost. Again, for an acceptable cost, one can suppose that \(\beta(n, C)\) is supported on \(n\) with

\[
(38) \quad \tau(n) \leq \tau := (\log x)^{A + 2^{20}}.
\]

(see [7, p.963-966, 1018]). For convenience of notation, we also restrict the support of \(\beta(n, C)\) to \(n\) satisfying

\[
(39) \quad (n, \Pi) = 1,
\]
where $\Pi$ is defined in (17). Finally, let $\alpha(m)$ be any complex numbers supported on $M < m \leq 2M$ with $|\alpha(m)| \leq 1$, and define

$$B^{**}(M, N) := \sum_{(m,n)=1} \alpha(m)\beta(n)\alpha'_m.$$  

where $\beta(n) = \beta(n, C)$ is defined as in (36) (see [7] (4.20), p.966)). To establish condition (B) it then suffices to prove

**Lemma 9.** Let $\eta > 0$ and $A > 0$ and take $B$ as in (30). Then there exists $x_0 = x_0(\eta, A) > 0$ such that for all $x \geq x_0$, for all $M$ and $N$ satisfying (31) and (37), and for all $C$ satisfying (32) we have

$$|B^{**}(M, N)| \leq \eta (MN)^{\frac{1}{2}}(\log MN)^{\frac{1}{5}}.$$  

6.3. **Proof of Lemma 9** In [7] Section 5, one begins to exploit the arithmetic in $\mathbb{Z}[i]$ and the inequality (B′) is reduced to another inequality involving sums over Gaussian integers. In our context, where $\alpha'_m$ are defined in (18), equation [7] (5.2), p.967] now becomes (for $(m, n) = 1$)

$$\alpha'_m = \sum_{|w|^2=m, |z|^2=n} 3'(\text{Re} wz),$$

where the sum over $z$ is restricted to primary Gaussian integers, i.e. $z$ satisfying

$$z \equiv 1 \text{ mod } 2(1+i).$$

Recall from (19) that the congruence condition $c \equiv c_0 \text{ mod } q_2$ is incorporated into the definition of $3'$. We now define $\alpha_w := \alpha(|w|^2)$ and $\beta_z := \beta(|z|^2)$ as on [7], p.967], so that (40) becomes

$$B^{**}(M, N) = \sum_{(wz, z) = 1} \alpha_w \beta_z 3'(\text{Re} wz).$$

Similarly as in [7] (5.7), p.967], we split the sum $B^{**}(M, N)$ into $O(q_1^4)$ sums by restricting the support of $\alpha_w$ to $w$ in a fixed residue class modulo $q_1$ and $\beta_z$ to $z$ in a fixed residue class $z_0$ modulo 64$q_1$, such that $z_0 \equiv 1 \text{ mod } 2(1+i)$. Now the residue class of $\text{Im} wz$ modulo $q_1$ is fixed, and so we can eliminate the condition $\text{Im} wz \equiv a_0 \text{ mod } q_1$.

We further modify the support of $\beta_z$ as in equation [7] (5.13), p.969]. Let $r(\alpha)$ be a smooth periodic function of period $2\pi$ supported on $\varphi \leq \alpha \leq \varphi + 2\pi\theta$ (where $\theta$ is as defined in (35) for some $-\pi < \varphi < \pi$ such that $r^{(j)} \ll \theta^{-j}$ for $j = 0, 1, 2$, and let

$$\beta_z = r(\alpha)p(n)\mu(n) \sum_{c|n, c \leq C} \mu(c),$$

where $\alpha = \arg z$ and $n = |z|^2$. Recall that by (38) and (39), $\beta_z = 0$ if either $\tau(|z|^2) > \tau$ or if $|z|^2$ is not coprime with $\Pi$. We remove the condition $(wz, z) = 1$ from (41) at an acceptable cost as in [7] (5.10), p.968] to get

$$B'(M, N) = B^{**}(M, N) + O \left(M^{\frac{1}{2}}N^{\frac{1}{2}} + P^{-1}M^{\frac{1}{2}}N^{\frac{1}{2}} \right)(\log N)^{\frac{3}{2}}$$

THE INFINITUDE OF $Q(\sqrt{-p})$ WITH CLASS NUMBER DIVISIBLE BY 16
where

\[
B'(M, N) := \sum_{\Im \tau \equiv a_0 \mod q_1} \alpha_\tau \beta_z \Im(\Re \tau z).
\]

We then apply Cauchy-Schwarz as in [7, (5.17), p.970] and introduce a smooth radial majorant \(f\) supported on the annulus \(1^{1/2} \leq |\tau| \leq 2\) (see [7, p.970]) to get

\[
B'(M, N) \ll M^{1/2} \mathcal{D}'(M, N)^{1/2},
\]

where

\[
\mathcal{D}'(M, N) := \sum_{\tau} f(\tau) \left| \sum_{z} \beta_z \Im(\Re \tau z) \right|^2.
\]

This eliminates the dependence on \(\alpha_\tau\), so that the sum over \(\tau\) above is free. After inserting a coprimality condition, we arrive at the sum

\[
\mathcal{D}'^*(M, N) := \sum_{(z_1, z_2) = 1} \beta_{z_1} \beta_{z_2} C'(z_1, z_2)
\]

(see [7 (5.26), p.972] and [7 (5.27), p.972]). The coprimality condition was inserted at the cost

\[
\mathcal{D}'^*(M, N) = \mathcal{D}'(M, N) + O \left( \varepsilon^2 (M^{1/2} N^{3/2} + P^{-1} M^{1/2} N^{5/2}) (\log MN)^{5/6} \right)
\]

(see [7 (5.22), p.972]). Recall that the congruence condition \(c \equiv c_0 \mod q_2\) is hidden in the definition of \(\mathcal{Y}'\), while the congruence condition \(a \equiv a_0 \mod q_1\) has been removed by restricting the support of \(\beta_z\). To prove Lemma 9, we now have left to prove

**Lemma 10.** Let \(\eta > 0\) and \(A > 0\), and take \(B\) as in (30). Then there exists \(x_0 = x_0(\eta, A)\) such that for all \(x \geq x_0\), for all \(M\) and \(N\) satisfying (31) and (37), and for all \(C\) satisfying (32), we have

\[
|\mathcal{D}'^*(M, N)| \leq C \eta^2 \theta^4 M^{1/2} N^{3/2} (\log MN)^{10}.
\]

Note the extra factor of \(\theta\) coming from the restriction of support of \(\beta\) to a sector of angle \(\theta\).

### 6.4. Proof of Lemma 10

In order to obtain this upper bound, Friedlander and Iwaniec introduce a quantity they call the “modulus”

\[
\Delta = \Delta(z_1, z_2) = \Im(z_1 z_2),
\]

which is non-zero whenever \((z_1, z_2) = 1\) and \(z_1\) and \(z_2\) are odd and primitive. The sum defining \(\mathcal{D}'^*(M, N)\) is split into several different sums depending on the size of the modulus \(\Delta\). Different techniques are used to treat each of these sums, but we will manage to avoid going into the details by reducing our sums to those already studied in [7].

The Fourier analysis carried out on [7, p.974] depends on the greatest common
denominator of $\Delta$ and $q_2$. Using the Poisson summation formula similarly as on [7, p.974], equation (44) can now be written as

$$D^*(M, N) = \sum_{\delta|q_2} \sum_{(z_1, z_2) = 1} \sum_{(q_2, |\Delta|) = \delta} \beta_{z_1} \overline{\beta}_{z_2} C'(z_1, z_2),$$

where

$$(45)$$

$$C'(z_1, z_2) = (q_2/\delta)^{-2} |z_1 z_2|^{-1/2} \sum_{h_1} \sum_{h_2} F \left( \frac{h_1}{|\Delta z_2|^{1/2} q_2 / \delta}, \frac{h_2}{|\Delta z_1|^{1/2} q_2 / \delta} \right) G'(h_1, h_2);$$

the Fourier integral

$$F(u_1, u_2) = \int \int f \left( \frac{z_2}{|z_2| t_1^2} - \frac{z_1}{|z_1| t_2^2} \right) e(u_1 t_1 + u_2 t_2) dt_1 dt_2$$

is the same as the one defined in [7, (6.8), p.974] and

$$G'(h_1, h_2) = \frac{1}{|\Delta|} \sum_{\gamma_1, \gamma_2 \mod |\Delta|} e \left( \frac{\gamma_1^2 h_1 + \gamma_2^2 h_2}{|\Delta| q_2 / \delta} \right)$$

is an arithmetic sum similar to $G(h_1, h_2)$ defined in [7, (6.10), p.974], but now incorporating the congruence condition $c \equiv c_0 \mod q_2$; here $\gamma_i'$ is the solution (modulo $|\Delta| q_2 / \delta$) to the system of congruences

$$\begin{align*}
\gamma_i' &\equiv \gamma_i \mod |\Delta| \\
\gamma_i' &\equiv c_0 \mod q_2.
\end{align*}$$

Such a solution is guaranteed to exist because $\gamma_1 \equiv \gamma_2 \equiv c_0 \mod \delta$. Note that similarly as in [7], we omit in the notation the dependence of $F$ and $G'$ on $z_1$ and $z_2$.

The main term in the above expansion for $C'(z_1, z_2)$ comes, as usual, from the terms with $h_1 = h_2 = 0$ in equation (45). Similarly as in the proof of condition (R) above, we don’t need to make any changes in the treatment of the Fourier integral; [7, Lemma 7.1, p.976] and [7, Lemma 7.2, p.977] are still valid, with the implied constants now depending on $q_2$ as well. We recall that [7, Lemma 7.2, p.977] states that for $z_1$ and $z_2$ in the support of $\beta_2$ we have

$$(46) \quad F_0(z_1, z_2) := F(0, 0) = 2 f(0) \log 2 |z_1 z_2| |\Delta| + O(\Delta^2 M^2 N^{-2} \log N).$$

We now have to give an upper bound for $G'(h_1, h_2)$ similar to the bound given in [7, Lemma 8.1, p.978], as well as give an exact formula for

$$G'_0(z_1, z_2) := G'(0, 0)$$

similar to the one in [7, Lemma 8.4, p.980]. This is where we now specialize to the case

$$q_2 = 4 \quad \text{and} \quad c_0 \in \{0, 2\}.$$  

Recall that we restricted the support of $\beta_2$ to $z$ in a fixed congruence class modulo $64 q_1$. Hence $z_1 \equiv z_2 \mod 64$, so that $\Delta = \text{Im}(\pi_{z_1, z_2}) \equiv 0 \mod 64$. This significantly simplifies our arguments since now $\delta = (4, |\Delta|) = 4$. 


The arithmetic sum $G'(h_1, h_2)$ now simplifies to

$$G'(h_1, h_2) = \frac{1}{|\Delta|} \sum_{\gamma_1, \gamma_2 \mod |\Delta|} \sum_{\gamma_1^2 Z_2 \equiv \gamma_1^2 Z_1 \mod |\Delta|} \sum_{\gamma_1 \equiv \gamma_2 \equiv \gamma_3 \mod 4} e\left(\frac{\gamma_1 h_1 + \gamma_2 h_2}{|\Delta|}\right).$$

We first prove a lemma analogous to [7, Lemma 8.1, p.978].

**Lemma 11.** Fix $\theta \in \{2, 4\}$ and let

$$G''(h_1, h_2; \theta) = \frac{1}{|\Delta|} \sum_{\omega_1, \omega_2 \mod |\Delta|/\theta} \sum_{\omega_1^2 Z_2 \equiv \omega_2 Z_1 \mod |\Delta|/\theta^2} e\left(\frac{\omega_1 h_1 + \omega_2 h_2}{|\Delta|/\theta^2}\right).$$

Then

$$(47) \quad \left|G''(h_1, h_2; \theta)\right| \leq 16 \tau_3(|\Delta|)|\Delta|^{-1}(z_1 h_1^2 - z_2 h_2^2, \Delta).$$

Introducing a change of variables $\gamma_1 = \theta \omega_1$ and $\gamma_2 = \theta \omega_2$, we get

$$G''(h_1, h_2; \theta) = \frac{1}{|\Delta|} \sum_{\omega_1, \omega_2 \mod |\Delta|/\theta} \sum_{\omega_1^2 Z_2 \equiv \omega_2 Z_1 \mod |\Delta|/\theta^2} e\left(\frac{\omega_1 h_1 + \omega_2 h_2}{|\Delta|/\theta^2}\right).$$

Proceeding in a similar fashion as on [7, p.977-978], we write

$$\Delta/\theta = \theta \Delta_1 (\Delta_2)^2,$$

with $\Delta_1$ squarefree. The condition $\omega_1^2 Z_2 \equiv \omega_2 Z_1 \mod |\Delta|/\theta^2$ implies that $(\omega_1^2, \Delta/\theta^2) = (\omega_2^2, \Delta/\theta^2)$, so we can write

$$(\omega_1^2/\theta^2, \Delta/\theta^2) = (\omega_2^2, \Delta/\theta^2) = d_1 d_2^2$$

with $d_1$ squarefree. Then $d_1 |\Delta_1, d_2 |\Delta_2, (d_1, d_2/d_2) = 1$, and we can make a change of variables $\omega_1 = d_1 d_2 \eta_1$, there $\eta_1$ runs over the residue classes modulo $|\Delta|/\theta d_1 d_2$ and coprime with $|\Delta|/\theta^2 d_1 d_2$. Setting $b_1 = \Delta_1 / d_1$ and $b_2 = \Delta_2 / d_2$, the analogue of the equation on top of [7, p.978] becomes

$$G''(h_1, h_2; \theta) = \frac{1}{|\Delta|} \sum_{b_1, d_1 |\Delta_1} \sum_{b_2, d_2 |\Delta_2} \sum_{d_1, d_2} \sum_{\eta_1, \eta_2 \mod \theta b_1 b_2^2} e((\eta_1 h_1 + \eta_2 h_2)/(\theta b_1 b_2^2 d_2)).$$

The innermost sum vanishes unless $h_1 \equiv h_2 \equiv 0 \mod \theta d_2$, so $G''(h_1, h_2)$ is equal to

$$\frac{1}{|\Delta|} \sum_{b_1, d_1 |\Delta_1} \sum_{b_2, d_2 |\Delta_2} \sum_{d_1, d_2} \sum_{\eta_1, \eta_2 \mod \theta b_1 b_2^2} e((\eta_1 h_1 + \eta_2 h_2)/(\theta b_1 b_2^2 d_2)).$$

Performing the change of variables $\eta_2 = \omega \eta_1$, the analogue of equation [7, (8.3), p.978] becomes

$$\frac{1}{|\Delta|} \sum_{b_1, d_1 |\Delta_1} \sum_{b_2, d_2 |\Delta_2} \sum_{d_1, d_2} \sum_{\omega \equiv \gamma_2 \equiv \gamma_3 \mod \theta b_1 b_2^2} R((h_1 + \omega h_2)/(\theta d_2)^{-1}; b_1 b_2^2).$$
where $R(h; b)$ is the classical Ramanujan sum defined on [7, p.978]. Now the same argument as on [7, p.978] yields the desired upper bound \(47\). □

We now turn our attention back to $G'(h_1, h_2)$. In case $c_0 = 0$, we’re in the case of Lemma 11 and

$$|G'(h_1, h_2)| = |G''(h_1, h_2; 4)| \leq 16\tau_3(\Delta)|\Delta|^{-1}(z_1h_1^2 - z_2h_2^2, \Delta).$$

If, on the other hand, $c_0 = 2$, we note that $G'(h_1, h_2) = G''(h_1, h_2; 2) - G''(h_1, h_2; 4)$ since $\Delta \equiv 0 \mod 16$. Hence

$$|G'(h_1, h_2)| \leq 32\tau_3(\Delta)|\Delta|^{-1}(z_1h_1^2 - z_2h_2^2, \Delta).$$

The same arguments as those in Section 9 of [7] now suffice to show that the main term in the Fourier expansion indeed comes from $h_1 = h_2 = 0$. We recall the result from [7, (9.10), p.983] here. Let

$$D'_0(M, N) := \sum_{(z_1, z_2)} \beta_{z_1} \beta_{z_2} C'_0(z_1, z_2),$$

where

$$C'_0(z_1, z_2) = |z_1z_2|^{-1/2} F_0(z_1, z_2) G'_0(z_1, z_2).$$

**Lemma 12.** Let $\eta > 0$ and $A > 0$, and take $B$ as in (30). Then there exists $x_0 = x_0(\eta, A)$ such that for all $x \geq x_0$, for all $M$ and $N$ satisfying (31) and (37), and for all $C$ satisfying (32), we have

$$|D'^0(M, N) - D'_0(M, N)| \leq \vartheta^{-1}r^2N^2(\log N)^{\eta - 1/8},$$

where $\vartheta$ is defined in (38).

It now remains to estimate $D'_0(M, N)$. We turn to obtaining an exact formula for $G'_0(z_1, z_2)$. Recall, from top of [7, p.979], that

$$G'_0(z_1, z_2) := \frac{1}{|\Delta|} \sum_{\gamma_1, \gamma_2 \mod |\Delta|} \sum_{\gamma_1 z_2 + \gamma_2 z_1 \mod |\Delta|} 1 = N(z_2/z_1; |\Delta|)/|\Delta|,$$

where $N(a; r)$ denotes the number of solutions $(\gamma_1, \gamma_2)$ modulo $r$ to

$$a\gamma_1^2 \equiv \gamma_2^2 \mod r.$$

Similarly,

$$G'_0(z_1, z_2) = N'(z_2/z_1; |\Delta|)/|\Delta|,$$

where $N'(a; r)$ is the number of solutions $(\gamma_1, \gamma_2)$ modulo $r$ to the congruences

$$\begin{cases} a\gamma_1^2 \equiv \gamma_2^2 \mod r \\ \gamma_1 \equiv \gamma_2 \equiv c_0 \mod 4. \end{cases}$$

Since $z_2/z_1 \equiv 1 \mod 64$ and $\Delta \equiv 0 \mod 64$, we are only concerned with the case $a \equiv 1 \mod 64$ and $r \equiv 0 \mod 64$.

### 6.5. Computation of $N'(a; r)/r$
6.5.1. Case $c_0 = 0$. First let us compute $N'(a; r)/r$ when $c_0 = 0$. Since $\gamma_1 \equiv \gamma_2 \equiv 0 \mod 4$, we can make a change of variables $\gamma_1 = 4\omega_1$ and $\gamma_2 = 4\omega_2$, where now $\omega_i$ are congruence classes modulo $r/4$, to find that $N'(a; r) = 16N(a; r/16)$, i.e.

$$N'(a; r)/r = N(a; r/16)/(r/16).$$

This leads to a formula of type \cite{7} (8.16), p.980. If $16 \cdot 2^\nu$ with $\nu \geq 1$ is the exact power of 2 dividing $\Delta$, we get

$$G'_0(z_1, z_2) = \nu \sum_{16d|\Delta \atop d \text{ odd}} \frac{\varphi(d)}{d} \left( \frac{z_2/z_1}{d} \right).$$

Since $\Delta \equiv 0 \mod 64$, we are only interested in the case $\nu \geq 2$, where this becomes

(49) $$G'_0(z_1, z_2) = 2 \sum_{64d|\Delta} \frac{\varphi(d)}{d} \left( \frac{z_2/z_1}{d} \right),$$

by the same reasoning as in \cite{7} Lemma 8.4, p.980.

6.5.2. Case $c_0 = 2$. When $c_0 = 2$ and $4|r$, we can make a change of variables $\gamma_1 = 2\omega_1$ and $\gamma_2 = 2\omega_2$ so that $N'(a; r)$ is 4 times the number of solutions $(\omega_1, \omega_2)$ modulo $r/4$ to the system of congruences

$$\begin{cases} 
\omega_1 \equiv \omega_2 \equiv 1 \mod 2 \\
\omega_1^2 \equiv \omega_2^2 \mod r/4.
\end{cases}$$

When $16|r$, we must subtract from $4N(a; r/4)$ those solutions with $\omega_1 \equiv \omega_2 \equiv 0 \mod 2$. This gives $N'(a; r) = 4N(a; r/4) - 16N(a; r/16)$, i.e.

$$\frac{N'(a; r)}{r} = \frac{N(a; r/4)}{r/4} - \frac{N(a; r/16)}{r/16}.$$  

Hence if $16 \cdot 2^\nu$ with $\nu \geq 2$ is the exact power of 2 dividing $\Delta$, we get

(50) $$G'_0(z_1, z_2) = 2 \sum_{16d|\Delta} \frac{\varphi(d)}{d} \left( \frac{z_2/z_1}{d} \right) - 2 \sum_{64d|\Delta} \frac{\varphi(d)}{d} \left( \frac{z_2/z_1}{d} \right),$$

which is the analogue of (49).

6.6. End of proof of Lemma \cite{10}. We now turn back to estimating $\mathcal{D}'_0(M, N)$. As in \cite{7} (10.4), p.985, we can use (49) to write

$$\mathcal{D}'_0(M, N) = 2f(0)N^{\frac{1}{2}}T'(\beta) + O \left( (r^{-1} + \theta)Y'(\beta)M^N N^{\frac{1}{2}} \log N \right)$$

where

$$T'(\beta) := \sum_{(z_1, z_2) = 1} |\beta_{z_1} \beta_{z_2}| G'_0(z_1, z_2) \log |z_1z_2/\Delta|$$

and

$$Y'(\beta) := \sum_{(z_1, z_2) = 1} |\beta_{z_1} \beta_{z_2}| \tau(|z_1|^2) \tau(|z_2|^2) \tau_3(\Delta).$$

Similarly as in \cite{7} Lemma 10.1, p.985, we can bound $Y'(\beta)$ by

$$Y'(\beta) \ll \theta^4 N^2 (\log N)^{219},$$
so that we are left with estimating the sum \( T'(\beta) \). In each of the cases \( c_0 = 0 \) and \( c_0 = 2 \), we can use the formula for \( G_0(z_1, z_2) \) and \( F_0(z_1, z_2) \) to write \( T'(\beta) \) as a sum similar to \([7, (10.13), p.986]\). If we define

\[
T'(\beta, \xi) := 2 \sum_d \frac{\varphi(d)}{d} \sum_{\Delta(z_1, z_2) \equiv 0 \text{ mod } \xi d} \beta_{z_1} \beta_{z_2} \left( \frac{z_2/z_1}{d} \right) \log 2|z_1 z_2/\Delta|,
\]

then

\[
T'(\beta) = \begin{cases} 
T'(\beta, 64) & \text{if } c_0 = 0 \\
T'(\beta, 16) - T'(\beta, 64) & \text{if } c_0 = 2
\end{cases}
\]

Lemma 10 now follows from this analogue of \([7, Proposition 10.2, p.986]\):}

**Lemma 13.** Fix \( \xi \in \{16, 64\} \). Let \( \eta > 0 \), \( A > 0 \), and \( \sigma > 0 \), and take \( B \) as in \((30)\). Then there exists \( x_0 = x_0(\eta, A) \) and \( C_0 = C_0(\eta, A, \sigma) > 0 \) such that for all \( x \geq x_0 \), for all \( N \) satisfying \((31)\), and for all \( C \) satisfying \((32)\), we have

\[
T'(\beta, \xi) \leq C_0 N^2 (\log N)^{-\sigma} + P^{-1} N^2 \log N,
\]

where \( P \) is any number in the range \((29)\).

We recall that \( N \) and \( P \) appear as parameters restricting the support of \( \beta_z \); see \((42)\).

### 6.7. Proof of Lemma 13: oscillations of characters and symbols.
Although complicated, the proof of \([7, Proposition 10.2]\) generalizes directly to the proof of Lemma 13. One can check in \([7, Sections 15-17]\) that the same arguments are valid when \( \xi = 16 \) or 64 instead of \( \xi = 4 \). For instance, on \([7, p.1005]\) and \([7, p.1015]\), one now sums over multiplicative characters of the groups \((\mathbb{Z}[i]/\xi d \mathbb{Z}[i])^\times\) and \((\mathbb{Z}[i]/\xi bd \mathbb{Z}[i])^\times\), respectively.

Moreover, the restriction on the support of \( \beta_z \) to \( z \) in a fixed primary congruence class modulo 64\( q_1 \) (where \( q_1 \) is as in \((18)\)) as opposed to modulo 8 is handled in the same way as in \([7, Sections 15-17]\). For sums over medium-size moduli, the estimation of \( \beta_z \) is trivial and so the restriction on the support is irrelevant (see bottom of \([7, p.1003]\)). For sums over small moduli, i.e. \( d \) of size at most a large power of \( \log N \), the key sum to bound from above is the character sum

\[
S^k_\chi(\beta) = \sum_z \beta_z \chi(z) \left( \frac{z}{|z|} \right)^k,
\]

where \( \chi \) is a multiplicative character of the group \((\mathbb{Z}[i]/\xi d \mathbb{Z}[i])^\times\) (see \([7, (16.14), p.1005]\)). The restriction on the support of \( \beta_z \) can be detected by multiplicative characters modulo 64\( q_1 \), so that we can simply transform \( \chi \) into a character for the group \((\mathbb{Z}[i]/64q_1d \mathbb{Z}[i])^\times\). The sum \((51)\) is bounded by studying the Hecke \( L \)-functions

\[
L(s, \psi) = \sum_a \psi(a)(Na)^{-s},
\]

where the sum ranges over the non-zero odd ideals \( a \) of \( \mathbb{Z}[i] \) and

\[
\psi(a) := \chi(z) \left( \frac{z}{|z|} \right)^k.
\]
where $z$ is the unique primary Gaussian integer which generates $a$. The dependence on $\chi$ of the bound given for $S^k_\chi(\beta)$ is only through the modulus of $\chi$ (see [7, Lemma 16.2, p.1012]) and this modulus is different from $4d$ by a fixed constant. Similarly, for the sums over large moduli, the key sum to bound from above is the character sum

\begin{equation}
S^k_\chi(\beta') = \sum_z \beta'_z \chi(z) \left( \frac{z}{|z|} \right)^k,
\end{equation}

where $\chi$ is a multiplicative character of the group $(\mathbb{Z}[i]/\xi bd\mathbb{Z}[i])^\times$ (where $b$ is an integer and $d$ is again bounded by a large power of $\log N$) but $\beta'_z$ is now

$$
\beta'_z = i^{\frac{r-1}{2}} \left( \frac{s}{|r|} \right) \beta_z
$$

if $z = r + is$ (see [7] (17.8), p.1014 and [7] (17.12), p.1015)). Again, the restriction on the support of $\beta_z$ (and hence also $\beta'_z$) can be detected by multiplicative characters modulo $64q_1$, so that we can transform $\chi$ into a character for the group $(\mathbb{Z}[i]/64q_1 bd\mathbb{Z}[i])^\times$. Cancellation in the sum (52) is now achieved due to the oscillation of the symbol

$$
\frac{r}{|r|}
$$

as $z$ varies over primary Gaussian integers, but again the dependence on $\chi$ of the bound given for (52) is only through the modulus of $\chi$ (see [7] Proposition 17.2, p.1016) and this modulus is again different from $4bd$ by a fixed constant. This shows that Lemma 13 follows from [7, Proposition 10.2] and hence Proposition 4 is proved.

7. Acknowledgements

I would like to give special thanks to my advisors Étienne Fouvry and Peter Stevenhagen for their unceasing support and useful advice as well as for helping me resolve numerous issues that arose during the course of this research. I would also like to thank Christian Elscholtz, Jan-Hendrik Evertse, Florent Jouve, and Hendrik Lenstra for useful discussions.

References

[1] P. Barrucand and H. Cohn. Note on primes of type $x^2 + 32y^2$, class number, and residuacity. J. Reine Angew. Math., 238:67–70, 1967.
[2] H. Cohen and H. W. Lenstra. Heuristics on class groups of number fields. In Number Theory, volume 1068 of Lecture Notes in Math., pages 33–62. Springer-Verlag, New York, 1984.
[3] H. Cohn and G. Cooke. Parametric form of an eight class field. Acta Arith., 30:367–377, 1976.
[4] E. Fouvry and H. Iwaniec. Gaussian primes. Acta Arith., 79:249–287, 1997.
[5] E. Fouvry and J. Klüners. The parity of the period of the continued fraction of $\sqrt{d}$. Proc. of the London Math. Soc., 101:337–391, 2010.
[6] J. Friedlander and H. Iwaniec. Asymptotic sieve for primes. Ann. of Math., 148:1041–1065, 1998.
[7] J. Friedlander and H. Iwaniec. The polynomial $X^2 + Y^4$ captures its primes. Ann. of Math., 148:945–1040, 1998.
[8] J. Friedlander and H. Iwaniec. Opera de Cribro. American Math. Soc., New York, 2010.
[9] P. Kaplan. Cycles d’ordre au moins 16 dans le 2-groupe des classes d’idéaux de certains corps quadratiques. Bull. Soc. Math. France Mém., 49-50:113–124, 1977.
[10] J.C. Lagarias. Signatures of units and congruences (mod 4) in certain real quadratic fields. J. reine angew. Math., 320:115–126, 1980.

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

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

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

[14] H. Reichardt. Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper. J. Reine Angew. Math., 170:75–82, 1933.

[15] P. Stevenhagen. Ray class groups and governing fields. Publ. Math. Fac. Sci. Besançon, 1989.

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

[17] K.S. Williams. On the class number of \( \mathbb{Q}(\sqrt{-p}) \) modulo 16 for \( p \equiv 1 \pmod{8} \) a prime. Acta Arith., 39:381–398, 1981.