Author: Milovic, D.
Title: On the 16-rank of class groups of quadratic number fields
Issue Date: 2016-07-04

Chapter 2

Infinitude of $\mathbb{Q}(\sqrt{-4p})$ with class number divisible by 16

Let p be a prime number, and let Cl and h be the class group and the class number of $\mathbb{Q}(\sqrt{-4p})$, respectively. Since the discriminant of this field is either $-p$ or $-4p$, Gauss's genus theory implies that the 2-part of Cl 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

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

The criterion

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

can be deduced easily from Rédei's work on the 4-rank of quadratic number fields [34]. 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

$$8|h \iff p = x^2 + 32y^2 \text{ for some integers } x \text{ and } y.$$

This can be restated as

$$8|h \iff p \equiv 1 \bmod 8 \text{ and } 1+i \text{ is a square modulo } p \tag{2.1}$$

where i is a square root of -1 modulo p (see [1, (10), p.68]). In [40], Stevenhagen also obtained the criterion (2.1), albeit by a more abstract argument using class field theory over the field $\mathbb{Q}(i)$.

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

$$S(n) = \{p \text{ prime } : n|h(-4p)\};$$

here we write $h(-4p)$ for the class number of $\mathbb{Q}(\sqrt{-4p})$ to emphasize its dependence on p. From the above, classical results about primes in arithmetic progressions imply that $\rho(S(2)) = 1/2$ and $\rho(S(4)) = 1/4$. From (2.1), we see that 8 divides h if and only if p splits completely in $\mathbb{Q}(\zeta_8, \sqrt{1+i})$, where ζ_8 is a primitive 8^{th} 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 [41, p.16-19].

The Cohen-Lenstra heuristics [4] 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, $\rho(S(2^k)) = \frac{1}{2}\rho(S(2^{k-1}))$ for $k \leq 3$, so we are led to conjecture

Conjecture 2.1. *For all $k \geq 1$, the limit $\lim_{X\to\infty} R(S(2^k), X)$ exists and is equal to 2^{-k}.*

While Conjecture 2.1 is true for $k \leq 3$, it has not been proven for any $k \geq 4$. In fact, proving the conjecture for $k \geq 4$ would likely require significant new ideas because a proof along the lines of the arguments for $k \leq 3$ seems far out of reach (see [41, p. 16]). Although several criteria for divisibility by 16 have been found already (see [26], [45], and [30]), none of them appear to be sufficient to produce even infinitely many primes p for which the class number of $\mathbb{Q}(\sqrt{-4p})$ is divisible by 16. This is precisely our aim in this chapter – 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 ϵ_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

$$p = a^2 + c^4, \quad c \text{ even.} \tag{2.2}$$

The main theorem that we prove gives a new and very explicit criterion for divisibility by 16 of class numbers of $\mathbb{Q}(\sqrt{-4p})$ for p of the form (2.2).

Theorem 2.1. *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 $\mathbb{Q}(\sqrt{-4p})$.*

(i) If $a \equiv \pm 1 \bmod 16$ and $c \equiv 0 \bmod 4$, then $h(-4p) \equiv 0 \bmod 16$.

(ii) If $a \equiv \pm 3 \bmod 16$ and $c \equiv 2 \bmod 4$, then $h(-4p) \equiv 0 \bmod 16$.

(iii) If $a \equiv \pm 7 \bmod 16$ and $c \equiv 0 \bmod 4$, then $h(-4p) \equiv 8 \bmod 16$.

(iv) If $a \equiv \pm 5 \bmod 16$ and $c \equiv 2 \bmod 4$, then $h(-4p) \equiv 8 \bmod 16$.

Once we prove Theorem 2.1, Theorem A follows from the following generalization of a powerful theorem of Friedlander and Iwaniec (see [19, Theorem 1]):

Proposition 2.1. *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*

$$\sum_{\substack{a^2+c^4 \leq X \\ a \equiv a_0 \bmod 16 \\ c \equiv c_0 \bmod 4 \\ a^2+c^4 \text{ prime}}} \sum 1 = \frac{\kappa}{2\pi} \frac{X^{3/4}}{\log X}\left(1 + O\left(\frac{\log\log X}{\log X}\right)\right), \tag{2.3}$$

where a *and* c *run over* $\mathbb{Z}$ *and*

$$\kappa = \int_0^1 (1-t^4)^{\frac{1}{2}}\, dt \approx 0.874\ldots.$$

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

Proposition 2.1 also implies the infinitude of primes p of the form as in the statements $(i) - (iv)$ Theorem 2.1. We have the following quantitative result:

Corollary 2.1. *For a prime* p, *let* $h(-4p)$ *denote the class number of* $\mathbb{Q}(\sqrt{-4p})$. *Then, for sufficiently large* X, *we have*

$$\#\{p \leq X : h(-4p) \equiv 0 \bmod 16\} \geq \frac{X^{3/4}}{8\log X}$$

and

$$\#\{p \leq X : h(-4p) \equiv 8 \bmod 16\} \geq \frac{X^{3/4}}{8\log X}.$$

The proof of Proposition 2.1 will take a significant portion of this chapter. Although the ideas required to generalize [19, Theorem 1] in this way are not particularly deep, implementing them turns out to be quite complicated simply because the proof of [19, Theorem 1] itself is very difficult. One can thus view Sections 2.4-2.6 as a summary of the proof of [19, 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 2.1. Nonetheless, each of the cases $(i) - (iv)$ in Theorem 2.1 occurs with the same density among all primes this form, so the analogous conjecture for $k = 4$ deduced from the Cohen-Lenstra heuristics above holds within the thin family of imaginary quadratic number fields $\mathbb{Q}(\sqrt{-4p})$ 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 2.1 is true for $k = 4$. However, we also note that Conjecture 2.1 for $k = 4$ does not imply Corollary 2.1, as knowledge of the behavior of the class numbers of $\mathbb{Q}(\sqrt{-4p})$ 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 [45]. Let $p \equiv 1 \bmod 8$, and let ϵ_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

$$h \equiv T + p - 1 \bmod 16, \tag{2.4}$$

so that $16|h$ if and only if $T \equiv 1 - p \bmod 16$. An immediate byproduct of Theorem 2.1 and criterion (2.4) is the following corollary.

Corollary 2.2. *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 $a \equiv \pm 1 \bmod 16$ and $c \equiv 0 \bmod 4$, then $T \equiv 0 \bmod 16$ and $U \equiv \pm 1 \bmod 8$.

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

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

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

This can be viewed as an extension of [27, Corollary 1.2(i), p.115-116] to primes of the form $p = a^2 + c^4$. Now Proposition 2.1 gives

Corollary 2.3. *For a prime $p \equiv 1 \bmod 8$, let $\epsilon_p = T + U\sqrt{p}$ denote the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Then, for sufficiently large X, we have*

$$\#\{p \le X : p \equiv 1 \bmod 8,\ T \equiv 0 \bmod 16\} \ge \frac{X^{3/4}}{8 \log X}$$

and

$$\#\{p \le X : p \equiv 1 \bmod 8,\ T \equiv 8 \bmod 16\} \ge \frac{X^{3/4}}{8 \log X}.$$

The existence of infinitely many $p \equiv 1 \bmod 8$ such that $T \equiv T_0 \bmod 16$ for a fixed $T_0 \in \{0, 8\}$ is not at all trivial. Hence Corollary 2.2 sheds some new light on the fundamental unit ϵ_p of $\mathbb{Q}(\sqrt{p})$, one of the most mysterious quantities in number theory.

2.1 Hilbert class fields

Suppose $p \equiv 1 \pmod 4$. Then there are two finite primes of $\mathbb{Q}$ which ramify in $\mathbb{Q}(\sqrt{-4p})$, namely 2 and p. The prime $\mathfrak{p} = (\sqrt{-p})$ of $\mathbb{Q}(\sqrt{-4p})$ lying above

p is principal, and so its ideal class in Cl is the identity. Genus theory then implies that the class of the prime ideal $\mathfrak{t} = (2, 1 + \sqrt{-p})$ of $\mathbb{Q}(\sqrt{-4p})$ lying above 2 is the unique element of order two in Cl. 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 $\mathfrak{t}$ belongs to Cl^{2^n}.

2.1.1 2^n-Hilbert class fields

Suppose that $2^n|h$ for some non-negative integer n. Then recall that (1.11) induces a canonical isomorphism of cyclic groups of order 2^n

$$\left(\frac{\cdot}{H_{2^n}/K}\right) : \mathrm{Cl}/\mathrm{Cl}^{2^n} \longrightarrow \mathrm{Gal}(H_{2^n}/K). \tag{2.5}$$

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

$$2^{n+1}|h \Longleftrightarrow [\mathfrak{t}] \text{ splits completely in } H_{2^n}. \tag{2.6}$$

The main idea of the proof of Theorem 2.1 is to write down explicitly the 8-Hilbert class field H_8 of $\mathbb{Q}(\sqrt{-4p})$, and then to characterize those p such that $\mathfrak{t}$ splits completely in H_8. We remark here that although Cohn and Cooke [7] have already written down H_8 in terms of the fundamental unit ϵ_p of the real quadratic number field $\mathbb{Q}(\sqrt{p})$ and certain integer solutions u and v to $p = 2u^2 - v^2$, not enough is known about either ϵ_p or u and v to deduce anything about the distribution of primes p such that $\mathfrak{t}$ splits completely in H_8.

2.1.2 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 $\mathbb{Q}(\sqrt{-4p})$, is known to be $H_2 = \mathbb{Q}(i, \sqrt{p})$. Hence every 2^n-Hilbert class field of $\mathbb{Q}(\sqrt{-4p})$ contains $\mathbb{Q}(i)$, and so we can study the splitting behavior of $\mathfrak{t}$ in H_{2^n} by working over the quadratic subfield $\mathbb{Q}(i)$ of H_2. With this in mind, we now state some well-known generalities about the completion of $\mathbb{Q}(i)$ with respect to the prime ideal $(1 + i)$ lying over 2.

This completion is $\mathbb{Q}_2(i)$, and its ring of integers $\mathbb{Z}_2[i]$ is a discrete valuation ring with uniformizer $m = 1 + i$ and maximal ideal $\mathfrak{m} = (m)$. Let $U = (\mathbb{Z}_2[i])^\times$ denote the group of units of $\mathbb{Z}_2[i]$ and for each positive integer k, define $U^{(k)} = 1 + \mathfrak{m}^k$. 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 $U^{(k)} \xrightarrow{\sim} U^{(k+2)}$. Indeed, let $1 + m^{k+2}y \in U^{(k+2)}$. Hensel's lemma implies that there exists $x \in \mathfrak{m}^{k-2}$ 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 $U^2 = \langle -1 \rangle \times U^{(5)}$. In other words, $u \in U$ is a square in $\mathbb{Q}_2(i)$ if and only if $u \equiv \pm 1 \pmod{\mathfrak{m}^5}$. Moreover, if $\omega \equiv \pm 1 \pmod{\mathfrak{m}^4}$, then $\mathbb{Q}_2(i, \sqrt{\omega})$ is generated over $\mathbb{Q}_2(i)$ by a root of the polynomial $X^2 - X + (1 \mp \omega)/4$, which reduces to $X^2 + X$ or $X^2 + X + 1$ modulo $\mathfrak{m}$. We collect these observations into the following lemma.

Lemma 2.1. *Let ω be a unit in $\mathbb{Z}_2[i]$. Then $\mathbb{Q}_2(i, \sqrt{\omega})$ is unramified over $\mathbb{Q}_2(i)$ if and only if $\omega \equiv \pm 1 \pmod{\mathfrak{m}^4}$. Moreover, $\mathbb{Q}_2(i, \sqrt{\omega}) = \mathbb{Q}_2(i)$, i.e., ω is a square in $\mathbb{Q}_2(i)$ if and only if $\omega \equiv \pm 1 \pmod{\mathfrak{m}^5}$.*

Next, we state two lemmas which we will use to check that the extensions of $\mathbb{Q}(\sqrt{-4p})$ which we construct are normal and cyclic. First, in both Chapter 2 and Chapter 3, we will make extensive use of the following lemma from Galois theory (see [29, Chapter VI, Exercise 4, p.321]).

Lemma 2.2. *Let F be a field of characteristic different from 2, let $E = F(\sqrt{d})$, where $d \in F^\times \setminus (F^\times)^2$, and let $L = E(\sqrt{x})$, where $x \in E^\times \setminus (E^\times)^2$. Let $N = \mathrm{Norm}_{E/F}(x)$. Then we have three cases:*

1. *If $N \notin (E^\times)^2 \cap F^\times = (F^\times)^2 \cup d \cdot (F^\times)^2$, then L/F has normal closure $L(\sqrt{N})$ and $\mathrm{Gal}(L(\sqrt{N})/F)$ is a dihedral group of order 8.*
2. *If $N \in (F^\times)^2$, then L/F is normal and $\mathrm{Gal}(L/F)$ is a Klein four-group.*
3. *If $N \in d \cdot (F^\times)^2$, then L/F is normal and $\mathrm{Gal}(L/F)$ is a cyclic group of order 4.*

Lemma 2.3. *Let K be a field. Suppose M/K is a cyclic extension of degree $2m$ and let σ be a generator of $\mathrm{Gal}(M/K)$. Let L be the subfield of M fixed by σ^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 σ_1 denote a lift of σ to $\mathrm{Gal}(N/K)$. The order of σ_1 is at least $2m$ since the order of σ is $2m$. As σ^m fixes L, σ_1^m is an element of $\mathrm{Gal}(N/L)$which is non-trivial on M and hence has order 4. Thus the order of σ_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 [36, 3. Satz, p.82]. His theorem proves the existence of generators $\sqrt{\varpi}$ for H_{2^n} over $H_{2^{n-1}}$ with $\varpi \in H_{2^{n-1}}$ of a certain form. We prove sufficient conditions for an element ϖ of a similar form to give rise to a generator, so that we can actually construct H_{2^n}.

Lemma 2.4. *Let h be the class number of $\mathbb{Q}(\sqrt{-4p})$, let $n \geq 2$, and suppose that 2^n divides h. Suppose that we have a sequence of field extensions*

$$\mathbb{Q} = A_1 \subset \mathbb{Q}(i) = A_2 \subset A_4 \subset \cdots \subset A_{2^{n-1}}$$

such that:

- A_{2^k} *is a degree 2^k extension of $\mathbb{Q}$ for $1 \leq k \leq n-1$,*
- $A_{2^k} \subset H_{2^k}$ *for $1 \leq k \leq n-1$,*
- $A_{2^k} \cap H_{2^{k-1}} = A_{2^{k-1}}$ *for $2 \leq k \leq n-1$,*
- $(1+i)$ *is unramified in $A_{2^{n-1}}/\mathbb{Q}(i)$, and*
- *there is a prime element ϖ in the ring of integers of $A_{2^{n-1}}$ such that:*
  - *ϖ lies above p and its ramification and inertia indices over p are equal to 1,*
  - *denoting the conjugate of ϖ over $A_{2^{n-2}}$ by ϖ', we have $H_{2^{n-1}} = H_{2^{n-2}}(\sqrt{\varpi\varpi'}) = A_{2^{n-1}}(\sqrt{\varpi\varpi'})$,*
  - *(U_2): $(1+i)$ remains unramified in $A_{2^n} = A_{2^{n-1}}(\sqrt{\varpi})$, and*
  - *(N): $H_{2^{n-1}}(\sqrt{\varpi})$ is normal over $\mathbb{Q}$.*

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

Proof. The ramification index of ϖ over p is 1, so ϖ and ϖ' are coprime in $A_{2^{n-1}}$.

First we check that ϖ is not a square in $H_{2^{n-1}}$. Since $[A_{2^n} : A_{2^{n-1}}] = [H_{2^{n-1}} : A_{2^{n-1}}] = 2$ and $A_{2^n} = A_{2^{n-1}}(\sqrt{\varpi})$, we deduce that ϖ is a square in $H_{2^{n-1}}$ if and only if $A_{2^n} = H_{2^{n-1}}$. But this cannot happen because the ramification index of p in $H_{2^{n-1}}$ is 2, while ϖ' has ramification index 1 over p and, as ϖ and ϖ' are coprime, ϖ' remains unramified in A_{2^n}.

By assumption, $H_{2^{n-1}}(\sqrt{\varpi})$ is normal over $\mathbb{Q}$, and hence also over $\mathbb{Q}(\sqrt{-4p})$ and $H_{2^{n-2}}$. Since ϖ and ϖ' are conjugates over $A_{2^{n-2}}$, they are also conjugates over $H_{2^{n-2}}$. As $H_{2^{n-1}} = H_{2^{n-2}}(\sqrt{\varpi\varpi'})$ and $\varpi\varpi' = \varpi\varpi' \cdot 1^2$, Lemma 2.2 implies that $H_{2^{n-1}}(\sqrt{\varpi})$ is degree 4 cyclic extension of $H_{2^{n-2}}$. Moreover, $H_{2^{n-1}}$ is a degree 2^{n-1} cyclic extension of $\mathbb{Q}(\sqrt{-4p})$, so Lemma 2.3 implies that $H_{2^{n-1}}(\sqrt{\varpi})$ is a degree 2^n cyclic extension of $\mathbb{Q}(\sqrt{-4p})$.

It remains to show that $H_{2^{n-1}}(\sqrt{\varpi})/\mathbb{Q}(\sqrt{-4p})$ is unramified. We will establish this by showing that each of the ramification indices of the primes 2 and p in $H_{2^{n-1}}(\sqrt{\varpi})$ is at most 2.

The prime 2 ramifies in $\mathbb{Q}(i)$, but by assumption $(1+i)$ is unramified in

A_{2^n}. As $H_{2^{n-1}}(\sqrt{\varpi}) = A_{2^n}(\sqrt{\varpi\varpi'})$ and $p \equiv 1 \bmod 4$, Lemma 2.1 ensures that $(1+i)$ is unramified in $H_{2^{n-1}}(\sqrt{\varpi})$. Hence the ramification index of 2 in $H_{2^{n-1}}(\sqrt{\varpi})$ is 2.

Now note that $[H_{2^{n-1}}(\sqrt{\varpi}) : A_{2^n}] = 2$, the ramification index of the prime ϖ' over p is 1, and ϖ' does not ramify in $A_{2^n}/A_{2^{n-1}}$. Hence the ramification index of p in $H_{2^{n-1}}(\sqrt{\varpi})$ is at most 2, and this completes the proof. $\square$

2.1.3 Explicit constructions of H_4 and H_8

Recall from (2.6) that 4 divides h if and only if the prime $\mathfrak{t}$ of $\mathbb{Q}(\sqrt{-4p})$ lying over 2 splits in H_2, which happens if and only if $(1+i)$ splits in $H_2/\mathbb{Q}(i)$. As H_2 is obtained from $\mathbb{Q}(i)$ by adjoining a square root of p, Lemma 2.1 implies that this happens if and only if $p \equiv \pm 1 \pmod{\mathfrak{m}^5}$, which, for $p \equiv 1 \pmod 4$, is true if and only if $p \equiv 1 \pmod 8$. Thus we have recovered the criterion for divisibility by 4.

From now on, assume that 4 divides h, i.e. that $p \equiv 1 \pmod 8$. We will now use Lemma 2.4 to construct the 4-Hilbert class field of $\mathbb{Q}(\sqrt{-4p})$.

A prime $p \equiv 1 \pmod 4$ splits in $\mathbb{Q}(i)$, so that there exists π in $\mathbb{Z}[i]$ such that $p = \pi\overline{\pi}$; here $\overline{\pi}$ denotes the conjugate of π over $A_1 := \mathbb{Q}$. If we write π as $a+bi$ with a and b integers, then we see that $p = a^2+b^2$. We choose π so that b is even. As $p \equiv 1 \pmod 8$, we see that b is in fact divisible by 4. Hence

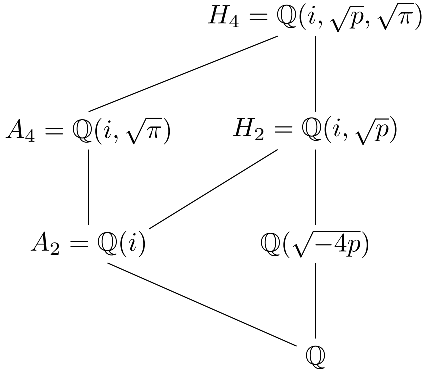
$$\pi = a + bi, \quad b \equiv 0 \bmod 4. \tag{2.7}$$

Now fix a square root of π and denote it by $\sqrt{\pi}$. Recall that $H_2 = \mathbb{Q}(i, \sqrt{p})$ is the 2-Hilbert class field of $\mathbb{Q}(\sqrt{-4p})$. We claim that the hypotheses of Lemma 2.4 for $n = 2$ are satisfied with $A_2 := \mathbb{Q}(i)$ and $\varpi = \pi$.

All of the hypotheses other than (U_2) and (N) are easy to check. Note that our choice of π ensures that $\pi \equiv \pm 1 \pmod 4$, so that (U_2) follows from Lemma 2.1. To see that (N) is satisfied, note that $H_2(\sqrt{\pi})$ is the splitting field (over $\mathbb{Q}$) of the polynomial $f_4(X) := (X^2-\pi)(X^2-\overline{\pi})$. 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 2.4 that the 4-Hilbert class field is given by

$$H_4 = H_2(\sqrt{\pi}) = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi}) \tag{2.8}$$

with π as in (2.7).



Next, we find a criterion for divisibility by 8. Recall that h is divisible by 8 if and only if $\mathfrak{t}$ splits completely in H_4, i.e. if and only if π is a square in $\mathbb{Q}_2(i)$. By Lemma 2.1, this happens if and only if $\pi \equiv \pm 1 \pmod{\mathfrak{m}^5}$. In terms of a and b from (2.7), this means that

$$8|h \Longleftrightarrow a + b \equiv \pm 1 \bmod 8.$$

We remark that Fouvry and Klüners developed similar methods in [16], 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 π by $-\pi$ if necessary, we assume that

$$\pi \equiv 1 \pmod{\mathfrak{m}^5}. \tag{2.9}$$

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

$$\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^3}. \tag{2.10}$$

In order to explicitly generate H_8 from H_4 using Lemma 2.4, we are led to the problem of finding a prime element in $A_4 = \mathbb{Q}(i, \sqrt{\pi})$ whose norm down to $\mathbb{Q}(i)$ is $\overline{\pi}$, 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 $-\overline{\pi}$. These are primes p of the form

$$p = a^2 + c^4, \quad c \text{ even}, \tag{2.11}$$

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 (2.11). Set

$$\varpi_0 = c(1 + i) + \sqrt{\pi}. \tag{2.12}$$

For $1 \le m \le 3$, set $\varpi_m = \sigma^m(\varpi)$, where σ is a generator for $\mathrm{Gal}(H_4/\mathbb{Q}(\sqrt{-4p}))$. [redacted] The restriction of σ to H_2 generates $\mathrm{Gal}(H_2/\mathbb{Q}(\sqrt{-4p}))$, so $\sigma(i) = -i$. Also, looking at the polynomial $f_4(X)$ above, we see that $\sigma(\sqrt{\pi}) = -\sqrt{\pi}$. Hence

$$\varpi_0 \cdot \varpi_2 = (c(1+i) + \sqrt{\pi})(c(1+i) - \sqrt{\pi}) = -\overline{\pi}. \tag{2.13}$$

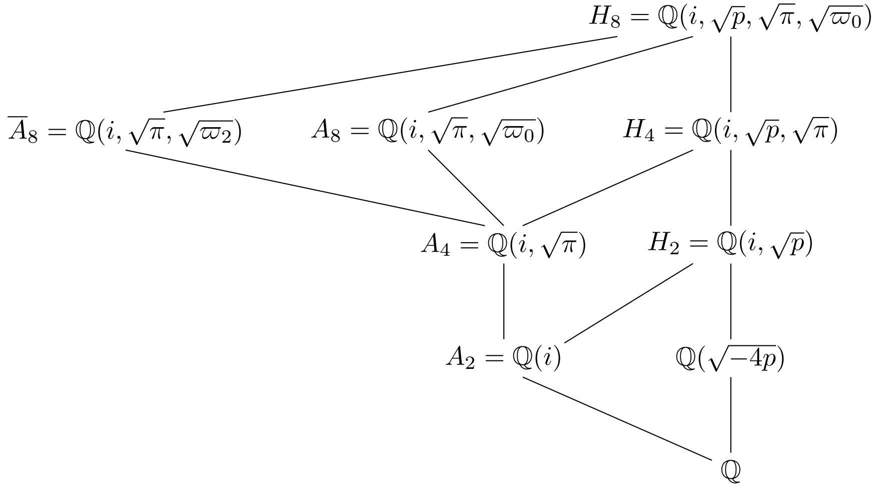
and

$$\varpi_1 \cdot \varpi_3 = (c(1-i) + \sigma(\sqrt{\pi}))(c(1-i) - \sigma(\sqrt{\pi})) = -\pi. \tag{2.14}$$

We can now prove the main result of this section.

Proposition 2.2. *Let p be a prime of the form* (2.11), *let π be as in* (2.9), *let $\sqrt{\pi}$ be as in* (2.10), *and let ϖ_0 be as in* (2.12). *Let $\sqrt{\varpi_0}$ denote a square root of ϖ_0. Then $H_4(\sqrt{\varpi_0})$ is the 8-Hilbert class field of $\mathbb{Q}(\sqrt{-4p})$.*

Proof. We again use Lemma 2.4, but this time with $n = 3$, $A_4 = \mathbb{Q}(i, \sqrt{\pi})$ and $\varpi = \varpi_0$. All of the hypotheses except for (U_2) and (N) immediately follow from the identity (2.13).



We now prove hypothesis (N). We claim that $H_4(\sqrt{\varpi_0})$ is the splitting field of the polynomial

$$f_8(X) = (X^2 - \varpi_0)(X^2 - \varpi_1)(X^2 - \varpi_2)(X^2 - \varpi_3).$$

It is easy to see that $\varpi_0\varpi_2 = -\overline{\pi}$ and $\varpi_1\varpi_3 = -\pi$ are squares in H_4. To prove (N), it now suffices to show that $\varpi_0\varpi_1$ is a square in H_4. Let

$$d = \frac{\sqrt{\pi} + \sigma(\sqrt{\pi})}{2} \quad \text{and} \quad e = \frac{\sqrt{\pi} - \sigma(\sqrt{\pi})}{2i} \in H_4.$$

Then

$$\begin{aligned}\varpi_0 \cdot \varpi_1 &= (c(1+i)+\sqrt{\pi})(c(1-i)+\sigma(\sqrt{\pi})) \\ &= 2c^2+\sqrt{\pi}\sigma(\sqrt{\pi})+c\left((1+i)\sigma(\sqrt{\pi})+(1-i)\sqrt{\pi}\right) \\ &= (c^2+2de)+(d^2+e^2)+c(2d+2e)=(c+d+e)^2,\end{aligned}$$

which completes the proof of hypothesis (N).

It remains to prove hypothesis (U_2). The assumption that $\pi \equiv 1 \pmod{\mathfrak{m}^5}$ actually means that π is a square in $\mathbb{Q}_2(i)$, i.e. that $(1+i)$ splits in A_4. Hence it remains to show that $\mathbb{Q}_2(i, \sqrt{\varpi_0})$ is unramified over $\mathbb{Q}_2(i)$, and Lemma 2.1 implies that it is enough to prove that $\varpi_0 \equiv \pm 1 \pmod{\mathfrak{m}^4}$.

Recall from (2.10) that $\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^3}$, so that $\sqrt{\pi} \equiv 1$ or $1+m^3 \pmod{\mathfrak{m}^4}$. Squaring, we find that $\pi \equiv 1$ or $1+m^5 \pmod{\mathfrak{m}^6}$, respectively. Also recall that $a+b \equiv 1 \bmod 8$, i.e., $a+c^2 \equiv 1 \pmod{\mathfrak{m}^6}$. We now split our argument into two cases, the first when $c \equiv 0 \bmod 4$ and the second when $c \equiv 2 \bmod 4$.

If $c \equiv 0 \pmod{\mathfrak{m}^4}$, then $c^2 \in \mathfrak{m}^6$, so $a-1 \in \mathfrak{m}^6$ as well. Then $\pi = a + c^2 i \equiv 1 \pmod{\mathfrak{m}^6}$, which means that $\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^4}$. Then

$$\varpi_0 = c(1+i)+\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^4}.$$

If $c \equiv 2 \pmod{\mathfrak{m}^4}$, then $c^2 \equiv -m^4 \pmod{\mathfrak{m}^6}$. In this case, we have $a-1+m^4 \in \mathfrak{m}^6$, so that $\pi = a+c^2 i \equiv 1-m^4-m^4 i \equiv 1+m^4(-1-i) \equiv 1+m^5 \pmod{\mathfrak{m}^6}$. This means that $\sqrt{\pi} \equiv 1+m^3 \pmod{\mathfrak{m}^4}$, and hence

$$\varpi_0 = \sqrt{\pi}+c(1+i) \equiv 1+m^3+m^3 \equiv \pm 1 \pmod{\mathfrak{m}^4}.$$

This finishes the proof that $\mathbb{Q}_2(i, \sqrt{\varpi_0})$ is unramified over $\mathbb{Q}_2(i)$. □

2.2 Proof of Theorem 2.1

The proof of Theorem 2.1 will proceed in much the same way as the last part of the proof of Proposition 2.2. 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 $\mathfrak{t}$ splits completely in H_8) and when it is unramified of degree 2 (i.e. when $\mathfrak{t}$ does not split completely in H_8). This is equivalent to determining when ϖ_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., $c \in \mathfrak{m}^4$. Recall from above that then $a \equiv 1 \pmod 8$ and $\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^4}$.

To check whether or not ϖ_0 is a square in $\mathbb{Q}_2(i)$, we must compute ϖ_0 modulo $\mathfrak{m}^5$. Since $c \equiv 0 \pmod 4$, we deduce that $\varpi_0 \equiv \sqrt{\pi}$ modulo $\mathfrak{m}^5$. Thus, we must determine conditions on a such that $\sqrt{\pi} \equiv \pm 1 \pmod{\mathfrak{m}^5}$, and for this, by Hensel's lemma, it is necessary to determine π modulo $\mathfrak{m}^7$. Hence, assuming $c \equiv 0 \pmod 4$,

$$\begin{aligned} 16|h \quad &\iff \quad \sqrt{\pi} \equiv \pm 1 \pmod{\mathfrak{m}^5} \\ &\iff \quad \pi \equiv 1 \pmod{\mathfrak{m}^7} \\ &\iff \quad a \equiv 1 \pmod{16}. \end{aligned}$$

This proves parts (i) and (iii) of Theorem 2.1.

We handle the second case similarly. Now $c \equiv 2 \pmod 4$, $a \equiv 5 \pmod 8$ and $\sqrt{\pi} \equiv 1 + m^3 \pmod{\mathfrak{m}^4}$. Then $\varpi_0 \equiv 2m + \sqrt{\pi}$ modulo $\mathfrak{m}^5$ and so we must determine conditions on a such that $\sqrt{\pi} \equiv \pm 1 - 2m \pmod{\mathfrak{m}^5}$. Under the current assumptions,

$$\begin{aligned} 16|h \quad &\iff \quad \sqrt{\pi} \equiv \pm 1 - 2m \pmod{\mathfrak{m}^5} \\ &\iff \quad \pi \equiv 1 + m^5 + m^6 \pmod{\mathfrak{m}^7} \\ &\iff \quad a \equiv -3 \pmod{16}. \end{aligned}$$

Note that because of the choice (2.9) 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 2.1.

2.3 Overview of the proof of Proposition 2.1

In [19], 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 [20, Chapter 21]. They use a new sieve that they developed to detect primes in relatively thin sequences [18]. This sieve has its roots in the work of Fouvry and Iwaniec [12], 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 the appropriate analogue of Proposition 2.1 is 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 2.1 involves certain alterations in the way that the sieve [18] is used. For this reason, we first briefly recall the inputs and the output of the sieve.

2.3.1 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 [18] yields an asymptotic formula for

$$S(x) = \sum_{\substack{p \le x \\ p \text{ prime}}} a_p \log p,$$

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 $d \ge 1$, let

$$A_d(x) = \sum_{\substack{n \le x \\ n \equiv 0 \bmod d}} a_n,$$

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

$$A_d(x) = g(d)A(x) + r_d(x). \tag{2.15}$$

The hypotheses which are not difficult to verify are listed in equations (2.1)-(2.8) in [19]. We briefly recall them here. We assume the bounds

$$A(x) \gg A(\sqrt{x})(\log x)^2 \tag{H1}$$

and

$$A(x) \gg x^{\frac{1}{3}} \left(\sum_{n \le x} a_n^2 \right)^{\frac{1}{2}}. \tag{H2}$$

We assume that the multiplicative function g satisfies

$$0 \le g(p^2) \le g(p) \le 1, \tag{H3}$$

$$g(p) \ll p^{-1}, \tag{H4}$$

and

$$g(p^2) \ll p^{-2}. \tag{H5}$$

We also assume that for all $y \ge 2$,

$$\sum_{p \le y} g(p) = \log\log y + c + O((\log y)^{-10}), \tag{H6}$$

where c is a constant depending only on g; this is the linear sieve assumption. Finally, we assume the bound

$$A_d(x) \ll d^{-1}\tau(d)^8 A(x) \tag{H7}$$

uniformly in $d \le x^{\frac{1}{3}}$; here τ 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 $L = (\log x)^{2^{24}}$.

Hypothesis (R). *There exists $x_r > 0$ and $D = D(x)$ in the range*

$$x^{\frac{2}{3}} < D < x \tag{2.16}$$

such that for all $x \ge x_r$, we have

$$\sum_{\substack{d \text{ cubefree} \\ d \le DL^2}} |r_d(t)| \le A(x)L^{-2} \tag{R}$$

uniformly in $t \le x$.

In our applications, D will be $x^{3/4-\varepsilon}$ for a sufficiently small ε. 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

$$\beta(n, C) = \mu(n) \sum_{c|n,\ c \le C} \mu(c). \tag{2.17}$$

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 δ, Δ, and P satisfying*

$$2 \le \delta \le \Delta,$$

$$2 \le P \le \Delta^{1/2^{35} \log\log x},$$

and such that for every C with

$$1 \le C \le xD^{-1},$$

and for every N with

$$\Delta^{-1}\sqrt{D} < N < \delta^{-1}\sqrt{x},$$

we have

$$\sum_m \left| \sum_{\substack{N \le n \le 2N \\ mn \le x \\ (n, m\Pi)=1}} \beta(n, C) a_{mn} \right| \le A(x)(\log x)^{-2^{26}}, \tag{B}$$

where

$$\Pi = \prod_{p \le P} p. \tag{2.18}$$

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 [18] is

Theorem 2.2. *Assuming hypotheses (H1)-(H7), (R), and (B), we have*

$$S(x) = HA(x)\left(1 + O\left(\frac{\log \delta}{\log \Delta}\right)\right),$$

where H is the positive constant given by the convergent product

$$H = \prod_{p} (1 - g(p)) \left(1 - \frac{1}{p}\right)^{-1}$$

and the constant implied in the O-symbol depends on the function g and the constants implicit in (H1), (H2), and (H7).

2.3.2 Preparing the sieve for Proposition 2.1

For our application, we will denote by v' the analogue of a quantity v from the proof of Friedlander and Iwaniec in [19]. 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

$$a_0 \bmod q_1 \qquad c_0 \bmod q_2$$

is *admissible* if for every pair of congruence classes

$$a_1 \bmod q \qquad c_1 \bmod q$$

such that $a_1 \equiv a_0 \bmod q_1$ and $c_1 \equiv c_0 \bmod q_2$, the congruence class $a_1^2 + c_1^4 \bmod q$ 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 $a_0 \bmod 16$ and $c_0 \bmod 4$ is admissible.

Example. Suppose that $a_0 = c_0 = 1$. Then the pair of congruence classes $a_0 \bmod 3$ and $c_0 \bmod 2$ is *not* admissible. Indeed, $1 \equiv a_0 \equiv c_0 \bmod 6$ but $2 \equiv 1^2 + 1^4 \bmod 6$ is not invertible modulo 6. This does not mean, however, that there are no primes of the form $a^2 + c^4$ with $a \equiv 1 \bmod 3$ and $c \equiv 1 \bmod 2$; 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 $a_0 \bmod q_1$ and $c_0 \bmod q_2$ is an admissible pair of congruence classes. We define

$$a'_n := \sum_{\substack{a,\ b\ \in\ \mathbb{Z} \\ a^2+b^2=n \\ a \equiv a_0 \bmod q_1}} \mathfrak{Z}'(b), \tag{2.19}$$

where

$$\mathfrak{Z}'(b) := \sum_{\substack{c \in \mathbb{Z} \\ c^2=b \\ c \equiv c_0 \bmod q_2}} 1. \tag{2.20}$$

Let g be the multiplicative function supported on cubefree integers defined in [19, Equation 3.16, p.961] as follows: let χ_4 denote the character of conductor 4; for $p \geq 3$ set

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

and

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

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 δ a large power of $\log x$ and Δ a small power of x, the asymptotic formula given by the sieve (see Theorem 2.2) is

$$S'(x) := \sum_{\substack{p \leq x \\ p \text{ prime}}} a'_p \log p = c(q_1, q_2)\frac{16\kappa}{\pi}x^{3/4}\left(1 + O\left(\frac{\log\log x}{\log x}\right)\right) \tag{2.21}$$

where

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

and κ is the integral given in the statement of Proposition 2.1. Note that the sieve applied to the original sequence (a_n) from [19], with

$$a_n = \sum_{\substack{a,\ b\ \in\ \mathbb{Z} \\ a^2+b^2=n}} \mathfrak{Z}(b), \tag{2.22}$$

where

$$\mathfrak{Z}(b) = \sum_{\substack{c \in \mathbb{Z} \\ c^2 = b}} 1, \tag{2.23}$$

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 [19, 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 $a \equiv a_0 \bmod q_1$ and $c \equiv c_0 \bmod q_2$ 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 $c_0 \in \{0, 2\}$.

2.4 Proof of condition (R)

Here we closely follow and refer to the arguments laid out in [19, Section 3, p.955-962]. Define

$$A'_d(x) := \sum_{\substack{n \le x \\ n \equiv 0 \bmod d}} a'_n$$

and

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

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

$$r'_d(x) := A'_d(x) - g'(d)A'(x) \tag{2.24}$$

are small on average. To do this, we will prove an analogue of [19, Lemma 3.1, p.956], with $M_d(x)$ (representing the *main term* and defined in [19, p.955]) replaced by

$$M'_d(x) = \frac{1}{dq_1} \sum\sum_{0 < a^2 + b^2 \le x} \mathfrak{Z}'(b)\rho(b; d) \qquad \text{if } (d, q) = 1$$

and $M'_d(x) = 0$ otherwise; here $\rho(b; d)$ is defined as in [19, p.955], i.e. it is the number of solutions α mod d to

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

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 [19, Lemma 3.1, p.956].

Lemma 2.5. *For any $D \geq 1$, any $\varepsilon > 0$, and any $x \geq 2$, we have*

$$\sum_{d \leq D} |A'_d(x) - M'_d(x)| \ll D^{\frac{1}{4}} x^{\frac{9}{16}+\varepsilon},$$

where the implied constant depends only on ε.

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 [19, (3.16), p.961] by

$$\begin{cases} h(p)p = 1 + 2(1 + \chi_4(p)) \\ h(p^2)p^2 = p + 2(1 + \chi_4(p)), \end{cases} \tag{2.25}$$

and define a multiplicative function h' by setting

$$h'(n) = \begin{cases} h(n) & \text{if } (n, q) = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{2.26}$$

Then following the same argument as in the proof of [19, Lemma 3.4, p.961], we get

Lemma 2.6. *For d cubefree we have*

$$M'_d(x) = g'(d) \frac{4\kappa x^{\frac{3}{4}}}{q_1 q_2} + O\left(h'(d) x^{\frac{1}{2}}\right),$$

where κ is the integral given in the statement of Proposition 2.1 and the implied constant is absolute. □

Combining Lemmas 2.5 and 2.6, we get, as in [19, Proposition 3.5, p.362],

Proposition 2.3. *Let*

$$a_0 \bmod q_1 \qquad c_0 \bmod q_2$$

be an admissible pair of congruence classes, let a'_n be defined as in (2.19), and let $r'_d(x)$ be defined as in (2.24). 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*

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

uniformly for $t \leq x$*.*

Choosing $D = x^{\frac{3}{4}-8\varepsilon}$, we obtain hypothesis (R).

It remains to prove Lemma 2.5. 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

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

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 $y = D^{\frac{1}{4}} x^{\frac{13}{16}}$ and the implied constants depend only on j (see [19, p.958]). Since a'_n is supported on integers of the form $a^2 + c^4$, we trivially have

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

where the implied constant depends only on ε. With the above choice of y, it remains to prove Lemma 2.5 with $A'_d(x)$ replaced by $A'_d(f)$. Similarly as on [19, p.958], we write

$$A'_d(f) = \sum_b \mathfrak{Z}'(b) \sum_{\substack{\alpha \bmod d \\ \alpha^2+b^2 \equiv 0 \bmod d}} \sum_{\substack{a \equiv \alpha \bmod d \\ a \equiv a_0 \bmod q_1}} f(a^2 + b^2). \tag{2.27}$$

Since $(d, q) = 1$, so also $(d, q_1) = 1$, and the two conditions $a \equiv \alpha \bmod d$ and $a \equiv a_0 \bmod q_1$ can be combined into one condition $a \equiv \alpha' \bmod dq_1$. In fact, fixing an integer $\bar{d}$ that is an inverse of d modulo q_1 and an integer $\bar{q}_1$ that is an inverse of q_1 modulo d, we can define α' as

$$\alpha' = \alpha q_1 \bar{q}_1 + a_0 d \bar{d}.$$

We apply Poisson's summation formula to the sum over a to obtain

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

Here and henceforth, we use the standard notation

$$e(t) := e^{2\pi i t}.$$

Substituting this into (2.27) we get

$$A'_d(f) = \frac{2}{dq_1} \sum_b \mathfrak{z}'(b) \sum_k \rho'(k, b; d) I(k, b; dq_1) dt,$$

where

$$\rho'(k, b; d) = \sum_{\substack{\alpha \bmod d \\ \alpha^2 + b^2 \equiv 0 \bmod d}} e\left(\frac{\alpha' k}{dq_1}\right),$$

and where

$$I(k, b; dq_1) = \int_0^\infty f(t^2 + b^2) \cos(2\pi t k / dq_1) dt$$

is defined exactly the same as on [19, p.959]. We define $M'_d(f)$ to be the main term in this expansion, i.e. the term corresponding to $k = 0$,

$$M'_d(f) = \frac{2}{dq_1} \sum_b \mathfrak{z}'(b) \rho(b; d) I(0, b; dq_1).$$

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

$$\sum_{\substack{d \le D \\ (d,q)=1}} |M'_d(f) - M'_d(x)| \ll y x^{-\frac{1}{4}} (\log x)^2 \ll D^{\frac{1}{4}} x^{\frac{9}{16} + \varepsilon},$$

where the implied constants depend only on ε. It remains to prove Lemma 2.5 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 [19, p.959-960], we see that it suffices to show an analogue of [19, Lemma 3.3, p.957] for $\rho'(k, l; d)$.

Lemma 2.7. *For any D, K, and $L \ge 1$, for any complex numbers $\xi(k, l)$, and for any $\varepsilon > 0$, we have the inequality*

$$\sum_{d \le D} \left| \sum_{\substack{0 < k \le K \\ 0 < l \le L}} \sum \xi(k, l) \rho'(k, l; d) \right| \ll (D + \sqrt{DKL})(DKL)^{\varepsilon} \|\xi\|$$

where

$$\|\xi\|^2 = \sum_{\substack{0 < k \le K \\ 0 < l \le L}} \sum |\xi(k, l)|^2,$$

and the implied constant depends only on ε.

Recall the following inequality from [19, (3.6), p.957]: for any complex numbers α_n and any $D, N \geq 1$, we have

$$\sum_{d \leq D} \sum_{\substack{\nu \bmod d \\ \nu^2+1 \equiv 0 \bmod d}} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu n}{d}\right) \right| \ll D^{\frac{1}{2}} (D+N)^{\frac{1}{2}} \|\alpha\|, \tag{2.28}$$

where

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

and the implied constant is absolute. Lemma 2.7 can be proved in the same way as [19, Lemma 3.3, p.957] given the following analogue of inequality (2.28).

Lemma 2.8. *Let $D, N \geq 1$ and let α_n be any complex numbers. For integers d such that $(d, q_1) = 1$, let ν' be an integer in the unique residue class modulo dq_1 that reduces to ν 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*

$$\sum_{\substack{d \leq D \\ (d,q_1)=1}} \sum_{\substack{\nu \bmod d \\ \nu^2+1 \equiv 0 \bmod d}} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu' n}{dq_1}\right) \right| \leq C D^{\frac{1}{2}} (D+N)^{\frac{1}{2}} \|\alpha\|. \tag{2.29}$$

Inequality (2.28) is a consequence of a large sieve inequality applied to the rationals $\nu/d \bmod 1$ with ν ranging over the roots of $\nu^2 + 1 \equiv 0 \bmod d$ for d in a range around D. The large sieve inequality can be applied because these rationals ν/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 [12]. In our analogue, however, it is not clear that ν'/dq_1 are also well-spaced modulo 1 for d in a similar range around D. Nonetheless, we can reduce Lemma 2.8 to inequality (2.28) as follows.

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

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

where

$$\alpha_{m,n_0} = \alpha_{mq_1+n_0}.$$

Since $e\left(\nu' n_0/dq_1\right)$ does not depends on m, the sum on the left-hand-side of (2.29) is

$$\leq \sum_{n_0 \bmod q_1} \sum_{\substack{d \leq D \\ (d,q_1)=1}} \sum_{\substack{\nu \bmod d \\ \nu^2+1 \equiv 0 \bmod d}} \left| \sum_{m \leq (N-n_0)/q_1} \alpha_{m,n_0} e\left(\frac{\nu' m}{d}\right) \right|.$$

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

$$\sum_m |\alpha_{m,n_0}|^2 \le \sum_n |\alpha_n|^2,$$

so that by (2.28) we get

$$\sum_{\substack{d\le D\\(d,q_1)=1}} \sum_{\substack{\nu \bmod d\\ \nu^2+1\equiv 0 \bmod d}} \left| \sum_{n\le N} \alpha_n e\left(\frac{\nu' n}{dq_1}\right)\right| \ll q_1 D^{1/2}(D+N/q_1)^{1/2}\|\alpha\|.$$

This finishes the proof of (2.8) and thus also the proof of condition (R).

2.5 Proof of condition (B)

Many of the upper bound estimates carried out in sections 4 and 5 of [19] require no changes since $0 \le a'_n \le a_n$ (compare (2.19) and (2.22)). 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 [19, 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 [19, Proposition 4.1, p.963]:

Proposition 2.4. *Let* $c_0 \in \{0,2\}$, *let* $q_2 = 4$, *and let*

$$a_0 \bmod q_1 \qquad c_0 \bmod q_2$$

be an admissible pair of congruence classes. Define $\beta(n,C)$ *as in* (2.17), Π *as in* (2.18), *and* a'_n *as in* (2.19). *Let* $x \ge 3$, $\eta > 0$, *and* $A > 0$. *Let* P *be in the range*

$$(\log\log x)^2 \le \log P \le (\log x)(\log\log x)^{-2}. \tag{2.30}$$

Let

$$B = 4A + 2^{20}. \tag{2.31}$$

Then there exists $x_0 = x_0(\eta, A)$ *such that for all* $x \ge x_0$, *for all* N *with*

$$x^{\frac{1}{4}+\eta} < N < x^{\frac{1}{2}}(\log x)^{-B}, \tag{2.32}$$

and for all C *with*

$$1 \le C \le N^{1-\eta}, \tag{2.33}$$

we have

$$\sum_m \left| \sum_{\substack{N\le n\le 2N\\ mn\le x\\ (n,m\Pi)=1}} \beta(n,C) a_{mn} \right| \le A'(x)(\log x)^{5-A}. \tag{2.34}$$

2.5.1 From Propositions 2.3 and 2.4 to Proposition 2.1

Before proving Proposition 2.4, we deduce Proposition 2.1 from Propositions 2.3 and 2.4. 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

$$a_0 \bmod q_1 \qquad c_0 \bmod q_2$$

is an admissible pair of congruences. We apply the asymptotic sieve for primes described in Section 2.3.1 to the sequence (a'_n) defined in (2.19). Hypotheses (H1)-(H7) for (a'_n) are verified in the same way as hypotheses (H1)-(H7) for the sequence (a_n) defined in (2.22) (see comment at the end of Section 2.3.2).

Proposition 2.3 implies that (a'_n) satisfies hypothesis (R) for $\varepsilon = 1/8000$,

$$D = x^{\frac{3}{4} - \frac{1}{1000}}, \tag{2.35}$$

which is indeed in the range (2.16), and $x_r = x_r(\varepsilon)$ large enough.

Applying Proposition 2.4 with the same D as in (2.35), with P any number in the range (2.30), with $A = 5+2^{26}$, and with $\eta = \frac{1}{100}$ establishes hypothesis (B) for the sequence (a'_n) with $\delta = (\log x)^B$, $\Delta = x^\eta$, and $x_b = \max\{x_r, x_0(\eta, A)\}$.

We then obtain the asymptotic formula (2.21) with

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

which proves (2.3).

2.5.2 Proof of Proposition 2.4

Suppose that we are in the setting of Proposition 2.4. Now take $A' = 2A + 2^{20}$ (see [19, p.1018]) and define

$$\vartheta := (\log x)^{-A}$$

and

$$\theta := (\log x)^{-A'} \tag{2.36}$$

as on [19, p.965]. We split the sum (2.34) 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 [19, (4.14), p.965]). It then suffices to show Proposition 2.4 with $\beta(n, C)$ replaced by a smoothed version

$$\beta(n) = \beta(n, C) = p(n)\mu(n) \sum_{c|n,\ c \le C} \mu(c) \tag{2.37}$$

and the bound $\le A'(x)(\log x)^{5-A}$ replaced by $\le C\vartheta\theta A'(x)(\log x)^5$ (see [19, (4.17), p.965]). Moreover, one can split the sum over m in (2.34) into dyadic segments $M \le m \le 2M$ with M satisfying

$$\vartheta x \le MN \le x. \tag{2.38}$$

We remark that (2.32) now implies that $N \le \vartheta\theta(MN)^{\frac{1}{2}}$. 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

$$\tau(n) \le \tau := (\log x)^{A+2^{20}}. \tag{2.39}$$

(see [19, p.963-966, 1018]). For convenience of notation, we also restrict the support of $\beta(n, C)$ to n satisfying

$$(n, \Pi) = 1, \tag{2.40}$$

where Π is defined in (2.18). Finally, let $\alpha(m)$ be any complex numbers supported on $M < m \le 2M$ with $|\alpha(m)| \le 1$, and define

$$\mathcal{B}'^*(M, N) := \sum\sum_{(m,n)=1} \alpha(m)\beta(n)a'_{mn}, \tag{2.41}$$

where $\beta(n) = \beta(n, C)$ is defined as in (2.37) (see [19, (4.20), p.966]). To establish condition (B) it then suffices to prove

Lemma 2.9. *Let $\eta > 0$ and $A > 0$ and take B as in* (2.31)*. Then there exists $x_0 = x_0(\eta, A) > 0$ such that for all $x \ge x_0$, for all M and N satisfying* (2.32) *and* (2.38)*, and for all C satisfying* (2.33) *we have*

$$|\mathcal{B}'^*(M, N)| \le \vartheta\theta(MN)^{\frac{3}{4}}(\log MN)^5. \tag{B'}$$

2.5.3 Proof of Lemma 2.9

In [19, 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 a'_n are defined in (2.19), equation [19, (5.2), p.967] now becomes (for $(m, n) = 1$)

$$a'_{mn} = \sum_{\substack{|w|^2=m \\ \mathrm{Im}\overline{w}z \equiv a_0 \bmod q_1}} \sum_{|z|^2=n} \mathfrak{Z}'(\mathrm{Re}\overline{w}z),$$

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

$$z \equiv 1 \bmod 2(1+i).$$

Recall from (2.20) that the congruence condition $c \equiv c_0 \bmod q_2$ is incorporated into the definition of $\mathfrak{Z}'$. We now define $\alpha_w := \alpha(|w|^2)$ and $\beta_z := \beta(|z|^2)$ as on [19, p.967], so that (2.41) becomes

$$\mathcal{B}'^*(M,N) = \sum_{\substack{(w\overline{w}, z\overline{z})=1 \\ \mathrm{Im}\overline{w}z \equiv a_0 \bmod q_1}}\sum \alpha_w \beta_z \mathfrak{Z}'(\mathrm{Re}\overline{w}z). \tag{2.42}$$

Similarly as in [19, (5.7), p.967], we split the sum $\mathcal{B}'^*(M,N)$ into $O(q_1^4)$ sums by restricting the support of α_w to w in a fixed residue class modulo q_1 and β_z to z in a fixed residue class z_0 modulo $64q_1$, such that $z_0 \equiv 1 \bmod 2(1+i)$. Now the residue class of $\mathrm{Im}\overline{w}z$ modulo q_1 is fixed, and so we can eliminate the condition $\mathrm{Im}\overline{w}z \equiv a_0 \bmod q_1$.

We further modify the support of β_z as in equation [19, (5.13), p.969]. Let $r(\alpha)$ be a smooth periodic function of period 2π supported on $\varphi < \alpha \leq \varphi + 2\pi\theta$ (where θ is as defined in (2.36)) for some $-\pi < \varphi < \pi$ such that $r^{(j)} \ll \theta^{-j}$ for $j = 0, 1, 2$, and let

$$\beta_z = r(\alpha)p(n)\mu(n) \sum_{c|n,\ c \leq C} \mu(c), \tag{2.43}$$

where $\alpha = \arg z$ and $n = |z|^2$. Recall that by (2.39) and (2.40), $\beta_z = 0$ if either $\tau(|z|^2) > \tau$ or if $|z|^2$ is not coprime with Π. We remove the condition $(w\overline{w}, z\overline{z}) = 1$ from (2.42) at an acceptable cost as in [19, (5.10), p.968] to get

$$\mathcal{B}'(M,N) = \mathcal{B}'^*(M,N) + O\left(\left(M^{\frac{1}{4}}N^{\frac{5}{4}} + P^{-1}M^{\frac{3}{4}}N^{\frac{3}{4}}\right)(\log N)^3\right)$$

where

$$\mathcal{B}'(M,N) := \sum_{\mathrm{Im}\overline{w}z \equiv a_0 \bmod q_1}\sum \alpha_w \beta_z \mathfrak{Z}'(\mathrm{Re}\overline{w}z). \tag{2.44}$$

We then apply Cauchy-Schwarz as in [19, (5.17), p.970] and introduce a smooth radial majorant f supported on the annulus $\frac{1}{2}\sqrt{M} \leq |w| \leq 2\sqrt{M}$ (see [19, p.970]) to get

$$\mathcal{B}'(M,N) \ll M^{\frac{1}{2}}\mathcal{D}'(M,N)^{\frac{1}{2}},$$

where

$$\mathcal{D}'(M,N) := \sum_w f(w)\left|\sum_z \beta_z \mathfrak{Z}'(\mathrm{Re}\overline{w}z)\right|^2.$$

This eliminates the dependence on α_w, so that the sum over w above is free. After inserting a coprimality condition, we arrive at the sum

$$\mathcal{D}'^*(M,N) := \sum_{(z_1,z_2)=1}\sum \beta_{z_1}\overline{\beta}_{z_2}\mathcal{C}'(z_1,z_2) \tag{2.45}$$

where

$$\mathcal{C}'(z_1, z_2) := \sum_w f(w)\mathfrak{Z}'(\mathrm{Re}\overline{w}z_1)\mathfrak{Z}'(\mathrm{Re}\overline{w}z_2)$$

(see [19, (5.26), p.972] and [19, (5.27), p.972]). The coprimality condition was inserted at the cost

$$\mathcal{D}'^*(M,N) = \mathcal{D}'(M,N) + O\left(\tau^2(M^{\frac{3}{4}}N^{\frac{3}{4}} + P^{-1}M^{\frac{1}{2}}N^{\frac{3}{2}})(\log MN)^{516}\right)$$

(see [19, (5.22), p.972]). Recall that the congruence condition $c \equiv c_0 \bmod q_2$ is hidden in the definition of $\mathfrak{Z}'$, while the congruence condition $a \equiv a_0 \bmod q_1$ has been removed by restricting the support of β_z. To prove Lemma 2.9, we now have left to prove

Lemma 2.10. *Let $\eta > 0$ and $A > 0$, and take B as in* (2.31). *Then there exists $x_0 = x_0(\eta, A)$ such that for all $x \geq x_0$, for all M and N satisfying* (2.32) *and* (2.38), *and for all C satisfying* (2.33), *we have*

$$|\mathcal{D}'^*(M,N)| \leq C\vartheta^2\theta^4 M^{\frac{1}{2}}N^{\frac{3}{2}}(\log MN)^{10}. \tag{B”}$$

Note the extra factor of θ coming from the restriction of support of β to a sector of angle θ.

2.5.4 Proof of Lemma 2.10

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

$$\Delta = \Delta(z_1, z_2) = \mathrm{Im}(\overline{z}_1 z_2),$$

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 Δ. 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 [19].

The Fourier analysis carried out on [19, p.974] depends on the greatest common divisor of Δ and q_2. Using the Poisson summation formula similarly as on [19, p.974], equation (2.45) can now be written as

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

where

$$\begin{aligned} \mathcal{C}'(z_1, z_2) \quad = \quad & (q_2/\delta)^{-2}|z_1 z_2|^{-1/2} \\ & \cdot \textstyle\sum_{h_1}\sum_{h_2} F\left(\frac{h_1}{|\Delta z_2|^{1/2}q_2/\delta}, \frac{h_2}{|\Delta z_1|^{1/2}q_2/\delta}\right) G'(h_1, h_2), \end{aligned} \tag{2.46}$$

the Fourier integral

$$F(u_1, u_2) = \int\int f\left(\frac{z_2}{|z_2|}t_1^2 - \frac{z_1}{|z_1|}t_2^2\right) e(u_1t_1 + u_2t_2)dt_1dt_2$$

is the same as the one defined in [19, (6.8), p.974] and

$$G'(h_1, h_2) = \frac{1}{|\Delta|} \sum_{\substack{\gamma_1,\gamma_2 \bmod |\Delta| \\ \gamma_1^2 z_2 \equiv \gamma_2^2 z_1 \bmod |\Delta| \\ \gamma_1 \equiv \gamma_2 \equiv c_0 \bmod \delta}} \sum e\left(\frac{\gamma_1' h_1 + \gamma_2' h_2}{|\Delta| q_2/\delta}\right)$$

is an arithmetic sum similar to $G(h_1, h_2)$ defined in [19, (6.10), p.974], but now incorporating the congruence condition $c \equiv c_0 \bmod q_2$; here γ_i' is the solution (modulo $\frac{|\Delta| q_2}{\delta}$) to the system of congruences

$$\begin{cases} \gamma_i' \equiv \gamma_i \bmod |\Delta| \\ \gamma_i' \equiv c_0 \bmod q_2. \end{cases}$$

Such a solution is guaranteed to exist because $\gamma_1 \equiv \gamma_2 \equiv c_0 \bmod \delta$. Note that similarly as in [19], 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 $\mathcal{C}'(z_1, z_2)$ comes, as usual, from the terms with $h_1 = h_2 = 0$ in equation (2.46). Similarly as in the proof of condition (R) above, we don't need to make any changes in the treatment of the Fourier integral; [19, Lemma 7.1, p.976] and [19, Lemma 7.2, p.977] are still valid, with the implied constants now depending on q_2 as well. We recall that [19, Lemma 7.2, p.977] states that for z_1 and z_2 in the support of β_z we have

$$F_0(z_1, z_2) := F(0, 0) = 2\hat{f}(0) \log 2|z_1 z_2/\Delta| + O(\Delta^2 M^{\frac{1}{2}} N^{-2} \log N). \quad (2.47)$$

We now have to give an upper bound for $G'(h_1, h_2)$ similar to the bound given in [19, 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 [19, Lemma 8.4, p.980]. This is where we now specialize to the case

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

Recall that we restricted the support of β_z to z in a fixed congruence class modulo $64q_1$. Hence $z_1 \equiv z_2 \bmod 64$, so that $\Delta = \mathrm{Im}(\overline{z}_1 z_2) \equiv 0 \bmod 64$. This significantly simplifies our arguments since now $\delta = (4, |\Delta|) = 4$.

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

$$G'(h_1,h_2) = \frac{1}{|\Delta|} \sum\sum_{\substack{\gamma_1,\gamma_2 \bmod |\Delta| \\ \gamma_1^2 z_2 \equiv \gamma_2^2 z_1 \bmod |\Delta| \\ \gamma_1\equiv\gamma_2\equiv c_0 \bmod 4}} e\left(\frac{\gamma_1 h_1+\gamma_2 h_2}{|\Delta|}\right).$$

We first prove a lemma analogous to [19, Lemma 8.1, p.978].

Lemma 2.11. *Fix $\theta \in \{2,4\}$ and let*

$$G''(h_1,h_2;\theta) = \frac{1}{|\Delta|} \sum\sum_{\substack{\gamma_1,\gamma_2 \bmod |\Delta| \\ \gamma_1^2 z_2 \equiv \gamma_2^2 z_1 \bmod |\Delta| \\ \gamma_1\equiv\gamma_2\equiv 0 \bmod \theta}} e\left(\frac{\gamma_1 h_1+\gamma_2 h_2}{|\Delta|}\right).$$

Then

$$|G''(h_1,h_2;\theta)| \le 16\tau_3(\Delta)|\Delta|^{-1}(z_1h_1^2 - z_2h_2^2, \Delta). \tag{2.48}$$

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

$$G''(h_1,h_2;\theta) = \frac{1}{|\Delta|} \sum\sum_{\substack{\omega_1,\omega_2 \bmod |\Delta|/\theta \\ \omega_1^2 z_2 \equiv \omega_2^2 z_1 \bmod |\Delta|/\theta^2}} e\left(\frac{\omega_1 h_1+\omega_2 h_2}{|\Delta|/\theta}\right).$$

Proceeding in a similar fashion as on [19, p.977-978], we write

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

with Δ_1 squarefree. The condition $\omega_1^2 z_2 \equiv \omega_2^2 z_1 \bmod |\Delta|/\theta^2$ implies that $(\omega_1^2, \Delta/\theta^2) = (\omega_2^2, \Delta/\theta^2)$, so we can write

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

with d_1 squarefree. Then $d_1|\Delta_1$, $d_2|\Delta_2$, $(d_1, \Delta_2/d_2)=1$, and we can make a change of variables $\omega_i = d_1d_2\eta_i$, there η_i runs over the residue classes modulo $|\Delta|/\theta d_1 d_2$ and coprime with $|\Delta|/\theta^2 d_1 d_2^2$. Setting $b_1=\Delta_1/d_1$ and $b_2=\Delta_2/d_2$, the analogue of the equation on top of [19, p.978] becomes

$$G''(h_1,h_2;\theta) = \frac{1}{|\Delta|} \sum\sum_{\substack{b_1d_1=|\Delta_1| \\ b_2d_2=\Delta_2 \\ (d_1,b_2)=1}} \sum\sum_{\substack{\eta_1,\eta_2 \bmod \theta b_1 b_2^2 d_2 \\ (\eta_1\eta_2, b_1b_2)=1 \\ \eta_1^2 z_2 \equiv \eta_2^2 z_1 \bmod b_1 b_2^2}} e((\eta_1h_1+\eta_2h_2)/\theta b_1 b_2^2 d_2)$$

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

$$\frac{1}{|\Delta|} \sum_{\substack{b_1d_1=|\Delta_1| \\ (d_1,b_2)=1}} \sum_{\substack{b_2d_2=\Delta_2 \\ \theta d_2|(h_1,h_2)}} \theta^2 d_2^2 \sum\sum_{\substack{\eta_1,\eta_2 \bmod b_1 b_2^2 \\ (\eta_1\eta_2, b_1b_2)=1 \\ \eta_1^2 z_2 \equiv \eta_2^2 z_1 \bmod b_1 b_2^2}} e((\eta_1h_1+\eta_2h_2)/\theta b_1 b_2^2 d_2).$$

Performing the change of variables $\eta_2 = \omega\eta_1$, the analogue of equation [19, (8.3), p.978] becomes

$$\frac{1}{|\Delta|}\sum_{\substack{b_1d_1=|\Delta_1|\\(d_1,b_2)=1}}\sum_{\substack{b_2d_2=\Delta_2\\ \theta d_2|(h_1,h_2)}}\theta^2 d_2^2\sum_{\omega\equiv z_2/z_1 \bmod b_1b_2^2} R((h_1+\omega h_2)(\theta d_2)^{-1}; b_1b_2^2),$$

where $R(h;b)$ is the classical Ramanujan sum defined on [19, p.978]. Now the same argument as on [19, p.978] yields the desired upper bound (2.48).□

We now turn our attention back to $G'(h_1,h_2)$. In case $c_0 = 0$, we're in the case of Lemma 2.11 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 $\Delta \equiv 0 \bmod 16$. 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 [19] now suffice to show that the main term in the Fourier expansion indeed comes from $h_1 = h_2 = 0$. Specifically, if we define

$$\mathcal{D}'_0(M,N) := \sum\sum_{(z_1,z_2)=1}\beta_{z_1}\overline{\beta}_{z_2}\mathcal{C}'_0(z_1,z_2),$$

where

$$\mathcal{C}'_0(z_1,z_2) = |z_1z_2|^{-1/2}F_0(z_1,z_2)G'_0(z_1,z_2), \tag{2.49}$$

then the reader may easily check that the above estimates yield the following analogue of [19, (9.10), p.983].

Lemma 2.12. *Let $\eta > 0$ and $A > 0$, and take B as in* (2.31)*. Then there exists $x_0 = x_0(\eta, A)$ such that for all $x \geq x_0$, for all M and N satisfying* (2.32) *and* (2.38)*, and for all C satisfying* (2.33)*, we have*

$$|\mathcal{D}'^*(M,N) - \mathcal{D}'_0(M,N)| \leq \vartheta^{-1}\tau^2 N^2(\log N)^{\eta^{-1/\eta}},$$

where τ is defined in (2.39)*.*

It now remains to estimate $\mathcal{D}'_0(M,N)$. We turn to obtaining an exact formula for $G'_0(z_1,z_2)$. Recall, from top of [19, p.979], that

$$G_0(z_1,z_2) := \frac{1}{|\Delta|}\sum\sum_{\substack{\gamma_1,\gamma_2 \bmod |\Delta|\\ \gamma_1^2 z_2\equiv\gamma_2^2 z_1 \bmod |\Delta|}} 1 = N(z_2/z_1;|\Delta|)/|\Delta|,$$

where $N(a;r)$ denotes the number of solutions (γ_1, γ_2) modulo r to

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

Similarly,

$$G_0'(z_1, z_2) = N'(z_2/z_1; |\Delta|)/|\Delta|,$$

where $N'(a;r)$ is the number of solutions (γ_1, γ_2) modulo r to the congruences

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

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

2.5.5 Computation of $N'(a;r)/r$

Case $c_0 = 0$

First let us compute $N'(a;r)/r$ when $c_0 = 0$. Since $\gamma_1 \equiv \gamma_2 \equiv 0 \bmod 4$, we can make a change of variables $\gamma_1 = 4\omega_1$ and $\gamma_2 = 4\omega_2$, where now ω_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 [19, (8.16), p.980]. If $16 \cdot 2^\nu$ with $\nu \geq 1$ is the exact power of 2 dividing Δ, we get

$$G_0'(z_1, z_2) = \nu \sum_{\substack{16d|\Delta \\ d \text{ odd}}} \frac{\varphi(d)}{d} \left(\frac{z_2/z_1}{d}\right).$$

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

$$G_0'(z_1, z_2) = 2 \sum_{64d|\Delta} \frac{\varphi(d)}{d} \left(\frac{z_2/z_1}{d}\right), \tag{2.50}$$

by the same reasoning as in [19, Lemma 8.4, p.980].

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 (ω_1, ω_2) modulo $r/4$ to the system of congruences

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

When $16|r$, we must subtract from $4N(a;r/4)$ those solutions with $\omega_1 \equiv \omega_2 \equiv 0 \bmod 2$. 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 Δ, we get

$$G_0'(z_1,z_2) = 2\sum_{16d|\Delta} \frac{\varphi(d)}{d}\left(\frac{z_2/z_1}{d}\right) - 2\sum_{64d|\Delta} \frac{\varphi(d)}{d}\left(\frac{z_2/z_1}{d}\right), \tag{2.51}$$

which is the analogue of (2.50).

2.5.6 End of proof of of Lemma 2.10

We now turn back to estimating $\mathcal{D}_0'(M,N)$. As in [19, (10.4), p.985], we can use (2.47) to write

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

where

$$T'(\beta) := \sum\sum_{(z_1,z_2)=1} \beta_{z_1}\overline{\beta}_{z_2} G_0'(z_1,z_2)\log 2|z_1z_2/\Delta|$$

and

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

Similarly as in [19, Lemma 10.1, p.985], we can bound $Y'(\beta)$ by

$$Y'(\beta) \ll \theta^4 N^2 (\log N)^{2^{19}},$$

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 [19, (10.13), p.986]. If we define

$$T'(\beta,\xi) := 2\sum_d \frac{\varphi(d)}{d} \sum\sum_{\substack{(z_1,z_2)=1\\ \Delta(z_1,z_2)\equiv 0 \bmod \xi d}} \beta_{z_1}\overline{\beta}_{z_2}\left(\frac{z_2/z_1}{d}\right)\log 2|z_1z_2/\Delta|,$$

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 2.10 now follows from this analogue of [19, Proposition 10.2, p.986]:

Lemma 2.13. *Fix $\xi \in \{16, 64\}$. Let $\eta > 0$, $A > 0$, and $\sigma > 0$, and take B as in* (2.31)*. 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* (2.32)*, and for all C satisfying* (2.33)*, 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 (2.30)*.*

We recall that N and P appear as parameters restricting the support of β_z; see (2.43).

2.5.7 Proof of Lemma 2.13: oscillations of characters and symbols

Although complicated, the proof of [19, Proposition 10.2] generalizes directly to the proof of Lemma 2.13. One can check in [19, Sections 15-17] that the same arguments are valid when $\xi = 16$ or 64 instead of $\xi = 4$. For instance, on [19, p. 1005] and [19, 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. Here b is a variable appearing from the Möbius inversion formula $\varphi(\Delta) = \sum_{b|\Delta} \mu(b) b^{-1}$ (see [19, p. 1013]).

Moreover, the restriction on the support of β_z to z in a fixed primary congruence class modulo $64q_1$ (where q_1 is as in (2.19)) as opposed to modulo 8 is handled in the same way as in [19, Sections 15-17]. For sums over medium-size moduli, the estimation of β_z is trivial and so the restriction on the support is irrelevant (see bottom of [19, 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

$$S_\chi^k(\beta) = \sum_z \beta_z \chi(z) \left(\frac{z}{|z|}\right)^k, \tag{2.52}$$

where χ is a multiplicative character of the group $(\mathbb{Z}[i]/\xi d\mathbb{Z}[i])^\times$ (see [19, (16.14), p. 1005]). The restriction on the support of β_z can be detected by multiplicative characters modulo $64q_1$, so that we can simply transform χ into a character for the group $(\mathbb{Z}[i]/64q_1 d\mathbb{Z}[i])^\times$. The sum (2.52) is bounded by studying the Hecke L-functions

$$L(s, \psi) = \sum_{\mathfrak{a}} \psi(\mathfrak{a})(N\mathfrak{a})^{-s},$$

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

$$\psi(\mathfrak{a}) := \chi(z) \left(\frac{z}{|z|}\right)^k$$

where z is the unique primary Gaussian integer which generates $\mathfrak{a}$. The dependence on χ of the bound given for $S_\chi^k(\beta)$ is only through the modulus of

χ (see [19, 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

$$S_\chi^k(\beta') = \sum_z \beta'_z \chi(z) \left(\frac{z}{|z|}\right)^k, \tag{2.53}$$

where χ 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 β'_z is now

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

if $z = r + is$ (see [19, (17.8), p. 1014] and [19, (17.12), p. 1015]). Again, the restriction on the support of β_z (and hence also β'_z) can be detected by multiplicative characters modulo $64q_1$, so that we can transform χ into a character for the group $(\mathbb{Z}[i]/64q_1 bd\mathbb{Z}[i])^\times$. Cancellation in the sum (2.53) is now achieved due to the oscillation of the symbol

$$i^{\frac{r-1}{2}} \left(\frac{s}{|r|}\right)$$

as z varies over primary Gaussian integers, but again the dependence on χ of the bound given for (2.53) is only through the modulus of χ (see [19, Proposition 17.2, p. 1016]) and this modulus is again different from $4bd$ by a fixed constant. This shows that Lemma 2.13 follows from [19, Proposition 10.2] and hence Proposition 2.4 is proved.