

## The infinitude of $\mathbb{Q}(\sqrt{-p})$ with class number divisible by 16

by

DJORDJO Z. MILOVIC (Princeton, NJ)

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

$$2 \mid h \Leftrightarrow p \equiv 1 \pmod{4}.$$

The criterion

$$4 \mid h \Leftrightarrow p \equiv 1 \pmod{8}$$

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

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

This can be restated as

$$(1.1) \quad 8 \mid h \Leftrightarrow p \equiv 1 \pmod{8} \text{ and } 1 + i \text{ is a square modulo } p,$$

where  $i$  is a square root of  $-1$  modulo  $p$  (see [BC, (10), p. 68]). In [St1], Stevnhagen also obtained criterion (1.1), 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

$$R(S, X) := \frac{\#\{p \leq X \text{ prime} : p \in S\}}{\#\{p \leq X \text{ prime}\}}.$$

---

2010 *Mathematics Subject Classification*: Primary 11R29; Secondary 11N36.

*Key words and phrases*: class groups, sieve theory.

Received 26 April 2015; revised 16 February 2017.

Published online 26 April 2017.

If  $\lim_{X \rightarrow \infty} R(S, X)$  exists, we denote it by  $\rho(S)$  and call it the *natural density* of  $S$ . Let

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

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 (1.1), 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  $\mathbb{Q}$ , Chebotarev's density theorem implies that  $\rho(S(8)) = 1/8$ . For a discussion of these and similar density results, see [St2, pp. 16–19].

The Cohen–Lenstra heuristics [CL] 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 1.1.** *For all  $k \geq 1$ ,  $\lim_{X \rightarrow \infty} R(S(2^k), X)$  exists and is equal to  $2^{-k}$ .*

While Conjecture 1.1 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 [St2, p. 16]). Although several criteria for divisibility by 16 have been found already (see [K], [W], and [LW]), none of them appears 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 are an infinite number of primes  $p$  for which  $16 \mid h$  and also an infinite number of primes  $p$  for which  $8 \mid h$  but  $16 \nmid h$ . We also derive some consequences for the fundamental unit  $\epsilon_p$  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

$$(1.2) \quad p = a^2 + c^4, \quad c \text{ even.}$$

We note that in this case  $8 \mid h$  if and only if  $a \equiv \pm 1 \pmod{8}$  and  $c \equiv 0 \pmod{4}$  or  $a \equiv \pm 3 \pmod{8}$  and  $c \equiv 2 \pmod{4}$  (see (2.6)). The main theorem that we prove gives a new and explicit criterion for divisibility by 16 of the class numbers of  $\mathbb{Q}(\sqrt{-p})$  for  $p$  of the form (1.2):

**THEOREM 1.2.** *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  $a \equiv \pm 1 \pmod{16}$  and  $c \equiv 0 \pmod{4}$ , then  $h_{-4p} \equiv 0 \pmod{16}$ .*
- (ii) *If  $a \equiv \pm 3 \pmod{16}$  and  $c \equiv 2 \pmod{4}$ , then  $h_{-4p} \equiv 0 \pmod{16}$ .*
- (iii) *If  $a \equiv \pm 7 \pmod{16}$  and  $c \equiv 0 \pmod{4}$ , then  $h_{-4p} \equiv 8 \pmod{16}$ .*
- (iv) *If  $a \equiv \pm 5 \pmod{16}$  and  $c \equiv 2 \pmod{4}$ , then  $h_{-4p} \equiv 8 \pmod{16}$ .*

Once we prove Theorem 1.2, the infinitude of primes  $p$  of the form as in (i)–(iv) follows from the following generalization of a powerful theorem of Friedlander and Iwaniec (see [FI1, Theorem 1, p. 946]):

**PROPOSITION 1.3.** *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*

$$(1.3) \quad \sum_{\substack{a^2+c^4 \leq X \\ a \equiv a_0 \pmod{16} \\ c \equiv c_0 \pmod{4} \\ a^2+c^4 \text{ prime}}} 1 = \frac{\kappa}{2\pi} \frac{X^{3/4}}{\log X} \left( 1 + O\left(\frac{\log \log X}{\log X}\right) \right),$$

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

$$\kappa = \int_0^1 (1 - t^4)^{1/2} dt \approx 0.874\dots$$

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

Theorem 1.2 and Proposition 1.3 immediately imply:

**COROLLARY 1.4.** *For a prime  $p$ , let  $h_{-4p}$  denote the class number of  $\mathbb{Q}(\sqrt{-p})$ . Then, for sufficiently large  $X$ , we have*

$$\begin{aligned} \#\{p \leq X : h_{-4p} \equiv 0 \pmod{16}\} &\geq \frac{X^{3/4}}{8 \log X}, \\ \#\{p \leq X : h_{-4p} \equiv 8 \pmod{16}\} &\geq \frac{X^{3/4}}{8 \log X}. \end{aligned}$$

The proof of Proposition 1.3 will take a significant portion of our paper. Although the ideas required to generalize [FI1, Theorem 1, p. 946] in this way are not particularly deep, implementing them turns out to be quite complicated simply because the proof of [FI1, Theorem 1] itself is very difficult. One can thus view Sections 4–6 as a summary of the proof of [FI1, 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 1.1. Nonetheless, each of the cases (i)–(iv) in Theorem 1.2 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 1.1 is true for  $k = 4$ . However, we also note that Conjecture 1.1 for  $k = 4$  does not imply Corollary 1.4, 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 [W]. Let  $p \equiv 1 \pmod{8}$ , and let  $\epsilon_p$  be the 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  $8 \mid h$ , then

$$(1.4) \quad h \equiv T + p - 1 \pmod{16},$$

so that  $16 \mid h$  if and only if  $T \equiv 1 - p \pmod{16}$ . An immediate byproduct of Theorem 1.2 and criterion (1.4) is the following corollary.

**COROLLARY 1.5.** *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 the fundamental unit of  $\mathbb{Q}(\sqrt{p})$ .*

- (i) *If  $a \equiv \pm 1 \pmod{16}$  and  $c \equiv 0 \pmod{4}$ , then  $T \equiv 0 \pmod{16}$  and  $U \equiv \pm 1 \pmod{16}$ .*
- (ii) *If  $a \equiv \pm 3 \pmod{16}$  and  $c \equiv 2 \pmod{4}$ , then  $T \equiv 8 \pmod{16}$  and  $U \equiv \pm 3 \pmod{16}$ .*
- (iii) *If  $a \equiv \pm 7 \pmod{16}$  and  $c \equiv 0 \pmod{4}$ , then  $T \equiv 8 \pmod{16}$  and  $U \equiv \pm 7 \pmod{16}$ .*
- (iv) *If  $a \equiv \pm 5 \pmod{16}$  and  $c \equiv 2 \pmod{4}$ , then  $T \equiv 0 \pmod{16}$  and  $U \equiv \pm 5 \pmod{16}$ .*

This can be viewed as an extension of [Lag, Corollary 1.2(i), pp. 115–116] to primes of the form  $p = a^2 + c^4$ . Now Proposition 1.3 gives

**COROLLARY 1.6.** *For a prime  $p \equiv 1 \pmod{8}$ , let  $\epsilon_p = T + U\sqrt{p}$  denote the fundamental unit of  $\mathbb{Q}(\sqrt{p})$ . Then, for sufficiently large  $X$ , we have*

$$\begin{aligned} \#\{p \leq X : p \equiv 1 \pmod{8}, T \equiv 0 \pmod{16}\} &\geq \frac{X^{3/4}}{8 \log X}, \\ \#\{p \leq X : p \equiv 1 \pmod{8}, T \equiv 8 \pmod{16}\} &\geq \frac{X^{3/4}}{8 \log X}. \end{aligned}$$

The existence of infinitely many  $p \equiv 1 \pmod{8}$  such that  $T \equiv T_0 \pmod{16}$  for a fixed  $T_0 \in \{0, 8\}$  is not at all trivial. Hence Corollary 1.5 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  $p \equiv 1 \pmod{4}$ . Then there are two prime ideals of  $\mathbb{Z}$  which ramify in the ring of integers  $\mathbb{Z}[\sqrt{-p}]$  of  $\mathbb{Q}(\sqrt{-p})$ , namely  $(2)$  and  $(p)$ . The prime ideal  $\mathfrak{p} = (\sqrt{-p})$  of  $\mathbb{Z}[\sqrt{-p}]$  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  $\mathfrak{t} = (2, 1 + \sqrt{-p})$  of  $\mathbb{Z}[\sqrt{-p}]$  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  $\mathfrak{t}$  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

$$(2.1) \quad \left( \frac{\cdot}{H/K} \right) : \mathcal{C} \rightarrow \text{Gal}(H/\mathbb{Q}(\sqrt{-p})).$$

Suppose for the moment that  $2^n \mid h$  for some non-negative integer  $n$ . Then  $\mathcal{C}^{2^n}$  is a subgroup of  $\mathcal{C}$  of index  $2^n$ . We define the  *$2^n$ -Hilbert class field*  $H_{2^n}$  to be the subfield of  $H$  fixed by the image of  $\mathcal{C}^{2^n}$  under the isomorphism (2.1). Since the 2-primary part of  $\mathcal{C}$  is cyclic, it follows immediately that  $H_{2^n}$  is the *unique* unramified, cyclic, degree- $2^n$  extension of  $K$ . This characterization implies that  $H_{2^n}$  is normal not just over  $K$  but also over  $\mathbb{Q}$ . Indeed, let  $F$  be a field normal over  $\mathbb{Q}$  such that  $H_{2^n} \subset F$  and let  $\sigma \in \text{Gal}(F/\mathbb{Q})$ . Since  $\sigma(H_{2^n})$  is an unramified, cyclic, degree- $2^n$  extension of  $\sigma(K)$ , and since  $\sigma(K) = K$  (because  $K/\mathbb{Q}$  is normal), we see that  $\sigma(H_{2^n}) = H_{2^n}$ . This holds for all  $\sigma \in \text{Gal}(F/\mathbb{Q})$ , so  $H_{2^n}/\mathbb{Q}$  is normal.

Now, (2.1) induces a canonical isomorphism of cyclic groups of order  $2^n$ ,

$$(2.2) \quad \left( \frac{\cdot}{H_{2^n}/K} \right) : \mathcal{C}/\mathcal{C}^{2^n} \rightarrow \text{Gal}(H_{2^n}/K).$$

Hence the class  $[\mathfrak{t}]$  belongs to  $\mathcal{C}^{2^n}$  if and only if  $\mathfrak{t}$  has trivial Artin symbol in  $\text{Gal}(H_{2^n}/K)$ . By class field theory, this is equivalent to  $\mathfrak{t}$  splitting completely in  $H_{2^n}$ . We conclude that if  $2^n \mid h$ , then

$$(2.3) \quad 2^{n+1} \mid h \Leftrightarrow \mathfrak{t} \text{ splits completely in } H_{2^n}.$$

The main idea of the proof of Theorem 1.2 is to write down explicitly the 8-Hilbert class field  $H_8$  of  $\mathbb{Q}(\sqrt{-p})$ , and then to characterize those  $p$  such that  $\mathfrak{t}$  splits completely in  $H_8$ . We remark here that although Cohn and Cooke [CC] have already written down  $H_8$  in terms of the fundamental unit  $\epsilon_p$  of  $\mathbb{Q}(\sqrt{p})$  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  $\mathfrak{t}$  splits completely in  $H_8$ .

**2.2. Generating  $2^n$ -Hilbert class fields.** We first state 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  $\mathbb{Q}(\sqrt{-p})$ , is known to be  $H_2 = \mathbb{Q}(i, \sqrt{p})$ . Hence, for every  $n \geq 1$ , the  $2^n$ -Hilbert class field of  $\mathbb{Q}(\sqrt{-p})$  contains  $\mathbb{Q}(i)$ , 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  $(1 + i)$  of  $\mathbb{Z}[i]$  lying over the prime ideal  $(2)$  of  $\mathbb{Z}$ .

This completion is  $\mathbb{Q}_2(i)$ , and its ring of integers  $\mathbb{Z}_2[i]$  is a discrete valuation ring with maximal ideal  $\mathfrak{m}$  and uniformizer  $m = 1 + i$ . 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

$$U = U^{(1)} \supset U^{(2)} \supset \dots$$

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  $\omega$  be a unit in  $\mathbb{Z}_2[i]$ . If  $\omega \equiv \pm 1 \pmod{\mathfrak{m}^4}$ , then  $\mathbb{Q}_2(i, \sqrt{\omega})$  is unramified over  $\mathbb{Q}_2(i)$ . Moreover,  $\omega$  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  $\mathbb{Q}(\sqrt{-p})$  which we construct are normal and cyclic.

LEMMA 2.2. *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  $\alpha$  be an element of  $L$  which is not a square in  $L$ , and let  $M = L(\sqrt{\alpha})$ . Then  $M/K$  is cyclic of degree 4 if and only if  $\text{Norm}_{L/K}(\alpha) \in dK^2$ .*

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

LEMMA 2.3. *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 lift 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 [Rei, Satz 3, 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  $\varpi$  of a similar form to give rise to a generator, so that we can actually construct  $H_{2^n}$ . We will use certain auxiliary extensions over  $\mathbb{Q}(i)$ . In the following lemma, the first hypothesis simply describes the basic properties of these auxiliary extensions and their interactions with 2-power-Hilbert class fields, while the rest of the hypotheses describe an element  $\varpi$  which is key to our construction. We recall that in the notation which we adopted, we have  $H_1 = \mathbb{Q}(\sqrt{-p})$  and  $\mathbb{Q}(i) \subset H_2 = \mathbb{Q}(i, \sqrt{p})$ . We use  $\mathcal{O}_F$  to denote the ring of integers of a number field  $F$ . Furthermore, if  $E/F$  is an extension of number fields,  $\mathfrak{q}$  is a prime ideal of  $\mathcal{O}_F$ , and  $\mathfrak{Q}$  is a prime ideal of  $\mathcal{O}_E$  lying over  $\mathfrak{q}$ , then we denote the ramification index of  $\mathfrak{Q}$  over  $\mathfrak{q}$  by  $e(\mathfrak{Q}/\mathfrak{q})$ , and we denote the inertia degree  $[\mathcal{O}_E/\mathfrak{Q} : \mathcal{O}_F/\mathfrak{q}]$  by  $f(\mathfrak{Q}/\mathfrak{q})$ .

Before stating the lemma, we make one final remark. Suppose that  $2^n \mid h$ . By (2.3), the prime ideal  $\mathfrak{t}$  of  $\mathbb{Z}[\sqrt{-p}]$  lying above (2) splits completely in  $H_{2^{n-1}}/\mathbb{Q}(\sqrt{-p})$ . Suppose also that  $n \geq 2$ , so that  $\mathbb{Q}(i) \subset H_{2^{n-1}}$ . Since (2) ramifies in both  $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$  and  $\mathbb{Q}(i)/\mathbb{Q}$ , we see that  $(1+i)$  must also split completely in  $H_{2^{n-1}}/\mathbb{Q}(i)$ . Hence, if  $\mathfrak{T}$  is *any* prime ideal of  $\mathcal{O}_{H_{2^{n-1}}}$  lying above  $(1+i)$  (or, equivalently, above  $\mathfrak{t}$ ), then the completion  $(H_{2^{n-1}})_{\mathfrak{T}}$  is isomorphic to  $\mathbb{Q}_2(i)$ . We are now ready to state the lemma.

LEMMA 2.4. *Let  $h$  be the class number of  $\mathbb{Q}(\sqrt{-p})$ , let  $n \geq 2$ , and suppose that  $2^n$  divides  $h$ . Suppose that there exist number fields  $A_{2^{n-2}} \subset A_{2^{n-1}}$  such that*

(i)  $[A_{2^k} : \mathbb{Q}] = 2^k$  and  $A_{2^k} \subset H_{2^k}$  for  $k \in \{n-2, n-1\}$ ,

*and suppose that there is an element  $\varpi \in \mathcal{O}_{A_{2^{n-1}}} \subset \mathcal{O}_{H_{2^{n-1}}}$  such that*

(ii)  $\Pi := \text{Norm}_{A_{2^{n-1}}/A_{2^{n-2}}}(\varpi)$  generates a prime ideal  $\mathfrak{P}$  of  $\mathcal{O}_{A_{2^{n-2}}}$  that is unramified in  $A_{2^{n-1}}/A_{2^{n-2}}$ , lies above the prime ideal  $(p)$  of  $\mathbb{Z}$ , and satisfies  $e(\mathfrak{P}/(p)) = f(\mathfrak{P}/(p)) = 1$ ,

(iii)  $H_{2^{n-1}} = H_{2^{n-2}}(\sqrt{\Pi})$ ,

(iv)  $\varpi \equiv \pm 1 \pmod{\mathfrak{m}^4}$  in the completion  $(H_{2^{n-1}})_{\mathfrak{T}} \cong \mathbb{Q}_2(i)$ , where  $\mathfrak{T}$  is any prime ideal of  $\mathcal{O}_{H_{2^{n-1}}}$  lying above the prime ideal  $(1+i)$  of  $\mathbb{Z}[i]$ ,

(v)  $H_{2^{n-1}}(\sqrt{\varpi})$  is normal over  $\mathbb{Q}$ .

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

*Proof.* We first deduce several facts about  $\varpi$ . By hypothesis (i),  $A_{2n-1}/A_{2n-2}$  is an extension of degree 2 and hence normal. Let  $\sigma$  be the non-trivial element of  $\text{Gal}(A_{2n-1}/A_{2n-2})$ , and set  $\varpi' = \sigma(\varpi)$ . Hypothesis (ii) implies that  $\mathfrak{P}$  factors into prime ideals in  $\mathcal{O}_{A_{2n-1}}$  as  $\mathfrak{P}\mathcal{O}_{A_{2n-1}} = (\varpi)(\varpi')$ , and, as  $\mathfrak{P}$  does not ramify in  $A_{2n-1}$ , that  $\varpi$  and  $\varpi'$  are co-prime. We then also deduce that  $e((\varpi)/(p)) = e((\varpi')/(p)) = f((\varpi)/(p)) = f((\varpi')/(p)) = 1$ .

We need to prove that  $H_{2n-1}(\sqrt{\varpi})$  is an unramified cyclic extension of  $\mathbb{Q}(\sqrt{-p})$  of degree  $2^n$ .

As  $[H_{2n-1} : \mathbb{Q}(\sqrt{-p})] = 2^{n-1}$ , in order to establish that  $H_{2n-1}(\sqrt{\varpi})$  is an extension of  $\mathbb{Q}(\sqrt{-p})$  of degree  $2^n$ , it suffices to show that  $\sqrt{\varpi}$  is not in  $H_{2n-1}$ . As  $\varpi$  is a prime and hence not a square in  $\mathcal{O}_{A_{2n-1}}$ , we deduce that  $[A_{2n-1}(\sqrt{\varpi}) : A_{2n-1}] = 2$ . Hypothesis (i) implies that  $A_{2n-1} \subset H_{2n-1}$  and  $[H_{2n-1} : A_{2n-1}] = 2$ . Hence  $\sqrt{\varpi} \in H_{2n-1}$  if and only if  $H_{2n-1} = A_{2n-1}(\sqrt{\varpi})$ . Now, recall that  $H_{2n-1}/\mathbb{Q}$  is a normal extension. Since  $H_{2n-1}/\mathbb{Q}(\sqrt{-p})$  is unramified (by definition of  $H_{2n-1}$ ) and  $(p)$  ramifies in  $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$ , it follows that the ramification index of  $(p)$  in  $H_{2n-1}/\mathbb{Q}$  is 2. However, as shown above,  $e((\varpi')/(p)) = 1$ , and as  $\varpi$  and  $\varpi'$  are coprime,  $(\varpi')$  is unramified in  $A_{2n-1}(\sqrt{\varpi})/A_{2n-1}$ . Hence  $H_{2n-1} \neq A_{2n-1}(\sqrt{\varpi})$  and thus  $[H_{2n-1}(\sqrt{\varpi}) : \mathbb{Q}(\sqrt{-p})] = 2^n$ .

Next, we show that  $H_{2n-1}(\sqrt{\varpi})/\mathbb{Q}(\sqrt{-p})$  is cyclic. By hypothesis (v), the field  $H_{2n-1}(\sqrt{\varpi})$  is normal over  $\mathbb{Q}$ , and hence also over the subfields  $\mathbb{Q}(\sqrt{-p})$  and  $H_{2n-2}$ . Similarly to the above, we see that  $A_{2n-1} \neq H_{2n-2}$  (the ramification index of  $(p)$  in  $H_{2n-2}/\mathbb{Q}$  is 2, while  $e((\varpi)/(p)) = 1$ ). Hence, by comparing field extension degrees from hypothesis (i), we have  $H_{2n-1} = H_{2n-2}A_{2n-1}$  and  $\text{Gal}(H_{2n-1}/H_{2n-2}) \cong \text{Gal}(A_{2n-1}/A_{2n-2})$ , the isomorphism being given by restriction to  $A_{2n-1}$ . Thus if  $\sigma'$  is the non-trivial element in  $\text{Gal}(H_{2n-1}/H_{2n-2})$ , then  $\sigma'(\varpi) = \sigma(\varpi) = \varpi'$ , and so  $\varpi$  and  $\varpi'$  are also conjugates over  $H_{2n-2}$ . By hypothesis (iii),  $H_{2n-1} = H_{2n-2}(\sqrt{\varpi\varpi'})$ . Note also that  $\varpi\varpi' = \varpi\varpi' \cdot 1^2$ . Lemma 2.2 with  $(K, L, M, d, \alpha) = (H_{2n-2}, H_{2n-1}, H_{2n-1}(\sqrt{\varpi}), \varpi\varpi', \varpi)$  then implies that  $H_{2n-1}(\sqrt{\varpi})$  is a cyclic degree-4 extension of  $H_{2n-2}$ . Moreover,  $H_{2n-1}$  is a cyclic degree- $2^{n-1}$  extension of  $\mathbb{Q}(\sqrt{-p})$ , so Lemma 2.3 with  $(K, L, M, N, m) = (\mathbb{Q}(\sqrt{-p}), H_{2n-2}, H_{2n-1}, H_{2n-1}(\sqrt{\varpi}), 2^{n-2})$  implies that  $H_{2n-1}(\sqrt{\varpi})$  is a cyclic degree- $2^n$  extension of  $\mathbb{Q}(\sqrt{-p})$ .

We will now prove that  $H_{2n-1}(\sqrt{\varpi})/\mathbb{Q}(\sqrt{-p})$  is unramified. By definition of  $H_{2n-1}$ , the extension  $H_{2n-1}/\mathbb{Q}(\sqrt{-p})$  is unramified, so it suffices to prove that  $H_{2n-1}(\sqrt{\varpi})/H_{2n-1}$  is unramified. The discriminant of this quadratic extension divides  $(4\varpi)$ , so hypothesis (ii) implies that the only prime ideals that could possibly ramify in  $H_{2n-1}(\sqrt{\varpi})/H_{2n-1}$  are those lying above the prime ideals  $\mathfrak{t}$  and  $\mathfrak{p}$  of  $\mathbb{Z}[\sqrt{-p}]$ .



For the prime ideals above  $\mathfrak{t}$ , we can check the claim locally. Indeed, as noted in the remark preceding this lemma, if  $\mathfrak{F}$  is a prime ideal of  $\mathcal{O}_{H_{2^{n-1}}}$  lying above  $\mathfrak{t}$ , then  $(H_{2^{n-1}})_{\mathfrak{F}} \cong \mathbb{Q}_2(i)$ . Now hypothesis (iv) in conjunction with Lemma 2.1 implies that  $(H_{2^{n-1}})_{\mathfrak{F}}(\sqrt{\varpi})/(H_{2^{n-1}})_{\mathfrak{F}}$  is unramified, and this proves the claim.

Note that  $e((\varpi')/(p)) = 1$ , and since  $\varpi'$  is coprime to  $4\varpi$ ,  $(\varpi')$  does not ramify in  $A_{2^{n-1}}(\sqrt{\varpi})/A_{2^{n-1}}$ . Hence the ramification index of  $(p)$  in  $H_{2^{n-1}}(\sqrt{\varpi})$  is at most  $[H_{2^{n-1}}(\sqrt{\varpi}) : A_{2^{n-1}}(\sqrt{\varpi})] = 2$ . Since  $e(\mathfrak{p}/(p)) = 2$ , we conclude that the ideal  $\mathfrak{p}$  does not ramify in  $H_{2^{n-1}}(\sqrt{\varpi})/\mathbb{Q}(\sqrt{-p})$ . ■

**2.3. Explicit constructions of  $H_4$  and  $H_8$ .** Recall from (2.3) that 4 divides  $h$  if and only if the prime ideal  $\mathfrak{t}$  lying above 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.,  $p \equiv 1 \pmod 8$ . We will now use Lemma 2.4 to construct the 4-Hilbert class field of  $\mathbb{Q}(\sqrt{-p})$ .

A prime  $p \equiv 1 \pmod 4$  splits in  $\mathbb{Q}(i)$ , so that there exists  $\pi$  in  $\mathbb{Z}[i]$  such that  $p = \pi\bar{\pi}$ ; here  $\bar{\pi}$  denotes the conjugate of  $\pi$  over  $\mathbb{Q}$ . 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  $p \equiv 1 \pmod 8$ , we see that  $b$  is in fact divisible by 4. Hence

$$(2.4) \quad \pi = a + bi, \quad b \equiv 0 \pmod 4.$$

Now fix a square root of  $\pi$  and denote it by  $\sqrt{\pi}$ . Recall that  $H_2 = \mathbb{Q}(i, \sqrt{p})$  is the 2-Hilbert class field of  $\mathbb{Q}(\sqrt{-p})$ . We claim that the hypotheses of Lemma 2.4 for  $n = 2$  are satisfied with  $A_1 = \mathbb{Q}$ ,  $A_2 = \mathbb{Q}(i)$ , and  $\varpi = \pi$ .

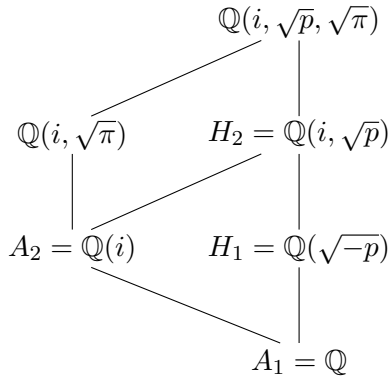
Hypothesis (i) is easy to check. To verify (ii), note that  $\text{Norm}_{\mathbb{Q}(i)/\mathbb{Q}}(\pi) = p$  and that  $p$  splits completely in  $\mathbb{Q}(i)/\mathbb{Q}$ . Hypothesis (iii) follows because  $H_1(\sqrt{\pi\bar{\pi}}) = \mathbb{Q}(\sqrt{-p}, \sqrt{p}) = \mathbb{Q}(i, \sqrt{p})$ . As for (iv), our choice of  $\pi$  as in (2.4) ensures that  $\pi \equiv \pm 1 \pmod 4$ . To see that (v) is satisfied, note that  $H_2(\sqrt{\pi})$  is the splitting field (over  $\mathbb{Q}$ ) of the polynomial

$$f_4(X) := (X^2 - \pi)(X^2 - \bar{\pi}) = X^4 - 2aX^2 + p.$$

Indeed,  $\pi\bar{\pi}$  is a square in  $H_2$ , so both square roots of  $\bar{\pi}$  are also contained in  $H_2(\sqrt{\pi})$ . We conclude by Lemma 2.4 that the 4-Hilbert class field is given by

$$(2.5) \quad H_4 = H_2(\sqrt{\pi}) = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi})$$

with  $\pi$  as in (2.4). Relations between the relevant fields are illustrated in the diagram below.



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  $\pi$  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 (2.4), this means that

$$(2.6) \quad 8 \mid h \Leftrightarrow a + b \equiv \pm 1 \pmod{8}.$$

We remark that Fouvry and Klüners developed similar methods in [FK], 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  $8 \mid h$ . Replacing  $\pi$  by  $-\pi$  if necessary, we assume that

$$(2.7) \quad \pi \equiv 1 \pmod{\mathfrak{m}^5}.$$

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

$$(2.8) \quad \sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^3}.$$

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  $\bar{\pi}$ , 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  $-\bar{\pi}$ . These are primes  $p$  of the form

$$(2.9) \quad p = a^2 + c^4, \quad c \text{ even},$$

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 (2.9). Set

$$(2.10) \quad \varpi_0 = c(1 + i) + \sqrt{\pi}.$$

Let  $\sigma$  be a generator for  $\text{Gal}(H_4/\mathbb{Q}(\sqrt{-p}))$  and set  $\varpi_m = \sigma^m(\varpi_0)$  for  $1 \leq m \leq 3$ . The restriction of  $\sigma$  to  $H_2$  generates  $\text{Gal}(H_2/\mathbb{Q}(\sqrt{-p}))$ , so  $\sigma(i) = -i$ .

Also, looking at the polynomial  $f_4(X)$  above, we see that  $\sigma^2(\sqrt{\pi}) = -\sqrt{\pi}$ . Hence

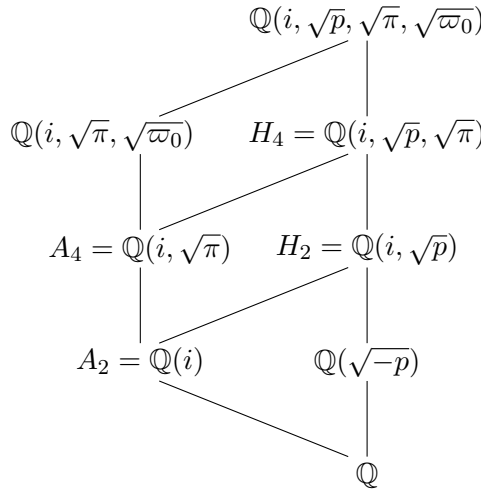
$$(2.11) \quad \varpi_0 \cdot \varpi_2 = (c(1+i) + \sqrt{\pi})(c(1+i) - \sqrt{\pi}) = -\bar{\pi},$$

$$(2.12) \quad \varpi_1 \cdot \varpi_3 = (c(1-i) + \sigma(\sqrt{\pi}))(c(1-i) - \sigma(\sqrt{\pi})) = -\pi.$$

We can now prove the main result of this section.

**PROPOSITION 2.5.** *Let  $p$  be a prime of the form (2.9), let  $\pi$  be as in (2.7), let  $\sqrt{\pi}$  be as in (2.8), and let  $\varpi_0$  be as in (2.10). Let  $\sqrt{\varpi_0}$  denote a square root of  $\varpi_0$ . Then  $H_4(\sqrt{\varpi_0})$  is the 8-Hilbert class field of  $\mathbb{Q}(\sqrt{-p})$ .*

*Proof.* We again use Lemma 2.4, but this time with  $n = 3$ ,  $A_2 = \mathbb{Q}(i)$ ,  $A_4 = \mathbb{Q}(i, \sqrt{\pi})$ , and  $\varpi = \varpi_0$ . Hypotheses (i)–(iii) easily follow from (2.11). Indeed,  $\Pi = -\bar{\pi}$ , and  $(\bar{\pi})$  is unramified and splits in  $\mathbb{Q}(i, \sqrt{\pi})/\mathbb{Q}(i)$  by (2.11) and because  $\bar{\pi}$  and  $4\pi$  are coprime. Moreover,  $H_2(\sqrt{-\bar{\pi}}) = \mathbb{Q}(i, \sqrt{p}, \sqrt{-\bar{\pi}}) = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi}) = \mathbb{Q}(i, \sqrt{p}, \sqrt{\pi})$ ; see the diagram.



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

$$\begin{aligned} f_8(X) &= (X^2 - \varpi_0)(X^2 - \varpi_2)(X^2 - \varpi_1)(X^2 - \varpi_3) \\ &= (X^4 - 2c(1+i)X^2 - \bar{\pi})(X^4 - 2c(1-i)X^2 - \pi) \\ &= X^8 - 4cX^6 + (8c^2 - 2a)X^4 + (4ac - 4c^3)X^2 + p. \end{aligned}$$

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

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

Then

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

which completes the proof of (v).

It remains to prove hypothesis (iv), i.e., that  $\varpi_0 \equiv \pm 1 \pmod{\mathfrak{m}^4}$ . Recall from (2.8) 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  $a+b \equiv 1 \pmod{8}$ , i.e.,  $a+c^2 \equiv 1 \pmod{\mathfrak{m}^6}$ . We now split our argument into two cases, the first when  $c \equiv 0 \pmod{4}$  and the second when  $c \equiv 2 \pmod{4}$ .

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  $\pi = a+c^2i \equiv 1 \pmod{\mathfrak{m}^6}$ , which means that  $\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^4}$ . Therefore

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

If  $c \equiv 2 \pmod{\mathfrak{m}^4}$ , then  $c^2 \equiv -m^4 \pmod{\mathfrak{m}^6}$ . In this case,  $a-1+m^4 \in \mathfrak{m}^6$ , so that  $\pi = a+c^2i \equiv 1-m^4-m^4i \equiv 1+m^4(-1-i) \equiv 1+m^5 \pmod{\mathfrak{m}^6}$ . 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 completes the proof of Proposition 2.5. ■

**3. Proof of Theorem 1.2.** The proof will proceed in much the same way as the last part of the proof of Proposition 2.5. 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  $H_8$ ). By Lemma 2.1, this is equivalent to determining when  $\varpi_0 \equiv \pm 1 \pmod{\mathfrak{m}^5}$ .

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  $\sqrt{\pi} \equiv 1 \pmod{\mathfrak{m}^4}$ .

We now compute  $\varpi_0$  modulo  $\mathfrak{m}^5$ . Since  $c \equiv 0 \pmod{4}$ , we deduce that  $\varpi_0 \equiv \sqrt{\pi} \pmod{\mathfrak{m}^5}$ . 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  $\pi$  modulo  $\mathfrak{m}^7$ . Hence, assuming  $c \equiv 0 \pmod{4}$ , we get

$$16 \mid h \Leftrightarrow \sqrt{\pi} \equiv \pm 1 \pmod{\mathfrak{m}^5} \Leftrightarrow \pi \equiv 1 \pmod{\mathfrak{m}^7} \Leftrightarrow a \equiv 1 \pmod{16}.$$

This proves parts (i) and (iii) of Theorem 1.2.

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  $\varpi_0 \equiv 2m + \sqrt{\pi} \pmod{\mathfrak{m}^5}$ , and so we must determine conditions on  $a$  such that  $\sqrt{\pi} \equiv \pm 1 - 2m \pmod{\mathfrak{m}^5}$ . Under the

current assumptions,

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

Note that because of the choice (2.7) 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 1.2.

**4. Overview of the proof of Proposition 1.3.** In [FI1], Friedlander and Iwaniec prove an asymptotic formula for the number of primes of the form  $a^2 + c^4$ , that is, of the form  $a^2 + b^2$  where  $b$  itself is a square. For a summary of their proof, see the exposition in [FI3, Chapter 21]. They use a new sieve that they developed to detect primes in relatively thin sequences [FI2]. This sieve has its roots in the work of Fouvry and Iwaniec [FoI], where similar sieve hypotheses were used 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 1.3 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 1.3 involves certain alterations to the way that the sieve [FI2] 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 [FI2] yields an asymptotic formula for

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

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

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

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

$$(4.1) \quad A_d(x) := g(d)A(x) + r_d(x).$$

The hypotheses which are not difficult to verify are listed in [FI1, equations (2.1)–(2.8)]. We briefly recall them here. We assume the bounds

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

$$(H2) \quad A(x) \gg x^{1/3} \left( \sum_{n \leq x} a_n^2 \right)^{1/2}.$$

We assume that the multiplicative function  $g$  satisfies

$$(H3) \quad 0 \leq g(p^2) \leq g(p) \leq 1,$$

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

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

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

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

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

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

uniformly in  $d \leq x^{1/3}$ ; 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, named (R) for *remainders*; it is a condition on the average value of the error terms  $r_d(x)$ . Let  $L = (\log x)^{24}$ .

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

$$(4.2) \quad x^{2/3} < D < x$$

*such that for all  $x \geq x_r$ , we have*

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

*uniformly in  $t \leq x$ .*

In our applications,  $D$  will be  $x^{3/4-\varepsilon}$  for a sufficiently small  $\varepsilon$ ; see Proposition 5.3 below.

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

$$(4.3) \quad \beta(n, C) = \mu(n) \sum_{c|n, c \leq C} \mu(c).$$

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 hypothesis (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*

$$2 \leq \delta \leq \Delta, \quad 2 \leq P \leq \Delta^{1/2^{35} \log \log x},$$

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

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

where

$$(4.4) \quad \Pi = \prod_{p \leq P} p.$$

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

The main result of [FI2] is

THEOREM 4.1. *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).

**4.2. Preparing the sieve for Proposition 1.3.** For our application, we will denote by  $v'$  the analogue of a quantity  $v$  from the proof of Friedlander and Iwaniec [FI1]. 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

$$a_0 \bmod q_1, \quad c_0 \bmod q_2$$

is *admissible* if for every pair of congruence classes

$$a_1 \pmod{q}, \quad c_1 \pmod{q}$$

such that  $a_1 \equiv a_0 \pmod{q_1}$  and  $c_1 \equiv c_0 \pmod{q_2}$ , the congruence class  $a_1^2 + c_1^4 \pmod{q}$  is a unit modulo  $q$ .

EXAMPLE 4.2. 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  $a_0 \pmod{16}$  and  $c_0 \pmod{4}$  is admissible.

EXAMPLE 4.3. Suppose that  $a_0 = c_0 = 1$ . Then the pair of congruence classes  $a_0 \pmod{3}$  and  $c_0 \pmod{2}$  is *not* admissible. Indeed,  $1 \equiv a_0 \equiv c_0 \pmod{6}$  but  $2 \equiv 1^2 + 1^4 \pmod{6}$  is not invertible modulo 6. This does not mean, however, that there are no primes of the form  $a^2 + c^4$  with  $a \equiv 1 \pmod{3}$  and  $c \equiv 1 \pmod{2}$ ; one such prime is  $4^2 + 1^4$ .

Henceforth, suppose  $q_1$  and  $q_2$  are positive integers, let  $q$  be their least common multiple, and suppose  $a_0 \pmod{q_1}$  and  $c_0 \pmod{q_2}$  is an admissible pair of congruence classes. We define

$$(4.5) \quad a'_n := \sum_{\substack{a, b \in \mathbb{Z} \\ a^2 + b^2 = n \\ a \equiv a_0 \pmod{q_1}}} 3'(b),$$

where

$$(4.6) \quad 3'(b) := \sum_{\substack{c \in \mathbb{Z} \\ c^2 = b \\ c \equiv c_0 \pmod{q_2}}} 1.$$

Let  $g$  be the multiplicative function supported on cubefree integers defined in [FI1, equation (3.16), p. 961] as follows: let  $\chi_4$  denote the character of conductor 4; for  $p \geq 3$  set

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

finally, set  $g(2) = 1/2$  and  $g(4) = 1/4$ . 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 hypotheses (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 4.1) is

$$(4.7) \quad S'(x) := \sum_{\substack{p \leq x \\ p \text{ prime}}} a'_p \log p = c(q_1, q_2) \frac{16\kappa}{\pi} x^{3/4} \left(1 + O\left(\frac{\log \log x}{\log x}\right)\right),$$



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 1.3. Note that the sieve applied to the original sequence  $(a_n)$  from [FI1], with

$$(4.8) \quad a_n = \sum_{\substack{a, b \in \mathbb{Z} \\ a^2 + b^2 = n}} \mathfrak{z}(b),$$

where

$$(4.9) \quad \mathfrak{z}(b) = \sum_{\substack{c \in \mathbb{Z} \\ c^2 = b}} 1,$$

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 [FI1, 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  $a \equiv a_0 \pmod{q_1}$  and  $c \equiv c_0 \pmod{q_2}$  within the set of all primes of the form  $a^2 + c^4$ .

REMARK 4.4. 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  $(a'_n)$  satisfies hypothesis (R) for general  $q_1$  and  $q_2$ . The congruence condition on  $c$  is more difficult to insert into the proof of hypothesis (B), so we prove hypothesis (B) only for the special case where  $q_2 = 4$  and  $c_0 \in \{0, 2\}$ .

**5. Proof of hypothesis (R).** Here we closely follow and refer to the arguments laid out in [FI1, Section 3, pp. 955–962]. Define

$$A'_d(x) := \sum_{\substack{n \leq x \\ n \equiv 0 \pmod{d}}} a'_n \quad \text{and} \quad A'(x) := A'_1(x).$$

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

$$(5.1) \quad r'_d(x) := A'_d(x) - g'(d)A'(x)$$

are small on average. To do this, we will prove an analogue of [FI1, Lemma 3.1, p. 956], with  $M_d(x)$  (representing the *main term* and defined in [FI1, p. 955]) replaced by

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

and  $M'_d(x) = 0$  otherwise; here  $\rho(b; d)$  is defined as in [FI1, p. 955], i.e. it is the number of solutions  $\alpha \pmod d$  to

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

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  $a_0 \pmod{q_1}$  and  $c_0 \pmod{q_2}$  is admissible, and hence  $a'_n$  is supported on  $n$  coprime to  $q$ . The lemma we wish to prove is now identical to [FI1, Lemma 3.1, p. 956].

LEMMA 5.1. *For any  $D \geq 1$ , any  $\varepsilon > 0$ , and any  $x \geq 2$ , we have*

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

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 [FI1, (3.16), p. 961] by

$$(5.2) \quad \begin{cases} h(p)p = 1 + 2(1 + \chi_4(p)), \\ h(p^2)p^2 = p + 2(1 + \chi_4(p)), \end{cases}$$

and define a multiplicative function  $h'$  by setting

$$(5.3) \quad h'(n) = \begin{cases} h(n) & \text{if } (n, q) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then following the same argument as in the proof of [FI1, Lemma 3.4, p. 961], we get

LEMMA 5.2. *For  $d$  cubefree we have*

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

where  $\kappa$  is the integral given in the statement of Proposition 1.3 and the implied constant is absolute.

Combining Lemmas 5.1 and 5.2, we get, as in [FI1, Proposition 3.5, p. 962]:

PROPOSITION 5.3. *Let*

$$a_0 \pmod{q_1}, \quad c_0 \pmod{q_2}$$

be an admissible pair of congruence classes, let  $a'_n$  be defined as in (4.5), and let  $r'_d(x)$  be defined as in (5.1). Then for every  $\varepsilon > 0$  and every  $D \geq 1$ , there exist  $x_0 = x_0(\varepsilon) > 0$  and  $C = C(\varepsilon) > 0$  such that for every  $x \geq x_0$ , we have

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

uniformly for  $t \leq x$ .

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

It remains to prove Lemma 5.1. 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

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

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  $x - y < u < x$ ,

with  $y = D^{1/4}x^{13/16}$  and the implied constants depending only on  $j$  (see [FI1, p. 958]). Since  $a'_n$  is supported on integers of the form  $a^2 + c^4$ , we trivially have

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

where the implied constant depends only on  $\varepsilon$ . With the above choice of  $y$ , it remains to prove Lemma 5.1 with  $A'_d(x)$  replaced by  $A'_d(f)$ .

Similarly to [FI1, p. 958], we write

$$(5.4) \quad A'_d(f) = \sum_b \mathfrak{Z}'(b) \sum_{\substack{\alpha \pmod d \\ \alpha^2 + b^2 \equiv 0 \pmod d}} \sum_{\substack{a \equiv \alpha \pmod d \\ a \equiv a_0 \pmod{q_1}}} f(a^2 + b^2).$$

Since  $(d, q) = 1$ , we have  $(d, q_1) = 1$ , and the two conditions  $a \equiv \alpha \pmod d$  and  $a \equiv a_0 \pmod{q_1}$  can be combined into one condition  $a \equiv \alpha' \pmod{dq_1}$ . 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  $\alpha'$  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

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

Here and henceforth, we use the standard notation

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

Substituting this into (5.4) 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

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

and where

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

is defined exactly as in [FI1, p. 959]. We define  $M'_d(f)$  to be the main term in this expansion, 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 in [FI1, p. 959] shows that

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

where the implied constants depend only on  $\varepsilon$ . It remains to prove Lemma 5.1 with  $A'_d(f)$  in place of  $A'_d(x)$  and with  $M'_d(f)$  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 [FI1, pp. 959–960], we see that it suffices to show an analogue of [FI1, Lemma 3.3, p. 957] for  $\rho'(k, l; d)$ :

LEMMA 5.4. *For any  $D, K$ , and  $L \geq 1$ , for any complex numbers  $\xi(k, l)$ , and for any  $\varepsilon > 0$ , we have*

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

where

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

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

Recall the following inequality from [FI1, (3.6), p. 957]: for any complex numbers  $\alpha_n$  and any  $D, N \geq 1$ , we have

$$(5.5) \quad \sum_{d \leq D} \sum_{\substack{\nu \bmod d \\ \nu^2 + 1 \equiv 0 \bmod d}} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu n}{d}\right) \right| \ll D^{1/2} (D + N)^{1/2} \|\alpha\|,$$

where

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

and the implied constant is absolute. Lemma 5.4 can be proved in the same way as [FI1, Lemma 3.3, p. 957] given the following analogue of inequality (5.5).

LEMMA 5.5. *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*

$$(5.6) \quad \sum_{\substack{d \leq D \\ (d, q_1) = 1}} \sum_{\substack{\nu \bmod d \\ \nu^2 + 1 \equiv 0 \bmod d}} \left| \sum_{n \leq N} \alpha_n e\left(\frac{\nu' n}{dq_1}\right) \right| \leq CD^{1/2} (D + N)^{1/2} \|\alpha\|.$$

Inequality (5.5) is a consequence of a large sieve inequality applied to the rationals  $\nu/d \bmod 1$  with  $\nu$  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  $\nu/d$  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 [Fol]. 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 5.5 to inequality (5.5) as follows.

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

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

where

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

Since  $e(\nu'n_0/(dq_1))$  does not depend on  $m$ , the sum on the left-hand side of (5.6) is

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

Now  $e(\nu'm/d) = e(\nu m/d)$  and

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

so that by (5.5) we get

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

This finishes the proof of (5.5) and thus also the proof of hypothesis (R).

**6. Proof of hypothesis (B).** Many of the upper bound estimations carried out in [FI1, Sections 4 and 5] require no changes since  $0 \leq a'_n \leq a_n$  (compare (4.5) and (4.8)). In most cases, we now sum over fewer non-negative terms.

Recall that we established hypothesis (R) with  $D = x^{3/4-8\epsilon}$ . All of the refinements from [FI1, Section 4, pp. 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 [FI1, Proposition 4.1, p. 963]:

PROPOSITION 6.1. *Let  $c_0 \in \{0, 2\}$ , let  $q_2 = 4$ , and let*

$$a_0 \bmod q_1, \quad c_0 \bmod q_2$$

*be an admissible pair of congruence classes. Define  $\beta(n, C)$  as in (4.3),  $\Pi$  as in (4.4), and  $a'_n$  as in (4.5). Let  $x \geq 3$  and  $\eta, A > 0$ . Let  $P$  be in the range*

$$(6.1) \quad (\log \log x)^2 \leq \log P \leq (\log x)(\log \log x)^{-2}.$$

*Let*

$$(6.2) \quad B = 4A + 2^{20}.$$

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

$$(6.3) \quad x^{1/4+\eta} < N < x^{1/2}(\log x)^{-B},$$

*and for all  $C$  with*

$$(6.4) \quad 1 \leq C \leq N^{1-\eta},$$

we have

$$(6.5) \quad \sum_m \left| \sum_{\substack{N \leq n \leq 2N \\ mn \leq x \\ (n,m\bar{1})=1}} \beta(n, C) a_{mn} \right| \leq A'(x)(\log x)^{5-A}.$$

**6.1. From Propositions 5.3 and 6.1 to Proposition 1.3.** 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

$$a_0 \pmod{q_1}, \quad c_0 \pmod{q_2}$$

is an admissible pair of congruence classes. We apply the asymptotic sieve for primes described in Section 4.1 to the sequence  $(a'_n)$  defined in (4.5). Hypotheses (H1)–(H7) for  $(a'_n)$  are verified in the same way as for  $(a_n)$  defined in (4.8) (see comment at the end of Section 4.2).

Proposition 5.3 implies that  $(a'_n)$  satisfies hypothesis (R) for  $\varepsilon = 1/8000$ ,

$$(6.6) \quad D = x^{3/4-1/1000},$$

which is indeed in the range (4.2), and  $x_r = x_r(\varepsilon)$  large enough.

Applying Proposition 6.1 with the same  $D$  as in (6.6), with  $P$  any number in the range (6.1), with  $A = 5 + 2^{26}$ , and with  $\eta = 1/100$ , 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 (4.7) with  $c(q_1, q_2) = 1/32$ , which proves (1.3).

**6.2. Proof of Proposition 6.1.** Take  $A' = 2A + 2^{20}$  (see [FI1, p. 1018]) and define

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

and

$$(6.7) \quad \theta := (\log x)^{-A'}$$

as in [FI1, p. 965]. We split the sum (6.5) 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 [FI1, (4.14), p. 965]). It then suffices to show Proposition 6.1 with  $\beta(n, C)$  replaced by a smoothed version

$$(6.8) \quad \beta(n) = \beta(n, C) = p(n)\mu(n) \sum_{c|n, c \leq C} \mu(c)$$

and the bound  $\leq A'(x)(\log x)^{5-A}$  replaced by  $\leq C\vartheta\theta A'(x)(\log x)^5$  (see [FI1, (4.17), p. 965]). Moreover, one can split the sum over  $m$  in (6.5) into dyadic

segments  $M \leq m \leq 2M$  with  $M$  satisfying

$$(6.9) \quad \vartheta x \leq MN \leq x.$$

We remark that (6.3) now implies that  $N \leq \vartheta\theta(MN)^{1/2}$ . 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

$$(6.10) \quad \tau(n) \leq \tau := (\log x)^{A+2^{20}}$$

(see [FI1, pp. 963–966, 1018]). For convenience of notation, we also restrict the support of  $\beta(n, C)$  to  $n$  satisfying

$$(6.11) \quad (n, II) = 1,$$

where  $II$  is defined in (4.4). Finally, let  $\alpha(m)$  be any complex numbers supported on  $M < m \leq 2M$  with  $|\alpha(m)| \leq 1$ , and define

$$(6.12) \quad \mathcal{B}'^*(M, N) := \sum_{(m,n)=1} \alpha(m)\beta(n)a'_{mn},$$

where  $\beta(n) = \beta(n, C)$  is defined as in (6.8) (see [FI1, (4.20), p. 966]).

To establish hypothesis (B) it then suffices to prove

LEMMA 6.2. *Let  $\eta, A > 0$  and take  $B$  as in (6.2). Then there exists  $x_0 = x_0(\eta, A) > 0$  such that for all  $x \geq x_0$ , for all  $M$  and  $N$  satisfying (6.3) and (6.9), and for all  $C$  satisfying (6.4) we have*

$$(B') \quad |\mathcal{B}'^*(M, N)| \leq \vartheta\theta(MN)^{3/4}(\log MN)^5.$$

**6.3. Proof of Lemma 6.2.** In [FI1, 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 (4.5), equation [FI1, (5.2), p. 967] now becomes (for  $(m, n) = 1$ )

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

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

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

Recall from (4.6) that the congruence condition  $c \equiv c_0 \pmod{q_2}$  is incorporated into the definition of  $\mathfrak{Z}'$ . We now define  $\alpha_w := \alpha(|w|^2)$  and  $\beta_z := \beta(|z|^2)$  as in [FI1, p. 967], so that (6.12) becomes

$$(6.13) \quad \mathcal{B}'^*(M, N) = \sum_{\substack{(w\bar{w}, z\bar{z})=1 \\ \text{Im } \bar{w}z \equiv a_0 \pmod{q_1}}} \alpha_w \beta_z \mathfrak{Z}'(\text{Re } \bar{w}z).$$

Similarly to [FI1, (5.7), p. 967], we split the sum  $\mathcal{B}'^*(M, N)$  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  $64q_1$ , such that  $z_0 \equiv 1 \pmod{2(1+i)}$ . Now the residue class of  $\text{Im } \bar{w}z$  modulo  $q_1$  is fixed, and so we can eliminate the condition  $\text{Im } \bar{w}z \equiv a_0 \pmod{q_1}$ .

We further modify the support of  $\beta_z$  as in [FI1, equation (5.13), p. 969]. Let  $r(\alpha)$  be a smooth periodic function of period  $2\pi$  supported on  $\varphi < \alpha \leq \varphi + 2\pi\theta$  (where  $\theta$  is as defined in (6.7)) for some  $-\pi < \varphi < \pi$  such that  $r^{(j)} \ll \theta^{-j}$  for  $j = 0, 1, 2$ , and let

$$(6.14) \quad \beta_z = r(\alpha)p(n)\mu(n) \sum_{c|n, c \leq C} \mu(c),$$

where  $\alpha = \arg z$  and  $n = |z|^2$ . Recall that by (6.10) and (6.11),  $\beta_z = 0$  if either  $\tau(|z|^2) > \tau$  or  $|z|^2$  is not coprime to  $\Pi$ . We remove the condition  $(w\bar{w}, z\bar{z}) = 1$  from (6.13) at an acceptable cost as in [FI1, (5.10), p. 968] to get

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

where

$$(6.15) \quad \mathcal{B}'(M, N) := \sum_{\text{Im } \bar{w}z \equiv a_0 \pmod{q_1}} \sum \alpha_w \beta_z \mathfrak{Z}'(\text{Re } \bar{w}z).$$

We then apply Cauchy–Schwarz as in [FI1, (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 [FI1, p. 970]) to get

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

where

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

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

$$(6.16) \quad \mathcal{D}^{*'}(M, N) := \sum_{(z_1, z_2)=1} \sum \beta_{z_1} \bar{\beta}_{z_2} \mathcal{C}'(z_1, z_2),$$

where

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

(see [FI1, (5.26) and (5.27), p. 972]). The coprimality condition was inserted at the cost of

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

(see [FI1, (5.22), p. 972]). Recall that the condition  $c \equiv c_0 \pmod{q_2}$  is hidden in the definition of  $\mathfrak{Z}'$ , while the condition  $a \equiv a_0 \pmod{q_1}$  has been removed by restricting the support of  $\beta_z$ . To prove Lemma 6.2, it now remains to prove

LEMMA 6.3. *Let  $\eta, A > 0$ , and take  $B$  as in (6.2). Then there exists  $x_0 = x_0(\eta, A)$  such that for all  $x \geq x_0$ , for all  $M$  and  $N$  satisfying (6.3) and (6.9), and for all  $C$  satisfying (6.4), we have*

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

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

$$\Delta = \Delta(z_1, z_2) = \text{Im } \bar{z}_1 z_2,$$

which is non-zero whenever  $(z_1, z_2) = 1$  and  $z_1, z_2$  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 [FI1].

The Fourier analysis carried out in [FI1, p. 974] depends on the greatest common divisor of  $\Delta$  and  $q_2$ . Using the Poisson summation formula similarly to [FI1, p. 974], we can now write (6.16) as

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

where

$$(6.17) \quad \mathcal{C}'(z_1, z_2) = (q_2/\delta)^{-2} |z_1 z_2|^{-1/2} \cdot \sum_{h_1} \sum_{h_2} F\left(\frac{h_1}{|\Delta z_2|^{1/2} q_2/\delta}, \frac{h_2}{|\Delta z_1|^{1/2} q_2/\delta}\right) G'(h_1, h_2);$$

the Fourier integral

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

is the same as in [FI1, (6.8), p. 974], and

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

is an arithmetic sum similar to  $G(h_1, h_2)$  defined in [FI1, (6.10), p. 974], but now incorporating the congruence condition  $c \equiv c_0 \pmod{q_2}$ . Here  $\gamma_i'$  is the solution (modulo  $|\Delta| q_2/\delta$ ) to the system of congruences

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

Such a solution is guaranteed to exist because  $\gamma_1 \equiv \gamma_2 \equiv c_0 \pmod{\delta}$ . Note that similarly to [FI1], 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 (6.17). Similarly to the proof of hypothesis (R) above, we do not need to make any changes in the treatment of the Fourier integral; [FI1, Lemmas 7.1, p. 976, and 7.2, p. 977] are still valid (with  $u_1 = h_1|\Delta z_2|^{-1/2}\delta/q_2$  and  $u_2 = h_2|\Delta z_1|^{-1/2}\delta/q_1$  in the case of [FI1, Lemma 7.1]), with the implied constants now depending on  $q_2$  as well. We recall that [FI1, Lemma 7.2] states that for  $z_1$  and  $z_2$  in the support of  $\beta_z$  we have

$$(6.18) \quad F_0(z_1, z_2) := F(0, 0) = 2\hat{f}(0) \log 2|z_1 z_2/\Delta| + O(\Delta^2 M^{1/2} N^{-2} \log N).$$

We now have to give an upper bound for  $G'(h_1, h_2)$  similar to that given in [FI1, 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 [FI1, Lemma 8.4, p. 980]. It is here that we specialize to the case

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

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

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

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

We first prove a lemma analogous to [FI1, Lemma 8.1, p. 978].

LEMMA 6.4. *Fix  $\theta \in \{2, 4\}$  and let*

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

Then

$$(6.19) \quad |G''(h_1, h_2; \theta)| \leq 16\tau_3(\Delta)|\Delta|^{-1}(z_1 h_1^2 - z_2 h_2^2, \Delta).$$

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

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

Proceeding in a similar fashion to [FI1, pp. 977–978], we write

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

with  $\Delta_1$  squarefree. The condition  $\omega_1^2 z_2 \equiv \omega_2^2 z_1 \pmod{|\Delta|/\theta^2}$  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  $d_1 \mid \Delta_1$ ,  $d_2 \mid \Delta_2$ ,  $(d_1, \Delta_2/d_2) = 1$ , and we can make a change of variables  $\omega_i = d_1 d_2 \eta_i$ , where  $\eta_i$  runs over the residue classes modulo  $|\Delta|/\theta d_1 d_2$  and coprime to  $|\Delta|/\theta^2 d_1 d_2^2$ . If we set  $b_1 = \Delta_1/d_1$  and  $b_2 = \Delta_2/d_2$ , the analogue of the equation on top of [FI1, p. 978] becomes

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

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

$$\frac{1}{|\Delta|} \sum_{\substack{b_1 d_1 = |\Delta_1| \\ (d_1, b_2) = 1}} \sum_{\substack{b_2 d_2 = \Delta_2 \\ \theta d_2 \mid (h_1, h_2)}} \theta^2 d_2^2 \sum_{\substack{\eta_1, \eta_2 \pmod{b_1 b_2^2} \\ (\eta_1 \eta_2, b_1 b_2) = 1 \\ \eta_1^2 z_2 \equiv \eta_2^2 z_1 \pmod{b_1 b_2^2}}} e((\eta_1 h_1 + \eta_2 h_2)/\theta b_1 b_2^2 d_2).$$

After the change of variables  $\eta_2 = \omega \eta_1$ , the analogue of [FI1, equation (8.3), p. 978] becomes

$$\frac{1}{|\Delta|} \sum_{\substack{b_1 d_1 = |\Delta_1| \\ (d_1, b_2) = 1}} \sum_{\substack{b_2 d_2 = \Delta_2 \\ \theta d_2 \mid (h_1, h_2)}} \theta^2 d_2^2 \sum_{\omega \equiv z_2/z_1 \pmod{b_1 b_2^2}} R((h_1 + \omega h_2)(\theta d_2)^{-1}; b_1 b_2^2),$$

where  $R(h; b)$  is the classical Ramanujan sum defined in [FI1, p. 978]. Now the same argument as in [FI1, p. 978] yields the desired upper bound (6.19). ■

We turn our attention back to  $G'(h_1, h_2)$ . In case  $c_0 = 0$ , we are in the case of Lemma 6.4 and

$$|G'(h_1, h_2)| = |G''(h_1, h_2; 4)| \leq 16\tau_3(\Delta)|\Delta|^{-1}(z_1 h_1^2 - z_2 h_2^2, \Delta).$$

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  $\Delta \equiv 0 \pmod{16}$ . Hence

$$|G'(h_1, h_2)| \leq 32\tau_3(\Delta)|\Delta|^{-1}(z_1 h_1^2 - z_2 h_2^2, \Delta).$$

The same arguments as in [FI1, Section 9] now suffice to show that the main term in the Fourier expansion indeed comes from  $h_1 = h_2 = 0$ . Specifically,

if we define

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

where

$$(6.20) \quad \mathcal{C}'_0(z_1, z_2) = |z_1 z_2|^{-1/2} F_0(z_1, z_2) G'_0(z_1, z_2),$$

then the reader may easily check that the above estimates yield the following analogue of [FI1, (9.10), p. 983].

LEMMA 6.5. *Let  $\eta, A > 0$ , and take  $B$  as in (6.2). Then there exists  $x_0 = x_0(\eta, A)$  such that for all  $x \geq x_0$ , for all  $M$  and  $N$  satisfying (6.3) and (6.9), and for all  $C$  satisfying (6.4), we have*

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

where  $\tau$  is defined in (6.10).

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 [FI1, p. 979], that

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

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

$$a\gamma_1^2 \equiv \gamma_2^2 \pmod{r}.$$

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

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

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

### 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  $\gamma_1 \equiv \gamma_2 \equiv 0 \pmod{4}$ , 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 [FI1, (8.16), p. 980]. If  $16 \cdot 2^\nu$  with  $\nu \geq 1$  is the exact power of 2 dividing  $\Delta$ , we get

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

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

$$(6.21) \quad G'_0(z_1, z_2) = 2 \sum_{64d|\Delta} \frac{\varphi(d)}{d} \left( \frac{z_2/z_1}{d} \right),$$

by the same reasoning as in [FI1, 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

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

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

$$(6.22) \quad G'_0(z_1, z_2) = 2 \sum_{16d|\Delta} \frac{\varphi(d)}{d} \left( \frac{z_2/z_1}{d} \right) - 2 \sum_{64d|\Delta} \frac{\varphi(d)}{d} \left( \frac{z_2/z_1}{d} \right),$$

which is the analogue of (6.21).

**6.6. End of proof of Lemma 6.3.** We now turn back to estimating  $\mathcal{D}'_0(M, N)$ . As in [FI1, (10.4), p. 985], we can use (6.18) to write

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

where

$$\begin{aligned} T'(\beta) &:= \sum_{(z_1, z_2)=1} \sum \beta_{z_1} \bar{\beta}_{z_2} G'_0(z_1, z_2) \log 2|z_1 z_2 / \Delta|, \\ Y'(\beta) &:= \sum_{(z_1, z_2)=1} \sum |\beta_{z_1} \bar{\beta}_{z_2}| \tau(|z_1|^2) \tau(|z_2|^2) \tau_3(\Delta). \end{aligned}$$

Similarly to [FI1, 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 [FI1, (10.13), p. 986]. If we define

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

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 6.3 now follows from this analogue of [FI1, Proposition 10.2, p. 986]:

LEMMA 6.6. *Fix  $\xi \in \{16, 64\}$ . Let  $\eta, A, \sigma > 0$ , and take  $B$  as in (6.2). 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 (6.3), and for all  $C$  satisfying (6.4), 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 (6.1).

We recall that  $N$  and  $P$  appear as parameters restricting the support of  $\beta_z$ ; see (6.14).

**6.7. Proof of Lemma 6.6: oscillations of characters and symbols.**

Although complicated, the proof of [FI1, Proposition 10.2, p. 986] generalizes directly to the proof of Lemma 6.6. One can check in [FI1, Sections 15–17] that the same arguments are valid when  $\xi = 16$  or  $64$  instead of  $\xi = 4$ . For instance, in [FI1, p. 1005 and p. 1015], one now sums over multiplicative characters of the groups  $(\mathbb{Z}[i]/\xi d\mathbb{Z}[i])^\times$  and  $(\mathbb{Z}[i]/\xi b d\mathbb{Z}[i])^\times$ , respectively.

Moreover, the restriction on the support of  $\beta_z$  to  $z$  in a fixed primary congruence class modulo  $64q_1$  (where  $q_1$  is as in (4.5)) as opposed to modulo  $8$  is handled as in [FI1, 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 [FI1, 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

$$(6.23) \quad S_\chi^k(\beta) = \sum_z \beta_z \chi(z) (z/|z|)^k,$$

where  $\chi$  is a multiplicative character of the group  $(\mathbb{Z}[i]/\xi d\mathbb{Z}[i])^\times$  (see [FI1, (16.14), p. 1005]). The restriction on the support of  $\beta_z$  can be detected by multiplicative characters modulo  $64q_1$ , so that we can simply transform  $\chi$  into a character for the group  $(\mathbb{Z}[i]/64q_1 d\mathbb{Z}[i])^\times$ . The sum (6.23) 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

$$\psi(\mathfrak{a}) := \chi(z)(z/|z|)^k,$$

where  $z$  is the unique primary Gaussian integer which generates  $\mathfrak{a}$ . The dependence on  $\chi$  of the bound given for  $S_\chi^k(\beta)$  is only through the modulus of  $\chi$  (see [FI1, 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

$$(6.24) \quad S_\chi^k(\beta') = \sum_z \beta'_z \chi(z)(z/|z|)^k,$$

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

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

if  $z = r + is$  (see [FI1, (17.8), p. 1014, and (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  $(\mathbb{Z}[i]/64q_1bd\mathbb{Z}[i])^\times$ . Cancellation in the sum (6.24) is now achieved due to the oscillation of the symbol

$$i^{(r-1)/2}(s/|r|)$$

as  $z$  varies over primary Gaussian integers, but again the dependence on  $\chi$  of the bound given for (6.24) is only through the modulus of  $\chi$  (see [FI1, Proposition 17.2, p. 1016]) and this modulus is again different from  $4bd$  by a fixed constant. This shows that Lemma 6.6 follows from [FI1, Proposition 10.2, p. 986], and hence Proposition 6.1 is proved.

**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 Elsholtz, Jan-Hendrik Evertse, John Friedlander, Henryk Iwaniec, Florent Jouve, Hendrik Lenstra, Marco Streng, and the anonymous referee for useful discussions and improvements. Partially supported by an ALGANT Erasmus Mundus Scholarship and by National Science Foundation agreement No. DMS-1128155.

## References

- [BC] P. Barrucand and H. Cohn, *Note on primes of type  $x^2 + 32y^2$ , class number, and residuacity*, J. Reine Angew. Math. 238 (1969), 67–70.
- [CL] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, in: Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math. 1068, Springer, Berlin, 1984, 33–62.



- [CC] H. Cohn and G. Cooke, *Parametric form of an eight class field*, Acta Arith. 30 (1976), 367–377.
- [Fol] É. Fouvry and H. Iwaniec, *Gaussian primes*, Acta Arith. 79 (1997), 249–287.
- [FK] É. Fouvry and J. Klüners, *The parity of the period of the continued fraction of  $\sqrt{d}$* , Proc. London Math. Soc. (3) 101 (2010), 337–391.
- [FI1] J. Friedlander and H. Iwaniec, *The polynomial  $X^2 + Y^4$  captures its primes*, Ann. of Math. (2) 148 (1998), 945–1040.
- [FI2] J. Friedlander and H. Iwaniec, *Asymptotic sieve for primes*, Ann. of Math. (2) 148 (1998), 1041–1065.
- [FI3] J. Friedlander and H. Iwaniec, *Opera de Cribro*, Amer. Math. Soc., Providence, RI, 2010.
- [K] P. Kaplan, *Cycles d'ordre au moins 16 dans le 2-groupe des classes d'idéaux de certains corps quadratiques*, Bull. Soc. Math. France Mém. 49–50 (1977), 113–124.
- [Lag] J. C. Lagarias, *Signatures of units and congruences (mod 4) in certain real quadratic fields. II*, J. Reine Angew. Math. 320 (1980), 115–126.
- [Lan] S. Lang, *Algebra*, 3rd ed., Springer, New York, 2002.
- [LW] P. A. Leonard and K. S. Williams, *On the divisibility of the class numbers of  $Q(\sqrt{-p})$  and  $Q(\sqrt{-2p})$  by 16*, Canad. Math. Bull. 25 (1982), 200–206.
- [Réd] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. 171 (1934), 55–60.
- [Rei] H. Reichardt, *Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. 170 (1934), 75–82.
- [St1] P. Stevenhagen, *Ray class groups and governing fields*, in: Théorie des nombres 1988/89, Publ. Math. Fac. Sci. Besançon, Univ. de Franche-Comté, Besançon, 1989, no. 1, 93 pp.
- [St2] P. Stevenhagen, *Divisibility by 2-powers of certain quadratic class numbers*, J. Number Theory 43 (1993), 1–19.
- [W] 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 (1981), 381–398.

Djordjo Z. Milovic  
Institute for Advanced Study  
1 Einstein Dr.  
Princeton, NJ 08540, U.S.A.  
E-mail: dmilovic@math.ias.edu

