

# *Algebra & Number Theory*

Volume 14

2020

No. 1

The 16-rank of  $\mathbb{Q}(\sqrt{-p})$

Peter Koymans



# The 16-rank of $\mathbb{Q}(\sqrt{-p})$

Peter Koymans

Recently, a density result for the 16-rank of  $\text{Cl}(\mathbb{Q}(\sqrt{-p}))$  was established when  $p$  varies among the prime numbers, assuming a short character sum conjecture. We prove the same density result unconditionally.

## 1. Introduction

If  $K$  is a quadratic number field with narrow class group  $\text{Cl}(K)$ , there is an explicit description of  $\text{Cl}(K)[2]$  due to Gauss. Since then the class group of quadratic number fields has been extensively studied. If one is interested in the 2-part of the class group, i.e.,  $\text{Cl}(K)[2^\infty]$ , the explicit description of  $\text{Cl}(K)[2]$  is often very useful. It is for this reason that our current understanding of the 2-part of the class group is much better than the  $p$ -part for odd  $p$ .

In 1984, Cohen and Lenstra put forward conjectures regarding the average behavior of the class group  $\text{Cl}(K)$  of imaginary and real quadratic fields  $K$ . Despite significant effort, there has been relatively little progress in proving these conjectures. Almost all major results are about the 2-part with the most notable exception being the classical result of Davenport and Heilbronn [1971] regarding the distribution of  $\text{Cl}(K)[3]$ . Very little is known about  $\text{Cl}(K)[p]$  for  $p > 3$ . The nonabelian version of Cohen–Lenstra has recently also attracted great interest; see [Alberts 2016; Alberts and Klys 2016; Klys 2017; Wood 2019].

Gerth [1984] studied the distribution of  $2\text{Cl}(K)[4]$ , when the number of prime factors of the discriminant of  $K$  is fixed. Fouvry and Klüners [2007] computed all the moments of  $2\text{Cl}(K)[4]$ , when  $K$  varies among imaginary or real quadratic fields. In [Fouvry and Klüners 2006], they deduced the probability that the 4-rank of a quadratic field has a given value. Their work was based on earlier ideas of Heath-Brown [1994].

The study of  $\text{Cl}(K)[2^\infty]$  has often been conducted through the lens of *governing fields*. Let  $k \geq 1$  be an integer and let  $d$  be an integer with  $d \not\equiv 2 \pmod{4}$ . For a

---

MSC2010: primary 11R29; secondary 11N45, 11R45.

Keywords: arithmetic statistics, class groups.

finite abelian group  $A$  we define the  $2^k$ -rank of  $A$  to be  $\text{rk}_{2^k} A := \dim_{\mathbb{F}_2} 2^{k-1} A / 2^k A$ . Then a governing field  $M_{d,k}$  is a normal field extension of  $\mathbb{Q}$  such that

$$\text{rk}_{2^k} \text{Cl}(\mathbb{Q}(\sqrt{dp}))$$

is determined by the splitting of  $p$  in  $M_{d,k}$ . Cohn and Lagarias [1983] were the first to define the concept of a governing field, and conjectured that they always exist.

If  $k \leq 3$ , then governing fields are known to exist for all values of  $d$ . In case  $k = 2$  this follows from [Rédei 1934]. Stevenhagen dealt with the case  $k = 3$  [1988]. The topic was recently revisited by Smith [2016], who found a very explicit description for  $M_{d,3}$  for most values of  $d$ . He then used this description to prove density results for  $4\text{Cl}(K)[8]$  assuming GRH. Not much later Smith [2017] introduced *relative governing fields*, which allowed him to prove the most impressive result that  $2\text{Cl}(K)[2^\infty]$  has the expected distribution when  $K$  varies among all imaginary quadratic fields.

If we let  $P(d, k)$  be the statement that a governing field  $M_{d,k}$  exists, then there is currently not a single value of  $d$  for which the truth or falsehood of  $P(d, 4)$  is known. This has been the most significant obstruction in proving density results for the 16-rank in thin families of the shape  $\{\mathbb{Q}(\sqrt{dp})\}_p$  prime.

This barrier was first broken by Milovic [2017a], who dealt with the 16-rank in the family  $\{\mathbb{Q}(\sqrt{-2p})\}_{p \equiv -1 \pmod{4}}$ . Milovic proves his density result with Vinogradov's method, and does not rely on the existence of a governing field. His use of Vinogradov's method was inspired by work of Friedlander et al. [2013], which is based on earlier work of Friedlander and Iwaniec [1998].

Density results for the families  $\{\mathbb{Q}(\sqrt{-2p})\}_{p \equiv 1 \pmod{4}}$  and  $\{\mathbb{Q}(\sqrt{-p})\}_p$  were established by Milovic and the author; see respectively [Koymans and Milovic 2019a; 2019b] with the latter work being conditional on a short character sum conjecture. Both of these works follow the ideas of [Friedlander et al. 2013] closely in their treatment of the sums of type I; see Section 3 for a definition. However, if one applies the method of [Friedlander et al. 2013] to a number field of degree  $n$ , one is naturally led to consider character sums of modulus  $q$  and length  $q^{1/n}$ .

In [Koymans and Milovic 2019a] we apply the method from [Friedlander et al. 2013] to a number field of degree 4. This leads to character sums just outside the range of the Burgess bound. Fortunately, the lemmas in Section 3.2 of [Koymans and Milovic 2019a] allow us to reduce the size of the modulus from  $q$  to  $q^{1/2}$ , and this enables us to deal with the sums of type I unconditionally. In [Koymans and Milovic 2019b] we use a criterion for the 16-rank of  $\mathbb{Q}(\sqrt{-p})$  due to [Bruin and Hemenway 2013], and this criterion is stated most naturally over  $\mathbb{Q}(\xi_8, \sqrt{1+i})$ , which has degree 8. The resulting character sums are far outside the reach of the Burgess bound and we resort to assuming a short character sum conjecture; see [Koymans and Milovic 2019b, p. 8].

In this paper we manage to deal with the 16-rank of  $\mathbb{Q}(\sqrt{-p})$  unconditionally by using a criterion of Leonard and Williams [1982], which one can naturally state over  $\mathbb{Q}(\zeta_8)$ . However, the Leonard–Williams criterion has the significant downside that it is the product of two residue symbols instead of one residue symbol, namely a quadratic and a quartic residue symbol. The resulting sums of type I can still not be treated unconditionally with the method from [Friedlander et al. 2013]. Instead, we use a rather ad hoc argument to deal with the resulting character sum.

**Theorem 1.1.** *Let  $h(-p)$  be the class number of  $\mathbb{Q}(\sqrt{-p})$ . Then*

$$\lim_{X \rightarrow \infty} \frac{|\{p \text{ prime} : p \leq X \text{ and } 16 \mid h(-p)\}|}{|\{p \text{ prime} : p \leq X\}|} = \frac{1}{16}.$$

Milovic [2017b] has previously shown that there are infinitely many primes  $p$  with 16 dividing  $h(-p)$ . Theorem 1.1 gives an affirmative answer to conjectures in both [Cohn and Lagarias 1984] and [Stevenhagen 1993]. For  $p$  a prime number, we define  $e_p$  by

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

Theorem 1.1 is an immediate consequence of the following theorem.

**Theorem 1.2.** *We have*

$$\sum_{p \leq X} e_p \ll \frac{X}{\exp((\log X)^{0.1})}.$$

It is natural to wonder if the other conditional results in [Koymans and Milovic 2019b] can be proven unconditionally using the methods from this paper. This is likely to be the case, but it would require some effort to obtain suitable algebraic results similar to the Leonard–Williams criterion [1982] used in this paper.

We believe that the ideas introduced by Smith [2017] do not apply to the thin families that we deal with here. Indeed, in Smith’s paper a crucial ingredient for both the algebraic and analytic part is the fact that a typical integer  $N$  has roughly  $\log \log N$  prime divisors and that  $\log \log N$  goes to infinity as  $N$  goes to infinity.

## 2. Preliminaries

**Quadratic and quartic reciprocity.** Let  $K$  be a number field with ring of integers  $O_K$ . We say that an ideal  $\mathfrak{n}$  of  $O_K$  is odd if  $(\mathfrak{n}, 2) = (1)$ . Similarly, we say that an element  $w$  of  $O_K$  is odd if the ideal generated by  $w$  is odd. If  $\mathfrak{p}$  is an odd prime ideal of  $O_K$  and  $\alpha \in O_K$ , we define the quadratic residue symbol

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{2,K} := \begin{cases} 1 & \text{if } \alpha \notin \mathfrak{p} \text{ and } \alpha \equiv \beta^2 \pmod{\mathfrak{p}} \text{ for some } \beta \in O_K, \\ -1 & \text{if } \alpha \notin \mathfrak{p} \text{ and } \alpha \not\equiv \beta^2 \pmod{\mathfrak{p}} \text{ for all } \beta \in O_K, \\ 0 & \text{if } \alpha \in \mathfrak{p}. \end{cases}$$

Then Euler's criterion states

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{2,K} \equiv \alpha^{\frac{1}{2}(N(\mathfrak{p})-1)} \pmod{\mathfrak{p}}.$$

For a general odd ideal  $\mathfrak{n}$  of  $O_K$ , we define

$$\left(\frac{\alpha}{\mathfrak{n}}\right)_{2,K} := \prod_{\mathfrak{p}^e \parallel \mathfrak{n}} \left(\left(\frac{\alpha}{\mathfrak{p}}\right)_{2,K}\right)^e.$$

Furthermore, for odd  $\beta \in O_K$  we set

$$\left(\frac{\alpha}{\beta}\right)_{2,K} := \left(\frac{\alpha}{(\beta)}\right)_{2,K}.$$

We say that an element  $\alpha \in K$  is totally positive if for all embeddings  $\sigma$  of  $K$  into  $\mathbb{R}$  we have  $\sigma(\alpha) > 0$ . In particular, all elements of a totally complex number field are totally positive. We will make extensive use of the law of quadratic reciprocity.

**Theorem 2.1.** *Let  $\alpha, \beta \in O_K$  be odd. If  $\alpha$  or  $\beta$  is totally positive, we have*

$$\left(\frac{\alpha}{\beta}\right)_{2,K} = \mu(\alpha, \beta) \left(\frac{\beta}{\alpha}\right)_{2,K},$$

where  $\mu(\alpha, \beta) \in \{\pm 1\}$  depends only on the congruence classes of  $\alpha$  and  $\beta$  modulo 8.

*Proof.* This follows from Lemma 2.1 of [\[Friedlander et al. 2013\]](#). □

If  $K = \mathbb{Q}$ , we shall drop the subscript. In this case the symbol

$$\left(\frac{\cdot}{\cdot}\right)$$

is to be interpreted as the Kronecker symbol, which is an extension of the quadratic residue symbol to allow for even arguments in the bottom. We presume that the reader is familiar with the quadratic reciprocity law for the Kronecker symbol. Now let  $K$  be a number field containing  $\mathbb{Q}(i)$  still with ring of integers  $O_K$ . For  $\alpha \in O_K$  and  $\mathfrak{p}$  an odd prime ideal of  $O_K$ , we define the quartic residue symbol  $(\alpha/\mathfrak{p})_{4,K}$  to be the unique element in  $\{\pm 1, \pm i, 0\}$  such that

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{4,K} \equiv \alpha^{\frac{1}{4}(N(\mathfrak{p})-1)} \pmod{\mathfrak{p}}.$$

We extend the quartic residue symbol to all odd ideals  $\mathfrak{n}$  and then to all odd elements  $\beta$  in the same way as the quadratic residue symbol. Then we have the following theorem.

**Theorem 2.2.** *Let  $\alpha, \beta \in \mathbb{Z}[\zeta_8]$  with  $\beta$  odd. Then for fixed  $\alpha$ , the symbol  $(\alpha/\beta)_{4, \mathbb{Q}(\zeta_8)}$  depends only on  $\beta$  modulo  $16\alpha\mathbb{Z}[\zeta_8]$ . Furthermore, if  $\alpha$  is also odd, we have*

$$\left(\frac{\alpha}{\beta}\right)_{4, \mathbb{Q}(\zeta_8)} = \mu(\alpha, \beta) \left(\frac{\beta}{\alpha}\right)_{4, \mathbb{Q}(\zeta_8)},$$

where  $\mu(\alpha, \beta) \in \{\pm 1, \pm i\}$  depends only on the congruence classes of  $\alpha$  and  $\beta$  modulo 16.

*Proof.* Use Proposition 6.11 of [Lemmermeyer 2000, p. 199].  $\square$

**A fundamental domain.** Let  $F$  be a number field of degree  $n$  over  $\mathbb{Q}$  and let  $O_F$  be its ring of integers. Suppose that  $F$  has  $r$  real embeddings and  $s$  pairs of conjugate complex embeddings so that  $r + 2s = n$ . Define  $T$  to be the torsion subgroup of  $O_F^*$ . Then, by Dirichlet's unit theorem, there exists a free abelian group  $V \subseteq O_F^*$  of rank  $r + s - 1$  with  $O_F^* = T \times V$ . Fix one choice of such a  $V$ .

There is a natural action of  $V$  on  $O_F$ . The goal of this subsection is to construct a fundamental domain  $\mathcal{D}$  for this action. Such a fundamental domain allows us to transform a sum over ideals into a sum over elements. It will be important that the resulting fundamental domain has nice geometrical properties, so that we have good control over the elements we are summing.

Fix an integral basis  $\omega_1, \dots, \omega_n$  for  $O_F$ . We view  $\omega_1, \dots, \omega_n$  as an ordered list and write  $\omega$  for this ordered list. Then we get an isomorphism of  $\mathbb{Q}$ -vector spaces  $i_\omega : \mathbb{Q}^n \rightarrow F$ , where  $i_\omega$  is given by  $(a_1, \dots, a_n) \mapsto a_1\omega_1 + \dots + a_n\omega_n$ . For a subset  $S \subseteq \mathbb{R}^n$  and an element  $\alpha \in F$ , we will say that  $\alpha \in S$  if  $i_\omega^{-1}(\alpha) \in S$ . Define for our integral basis  $\omega$  and a real number  $X > 0$

$$B(X, \omega) := \left\{ (x_1, \dots, x_n) \in \mathbb{R}^n : \left| \prod_{i=1}^n (x_i \sigma_i(\omega_1) + \dots + x_n \sigma_i(\omega_n)) \right| \leq X \right\},$$

where  $\sigma_1, \dots, \sigma_n$  are the embeddings of  $F$  into  $\mathbb{C}$ .

**Lemma 2.3.** *Let  $F$  be a number field with ring of integers  $O_F$  and integral basis  $\omega = \{\omega_1, \dots, \omega_n\}$ . Choose a splitting  $O_F^* = T \times V$ , where  $T$  is the torsion subgroup of  $O_F^*$ . There exists a subset  $\mathcal{D} \subseteq \mathbb{R}^n$  such that:*

- (i) *For all  $\alpha \in O_F \setminus \{0\}$ , there exists a unique  $v \in V$  such that  $v\alpha \in \mathcal{D}$ . Furthermore, we have the equality*

$$\{u \in O_F^* : u\alpha \in \mathcal{D}\} = \{tv : t \in T\}.$$

- (ii)  *$\mathcal{D} \cap B(1, \omega)$  has an  $(n-1)$ -Lipschitz parametrizable boundary.*
- (iii) *There is a constant  $C(\omega)$  depending only on  $\omega$  such that for all  $\alpha \in \mathcal{D}$  we have  $|a_i| \leq C(\omega) \cdot |\mathcal{N}(\alpha)|^{\frac{1}{n}}$ , where  $a_i \in \mathbb{Z}$  are such that  $\alpha = a_1\omega_1 + \dots + a_n\omega_n$ .*

*Proof.* This is Lemma 3.5 of [Koymans and Milovic 2019a].  $\square$

We will use [Lemma 2.3](#) for  $F := \mathbb{Q}(\zeta_8)$ ; in order to do so we must make some choices. We choose  $V := \langle 1 + \sqrt{2} \rangle$  and integral basis  $\omega := \{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$ . The resulting fundamental domain will be called  $\mathcal{D}$ , and we define  $\mathcal{D}(X) := \mathcal{D} \cap \mathcal{B}(X, \omega)$ .

### 3. The sieve

Let  $\{a_p\}$  be a sequence of complex numbers indexed by the primes and define

$$S(X) := \sum_{p \leq X} a_p.$$

To prove our main theorem, we must prove oscillation of  $S(X)$  for the specific sequence  $\{e_p\}$  defined in (1-1). There are relatively few methods that can deal with such sums. The most common approach is to attach an  $L$ -function and then use the zero-free region. This approach requires that our sequence  $\{e_p\}$  has good multiplicative properties. It turns out that  $\{e_p\}$  is instead twisted multiplicative (see [Lemmas 6.1](#) and [6.3](#)), and this suggests we use Vinogradov's method instead.

Recall that  $h(-p)$  denotes the class number of  $\text{Cl}(\mathbb{Q}(\sqrt{-p}))$ . By definition of  $e_p$  we have  $e_p = 0$  if and only if  $8 \nmid h(-p)$ . It is well-known that  $\mathbb{Q}(\zeta_8, \sqrt{1+i})$  is a *governing field* for the 8-rank of  $\text{Cl}(\mathbb{Q}(\sqrt{-p}))$ , in fact a prime  $p$  splits completely in  $\mathbb{Q}(\zeta_8, \sqrt{1+i})$  if and only if  $8 \mid h(-p)$ . This is extremely convenient. Indeed, if we apply Vinogradov's method to our governing field, primes of degree 1 will give the dominant contribution and these primes automatically have  $e_p \neq 0$ .

Unfortunately,  $\mathbb{Q}(\zeta_8, \sqrt{1+i})$  is a field of degree 8, which is simply too large to make our analytic methods work unconditionally. Indeed, using the same approach for the sums of type I as in [\[Friedlander et al. 2013\]](#), one ends up with short character sums of modulus  $q$  and length roughly  $q^{1/8}$ , which is far outside the reach of the Burgess bound. However, assuming a short character sum conjecture, one still obtains the desired oscillation and this is the approach taken in [\[Koymans and Milovic 2019b\]](#). Instead we work over  $\mathbb{Q}(\zeta_8)$ ; fortunately,  $\mathbb{Q}(\zeta_8, \sqrt{1+i})$  is an abelian extension of  $\mathbb{Q}(\zeta_8)$ , which implies that the splitting of a prime  $\mathfrak{p}$  of  $\mathbb{Q}(\zeta_8)$  in the extension  $\mathbb{Q}(\zeta_8, \sqrt{1+i})/\mathbb{Q}(\zeta_8)$  is determined by a congruence condition. Such a congruence condition can easily be incorporated in Vinogradov's method.

We will follow Section 5 of [\[Friedlander et al. 2013\]](#), which adapted Vinogradov's method to number fields. Let  $F$  be a number field. Define for a nonzero ideal  $\mathfrak{n}$  of  $\mathcal{O}_F$

$$\Lambda(\mathfrak{n}) := \begin{cases} \log N\mathfrak{p} & \text{if } \mathfrak{n} = \mathfrak{p}^l, \\ 0 & \text{otherwise.} \end{cases}$$

and suppose that we want to prove oscillation of

$$S(X) := \sum_{N\mathfrak{n} \leq X} a_{\mathfrak{n}} \Lambda(\mathfrak{n}),$$

where  $a_{\mathfrak{n}}$  is of absolute value at most 1. The power of Vinogradov's method lies in

the fact that one does not have to deal with  $S(X)$  directly. Instead one has to prove cancellations of

$$A(X, \mathfrak{d}) := \sum_{\substack{Nn \leq X \\ \mathfrak{d}|n}} a_n,$$

which are traditionally called sums of type I or linear sums, and

$$B(M, N) := \sum_{Nm \leq M} \sum_{Nn \leq N} \alpha_m \beta_n a_{mn},$$

which are traditionally called sums of type II or bilinear sums. It is important to remark that  $S(X)$  depends only on  $a_n$  with  $n$  a prime power, while  $A(X, \mathfrak{d})$  and  $B(M, N)$  certainly do not. This gives a substantial amount of flexibility, since we may define  $a_n$  on composite ideals  $n$  in any way we like provided that we can prove oscillation of  $A(X, \mathfrak{d})$  and  $B(M, N)$ . Constructing a suitable sequence  $a_n$  will be the goal of [Section 4](#). We are now ready to state the precise version of Vinogradov's method we are going to use.

**Proposition 3.1.** *Let  $F$  be a number field and let  $a_n$  be a sequence of complex numbers, indexed by the ideals of  $O_F$ , with  $|a_n| \leq 1$ . If  $0 < \theta_1, \theta_2 < 1$  and  $\theta_3 > 0$  are such that*

- we have for all ideals  $\mathfrak{d}$  of  $O_F$

$$A(X, \mathfrak{d}) \ll_{F, a_n, \theta_1} \frac{X}{\exp((\log X)^{\theta_1})}; \quad (3-1)$$

- we have for all sequences of complex numbers  $\{\alpha_m\}$  and  $\{\beta_n\}$  of absolute value at most 1

$$B(M, N) \ll_{F, a_n, \theta_2} (M + N)^{\theta_2} (MN)^{1-\theta_2} (\log MN)^{\theta_3}, \quad (3-2)$$

then we have for all  $c < \theta_1$

$$S(X) \ll_{c, F, a_n, \theta_1, \theta_2, \theta_3} \frac{X}{\exp((\log X)^c)}.$$

*Proof.* This quickly follows from Proposition 5.1 of [[Friedlander et al. 2013](#)] with  $y := \exp((\log X)^{\frac{1}{2}(c+\theta_1)})$ .  $\square$

The remainder of this paper is devoted to the three major tasks that are left. We start by constructing a suitable sequence  $a_n$  in [Section 4](#) to which we will apply [Proposition 3.1](#) with  $F = \mathbb{Q}(\zeta_8)$ . The main result of [Section 5](#) is [Proposition 5.1](#), which proves (3-1) for  $\theta_1 = 0.2$ . Finally, we prove in [Section 6](#) that (3-2) holds with  $\theta_2 = \frac{1}{24}$ ; this is the content of [Proposition 6.6](#). Once we have proven [Propositions 5.1](#) and [6.6](#), the proof of [Theorem 1.2](#) is complete.

#### 4. Definition of the sequence

By Gauss genus theory we know that the 2-part of  $\text{Cl}(\mathbb{Q}(\sqrt{-p}))$  is cyclic, and the 2-part of  $\text{Cl}(\mathbb{Q}(\sqrt{-p}))$  is trivial if and only if  $p \equiv 3 \pmod{4}$ . Let us recall a criterion for  $16 \mid h(-p)$  due to Leonard and Williams [1982]. We have

$$4 \mid h(-p) \iff p \equiv 1 \pmod{8}.$$

Now suppose that  $4 \mid h(-p)$ . There exist positive integers  $g$  and  $h$  satisfying

$$p = 2g^2 - h^2.$$

Then a classical result of Hasse [1969] is

$$8 \mid h(-p) \iff \left(\frac{g}{p}\right) = 1 \text{ and } p \equiv 1 \pmod{8}$$

or equivalently

$$8 \mid h(-p) \iff \left(\frac{-1}{g}\right) = 1 \text{ and } p \equiv 1 \pmod{8}.$$

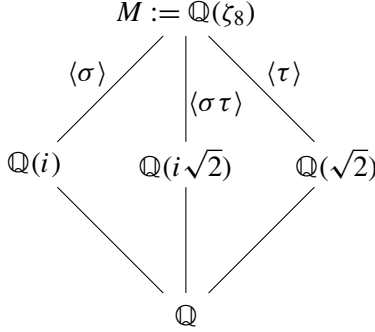
We are now ready to state the result of Leonard and Williams [1982]. If  $p$  is a prime number with  $8 \mid h(-p)$ , we have

$$16 \mid h(-p) \iff \left(\frac{g}{p}\right)_4 \left(\frac{2h}{g}\right) = 1.$$

With this in mind, we are going to define a sequence  $\{a_n\}$ , indexed by the integral ideals of  $\mathbb{Z}[\zeta_8]$ , such that for all unramified prime ideals  $\mathfrak{p}$  in  $\mathbb{Z}[\zeta_8]$  of norm  $p$

$$a_{\mathfrak{p}} = \begin{cases} 1 & \text{if } 16 \mid h(-p), \\ -1 & \text{if } 8 \mid h(-p), 16 \nmid h(-p), \\ 0 & \text{otherwise.} \end{cases} \quad (4-1)$$

The sequence  $\{a_n\}$  will be constructed in such a way that we can prove the two estimates in Propositions 5.1 and 6.6. Before we move on, it will be useful to recall some standard facts about  $\mathbb{Z}[\zeta_8]$ . The ring  $\mathbb{Z}[\zeta_8]$  is a PID with unit group generated by  $\zeta_8$  and  $\epsilon := 1 + \sqrt{2}$ . Odd primes are unramified in  $\mathbb{Z}[\zeta_8]$ , while 2 is totally ramified. Furthermore, an odd prime  $p$  splits completely in  $\mathbb{Z}[\zeta_8]$  if and only if  $p \equiv 1 \pmod{8}$  if and only if  $4 \mid h(-p)$ . We will make extensive use of the following field diagram.



If  $n$  is not odd, we set  $a_n := 0$ . From now on  $n$  is an odd, integral, nonzero ideal of  $\mathbb{Z}[\zeta_8]$  and  $w$  is a generator of  $\mathfrak{n}$ . We can write  $w$  as

$$w = a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3$$

for certain  $a, b, c, d \in \mathbb{Z}$ . Define  $u, v \in \mathbb{Z}$  by

$$w\tau(w) = u + v\sqrt{2}.$$

We can explicitly compute  $u$  and  $v$  using the formulas

$$u = \frac{w\tau(w) + \sigma(w)\sigma\tau(w)}{2} = a^2 + b^2 + c^2 + d^2, \quad (4-2)$$

$$v = \frac{w\tau(w) - \sigma(w)\sigma\tau(w)}{2\sqrt{2}} = ab - ad + bc + cd. \quad (4-3)$$

Since  $w$  is odd, it follows that  $Nw \equiv 1 \pmod{8}$ . Then it follows from

$$Nw = u^2 - 2v^2$$

that  $u$  is an odd integer and  $v$  is an even integer. Set

$$g := u + v, \quad h := u + 2v,$$

so that  $g$  is an odd integer and  $h$  is an odd integer, not necessarily positive. We claim that  $g$  is positive. Indeed

$$\begin{aligned}
 g &= a^2 + b^2 + c^2 + d^2 + ab - ad + bc + cd \\
 &= \frac{1}{2}(a+b)^2 + \frac{1}{2}(a-d)^2 + \frac{1}{2}(b+c)^2 + \frac{1}{2}(c+d)^2 > 0.
 \end{aligned}$$

By construction  $g$  and  $h$  satisfy

$$Nw = 2g^2 - h^2.$$

We start by showing that the value of

$$\left(\frac{-1}{g}\right) \quad (4-4)$$

does not depend on the choice of generator  $w$  of our ideal  $\mathfrak{n}$ .

**Lemma 4.1.** *Let  $\mathfrak{n}$  be an odd, integral ideal of  $\mathbb{Z}[\zeta_8]$ . Then the value of (4-4) is the same for all generators  $w$  of  $\mathfrak{n}$ .*

*Proof.* Suppose that we replace  $w$  by  $\zeta_8 w$ . Because  $\zeta_8 \tau(\zeta_8) = 1$ , it follows that  $u$  and  $v$ , hence also  $g$ , do not change. Suppose instead that we replace  $w$  by  $\epsilon w$ . In this case  $u$  becomes  $3u + 4v$  and  $v$  becomes  $2u + 3v$ , so  $g$  becomes  $5u + 7v$ . Hence our lemma boils down to

$$\left(\frac{-1}{u+v}\right) = \left(\frac{-1}{5u+7v}\right),$$

which holds if and only if

$$u + v \equiv 5u + 7v \pmod{4}.$$

But recall that  $v$  is even by our assumption that  $w$  is odd. □

We define for odd  $w \in \mathbb{Z}[\zeta_8]$  the following symbol:

$$[w] := \left(\frac{g}{w}\right)_{4,M} \left(\frac{2h}{g}\right),$$

where we remind the reader that  $M$  is defined to be  $\mathbb{Q}(\zeta_8)$ . We express this as

$$[w] = [w]_1 [w]_2, \quad [w]_1 := \left(\frac{g}{w}\right)_{4,M}, \quad [w]_2 := \left(\frac{2h}{g}\right). \quad (4-5)$$

It is easily checked that  $[\zeta_8 w] = [w]$ . Unfortunately, it is not always true that  $[\epsilon w] = [w]$ . To get around this, we need the following lemma.

**Lemma 4.2.** *We have for all odd  $w$*

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

*Proof.* We have for any odd  $w$

$$[w]_1 = \left(\frac{g}{w}\right)_{4,M} = \left(\frac{u+v}{w}\right)_{4,M} = \left(\frac{\left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)\sigma(w)\sigma\tau(w)}{w}\right)_{4,M}, \quad (4-6)$$

where we use the explicit formulas for  $u$  and  $v$ , see (4-2) and (4-3), in terms of  $w$ .

From this expression it quickly follows that  $[\epsilon^2 w]_1 = [w]_1$ . We also have

$$\begin{aligned} [w]_2 &= \left(\frac{2h}{g}\right) = \left(\frac{2u+4v}{u+v}\right) = \left(\frac{2}{u+v}\right) \left(\frac{v}{u+v}\right) \\ &= \left(\frac{2}{u+v}\right) \left(\frac{-u}{u+v}\right) = \left(\frac{-2}{u+v}\right) \left(\frac{v}{u}\right) (-1)^{\frac{1}{2}(u-1) \cdot \frac{1}{2}(u+v-1)}. \end{aligned} \quad (4-7)$$

A straightforward computation shows that the  $u$  and  $v$  associated to  $\epsilon^4 w$  are respectively  $u_1 := 577u + 816v$  and  $v_1 := 408u + 577v$ . Then we have

$$\left(\frac{v}{u}\right) = \left(\frac{408u+577v}{577u+816v}\right) = \left(\frac{v_1}{u_1}\right) \quad (4-8)$$

due to Proposition 2 in [Milovic 2017a]. It will be useful to observe that the following congruences hold true:

$$u \equiv u_1 \pmod{8}, \quad v \equiv v_1 \pmod{8}.$$

This immediately implies

$$\left(\frac{-2}{u+v}\right) = \left(\frac{-2}{u_1+v_1}\right), \quad (4-9)$$

and therefore the lemma.  $\square$

With this out of the way, we have all the tools necessary to define  $a_n$ . Suppose that  $\mathfrak{n}$  is an odd, integral ideal of  $\mathbb{Z}[\zeta_8]$  with generator  $w$ . Then we define

$$a_n := \begin{cases} \frac{1}{4}([w] + [\epsilon w] + [\epsilon^2 w] + [\epsilon^3 w]) & \text{if } w \text{ satisfies (4-4),} \\ 0 & \text{otherwise.} \end{cases} \quad (4-10)$$

for any generator  $w$  of  $\mathfrak{n}$ . Here we say that  $w$  satisfies (4-4) if  $(-1/g) = 1$ , where  $g$  is defined in terms of  $w$  as above. Then an application of Lemmas 4.1 and 4.2 shows that (4-10) is indeed well-defined.

**Lemma 4.3.** *The sequence  $a_n$  satisfies (4-1) for all unramified prime ideals  $\mathfrak{p}$  of degree 1 in  $\mathbb{Z}[\zeta_8]$ .*

*Proof.* Let  $\mathfrak{p}$  be an unramified prime ideal of degree 1 in  $\mathbb{Z}[\zeta_8]$  and let  $w$  be a generator of  $\mathfrak{p}$ . Put  $p := Nw$ . Lemma 4.1 and the aforementioned result of Hasse imply

$$w \text{ does not satisfy (4-4)} \iff 8 \nmid h(-p),$$

and  $a_{\mathfrak{p}}$  is indeed 0 in this case. Now suppose that  $w$  does satisfy (4-4). Recall that

$$[w] = \left(\frac{g}{w}\right)_{4,M} \left(\frac{2h}{g}\right),$$

where  $g$  and  $h$  are explicit functions of  $w$ . We stress that these  $g$  and  $h$  are not necessarily the same  $g$  and  $h$  from Leonard and Williams. Indeed, Leonard and

Williams require  $g$  and  $h$  to be positive, while our  $h$  is not necessarily positive. However, since  $w$  satisfies (4-4), their criterion remains valid irrespective of the sign of  $h$ . Then, the criterion implies

$$[w] = [\epsilon w] = [\epsilon^2 w] = [\epsilon^3 w].$$

Furthermore, the criterion also shows that

$$[w] = 1 \iff 16 \mid h(-p).$$

This completes the proof of our lemma. □

### 5. Sums of type I

The goal of this section is to bound the sum

$$A(X, \mathfrak{d}) = \sum_{\substack{Nn \leq X \\ \mathfrak{d} \mid n}} a_n = \sum_{\substack{Nn \leq X \\ \mathfrak{d} \mid n, n \text{ odd}}} a_n.$$

By picking a generator for  $n$  we obtain

$$A(X, \mathfrak{d}) = \frac{1}{8} \sum_{\substack{w \in \mathcal{D}(X) \\ w \equiv 0 \pmod{\mathfrak{d}} \\ w \text{ odd}}} a_{(w)} = \frac{1}{32} \sum_{\substack{w \in \mathcal{D}(X) \\ w \equiv 0 \pmod{\mathfrak{d}} \\ w \text{ odd}}} \mathbf{1}_{w \text{ sat. (4-4)}} ([w] + [\epsilon w] + [\epsilon^2 w] + [\epsilon^3 w]).$$

We define for  $i = 0, \dots, 3$  and  $\rho$  an invertible congruence class modulo  $2^{10}$

$$A(X, \mathfrak{d}, u_i, \rho) := \sum_{\substack{w \in u_i \mathcal{D}(X) \\ w \equiv 0 \pmod{\mathfrak{d}} \\ w \equiv \rho \pmod{2^{10}}}} [w] = \sum_{\substack{w \in u_i \mathcal{D}(X) \\ w \equiv 0 \pmod{\mathfrak{d}} \\ w \equiv \rho \pmod{2^{10}}}} \left(\frac{g}{w}\right)_{4, M} \left(\frac{2h}{g}\right),$$

where  $u_i := \epsilon^i$ . With this definition in place, we may split  $A(X, \mathfrak{d})$  as follows

$$A(X, \mathfrak{d}) = \frac{1}{32} \sum_{i=0}^3 \sum_{\rho \in (O_M/2^{10} O_M)^*} \mathbf{1}_{\rho \text{ sat. (4-4)}} A(X, \mathfrak{d}, u_i, \rho),$$

since the truth of (4-4) depends only on  $w$  modulo 4. Then it is enough to bound each individual sum  $A(X, \mathfrak{d}, u_i, \rho)$ . In order to bound this sum, our first step is to carefully rewrite the symbol  $[w]$  in a more tractable form. While doing so, we will find some hidden cancellation between  $[w]_1$  and  $[w]_2$  that is vital for making our results unconditional.

Throughout this section we use the convention that  $\mu(\cdot) \in \{\pm 1, \pm i\}$  is a function depending only on the variables between the parentheses; at each occurrence  $\mu(\cdot)$  may be a different function. Since our cancellation will come from fixing  $b, c$  and  $d$

while varying  $a$ , factors of the shape  $\mu(\rho, b, c, d)$  will present no issues for us. Let us start by rewriting  $[w]_2$ . It follows from (4-7) that

$$\left(\frac{2h}{g}\right) = \left(\frac{v}{u}\right)\mu(\rho). \quad (5-1)$$

Using the formulas for  $u$  and  $v$  we get

$$\left(\frac{v}{u}\right) = \left(\frac{ab - ad + bc + cd}{a^2 + b^2 + c^2 + d^2}\right). \quad (5-2)$$

If  $v$  is not zero, we can uniquely factor  $v$  as

$$v := v_1 v_2 t, \quad (5-3)$$

where  $v_1$  is an odd, positive integer satisfying  $\gcd(v_1, b - d) = 1$ ,  $v_2$  is an odd integer consisting only of primes dividing  $b - d$  and  $t$  is positive and only divisible by powers of 2. Then we have

$$\left(\frac{ab - ad + bc + cd}{a^2 + b^2 + c^2 + d^2}\right) = \left(\frac{v_1}{a^2 + b^2 + c^2 + d^2}\right) \left(\frac{t v_2}{a^2 + b^2 + c^2 + d^2}\right). \quad (5-4)$$

Let  $\rho'$  be the congruence class of  $v_1$  modulo 8. Using the following identity modulo  $v$

$$a^2(b - d)^2 \equiv c^2(b + d)^2 \pmod{v}$$

and the fact that this identity continues to hold for any divisor of  $v$ , in particular for  $v_1$ , we rewrite the first factor of (5-4) as follows

$$\begin{aligned} \left(\frac{v_1}{a^2 + b^2 + c^2 + d^2}\right) &= \mu(\rho, \rho') \left(\frac{a^2 + b^2 + c^2 + d^2}{v_1}\right) \\ &= \mu(\rho, \rho') \left(\frac{(a^2 + b^2 + c^2 + d^2)(b - d)^2}{v_1}\right) \\ &= \mu(\rho, \rho') \left(\frac{a^2(b - d)^2 + (b^2 + c^2 + d^2)(b - d)^2}{v_1}\right) \\ &= \mu(\rho, \rho') \left(\frac{c^2(b + d)^2 + (b^2 + c^2 + d^2)(b - d)^2}{v_1}\right) \\ &= \mu(\rho, \rho') \left(\frac{(b^2 + d^2)(2c^2 + (b - d)^2)}{v_1}\right). \end{aligned} \quad (5-5)$$

Stringing together (5-1), (5-2), (5-4) and (5-5), we conclude that

$$\left(\frac{2h}{g}\right) = \mu(\rho, \rho') \left(\frac{(b^2 + d^2)(2c^2 + (b - d)^2)}{v_1}\right) \left(\frac{t v_2}{a^2 + b^2 + c^2 + d^2}\right). \quad (5-6)$$

Our next goal is to simplify  $[w]_1$ . We have, by (4-6) and Theorem 2.2,

$$\left(\frac{g}{w}\right)_{4,M} = \left(\frac{\left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)\sigma(w)\sigma\tau(w)}{w}\right)_{4,M} = \mu(\rho)\left(\frac{\sigma(w)\sigma\tau(w)}{w}\right)_{4,M}. \quad (5-7)$$

The quartic residue symbol in (5-7) is the product of two quartic residue symbols. One of them is equal to

$$\begin{aligned} \left(\frac{\sigma\tau(w)}{w}\right)_{4,M} &= \left(\frac{a+d\zeta_8 - c\zeta_8^2 + b\zeta_8^3}{a+b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} = \left(\frac{-2c\zeta_8^2 + (d-b)(\zeta_8 - \zeta_8^3)}{a+b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} \\ &= \left(\frac{\zeta_8^2}{a+b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} \left(\frac{-2c + (b-d)(\zeta_8 + \zeta_8^3)}{a+b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} \\ &= \mu(\rho)\left(\frac{-2c + (b-d)(\zeta_8 + \zeta_8^3)}{a+b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M}, \end{aligned} \quad (5-8)$$

where the last equality is due to Theorem 2.2. For the remainder of this section we assume that  $b-d$  is not zero. We factor  $-2c + (b-d)(\zeta_8 + \zeta_8^3)$  in the ring  $\mathbb{Z}[\sqrt{-2}]$  as

$$-2c + (b-d)(\zeta_8 + \zeta_8^3) = \eta^4 e_0 e$$

with  $\eta$  and  $e_0$  consisting only of even prime factors,  $e_0$  not divisible by a nontrivial fourth power and  $e$  odd. This factorization is unique up to multiplication by units. Then we have, by Theorem 2.2,

$$\left(\frac{-2c + (b-d)(\zeta_8 + \zeta_8^3)}{a+b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} = \mu(\rho, b, c, d)\left(\frac{a+b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}{e}\right)_{4,M}. \quad (5-9)$$

But a simple computation shows

$$a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3 \equiv \sigma\tau(a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3) \pmod{e}.$$

Let  $\mathfrak{p}$  be a prime in  $\mathbb{Z}[\sqrt{-2}]$  that divides  $e$ . Then we may replace  $a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3$  by some element in  $\mathbb{Z}[\sqrt{-2}]$  by Lemma 3.4 of [Koymans and Milovic 2019a]. In case  $\mathfrak{p}$  splits in  $M$ , we apply Lemma 3.2 of [Koymans and Milovic 2019a]. While if  $\mathfrak{p}$  remains inert, we see that  $\mathfrak{p}$  is of degree 1 and  $N\mathfrak{p} \equiv 3 \pmod{8}$ . In this case we apply Lemma 3.3 of [Koymans and Milovic 2019a]. Hence in all cases

$$\left(\frac{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}{\mathfrak{p}}\right)_{4,M} = \mathbb{1}_{\gcd(a+b\zeta_8+c\zeta_8^2+d\zeta_8^3, \mathfrak{p})=(1)}.$$

This yields

$$\left(\frac{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}{e}\right)_{4,M} = \mathbb{1}_{\gcd(w, \sigma\tau(w))=(1)}. \quad (5-10)$$

We deduce from (5-8)–(5-10) that

$$\left(\frac{\sigma\tau(w)}{w}\right)_{4,M} = \mu(\rho, b, c, d) \mathbb{1}_{\gcd(w, \sigma\tau(w))=1}. \quad (5-11)$$

We will now study the other quartic residue symbol in (5-7) using very similar methods. We start with the identity

$$\begin{aligned} \left(\frac{\sigma(w)}{w}\right)_{4,M} &= \left(\frac{a - b\zeta_8 + c\zeta_8^2 - d\zeta_8^3}{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} = \left(\frac{-2\zeta_8(b + d\zeta_8^2)}{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} \\ &= \left(\frac{-2\zeta_8}{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} \left(\frac{b + d\zeta_8^2}{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} \\ &= \mu(\rho) \left(\frac{b + d\zeta_8^2}{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M}, \end{aligned} \quad (5-12)$$

where we use [Theorem 2.2](#) once more. We choose  $i := \zeta_8^2$  and factor  $b + di$  in the ring  $\mathbb{Z}[i]$  as

$$b + di = \eta'^4 e'_0 e'$$

with  $\eta'$  and  $e'_0$  consisting only of even prime factors,  $e'_0$  not divisible by a nontrivial fourth power and  $e'$  odd. Such a factorization is unique up to multiplication by units. With this factorization we have due to [Theorem 2.2](#)

$$\left(\frac{b + di}{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}\right)_{4,M} = \mu(\rho, b, c, d) \left(\frac{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}{e'}\right)_{4,M}. \quad (5-13)$$

We claim that

$$\left(\frac{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3}{e'}\right)_{4,M} = \left(\frac{a + c\zeta_8^2}{e'}\right)_{4,M} = \left(\frac{a + ci}{e'}\right)_{2, \mathbb{Q}(i)}. \quad (5-14)$$

Indeed, let  $\mathfrak{p}$  be a prime in  $\mathbb{Z}[i]$  that divides  $e'$ . If  $\mathfrak{p}$  splits in  $M$ , [Lemma 3.2 of \[Koymans and Milovic 2019a\]](#) shows that

$$\left(\frac{a + c\zeta_8^2}{\mathfrak{p}}\right)_{4,M} = \left(\frac{a + ci}{\mathfrak{p}}\right)_{2, \mathbb{Q}(i)}.$$

Suppose instead that  $\mathfrak{p}$  remains inert. Then  $\mathfrak{p}$  is of degree 1 and  $N\mathfrak{p} \equiv 5 \pmod{8}$ . Now we apply [Lemma 3.3 of \[Koymans and Milovic 2019a\]](#) to obtain

$$\left(\frac{a + c\zeta_8^2}{\mathfrak{p}}\right)_{4,M} = \left(\frac{a + ci}{\mathfrak{p}}\right)_{2, \mathbb{Q}(i)}.$$

This establishes our claim and hence (5-13). Combining (5-12)–(5-14) acquires the validity of

$$\left(\frac{\sigma(w)}{w}\right)_{4,M} = \mu(\rho, b, c, d) \left(\frac{a+ci}{e'}\right)_{2,\mathbb{Q}(i)}. \quad (5-15)$$

Put

$$f(w, \rho) := \mu(\rho, \rho', b, c, d) \mathbb{1}_{\gcd(w, \sigma\tau(w))=1} \left(\frac{tv_2}{a^2 + b^2 + c^2 + d^2}\right).$$

Using (5-6), (5-11) and (5-15), we conclude that

$$\left(\frac{g}{w}\right)_{4,M} \left(\frac{2h}{g}\right) = f(w, \rho) \left(\frac{(b^2 + d^2)(2c^2 + (b-d)^2)}{v_1}\right) \left(\frac{a+ci}{e'}\right)_{2,\mathbb{Q}(i)}. \quad (5-16)$$

Our hidden cancellation will come from comparing the Jacobi symbols

$$\left(\frac{b^2 + d^2}{v_1}\right) \quad \text{and} \quad \left(\frac{a+ci}{e'}\right)_{2,\mathbb{Q}(i)}.$$

Our goal is to show that these two Jacobi symbols are equal up to some easily controlled factors. We can uniquely factor

$$b^2 + d^2 = z_1 z_2,$$

where  $z_1$  and  $z_2$  are positive integers satisfying

- $(z_1, z_2) = 1$ ;
- $z_1$  odd and squarefree;
- if  $p$  is odd and divides  $z_2$ , then  $p^2$  also divides  $z_2$ .

With this factorization we have

$$\left(\frac{b^2 + d^2}{v_1}\right) = \left(\frac{z_1}{v_1}\right) \left(\frac{z_2}{v_1}\right) = \mu(\rho', b, c, d) \left(\frac{v_1}{z_1}\right) \left(\frac{z_2}{v_1}\right).$$

In a similar vein we uniquely factor, up to multiplication by units,  $e'$  in  $\mathbb{Z}[i]$  as

$$e' = \gamma_1 \gamma_2$$

with  $(N\gamma_1, N\gamma_2) = 1$ ,  $N\gamma_1$  squarefree and  $N\gamma_2$  squarefull. The point of this factorization is that  $N\gamma_1 = z_1$ . This gives

$$\left(\frac{v_1}{z_1}\right) = \left(\frac{v_1}{\gamma_1}\right)_{2,\mathbb{Q}(i)}.$$

We claim that

$$(tv_2, \gamma_1) = (d, \gamma_1) = (1). \quad (5-17)$$

We clearly have  $(t, \gamma_1) = (1)$ , so we first show that  $(v_2, \gamma_1) = (1)$ . Let  $p$  be an odd prime of  $\mathbb{Z}[i]$  above  $p$  such that  $p \mid v_2$  and  $p \mid \gamma_1$ . Then we have  $p \mid v_2$  and  $Np \mid N\gamma_1$ . However,  $v_2$  is composed entirely of primes dividing  $b-d$ , while  $N\gamma_1$  divides  $b^2+d^2$ . We conclude that  $p$  divides both  $b$  and  $d$ . But then  $p$  can not divide  $\gamma_1$  by construction. We can prove in a similar way that  $(d, \gamma_1) = (1)$ , thus proving the claim.

From (5-17) we acquire the validity of

$$\begin{aligned} \left(\frac{v_1}{z_1}\right) &= \left(\frac{v_1}{\gamma_1}\right)_{2, \mathbb{Q}(i)} = \mu(b, c, d, t) \left(\frac{v_2}{\gamma_1}\right)_{2, \mathbb{Q}(i)} \left(\frac{v}{\gamma_1}\right)_{2, \mathbb{Q}(i)} \\ &= \mu(b, c, d, t) \left(\frac{v_2}{\gamma_1}\right)_{2, \mathbb{Q}(i)} \left(\frac{a+ci}{\gamma_1}\right)_{2, \mathbb{Q}(i)} \left(\frac{-d(1+i)}{\gamma_1}\right)_{2, \mathbb{Q}(i)} \\ &= \mu(b, c, d, t) \left(\frac{v_2}{\gamma_1}\right)_{2, \mathbb{Q}(i)} \left(\frac{a+ci}{\gamma_1}\right)_{2, \mathbb{Q}(i)}, \end{aligned}$$

where we use the identity

$$v = ab - ad + bc + cd \equiv -ad(1+i) + cd(1-i) = -d(1+i)(a+ci) \pmod{\gamma_1}.$$

We conclude that

$$\begin{aligned} \left(\frac{b^2+d^2}{v_1}\right) \left(\frac{a+ci}{e'}\right)_{2, \mathbb{Q}(i)} \\ = \mu(\rho, \rho', b, c, d, t) \left(\frac{z_2}{v_1}\right) \left(\frac{v_2}{\gamma_1}\right)_{2, \mathbb{Q}(i)} \left(\frac{a+ci}{\gamma_2}\right)_{2, \mathbb{Q}(i)} \mathbb{1}_{\gcd(a+ci, \gamma_1)=(1)}. \end{aligned} \quad (5-18)$$

Put

$$\begin{aligned} g(w, \rho) &:= \mu(\rho, \rho', b, c, d, t) \left(\frac{tv_2}{a^2+b^2+c^2+d^2}\right) \\ &\quad \times \left(\frac{z_2}{v_1}\right) \left(\frac{v_2}{\gamma_1}\right)_{2, \mathbb{Q}(i)} \left(\frac{a+ci}{\gamma_2}\right)_{2, \mathbb{Q}(i)} \mathbb{1}_{\gcd(a+ci, \gamma_1)=\gcd(w, \sigma\tau(w))=(1)}. \end{aligned}$$

After combining (5-16) and (5-18), we get

$$\begin{aligned} \left(\frac{g}{w}\right)_{4, M} \left(\frac{2h}{g}\right) &= g(w, \rho) \left(\frac{2c^2+(b-d)^2}{v_1}\right) \\ &= \mu(\rho, \rho', b, c, d, t) g(w, \rho) \left(\frac{v_1}{2c^2+(b-d)^2}\right). \end{aligned}$$

With this formula we have finally rewritten our symbol in a satisfactory manner; we now return to estimating the sum  $A(X, \mathfrak{d}, u_i, \rho)$ . We recall the factorization  $v = v_1 v_2 t$ , where  $v_1$  is an odd, positive integer satisfying  $\gcd(v_1, b-d) = 1$ ,  $v_2$  is an odd integer consisting only of primes dividing  $b-d$  and  $t$  is positive and only

divisible by powers of 2. We further recall that  $\rho'$  is the congruence class of  $v_1$  modulo 8.

Let  $2^\alpha$  be the closest integer power of 2 to  $X^{1/100}$ . We fix  $b, c, d$  such that  $b - d$  has 2-adic valuation at most  $\alpha/2$ . If  $a$  modulo  $2^\alpha$  is given, we claim that  $v_{\text{odd}}$  is determined modulo 8, where  $v_{\text{odd}}$  is the odd part of

$$v = a(b - d) + c(b + d), \quad (5-19)$$

with the exception of  $\ll X^{1/200}$  congruence classes  $\rho''$  for  $a$  modulo  $2^\alpha$ . Note that, for fixed  $b, c$  and  $d$ ,  $\rho''$  determines  $v$  modulo  $2^\alpha$ . If  $\alpha \geq 3$ ,  $v$  modulo  $2^\alpha$  determines  $v_{\text{odd}}$  modulo 8 unless  $v$  is divisible by  $2^{\alpha-3}$ . There are only 8 congruence classes modulo  $2^\alpha$  divisible by  $2^{\alpha-3}$ . Now take such a congruence class, say  $\rho'''$ . But there are  $\ll X^{1/200}$  congruence classes  $\rho''$  modulo  $2^\alpha$  with

$$\rho''(b - d) + c(b + d) \equiv \rho''' \pmod{2^\alpha}$$

by our assumption that the 2-adic valuation of  $b - d$  is at most  $\alpha/2$ , and our claim follows.

Similarly, we know the value of  $t$  with the exception of  $\ll X^{1/200}$  congruence classes for  $a$  modulo  $2^\alpha$ . We remove all such congruence classes from the sum, which gives an error of size at most  $X^{199/200}$ . From now on we assume that  $a$  does not lie in such a congruence class. For the remaining congruence classes modulo  $2^\alpha$ , we observe that  $\rho'$  is determined by  $v_{\text{odd}}$  modulo 8 together with  $b, c$  and  $d$ . Hence both  $\rho'$  and  $t$  are determined by  $a$  modulo  $2^\alpha$ .

We would also like to treat  $v_2$  as fixed, and we use a similar technique to achieve this. Once more we fix  $b, c$  and  $d$ . We assume that

$$\gcd(b - d, bc + cd) \leq \exp((\log X)^{0.25}).$$

We can uniquely factor a positive integer  $n$  as  $x_1 x_2$ , where  $\gcd(x_1, x_2) = 1$ ,  $x_1 > 0$  is squarefree and  $x_2 > 0$  is squarefull. We call  $x_1$  the squarefree part, and  $x_2$  the squarefull part. We further assume that the squarefull part of  $b - d$  is of size at most  $\exp((\log X)^{0.25})$ . We now factor

$$\gcd(b - d, bc + cd) = \prod_{i=1}^k p_i^{f_i}.$$

Define  $f'_i(p_i)$  to be the smallest integer such that

$$p_i^{f'_i(p_i)} \geq \exp(2(\log X)^{0.25})$$

and define

$$G := \prod_{i=1}^k p_i^{f'_i(p_i)}.$$

Clearly, we have that  $\gcd(b-d, bc+cd)$  divides  $G$ , since the squarefull part of  $b-d$  is of size at most  $\exp((\log X)^{0.25})$ . If  $a$  modulo  $G$  is given, we claim that  $v_2$  is determined modulo  $G$  with the exception of at most

$$\ll \log X \max_{1 \leq i \leq k} \frac{G}{p_i^{f'_i(p_i)/2}}$$

congruence classes  $\rho''$  for  $a$  modulo  $G$ . Take a prime divisor  $p_i$  of  $b-d$ . If  $p_i$  does not divide  $bc+cd$ , then clearly

$$p_i \nmid a(b-d) + bc + cd,$$

so we have found the  $p_i$  valuation of  $a(b-d) + bc + cd$ . Now suppose that  $p_i$  also divides  $bc+cd$ . Then we know the  $p_i$  valuation unless

$$a(b-d) + bc + cd \equiv 0 \pmod{p_i^{f'_i(p_i)}}.$$

However, we know that the  $p_i$  valuation of  $b-d$  is at most  $f'_i(p_i)/2$ . Hence there are at most  $p_i^{f'_i(p_i)/2}$  congruence classes for  $a$  modulo  $p_i^{f'_i(p_i)}$  for which

$$a(b-d) + bc + cd \equiv 0 \pmod{p_i^{f'_i(p_i)}},$$

and we call such a congruence class forbidden. We let  $G_i$  be the set of forbidden congruence classes modulo  $p_i^{f'_i(p_i)}$ . Now we discard all congruence classes  $\rho''$  modulo  $G$  for which there exists a prime  $p_i$  dividing  $\gcd(b-d, bc+cd)$  such that the reduction of  $\rho''$  modulo  $p_i^{f'_i(p_i)}$  lies in  $G_i$ . This proves the claim.

Set

$$m := \text{lcm}(G, z_2, N\gamma_2, 2^\alpha, 2^{10}). \quad (5-20)$$

Then

$$\left( \frac{tv_2}{a^2 + b^2 + c^2 + d^2} \right) \left( \frac{z_2}{v_1} \right) \left( \frac{v_2}{\gamma_1} \right)_{2, \mathbb{Q}(i)} \left( \frac{a+ci}{\gamma_2} \right)_{2, \mathbb{Q}(i)}$$

depends only on  $a$  modulo  $m$ ,  $b$ ,  $c$  and  $d$ . If we write  $\beta := b\zeta_8 + c\zeta_8^2 + d\zeta_8^3$ , we have the estimate

$A(X, \mathfrak{d}, u_i, \rho)$

$$\ll \sum_{\beta} \sum_{f \in \mathbb{Z}/m\mathbb{Z}} \left| \sum_{\substack{a \in \mathbb{Z} \\ a \text{ sat. } (*)}} \left( \frac{v_1}{2c^2 + (b-d)^2} \right) \mathbb{1}_{\gcd(a+ci, \gamma_1) = \gcd(a+\beta, \sigma\tau(a+\beta)) = (1)} \right|,$$

where  $(*)$  are the simultaneous conditions

$$a + \beta \in u_i \mathcal{D}(X), \quad a + \beta \equiv 0 \pmod{\mathfrak{d}}, \quad a + \beta \equiv \rho \pmod{2^{10}}, \quad a \equiv f \pmod{m}.$$

Recall that the condition  $a + \beta \in u_i \mathcal{D}(X)$  implies  $a, b, c, d \ll X^{1/4}$ ; see [Lemma 2.3](#). We will only consider  $\beta$  satisfying the following five properties:

- (i)  $z_2, N\gamma_2 \leq X^{1/200}$ .
- (ii)  $\gcd(b-d, bc+cd) \leq \exp((\log X)^{0.25})$ .
- (iii) The 2-adic valuation of  $b-d$  is at most  $\alpha/2$ .
- (iv) The squarefull part of  $b-d$  is of size at most  $\exp((\log X)^{0.25})$ .
- (v) The odd, squarefree part of  $2c^2 + (b-d)^2$  is at least  $X^{99/200}$ .

We claim that there are at most

$$\ll \frac{X^{3/4}}{\exp((\log X)^{0.2})}$$

elements  $\beta$  that do not satisfy all five conditions. To do so, we shall bound the number of  $\beta$  that fail a given property in the above list. For (iii) and (iv) this is easily verified. For (v), we use that  $2c^2 + (b-d)^2$  represents a given integer at most  $\ll_{\epsilon} X^{(1/4)+\epsilon}$  times, and this reduces the problem to an easy counting problem. A similar argument disposes with (i). Finally, for (ii), we count the number of  $\beta$  such that

$$\gcd(b-d, b+d) > \exp\left(\frac{1}{2}(\log X)^{0.25}\right) \text{ or } \gcd(b-d, c) > \exp\left(\frac{1}{2}(\log X)^{0.25}\right).$$

For those  $\beta$ , we bound the inner sum trivially by  $\ll X^{1/4}/m$  inducing an error of size

$$\ll \frac{X}{\exp((\log X)^{0.2})}.$$

For the remaining  $\beta$ , we have  $G \ll_{\epsilon} X^{\epsilon}$  and hence  $m \ll_{\epsilon} X^{(1/50)+\epsilon}$  by (i) and the definition of  $m$ ; see (5-20). Note that

$$\mathbb{1}_{\gcd(a+\beta, \sigma\tau(a+\beta))=1} = \mathbb{1}_{\gcd(a+\beta, \sigma\tau(\beta)-\beta)=1}.$$

We use the Möbius function to detect the coprimality conditions, which yields the upper bound

$$A(X, \mathfrak{d}, u_i, \rho) \ll \sum_{\beta} \sum_{f \in \mathbb{Z}/m\mathbb{Z}} \sum_{\mathfrak{d}_1 | \gamma_1} \sum_{\mathfrak{d}_2 | \sigma\tau(\beta) - \beta} \left| \sum_{\substack{a \in \mathbb{Z} \\ a \text{ sat. (**)}}} \left( \frac{v_1}{2c^2 + (b-d)^2} \right) \right|,$$

where (\*\*) are the simultaneous conditions

$$\begin{aligned} a + \beta \in u_i \mathcal{D}(X), & \quad a + \beta \equiv 0 \pmod{\mathfrak{d}}, & \quad a + \beta \equiv \rho \pmod{2^{10}}, & \quad a \equiv f \pmod{m}, \\ & \quad a + ci \equiv 0 \pmod{\mathfrak{d}_1}, & \quad a + \beta \equiv 0 \pmod{\mathfrak{d}_2}. \end{aligned}$$

Define  $m'$  to be the smallest positive integer that is divisible by  $\text{lcm}(\mathfrak{d}, \mathfrak{d}_1, \mathfrak{d}_2)$ . Put

$$M := \text{lcm}(m, m').$$

The congruence conditions for  $a$  in (\*\*) are equivalent to at most one congruence condition modulo  $M$ . We assume that it is equivalent to exactly one congruence condition modulo  $M$ , say  $F$ , otherwise the inner sum is empty. Then we have

$$A(X, \mathfrak{d}, u_i, \rho) \ll \sum_{\beta} \sum_{f \in \mathbb{Z}/m\mathbb{Z}} \sum_{\mathfrak{d}_1 | \gamma_1} \sum_{\mathfrak{d}_2 | \sigma \tau(\beta) - \beta} \left| \sum_{\substack{a \in \mathbb{Z} \\ a + \beta \in u_i \mathcal{D}(X) \\ a \equiv F \pmod{M}}} \left( \frac{v_1}{2c^2 + (b-d)^2} \right) \right|. \quad (5-21)$$

We assume that  $M \leq X^{1/8}$ , since otherwise the trivial bound suffices. Furthermore, for fixed  $\beta$ , the condition  $a + \beta \in u_i \mathcal{D}(X)$  means that  $a$  runs over  $\ll 1$  intervals with endpoints depending on  $\beta$  and  $u_i$ . Since  $a \ll X^{1/4}$ , we know that each interval has length  $\ll X^{1/4}$ . We have the factorization

$$2c^2 + (b-d)^2 = q_1 q_2,$$

where  $q_1$  is the odd, squarefree part. We know that  $q_2 \ll X^{1/200}$ , and we split the sum over  $a$  in congruence classes modulo  $q_2$ . For fixed  $b, c$  and  $d$ , the condition  $a \equiv F \pmod{M}$  implies that  $v_1$  is a linear function of  $a$  with linear term not divisible by  $q_1$  by our assumptions  $q_1 \geq X^{99/200}$  and  $M \leq X^{1/8}$ . Indeed,  $v_2$  and  $t$  are determined by  $F$ , so this follows immediately from (5-3). Hence we may employ the Burgess bound [1963] to (5-21) with  $r = 2$  and  $q = q_1 \ll X^{1/2}$  to prove

$$A(X, \mathfrak{d}, u_i, \rho) \ll_{\epsilon} X^{\frac{31}{32} + \frac{1}{50} + \frac{1}{200} + \epsilon} + X^{\frac{199}{200}} + X^{\frac{15}{16}} + \frac{X}{\exp((\log X)^{0.2})},$$

where the second term accounts for the discarded congruence classes for  $a$ , the third term accounts for those  $M$  with  $M > X^{1/8}$  and the fourth term accounts for the discarded  $\beta$ . This establishes the following proposition.

**Proposition 5.1.** *We have for all ideals  $\mathfrak{d}$  of  $\mathbb{Z}[\zeta_8]$*

$$A(X, \mathfrak{d}) \ll \frac{X}{\exp((\log X)^{0.2})}.$$

## 6. Sums of type II

In (4-5) we defined  $[w]_1$  and  $[w]_2$ . We have the useful decomposition

$$[w] = [w]_1 [w]_2.$$

In this section we need to carefully study the multiplicative properties of  $[w]$ , and we do so by studying the multiplicative properties of  $[w]_1$  and  $[w]_2$ . These properties will then be used to prove cancellation in sums of type II. We start by studying  $[w]_1$ ; our treatment is almost identical to [Koymans and Milovic 2019a]. If  $w$  is an odd element of  $\mathbb{Z}[\zeta_8]$ , we have

$$[w]_1 = \left( \frac{\left( \frac{1}{2} - \frac{1}{2\sqrt{2}} \right) \sigma(w) \sigma \tau(w)}{w} \right)_{4,M} = \left( \frac{(2 - \sqrt{2}) \sigma(w) \sigma \tau(w)}{w} \right)_{4,M}.$$

Define

$$\gamma_1(w, z) := \left( \frac{\sigma(z)}{w} \right)_{2,M}. \quad (6-1)$$

For the remainder of this section, we use the convention that  $\delta(w, z)$  is a function depending only on the congruence classes of  $w$  and  $z$  modulo  $2^{10}$ ; at each occurrence  $\delta(w, z)$  may be a different function.

**Lemma 6.1.** *We have for all odd  $w, z \in \mathbb{Z}[\zeta_8]$*

$$[wz]_1 = \delta(w, z)[w]_1[z]_1\gamma_1(w, z)\mathbb{1}_{\gcd(w, \sigma\tau(z))=1}.$$

*Proof.* By definition of  $[w]_1$  we have

$$\begin{aligned} [wz]_1 &= \left( \frac{(2 - \sqrt{2})\sigma(wz)\sigma\tau(wz)}{wz} \right)_{4,M} \\ &= [w]_1[z]_1 \left( \frac{\sigma(z)}{w} \right)_{4,M} \left( \frac{\sigma\tau(z)}{w} \right)_{4,M} \left( \frac{\sigma(w)}{z} \right)_{4,M} \left( \frac{\sigma\tau(w)}{z} \right)_{4,M}. \end{aligned}$$

Since  $\sigma$  fixes  $i$  and therefore any quartic residue symbol, [Theorem 2.2](#) yields

$$\begin{aligned} \left( \frac{\sigma(z)}{w} \right)_{4,M} \left( \frac{\sigma(w)}{z} \right)_{4,M} &= \delta(w, z) \left( \frac{\sigma(z)}{w} \right)_{4,M} \left( \frac{z}{\sigma(w)} \right)_{4,M} \\ &= \delta(w, z) \left( \frac{\sigma(z)}{w} \right)_{4,M} \sigma \left( \left( \frac{\sigma(z)}{w} \right)_{4,M} \right) \\ &= \delta(w, z) \left( \frac{\sigma(z)}{w} \right)_{2,M}. \end{aligned}$$

If we do the same computation for  $\sigma\tau$ , we obtain

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

since  $\sigma\tau$  does not fix  $i$ . This proves the lemma. □

In the next lemma we collect the most important properties of  $\gamma_1(w, z)$ .

**Lemma 6.2.** *Let  $w, z \in \mathbb{Z}[\zeta_8]$  be odd and define  $\gamma_1(w, z)$  as in (6-1).*

(i)  $\gamma_1(w, z)$  is essentially symmetric

$$\gamma_1(w, z) = \delta(w, z)\gamma_1(z, w).$$

(ii)  $\gamma_1(w, z)$  is multiplicative in both arguments

$$\gamma_1(w, z_1z_2) = \gamma_1(w, z_1)\gamma_1(w, z_2), \quad \gamma_1(w_1w_2, z) = \gamma_1(w_1, z)\gamma_1(w_2, z).$$

*Proof.* This is straightforward. □

With this lemma we have completed our study of  $[w]_1$  and  $\gamma_1(w, z)$ . We will now focus on  $[w]_2$ . Recall that

$$[w]_2 = \left( \frac{2h}{g} \right) = \delta(w) \left( \frac{v}{u} \right).$$

The second representation of  $[w]_2$  is very convenient, since it allows us to use earlier work of Milovic [2017a]. Define

$$\gamma_2(w, z) := \left( \frac{\sigma(wz)\sigma\tau(wz)}{w\tau(w)} \right)_{2,K}, \quad (6-2)$$

where  $K := \mathbb{Q}(\sqrt{2})$ .

**Lemma 6.3.** *The following formula is valid for all odd  $w, z \in \mathbb{Z}[\zeta_8]$ :*

$$[wz]_2 = \delta(w, z)[w]_2[z]_2\gamma_2(w, z).$$

*Proof.* Milovic [2017a, p. 1009] defined the symbol

$$[u + v\sqrt{2}]_3 := \left( \frac{v}{u} \right).$$

Then it is easily seen that  $[w]_2 = \delta(w)[w\tau(w)]_3$  and that  $w\tau(w)$  is totally positive. Now apply Proposition 8 of [Milovic 2017a].  $\square$

To further our study of  $\gamma_2(w, z)$ , it will be convenient to define a second function  $m(w)$  by the formula

$$m(w) := \gamma_2(w, 1) = \left( \frac{\sigma(w)\sigma\tau(w)}{w\tau(w)} \right)_{2,K}.$$

It turns out that  $\gamma_2(w, z)$  is neither symmetric nor multiplicative. Instead, it is symmetric and multiplicative twisted by the factor  $m$ .

**Lemma 6.4.** *Let  $w, z \in \mathbb{Z}[\zeta_8]$  be odd and define  $\gamma_2(w, z)$  as in (6-2).*

(i)  $\gamma_2(w, z)$  is twisted symmetric

$$\gamma_2(w, z)\gamma_2(z, w) = m(wz).$$

(ii)  $\gamma_2(w, z)$  is twisted multiplicative in  $z$

$$\gamma_2(w, z_1z_2) = m(w)\gamma_2(w, z_1)\gamma_2(w, z_2).$$

*Proof.* The proof is left to the reader.  $\square$

With this out of the way we are ready to tackle the sums of type II. Let  $\{\alpha_w\}$  and  $\{\beta_z\}$  be sequences of complex numbers of absolute value at most 1 and let  $\rho$  and  $\mu$  be invertible congruence classes modulo  $2^{10}$ . We define

$$B_1(M, N, \rho, \mu) := \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv \mu \pmod{2^{10}}}} \alpha_w \beta_z [wz],$$

where we suppress the dependence on  $\{\alpha_w\}$  and  $\{\beta_z\}$ . Then we have the following proposition.

**Proposition 6.5.** *There is an absolute constant  $\theta_3 > 0$  such that for all sequences of complex numbers  $\{\alpha_w\}$  and  $\{\beta_z\}$  of absolute value at most 1, all invertible congruence classes  $\rho$  and  $\mu$  modulo  $2^{10}$*

$$B_1(M, N, \rho, \mu) \ll (M^{-1/24} + N^{-1/24})MN(\log MN)^{\theta_3}.$$

*Proof.* We start by expanding  $[wz]$  using Lemmas 6.1 and 6.3. We may absorb  $[w]_1, [w]_2, [z]_1$  and  $[z]_2$  in the coefficients  $\alpha_w$  and  $\beta_z$ . Then it suffices to prove for all sequences of complex numbers  $\{\alpha_w\}$  and  $\{\beta_z\}$  of absolute value at most 1 and all invertible congruence classes  $\rho$  and  $\mu$  modulo  $2^{10}$  the following estimate:

$$\begin{aligned} B_2(M, N, \rho, \mu) &:= \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv \mu \pmod{2^{10}}}} \alpha_w \beta_z \gamma_1(w, z) \gamma_2(w, z) \mathbb{1}_{\gcd(w, \sigma\tau(z))=1} \\ &\ll (M^{-1/24} + N^{-1/24})MN(\log MN)^{\theta_3}. \end{aligned}$$

Define

$$\gamma_3(w, z) := \left( \frac{\sigma(z)\sigma\tau(z)}{w\tau(w)} \right)_{2, K},$$

so that we have the factorization  $\gamma_2(w, z) = m(w)\gamma_3(w, z)$ . Absorbing  $m(w)$  in  $\alpha_w$  and using the identity

$$\gamma_3(w, z) \mathbb{1}_{\gcd(w, \sigma\tau(z))=1} = \gamma_3(w, z),$$

we see that it is enough to establish

$$\begin{aligned} B_3(M, N, \rho, \mu) &:= \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv \mu \pmod{2^{10}}}} \alpha_w \beta_z \gamma_1(w, z) \gamma_3(w, z) \\ &\ll (M^{-1/24} + N^{-1/24})MN(\log MN)^{\theta_3}. \end{aligned}$$

**Theorem 2.1** shows that  $\gamma_3(w, z)$  is also essentially symmetric, i.e.,

$$\gamma_3(w, z) = \delta(w, z)\gamma_3(z, w).$$

Due to the symmetry of  $\gamma_1(w, z)$ , see [Lemma 6.2](#) (i), and the symmetry of  $\gamma_3(w, z)$ , we may further reduce to the case  $N \geq M$ . We take  $k := 12$  and apply Hölder's inequality with  $1 = \frac{k-1}{k} + \frac{1}{k}$  to the  $w$  variable to obtain

$$|B_3(M, N, \rho, \mu)|^k \leq \left( \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} |\alpha_w|^{\frac{k}{k-1}} \right)^{k-1} \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} \left| \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv \mu \pmod{2^{10}}}} \beta_z \gamma_1(w, z) \gamma_3(w, z) \right|^k.$$

The first factor is trivially bounded by  $\ll M^{k-1}$  with absolute implied constant. [Lemma 6.2](#) (ii) implies that  $\gamma_1(w, z)$  is multiplicative in  $z$  and [Lemma 6.4](#) (ii) implies that  $\gamma_3(w, z)$  is multiplicative in  $z$ . Hence  $\gamma_1(w, z)\gamma_3(w, z)$  is multiplicative in  $z$ . We conclude that

$$|B_3(M, N, \rho, \mu)|^k \ll M^{k-1} \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} \epsilon(w) \sum_z \beta'_z \gamma_1(w, z) \gamma_3(w, z), \quad (6-3)$$

where

$$\epsilon(w) := \left( \frac{\left| \sum_{z \in \mathcal{D}(N), z \equiv \mu \pmod{2^{10}}} \beta_z \gamma_1(w, z) \gamma_3(w, z) \right|}{\sum_{z \in \mathcal{D}(N), z \equiv \mu \pmod{2^{10}}} \beta_z \gamma_1(w, z) \gamma_3(w, z)} \right)^k$$

and

$$\beta'_z := \sum_{\substack{z = z_1 \cdots z_k \\ z_1, \dots, z_k \in \mathcal{D}(N) \\ z_1 \equiv \cdots \equiv z_k \equiv \mu \pmod{2^{10}}}} \beta_{z_1} \cdots \beta_{z_k}.$$

We will now study the summation condition for  $z$  in the inner sum of (6-3) more carefully. By construction,  $\mathcal{D}(N)$  contains exactly eight generators of any principal ideal. Furthermore, there are  $\ll N^k$  values of  $z$  for which  $\beta'_z \neq 0$ . Hence we obtain the bound

$$\sum_z (\beta'_z)^2 \ll (\log N)^{\theta_3} N^k$$

for some absolute constant  $\theta_3$ , since  $k$  is fixed. An application of the Cauchy–Schwarz inequality over the  $z$  variable yields

$$\begin{aligned} & \left( \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} \epsilon(w) \sum_z \beta'_z \gamma_1(w, z) \gamma_3(w, z) \right)^2 \\ &= \left( \sum_z \beta'_z \sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} \epsilon(w) \gamma_1(w, z) \gamma_3(w, z) \right)^2 \end{aligned}$$

$$\begin{aligned} &\ll (\log N)^{\theta_3} N^k \\ &\times \sum_{\substack{w_1 \in \mathcal{D}(M) \\ w_1 \equiv \rho \pmod{2^{10}}}} \sum_{\substack{w_2 \in \mathcal{D}(M) \\ w_2 \equiv \rho \pmod{2^{10}}}} \epsilon(w_1) \overline{\epsilon(w_2)} \sum_z \gamma_1(w_1 w_2, z) \gamma_3(w_1 w_2, z), \end{aligned} \quad (6-4)$$

because  $\gamma_1(w, z)$  and  $\gamma_3(w, z)$  are multiplicative in  $w$ . Conveniently, inequality (6-4) remains valid if we extend the sum over  $z$  to a larger domain. Let  $z_1, \dots, z_k \in \mathcal{D}(N)$  and write

$$z_i = \sum_{j=1}^4 a_{ij} \zeta_8^j.$$

Then we have  $|a_{ij}| \ll N^{1/4}$ . Now define

$$\mathcal{B}(C) := \left\{ \sum_{j=1}^4 a_j \zeta_8^j : a_j \in \mathbb{Z}, |a_j| \leq CN^{k/4} \right\}.$$

Then, if  $C$  is sufficiently large,  $\beta'_z \neq 0$  implies  $z \in \mathcal{B}(C)$ . For this choice of  $C$ , we extend the range of summation over  $z$  in (6-4) to the set  $\mathcal{B}(C)$ . We split the sum over  $z$  in congruence classes  $\zeta$  modulo  $N(w_1 w_2)$ ; we claim that for all odd  $w$

$$\sum_{\zeta \pmod{N(w)}} \gamma_1(w, \zeta) \gamma_3(w, \zeta) = 0$$

provided that  $N(w)$  is not squarefull. Substituting the definition of  $\gamma_1(w, \zeta)$  and  $\gamma_3(w, \zeta)$  gives

$$f(w) := \sum_{\zeta \pmod{N(w)}} \gamma_1(w, \zeta) \gamma_3(w, \zeta) = \sum_{\zeta \pmod{N(w)}} \left( \frac{\sigma(\zeta) \sigma \tau(\zeta)}{w \tau(w)} \right)_{2,K} \left( \frac{\sigma(\zeta)}{w} \right)_{2,M}.$$

Then a calculation shows that for all odd  $w$  and  $w'$  satisfying  $(N(w), N(w')) = 1$ ,

$$f(w w') = f(w) f(w').$$

Hence, to establish the claim, it is enough to prove that  $f(w) = 0$  if  $w$  is an odd prime of degree 1. To do so, we start with the identity

$$\left( \frac{\sigma(\zeta) \sigma \tau(\zeta)}{w \tau(w)} \right)_{2,K} = \left( \frac{\sigma(\zeta) \sigma \tau(\zeta)}{w} \right)_{2,M}.$$

Here we rely in an essential way that  $w$  is an odd prime of degree 1, so we have an isomorphism of finite fields  $O_M/w \cong O_K/w\tau(w)$ . We use this to give a simple expression for  $f(w)$ ,

$$f(w) = \sum_{\zeta \pmod{N(w)}} \left( \frac{\sigma \tau(\zeta)}{w} \right)_{2,M} \mathbb{1}_{(\sigma(\zeta), w) = (1)},$$

which apart from a nonzero factor is

$$\begin{aligned} \sum_{\zeta \bmod \sigma(w)\sigma\tau(w)} \left( \frac{\sigma\tau(\zeta)}{w} \right)_{2,M} \mathbb{1}_{(\sigma(\zeta),w)=(1)} \\ = \sum_{\zeta \bmod \sigma\tau(w)} \left( \frac{\sigma\tau(\zeta)}{w} \right)_{2,M} \sum_{\zeta \bmod \sigma(w)} \mathbb{1}_{(\sigma(\zeta),w)=(1)} = 0. \end{aligned}$$

Note that  $\sigma(w)$  and  $\sigma\tau(w)$  are coprime, so we are allowed to expand the sum over  $\sigma(w)\sigma\tau(w)$  as the product of the two sums over  $\sigma(w)$  and  $\sigma\tau(w)$ . With the claim established, we can give an upper bound for the sum over  $z \in \mathcal{B}(C)$

$$\sum_{z \in \mathcal{B}(C)} \gamma_1(w_1 w_2, z) \gamma_3(w_1 w_2, z) \ll \begin{cases} N^k & \text{if } N(w_1 w_2) \text{ is squarefull,} \\ \sum_{i=1}^4 M^{2i} N^{k(1-\frac{1}{4}i)} & \text{otherwise,} \end{cases}$$

where the second bound uses the claim and  $N(w_1 w_2) \leq M^2$ . Because of our choice of  $k$  and  $N \geq M$ , we can simplify the second bound to  $M^2 N^{\frac{3}{4}k}$ . Equations (6-3), (6-4) and the above bound acquire the validity of

$$\begin{aligned} |B_3(M, N, \rho, \mu)|^{2k} &\ll (\log N)^{\theta_3} M^{2k-2} N^k (M \cdot N^k + M^2 \cdot M^2 N^{\frac{3}{4}k}) \\ &\ll (\log N)^{\theta_3} (M^{2k-1} \cdot N^k + M^{2k+2} \cdot N^{\frac{7}{4}k}). \end{aligned}$$

Since the first term above dominates the second term due to our choice of  $k$  and  $N \geq M$ , the proof of the proposition is complete.  $\square$

Having dealt with sums of type II for the symbol  $[wz]$ , we now turn to sums of type II with  $a_{mn}$ . For sequences of complex numbers  $\{\alpha_m\}$  and  $\{\beta_n\}$  of absolute value at most 1 we defined in Section 3 the following sum:

$$B(M, N) = \sum_{Nm \leq M} \sum_{Nn \leq N} \alpha_m \beta_n a_{mn}.$$

**Proposition 6.6.** *There is an absolute constant  $\theta_3 > 0$  such that for all sequences of complex numbers  $\{\alpha_m\}$  and  $\{\beta_n\}$  of absolute value at most 1,*

$$B(M, N) \ll (M^{-1/24} + N^{-1/24}) MN (\log MN)^{\theta_3}.$$

*Proof.* By picking generators for  $\mathfrak{m}$  and  $\mathfrak{n}$  we obtain the identity

$$B(M, N) = \sum_{Nm \leq M} \sum_{Nn \leq N} \alpha_m \beta_n a_{mn} = \frac{1}{64} \sum_{w \in \mathcal{D}(M)} \sum_{z \in \mathcal{D}(N)} \alpha_w \beta_z a_{(wz)}.$$

We split the sum  $B(M, N)$  in congruence classes modulo  $2^{10}$ . We need only consider invertible congruence classes, since otherwise  $a_{wz} = 0$  by definition. Furthermore,

condition (4-4) depends only on  $g$  modulo 4, which is in turn determined by  $w$  modulo 4. Therefore, it suffices to bound the sum

$$\sum_{\substack{w \in \mathcal{D}(M) \\ w \equiv \rho \pmod{2^{10}}}} \sum_{\substack{z \in \mathcal{D}(N) \\ z \equiv \mu \pmod{2^{10}}}} \alpha_w \beta_z ([wz] + [\epsilon wz] + [\epsilon^2 wz] + [\epsilon^3 wz]),$$

where  $\rho$  and  $\mu$  are invertible congruence classes modulo  $2^{10}$  such that  $g \equiv 1 \pmod{4}$ . From Lemmas 6.1 and 6.3 we deduce that

$$[\epsilon wz] = \delta(w, z)[\epsilon][wz].$$

Now apply Proposition 6.5. □

### Acknowledgements

I am very grateful to Djordjo Milovic for his support during this project. I would also like to thank Jan-Hendrik Evertse for proofreading.

### References

- [Alberts 2016] B. Alberts, “Cohen–Lenstra moments for some nonabelian groups”, preprint, 2016. [arXiv](#)
- [Alberts and Klys 2016] B. Alberts and J. Klys, “The distribution of  $H_8$ -extensions of quadratic fields”, preprint, 2016. [arXiv](#)
- [Bruin and Hemenway 2013] N. Bruin and B. Hemenway, “On congruent primes and class numbers of imaginary quadratic fields”, *Acta Arith.* **159**:1 (2013), 63–87. [MR](#) [Zbl](#)
- [Burgess 1963] D. A. Burgess, “On character sums and  $L$ -series, II”, *Proc. Lond. Math. Soc.* (3) **13** (1963), 524–536. [MR](#) [Zbl](#)
- [Cohn and Lagarias 1983] H. Cohn and J. C. Lagarias, “On the existence of fields governing the 2-invariants of the classgroup of  $\mathbb{Q}(\sqrt{dp})$  as  $p$  varies”, *Math. Comp.* **41**:164 (1983), 711–730. [MR](#) [Zbl](#)
- [Cohn and Lagarias 1984] H. Cohn and J. C. Lagarias, “Is there a density for the set of primes  $p$  such that the class number of  $\mathbb{Q}(\sqrt{-p})$  is divisible by 16?”, pp. 257–280 in *Topics in classical number theory, I* (Budapest, 1981), edited by G. Halász, Colloq. Math. Soc. János Bolyai **34**, North-Holland, Amsterdam, 1984. [MR](#) [Zbl](#)
- [Davenport and Heilbronn 1971] H. Davenport and H. Heilbronn, “On the density of discriminants of cubic fields, II”, *Proc. Roy. Soc. Lond. Ser. A* **322**:1551 (1971), 405–420. [MR](#) [Zbl](#)
- [Fouvry and Klüners 2006] É. Fouvry and J. Klüners, “Cohen–Lenstra heuristics of quadratic number fields”, pp. 40–55 in *Algorithmic number theory* (Berlin, 2006), edited by F. Hess et al., Lect. Notes Comput. Sci. **4076**, Springer, 2006. [MR](#) [Zbl](#)
- [Fouvry and Klüners 2007] É. Fouvry and J. Klüners, “On the 4-rank of class groups of quadratic number fields”, *Invent. Math.* **167**:3 (2007), 455–513. [MR](#) [Zbl](#)
- [Friedlander and Iwaniec 1998] J. Friedlander and H. Iwaniec, “The polynomial  $X^2 + Y^4$  captures its primes”, *Ann. of Math.* (2) **148**:3 (1998), 945–1040. [MR](#) [Zbl](#)
- [Friedlander et al. 2013] J. B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin, “The spin of prime ideals”, *Invent. Math.* **193**:3 (2013), 697–749. Correction in **202**:2 (2015), 923–925. [MR](#) [Zbl](#)

- [Gerth 1984] F. Gerth, III, “The 4-class ranks of quadratic fields”, *Invent. Math.* **77**:3 (1984), 489–515. [MR](#) [Zbl](#)
- [Hasse 1969] H. Hasse, “Über die Klassenzahl des Körpers  $P(\sqrt{-2p})$  mit einer Primzahl  $p \neq 2$ ”, *J. Number Theory* **1** (1969), 231–234. [MR](#) [Zbl](#)
- [Heath-Brown 1994] D. R. Heath-Brown, “The size of Selmer groups for the congruent number problem, II”, *Invent. Math.* **118**:2 (1994), 331–370. [MR](#) [Zbl](#)
- [Klys 2017] J. Klys, “Moments of unramified 2-group extensions of quadratic fields”, preprint, 2017. [arXiv](#)
- [Koymans and Milovic 2019a] P. Koymans and D. Milovic, “On the 16-rank of class groups of  $\mathbb{Q}(\sqrt{-2p})$  for primes  $p \equiv 1 \pmod{4}$ ”, *Int. Math. Res. Not. IMRN* **2019**:23 (2019), 7406–7427. [MR](#) [Zbl](#)
- [Koymans and Milovic 2019b] P. Koymans and D. Z. Milovic, “Spins of prime ideals and the negative Pell equation  $x^2 - 2py^2 = -1$ ”, *Compos. Math.* **155**:1 (2019), 100–125. [MR](#) [Zbl](#)
- [Lemmermeyer 2000] F. Lemmermeyer, *Reciprocity laws: from Euler to Eisenstein*, Springer, 2000. [MR](#) [Zbl](#)
- [Leonard and Williams 1982] 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**:2 (1982), 200–206. [MR](#) [Zbl](#)
- [Milovic 2017a] D. Milovic, “On the 16-rank of class groups of  $\mathbb{Q}(\sqrt{-8p})$  for  $p \equiv -1 \pmod{4}$ ”, *Geom. Funct. Anal.* **27**:4 (2017), 973–1016. [MR](#) [Zbl](#)
- [Milovic 2017b] D. Z. Milovic, “The infinitude of  $\mathbb{Q}(\sqrt{-p})$  with class number divisible by 16”, *Acta Arith.* **178**:3 (2017), 201–233. [MR](#) [Zbl](#)
- [Rédei 1934] 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. [MR](#) [Zbl](#)
- [Smith 2016] A. Smith, “Governing fields and statistics for 4-Selmer groups and 8-class groups”, preprint, 2016. [arXiv](#)
- [Smith 2017] A. Smith, “ $2^\infty$ -Selmer groups,  $2^\infty$ -class groups, and Goldfeld’s conjecture”, preprint, 2017. [arXiv](#)
- [Stevenhagen 1988] P. Stevenhagen, *Class groups and governing fields*, Ph.D. thesis, University of California, Berkeley, 1988.
- [Stevenhagen 1993] P. Stevenhagen, “Divisibility by 2-powers of certain quadratic class numbers”, *J. Number Theory* **43**:1 (1993), 1–19. [MR](#) [Zbl](#)
- [Wood 2019] M. M. Wood, “Nonabelian Cohen–Lenstra moments”, *Duke Math. J.* **168**:3 (2019), 377–427. [MR](#) [Zbl](#)

Communicated by Peter Sarnak

Received 2018-09-19

Revised 2019-08-14

Accepted 2019-09-12

[p.h.koymans@math.leidenuniv.nl](mailto:p.h.koymans@math.leidenuniv.nl)

*Mathematisch Instituut, Leiden University, Leiden, Netherlands*

# Algebra & Number Theory

[msp.org/ant](http://msp.org/ant)

## EDITORS

### MANAGING EDITOR

Bjorn Poonen  
Massachusetts Institute of Technology  
Cambridge, USA

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

### BOARD OF EDITORS

Bhargav Bhatt	University of Michigan, USA	Raman Parimala	Emory University, USA
Richard E. Borcherds	University of California, Berkeley, USA	Jonathan Pila	University of Oxford, UK
Antoine Chambert-Loir	Université Paris-Diderot, France	Irena Peeva	Cornell University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Anand Pillay	University of Notre Dame, USA
Brian D. Conrad	Stanford University, USA	Michael Rapoport	Universität Bonn, Germany
Samit Dasgupta	Duke University, USA	Victor Reiner	University of Minnesota, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Joseph H. Silverman	Brown University, USA
Hubert Flenner	Ruhr-Universität, Germany	Michael Singer	North Carolina State University, USA
Sergey Fomin	University of Michigan, USA	Christopher Skinner	Princeton University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Wee Teck Gan	National University of Singapore	J. Toby Stafford	University of Michigan, USA
Andrew Granville	Université de Montréal, Canada	Shunsuke Takagi	University of Tokyo, Japan
Ben J. Green	University of Oxford, UK	Pham Huu Tiep	University of Arizona, USA
Joseph Gubeladze	San Francisco State University, USA	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Michel van den Bergh	Hasselt University, Belgium
Roger Heath-Brown	Oxford University, UK	Akshay Venkatesh	Institute for Advanced Study, USA
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Philippe Michel	École Polytechnique Fédérale de Lausanne	Kei-Ichi Watanabe	Nihon University, Japan
Susan Montgomery	University of Southern California, USA	Melanie Matchett Wood	University of California, Berkeley, USA
Shigefumi Mori	RIMS, Kyoto University, Japan	Shou-Wu Zhang	Princeton University, USA
Martin Olsson	University of California, Berkeley, USA		

## PRODUCTION

[production@msp.org](mailto:production@msp.org)

Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.

---

The subscription price for 2020 is US \$415/year for the electronic version, and \$620/year (+\$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.


---

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

---

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2020 Mathematical Sciences Publishers

# Algebra & Number Theory

Volume 14 No. 1 2020

---

Gorenstein-projective and semi-Gorenstein-projective modules CLAUS MICHAEL RINGEL and PU ZHANG	1
The 16-rank of $\mathbb{Q}(\sqrt{-p})$ PETER KOYMANS	37
Supersingular Hecke modules as Galois representations ELMAR GROSSE-KLÖNNE	67
Stability in the homology of unipotent groups ANDREW PUTMAN, STEVEN V SAM and ANDREW SNOWDEN	119
On the orbits of multiplicative pairs OLEKSIY KLURMAN and ALEXANDER P. MANGEREL	155
Birationally superrigid Fano 3-folds of codimension 4 TAKUZO OKADA	191
Coble fourfold, $\mathfrak{S}_6$ -invariant quartic threefolds, and Wiman–Edge sextics IVAN CHELTSOV, ALEXANDER KUZNETSOV and KONSTANTIN SHRAMOV	213