Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 179 NOVEMBER 2025 PART 3

Math. Proc. Camb. Phil. Soc. (2025), **179**, 519–539 © The Author(s), 2025. Published by Cambridge University Press on behalf of Cambridge Philosophical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

doi: 10.1017/S0305004125000428

First published online 11 July 2025

Elliptic curves and spin

BY PETER KOYMANS

Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 *TA Utrecht, The Netherlands.*

e-mail: p.h.koymans@uu.nl

AND PETER VANG UTTENTHAL

Department of Mathematics, Aarhus University, 8000 *Aarhus C, Denmark.*

e-mail: petervang@math.au.dk

(*Received* 24 *July* 2024*; revised* 04 *April* 2025*; accepted* 04 *April* 2025)

Abstract

In the early 2000s, Ramakrishna asked the question: for the elliptic curve

$$E : y^2 = x^3 - x,$$

what is the density of primes p for which the Fourier coefficient $a_p(E)$ is a cube modulo p? As a generalisation of this question, Weston–Zaurova formulated conjectures concerning the distribution of power residues of degree m of the Fourier coefficients of elliptic curves $E/\mathbb{Q}$ with complex multiplication. In this paper, we prove the conjecture of Weston–Zaurova for cubic residues using the analytic theory of spin. Our proof works for all elliptic curves E with complex multiplication.

2020 Mathematics Subject Classification: 11R44, 11N35, 11G05, 11G15 (Primary); 11R37, 11F80 (Secondary)

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

1. *Introduction*

For the elliptic curve

$$E : y^2 = x^3 - x,$$

with complex multiplication by $\mathbb{Q}(i)$ and error terms

$$a_p(E) = p + 1 - |E(\mathbb{F}_p)|,$$

are there infinitely many primes $p \equiv 1 \bmod 12$ such that $a_p(E)$ is a cubic residue modulo p? This question was formulated by Ramakrishna in the early 2000s. At that time, the question was perceived as interesting yet inaccessible. Note that it is natural to restrict to primes $p \equiv 1 \bmod 12$. Indeed, for $p \equiv 3 \bmod 4$, we have $a_p(E) = p + 1$ if $p \geq 5$, so $a_p(E)$ is a cube modulo p. Furthermore, all elements of $\mathbb{F}_p$ are automatically cubes if $p \equiv 2 \bmod 3$, so in particular $a_p(E)$ is once more a cube modulo p.

In 2005, Weston [**16**] formulated a family of conjectures inspired by the question, but only for elliptic curves without complex multiplication. In a subsequent paper, Weston and Zaurova considered the analogous conjectures for elliptic curves over $\mathbb{Q}$ with complex multiplication. Write w_K for the number of roots of unity contained in a number field K.

CONJECTURE 1·1 (Weston–Zaurova [**17**, conjecture 3·1]). *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field K. Let m be an integer coprime with w_K. Then the density of primes $p \equiv 1 \bmod m$ with $a_p(E) \neq 0$ for which $a_p(E)$ is an mth power residue modulo p is $1/m$. Furthermore, the density is independent of any Chebotarev class $\mathcal{P}$ contained in the set of primes $p \equiv 1 \bmod m$ with $a_p(E) \neq 0$ in the sense that if the primes are restricted to $\mathcal{P}$, the relative density remains $1/m$.*

Note that, for all but finitely many primes, $p \equiv 1 \bmod m$ and the reduction of E at p being ordinary is equivalent to p splitting completely in $K(\zeta_m)$.

In [**16, 17**], Weston and Zaurova prove the special cases of the conjecture to which classical techniques are applicable. In particular, they settle the case when $K = \mathbb{Q}(\sqrt{-3})$ and $m = 3$ by using that K contains the third roots of unity so that the classical cubic reciprocity law is available. For this reason, we exclude the field $K = \mathbb{Q}(\sqrt{-3})$ in the statements of this paper.

In contrast, the classical techniques do not apply to the case $K = \mathbb{Q}(i)$ and $m = 3$, and therefore the original question for the curve $E : y^2 = x^3 - x$ remained open. In this paper, we answer Ramakrishna's question in the affirmative, and prove that among the primes $p \equiv 1 \bmod 3$ for which $E : y^2 = x^3 - x$ has ordinary reduction (equivalently, $p \equiv 1 \bmod 4$ for $p \geq 5$), the density of $a_p(E)$ being a cubic residue modulo p is $1/3$. In addition, we prove Conjecture 1·1 for all elliptic curves with complex multiplication (CM) by an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ where $d \neq 3$ in the case of cubic power residues (i.e. $m = 3$). We do not need the curves to be defined over $\mathbb{Q}$, nor do we need them to have CM by a maximal order; it suffices that they have CM by some order $\mathcal{O}$ in K and are defined over the ring class field L of $\mathcal{O}$.

To prove the main theorems of this paper, we extend the analytic theory of spin to cubic symbols over totally imaginary biquadratic fields. Our results are *unconditional*, as we do not need to assume any standard conjectures on short character sums. This is atypical for results on spin symbols, which are most often conditional on such conjectures.

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

THEOREM 1·2. *Let K be an imaginary quadratic field satisfying* $\gcd(3, w_K) = 1$, *or equivalently* $K \neq \mathbb{Q}(\zeta_3)$. *For any prime p that splits completely in K as $(\pi\overline{\pi})$, where $\overline{\pi}$ is the conjugate of π, and where π lies below a prime ideal $\mathfrak{p}$ in $K(\zeta_3)$, there is a well-defined cubic spin symbol of the form*

$$[\mathfrak{p}] = \left(\frac{\overline{\pi}}{\mathfrak{p}}\right)_{K(\zeta_3),3}.$$

Furthermore, there is a constant $C > 0$ such that for all $X \geqslant 100$

$$\left|\sum_{N_{K(\zeta_3)/\mathbb{Q}}(\mathfrak{p}) \leqslant X} [\mathfrak{p}]\right| \leqslant CX^{1-\frac{1}{3200}}.$$

One readily checks that the symbol does not depend on the choice of generator π, see Proposition 2·3. The last part of Theorem 1·2 lies much deeper and its proof occupies the majority of this paper.

As a corollary, for any elliptic curve E with complex multiplication by an imaginary quadratic field K, we prove asymptotics with a power saving error term for the primes p that split completely in $K(\zeta_3)$ such that $a_p(E)$ is a cubic residue modulo p. Let us now explain what we mean by $a_p(E)$ in this context.

Let E be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K and let L be the ring class field of $\mathcal{O}$. Assume that E is defined over L. If we take a prime $\mathfrak{P}$ above p where E has good reduction, we may introduce the quantity

$$a_{\mathfrak{P}}(E) = p + 1 - |E(O_L/\mathfrak{P})|. \tag{1·1}$$

If $\mathcal{O}^\times = \{\pm 1\}$ and if $\mathfrak{P}'$ is another prime of L above p, it is a classical result of Deuring that $a_{\mathfrak{P}}(E)^2 = a_{\mathfrak{P}'}(E)^2$, i.e. $a_{\mathfrak{P}}(E)$ is determined up to sign (for a reference, see our Lemma 2·2). Therefore $a_{\mathfrak{P}}(E)$ being a cube modulo p does not depend on the choice of prime $\mathfrak{P}$. A somewhat more involved argument gives the same result if $\mathcal{O}^\times = \{\pm 1, \pm i\}$, see Proposition 2·3.

Since it is possible to impose arbitrary congruence conditions when handling spin symbols, we are able to get density results even when imposing arbitrary *abelian splitting conditions*.

COROLLARY 1·3. *Let E be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K different from $\mathbb{Q}(\zeta_3)$. Suppose E is defined over the ring class field L of $\mathcal{O}$. Then*

$$\frac{\#\{p \leqslant X, p \equiv 1 \bmod 3, p \text{ splits in } L : a_{\mathfrak{P}}(E) \text{ is a cube modulo } p\}}{\#\{p \leqslant X, p \equiv 1 \bmod 3, p \text{ splits in } L\}} = \frac{1}{3} + O\left(\frac{1}{X^{1/3200}}\right).$$

Here $a_{\mathfrak{P}}(E)$ is defined as in equation (1·1) with $\mathfrak{P}$ an arbitrary prime of L above p.

If $\mathcal{P}$ is a Chebotarev class of rational primes defined by a splitting condition in an abelian extension of $K(\zeta_3)$ containing L and projecting trivially in $Gal(L/\mathbb{Q})$, then the result remains valid when the set of primes is restricted to p with $p \in \mathcal{P}$.

The Chebotarev density theorem gives the density of unramified primes with given splitting behavior in a number field. However, several examples arise naturally in number theory

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

concerning the splitting behavior of primes in fields that depend on the prime itself, and in such instances, Chebotarev is insufficient. Instead, these types of questions often fall in the realm of spin symbols.

One example is the theory of level-raising. Level-raising goes back to work of Ribet in the 1980s on modular forms and their associated odd Galois representations. In the late 90s, Ramakrishna [**11**] initiated the study of an analogous theory of level-raising in the context of even Galois representations. Ramakrishna observed that level-raising at p is possible if and only if p splits correctly in a field depending on p.

More generally, in the theory of lifting Galois representations, the key objects controlling the situation are the so-called Selmer and dual Selmer groups. The ranks of Selmer groups can be modified by introducing ramification at new, auxiliary primes, given that such a prime splits correctly in a field that generally depends on p itself.

For an imaginary quadratic field K and a prime p, we let $K^{(m)}(p)$ be the maximal abelian extension of K killed by m and unramified away from p. We prove the following density theorem on the splitting of primes p in the number fields $K^{(m)}(p)$ that depend on p. In the statement of Theorem 1·4, the splitting condition on p is imposed to control the size of the maximal abelian extension of K unramified away from p.

Our next theorem is a prototypical example of this type of question: splitting of p in a number field depending on p. In order to state it, we let m be a prime and let ζ_m be a primitive mth root of unity. Let F be a number field, and define

$$V_{\emptyset} = \{x \in F^{\times} : (x) = J^m \text{ for some fractional ideal } J\},$$

where (x) is the fractional ideal generated by $x \in F^{\times}$. We define the m-governing field of F to be the field $F(\zeta_m, \sqrt[m]{V_{\emptyset}})$. These types of governing fields have been extensively studied in the literature, see for example [**3, 4**] for background material on governing fields.

THEOREM 1·4 (Splitting in number fields that depend on the prime). *Let K be an imaginary quadratic field and let $m \geq 3$ be a prime such that* $\gcd(m, w_K) = 1$. *Let $\mathcal{O}$ be an order in K, and let p be a prime that splits completely in the ring class field of $\mathcal{O}$ and the m-governing field of K. Let $K^{(m)}(p)$ be the maximal m-elementary abelian extension of K unramified away from p, and let $f(p, K^{(m)}(p)/\mathbb{Q})$ be the inertial degree at p in $K^{(m)}(p)/\mathbb{Q}$. Then $[\mathfrak{p}] = 1$ if and only if $f(p, K^{(m)}(p)/\mathbb{Q}) = 1$.*

In particular, for $m = 3$, among the primes p splitting completely in the ring class field of $\mathcal{O}$ and the 3-governing field, the set of primes p of residue field degree 1 at any prime in $K^{(3)}(p)$ above p has density $1/3$.

In this theorem, we are using implicitly that the density results on spin symbols remain valid when the class of primes considered is restricted to Chebotarev classes defined by Chebotarev conditions in abelian extensions of $K(\zeta_3)$. We expect that it is possible to prove the Weston–Zaurova conjecture for all power residues m by applying techniques from the joint distribution of spins from Koymans–Milovic [**6**]. However, such results would be conditional on short character sum conjectures.

Below, we state a corollary of Theorem 1·2.

COROLLARY 1·5. *Let ℓ be a prime, and let*

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(2, \mathbb{Z}_{\ell})$$

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

be a Galois representation arising from the Galois action on ℓ^∞-torsion points of an elliptic curve over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ where $d \neq -3$. Let S be the smallest set of places containing ℓ and the archimedean place of $\mathbb{Q}$ such that ρ is unramified outside S. For primes $p \notin S$, let Frob_p *be any lift of Frobenius to $Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Among the primes $p \equiv 1 \bmod 3$ splitting completely in the ring class field of* $\mathrm{End}_{\mathbb{C}}(E)$*,*

$$\mathrm{trace}\,(\rho(\,\mathrm{Frob}_p\,)) \in \mathbb{Z}$$

is a cube modulo p one third of the time.

Our method of proof of Theorem 1·2 relies on a version of Vinogradov's sieve extended to totally imaginary biquadratic fields. In [2], Friedlander–Iwaniec–Mazur–Rubin introduced quadratic spin symbols of primes in totally real, cyclic number fields (satisfying some additional technical conditions) and proved equidistribution of such symbols by extending Vinogradov's sieve to totally real, cyclic fields. In general, their results are conditional on standard conjectures on short character sums (denoted C_n in their paper where n is the degree of the totally real cyclic number field), and their results are only unconditional in the case $n = 3$. In this paper, we extend the methods in [2] to *cubic* spin symbols over biquadratic, totally imaginary fields of degree 4 over $\mathbb{Q}$. It is natural to compare this to work of Merikoski [8], although we should warn the reader that his spin symbol is not the same as ours.

Our main analytic accomplishment is to make our equidistribution results unconditional in this setting. To make our results unconditional, we follow a similar strategy strategy as employed previously by Koymans–Milovic [5] and Piccolo [10]. However, unlike the works [5, 10], we do not assume that our biquadratic field has class number 1 and we deal with cubic symbols instead of quartic symbols.

2. *General spin symbols*

In this section we introduce our cubic spin symbol of interest, and relate it to $a_p(E)$. This symbol is a natural generalisation of the spin symbol introduced in [2]. In fact, it turns out that the algebraic part of our theory readily generalises to all m, not just $m = 3$. We start by identifying a family of spin symbols, indexed by m, capturing whether the error terms $a_p(E)$ are power residues modulo m. This is achieved in Proposition 2·3. We will then relate this to splitting of p in a number field depending on p, see Lemma 2·10.

2·1. *Power residue symbols*

We shall briefly recall the required theory of power residue symbols that we need. Let M be a number field always containing a fixed primitive mth root of unity that we denote ζ_m. For $\alpha \in O_M$ and $\mathfrak{p}$ a prime of M not dividing m, we define $(\alpha/\mathfrak{p})_{M,m}$ as the unique element in $\langle \zeta_m \rangle \cup \{0\}$ satisfying

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{M,m} \equiv \alpha^{\frac{N_{M/\mathbb{Q}}(\mathfrak{p})-1}{m}} \bmod \mathfrak{p}.$$

We multiplicatively extend this to all ideals I coprime to m.

For our application, the case $m = 3$ is particularly important. We will use the following weak form of cubic reciprocity.

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

PROPOSITION 2·1. *Let M be a number field containing ζ_3. Take elements $\alpha, \beta \in O_M$ and assume that β is coprime to 3. Then the cubic residue symbol $(\alpha/\beta)_{M,3}$ depends only on the congruence class of β modulo $27\alpha O_M$. Moreover, if α is also coprime to 3, we have*

$$\left(\frac{\alpha}{\beta}\right)_{M,3} = \mu \cdot \left(\frac{\beta}{\alpha}\right)_{M,3},$$

where μ depends only on the congruence classes of α and β modulo $27O_M$.

2·2. *Power residues of degree m and spin*

Let K be an imaginary quadratic field with maximal order $\mathcal{O}_K$. For any order $\mathcal{O}$ of conductor f in K, there is a unique abelian extension L/K called the ring class field of $\mathcal{O}$. We refer to [**1**, p. 179] for the definition of ring class fields.

We write σ for the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. To keep our notation brief, we shall frequently use conjugation to denote this automorphism, so that we may speak of $\bar{\kappa}$ for elements κ but also of $\bar{\mathfrak{q}}$ for (prime) ideals $\mathfrak{q}$.

LEMMA 2·2. *Let K be an imaginary quadratic field and let $\mathcal{O}$ be an order in K. Let L be the ring class field of $\mathcal{O}$, and let E be an elliptic curve over L with $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$. Let p be a prime that splits completely in L and $\mathfrak{P}$ be a prime in L above p (in particular, $O_L/\mathfrak{P} \simeq \mathbb{F}_p$). Suppose E has good reduction at $\mathfrak{P}$. Then there is $\kappa \in \mathcal{O}$ such that $p = \kappa\overline{\kappa}$ and*

$$a_{\mathfrak{P}}(E) = p + 1 - |E(O_L/\mathfrak{P})| = \kappa + \overline{\kappa}.$$

Proof. See [**1**, theorem 14·16].

PROPOSITION 2·3. *Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field and let $m \geq 3$ be any odd integer such that $\gcd(m, w_K) = 1$. Let $M = \mathbb{Q}(\sqrt{D}, \zeta_m)$ and let*

$$\mathrm{Gal}(M/\mathbb{Q}) \simeq \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \{1, \sigma\} \times (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

Let $\mathcal{O}$ be an order in K and let E be an elliptic curve defined over the ring class field of $\mathcal{O}$ with $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$. Let $p \equiv 1 \bmod m$ be a prime that splits completely in the ring class field of $\mathcal{O}$. According to Lemma 2·2, there exists $\kappa \in \mathcal{O}$ such that

$$p = \kappa\overline{\kappa}$$

and

$$a_{\mathfrak{P}}(E) = \kappa + \overline{\kappa},$$

where $\mathfrak{P}$ is a prime of L above p.

Let $\mathfrak{q} = (\kappa)$ and let $\mathfrak{p}$ be a prime in M above $\mathfrak{q}$.

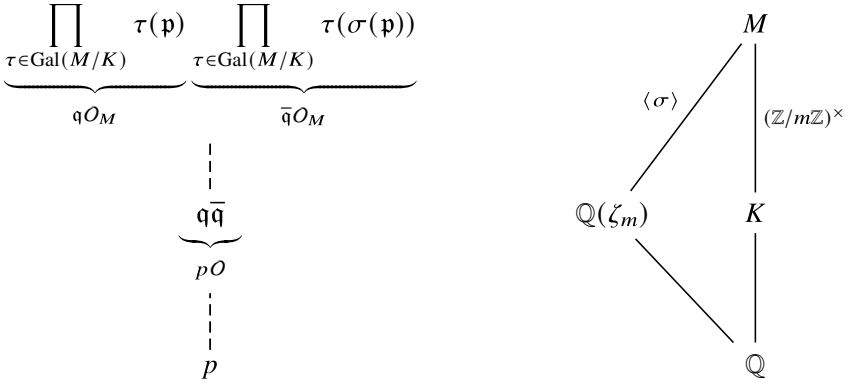
Define the spin symbol

$$[\mathfrak{p}] = \left(\frac{\overline{\kappa}}{\mathfrak{p}}\right)_{M,m} = \left(\frac{\sigma(\kappa)}{\mathfrak{p}}\right)_{M,m}.$$

If $u \in \mathcal{O}^{\times}$, then

$$\left(\frac{\overline{u\kappa}}{\mathfrak{p}}\right)_{M,m} = \left(\frac{\overline{\kappa}}{\mathfrak{p}}\right)_{M,m},$$

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press



so the spin symbol is well-defined, i.e. is independent on the choice of generator κ for $\mathfrak{q}$. Furthermore, $[\mathfrak{p}] = 1$ if and only if $a_{\mathfrak{P}}(E)$ is an mth power residue modulo p.

Proof. Since $p \equiv 1 \bmod m$, p splits completely in $\mathbb{Q}(\zeta_m)$. Since we assume p splits completely in K, we conclude that p splits completely in M. Since $\mathfrak{p}$ lies above $\mathfrak{q}$, $\sigma(\mathfrak{p})$ lies above $\sigma(\mathfrak{q}) = \overline{\mathfrak{q}}$. In M, the primes $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ decompose as follows:

$$\mathfrak{q}\mathcal{O}_M = \prod_{\tau\in\mathrm{Gal}(M/K)} \tau(\mathfrak{p}), \quad \overline{\mathfrak{q}}\mathcal{O}_M = \sigma(\mathfrak{q})\mathcal{O}_M = \prod_{\tau\in\mathrm{Gal}(M/K)} \tau(\sigma(\mathfrak{p})).$$

Since $\gcd(m, w_K) = 1$ by assumption, we see that all elements of $\mathcal{O}^\times$ are mth powers in K. We conclude that the spin symbol $[\mathfrak{p}]$ is independent of the choice of κ. Using that $\kappa \equiv 0 \bmod \mathfrak{p}$, we have by Lemma 2·2

$$[\mathfrak{p}] = \left(\frac{\overline{\kappa}}{\mathfrak{p}}\right)_{M,m} = \left(\frac{\overline{\kappa}+\kappa}{\mathfrak{p}}\right)_{M,m} = \left(\frac{a_{\mathfrak{P}}(E)}{\mathfrak{p}}\right)_{M,m}.$$

Hence $[\mathfrak{p}] = 1$ if and only if $a_{\mathfrak{P}}(E)$ is an mth power residue modulo $\mathfrak{p}$. Now, $\mathcal{O}_M/\mathfrak{p} \simeq \mathbb{F}_p$, so $a_{\mathfrak{P}}(E)$ is an mth power modulo $\mathfrak{p}$ if and only if $a_{\mathfrak{P}}(E)$ is an mth power modulo p.

2·3. *Definition of the spin symbol*

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with $d > 0$ squarefree. We will assume that $d \neq 3$. The field $M := K(\zeta_3)$ will play an important role throughout the paper. We fix the following data associated to M:

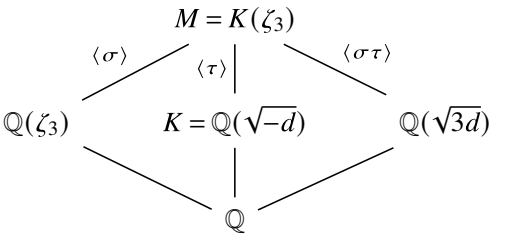
(1) we let $\{\eta_1, \ldots, \eta_4\}$ be an integral basis for O_M with $\eta_1 = 1$;
(2) the torsion subgroup of $O_M^\times$ is generated by ζ_{12} if $d = 1$, and otherwise the torsion subgroup is generated by ζ_6;
(3) we pick two disjoint collections of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_h$ coprime to $6d$, where each collection is a set of representatives for the class group $\mathrm{Cl}(M)$ of M. We let

$$\mathfrak{f} := \prod_{i=1}^{h} \mathfrak{p}_i \prod_{j=1}^{h} \mathfrak{q}_j, \qquad f := N_{M/\mathbb{Q}}(\mathfrak{f}). \tag{2·1}$$

Then $\mathfrak{f}$ is principal. Furthermore, we may choose $\mathfrak{p}_1, \ldots, \mathfrak{p}_h, \mathfrak{q}_1, \ldots, \mathfrak{q}_h$ in such a way that the norm f of $\mathfrak{f}$ is squarefree.

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

The field M is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to the Klein four group, say $\{1, \sigma, \tau, \sigma\tau\}$, which we depict diagrammatically as



Let $\mathfrak{p}$ be a completely split prime ideal of M. If $\mathfrak{p}\tau(\mathfrak{p})$ is a principal ideal of K, we define a symbol

$$[\mathfrak{p}] := \left(\frac{\sigma(\pi)}{\mathfrak{p}}\right)_{M,3} \in \{1, \zeta_3, \zeta_3^2\}, \qquad (\pi)O_K = \mathfrak{p}\tau(\mathfrak{p})O_K.$$

This does not depend on the choice of generator π of the O_K-ideal $\mathfrak{p}\tau(\mathfrak{p})O_K$, as changing π by a unit changes the total symbol by $(u/\mathfrak{p})_{M,3} = 1$ with $u \in \{\pm 1, \pm i\}$ for $d = 1$ and $u \in \{\pm 1\}$ for $d > 1$. One directly checks that

$$\sum_{\rho \in \mathrm{Gal}(M/\mathbb{Q})} [\rho(\mathfrak{p})] = \begin{cases} -2 & \text{if } [\mathfrak{p}] \in \{\zeta_3, \zeta_3^2\} \\ 4 & \text{if } [\mathfrak{p}] = 1. \end{cases}$$

More generally, if $\mathfrak{a}$ is any integral ideal of O_M such that $\mathfrak{a}\tau(\mathfrak{a})$ is a principal ideal of K, we define

$$[\mathfrak{a}] := \begin{cases} \left(\frac{\sigma(g)}{\mathfrak{a}}\right)_{M,3} & \text{if } \gcd(\mathfrak{a}, (3)) = 1 \\ 0 & \text{otherwise,} \end{cases}$$

where gO_K is any generator of $\mathfrak{a}\tau(\mathfrak{a})O_K$. This is once more independent of the choice of generator α of the ideal $\mathfrak{a}$. In particular, we have the useful formula

$$[(\alpha)] = \left(\frac{\sigma(\alpha)\sigma\tau(\alpha)}{\mathfrak{a}}\right)_{M,3} \tag{2·2}$$

for all $\alpha \in O_M$ coprime to 3.

2·4. *Field lowering*

The coming results are variations of the results in [5, subsection 3·2]. As these results play a key role in making our results unconditional, we shall provide full details for these variations. As the results in this subsection hold in significant generality, we allow K to be an arbitrary number field in this subsection only, and we shall return to the setting $K = \mathbb{Q}(\sqrt{-d})$ afterwards.

LEMMA 2·4. *Let K be a number field and let $\mathfrak{q}$ be a prime of K coprime to 3. Assume that M is a quadratic extension of K such that M contains ζ_3 and $\mathfrak{q}$ splits in M. Write σ for the*

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

non-trivial element of $\mathrm{Gal}(M/K)$. *Then we have for all* $\alpha \in O_K$

$$\left(\frac{\alpha}{\mathfrak{q}O_M}\right)_{M,3} = \begin{cases} \left(\frac{\alpha}{\mathfrak{q}O_K}\right)_{K,3}^2 & \text{if } \sigma \text{ fixes } \zeta_3 \\ \mathbf{1}_{\mathfrak{q}\nmid\alpha} & \text{if } \sigma \text{ does not fix } \zeta_3. \end{cases}$$

Proof. Since $\mathfrak{q}$ splits in M, we may write $\mathfrak{q}O_M = \mathfrak{Q}\sigma(\mathfrak{Q})$ for some prime $\mathfrak{Q}$ of M. This gives

$$\left(\frac{\alpha}{\mathfrak{q}O_M}\right)_{M,3} = \left(\frac{\alpha}{\mathfrak{Q}}\right)_{M,3}\left(\frac{\alpha}{\sigma(\mathfrak{Q})}\right)_{M,3} = \left(\frac{\alpha}{\mathfrak{Q}}\right)_{M,3}\left(\frac{\sigma(\alpha)}{\sigma(\mathfrak{Q})}\right)_{M,3} = \left(\frac{\alpha}{\mathfrak{Q}}\right)_{M,3}\sigma\left(\left(\frac{\alpha}{\mathfrak{Q}}\right)_{M,3}\right),$$

where we used that $\sigma(\alpha) = \alpha$ thanks to the assumption $\alpha \in O_K$. If σ fixes ζ_3, then the above becomes

$$\left(\frac{\alpha}{\mathfrak{Q}}\right)_{M,3}\sigma\left(\left(\frac{\alpha}{\mathfrak{Q}}\right)_{M,3}\right) = \left(\frac{\alpha}{\mathfrak{Q}}\right)_{M,3}^2 = \left(\frac{\alpha}{\mathfrak{q}O_K}\right)_{K,3}^2.$$

If σ does not fix ζ_3, then we get $\mathbf{1}_{\mathfrak{q}\nmid\alpha}$ by checking all possibilities for the cubic residue symbol $(\alpha/\mathfrak{Q})_{M,3} \in \{1, \zeta_3, \zeta_3^2, 0\}$.

LEMMA 2·5. *Let* K *be a number field and let* $\mathfrak{q}$ *be a prime of* K *coprime to* 3. *Assume that* M *is a quadratic extension of* K *such that* M *contains* ζ_3 *and assume that* $\mathfrak{q}$ *stays inert in* M. *Further assume that* $\mathfrak{q}$ *has degree* 1 *in* K *and let* q *be the prime of* $\mathbb{Q}$ *lying below* $\mathfrak{q}$. *Then we have for all* $\alpha \in O_K$

$$\left(\frac{\alpha}{\mathfrak{q}O_M}\right)_{M,3} = \begin{cases} \left(\frac{\alpha}{\mathfrak{q}O_K}\right)_{K,3}^2 & \text{if } q \equiv 1 \bmod 3 \\ \mathbf{1}_{\mathfrak{q}\nmid\alpha} & \text{if } q \equiv 2 \bmod 3. \end{cases}$$

Proof. We have the identities

$$\left(\frac{\alpha}{\mathfrak{q}O_M}\right)_{M,3} \equiv \alpha^{\frac{N_{M/\mathbb{Q}}(\mathfrak{q})-1}{3}} \equiv \alpha^{\frac{q^2-1}{3}} \bmod \mathfrak{q}O_M.$$

If $q \equiv 1 \bmod 3$, we rewrite this as

$$\alpha^{\frac{q^2-1}{3}} \equiv \left(\alpha^{\frac{q-1}{3}}\right)^{q+1} \equiv \left(\alpha^{\frac{N_{K/\mathbb{Q}}(\mathfrak{q})-1}{3}}\right)^{q+1} \equiv \left(\frac{\alpha}{\mathfrak{q}O_K}\right)_{K,3}^{q+1} \equiv \left(\frac{\alpha}{\mathfrak{q}O_K}\right)_{K,3}^2 \bmod \mathfrak{q}.$$

If $q \equiv 2 \bmod 3$, we instead rewrite this as

$$\alpha^{\frac{q^2-1}{3}} \equiv \left(\alpha^{q-1}\right)^{\frac{q+1}{3}} \equiv \left(\alpha^{N_{K/\mathbb{Q}}(\mathfrak{q})-1}\right)^{\frac{q+1}{3}} \equiv \mathbf{1}_{\mathfrak{q}\nmid\alpha}^{\frac{q+1}{3}} \equiv \mathbf{1}_{\mathfrak{q}\nmid\alpha} \bmod \mathfrak{q}O_M,$$

as desired.

LEMMA 2·6. *Let* K *be a number field and let* M *be a quadratic extension of* K. *Write* σ *for the non-trivial element of* $Gal(M/K)$. *Assume that* $\mathfrak{q}$ *is a prime ideal of* K *that stays unramified in* M. *Further suppose that* $\beta \in O_M$ *satisfies* $\beta \equiv \sigma(\beta) \bmod \mathfrak{q}O_M$. *Then there is* $\beta' \in O_K$ *such that* $\beta' \equiv \beta \bmod \mathfrak{q}O_M$.

Proof. This is proven in [5, lemma 3·4].

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

2·5. *Spin and inertial degrees of ramified primes*

Let m be a prime. For any set S of tame places in a number field F, define

$$V_S = \{x \in F^\times : (x) = J^m \text{ for some fractional ideal } J, \text{ and } x \in F_v^{\times m}\ \forall v \in S\}.$$

Note that, by definition, $F^{\times m} \subseteq V_S$. Let $\mathcal{O}_F^\times$ be the units in F and $\mathrm{Cl}_F[m]$ the m-torsion in the class group of F. There is an exact sequence

$$1 \longrightarrow \mathcal{O}_F^\times \otimes \mathbb{F}_m \longrightarrow V_\emptyset / F^{\times m} \longrightarrow \mathrm{Cl}_F[m] \longrightarrow 1.$$

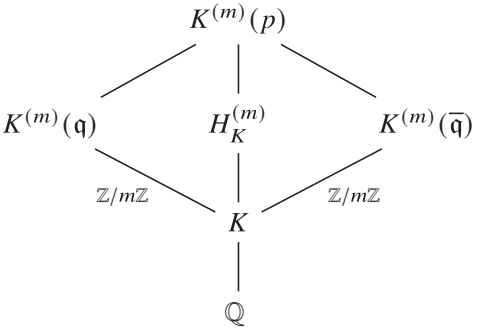
The m-governing field of F is the field $F(\zeta_m, \sqrt[m]{V_\emptyset})$, where ζ_m is a primitive mth root of unity.

Recall that $K^{(m)}(p)$ denotes the maximal m-elementary abelian extension of K unramified away from the primes above p. Write $H_K^{(m)}$ for the maximal unramified m-elementary abelian extension of K.

LEMMA 2·7. *Let K be an imaginary quadratic field and let m be a prime. Let p be a prime that splits completely in the m-governing field of K, and factor $pO_K = \mathfrak{q}\overline{\mathfrak{q}}$. Then there exists a $\mathbb{Z}/m\mathbb{Z}$-extension $K^{(m)}(\mathfrak{q})/K$ ramified exactly at $\mathfrak{q}$ and a $\mathbb{Z}/m\mathbb{Z}$-extension $K^{(m)}(\overline{\mathfrak{q}})/K$ ramified exactly at $\overline{\mathfrak{q}}$. For any choice of $K^{(m)}(\mathfrak{q})/K$ and $K^{(m)}(\overline{\mathfrak{q}})/K$ as above, we have*

$$K^{(m)}(p) = K^{(m)}(\mathfrak{q})K^{(m)}(\overline{\mathfrak{q}})H_K^{(m)},$$

and thus $[K^{(m)}(p) : \mathbb{Q}] = 2m^2 \cdot |Cl(K)[m]|$. Diagramatically



Proof. Since p splits completely in the m-governing field and since the m-governing field is ramified at m, it follows that $p \neq m$. Therefore, all primes of K above p must be tamely ramified in $K^{(m)}(p)/K$.

By the tame Gras–Munnier theorem, there exists a $\mathbb{Z}/m\mathbb{Z}$-extension of K ramified exactly at $\mathfrak{q}$. Likewise, there exists a $\mathbb{Z}/m\mathbb{Z}$-extension of K ramified exactly at $\overline{\mathfrak{q}}$. The compositum $K^{(m)}(\mathfrak{q})K^{(m)}(\overline{\mathfrak{q}})H_K^{(m)}$ is an m-elementary abelian extension of K unramified away from p with degree $m^2 \cdot |\mathrm{Cl}(K)[m]|$ over K, and hence has degree $2m^2 \cdot |\mathrm{Cl}(K)[m]|$ over $\mathbb{Q}$. We will now show that this implies $K^{(m)}(p) = K^{(m)}(\mathfrak{q})K^{(m)}(\overline{\mathfrak{q}})H_K^{(m)}$.

The inclusion $K^{(m)}(\mathfrak{q})K^{(m)}(\overline{\mathfrak{q}})H_K^{(m)} \subseteq K^{(m)}(p)$ is by definition, so it suffices to show that the degree of $K^{(m)}(p)$ over K is at most $m^2 \cdot |\mathrm{Cl}(K)[m]|$. By class field theory, we have a canonical isomorphism

$$\frac{\mathrm{Cl}(K,p)}{m\mathrm{Cl}(K,p)} = \mathrm{Gal}(K^{(m)}(p)/K),$$

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

Table 1. *The (e, f, g)-decomposition of p in* $K^{(m)}(p)/\mathbb{Q}$

$e(p, K^{(m)}(p)/\mathbb{Q})$	$f(p, K^{(m)}(p)/\mathbb{Q})$	$g(p, K^{(m)}(p)/\mathbb{Q})$	$[K^{(m)}(p):\mathbb{Q}]$
m	1	$2m \cdot \lvert\mathrm{Cl}(K)[m]\rvert$	$2m^2 \cdot \lvert\mathrm{Cl}(K)[m]\rvert$
m	m	$2 \cdot \lvert\mathrm{Cl}(K)[m]\rvert$	$2m^2 \cdot \lvert\mathrm{Cl}(K)[m]\rvert$

where $\mathrm{Cl}(K, p)$ denotes the ray class group of conductor p. By the ray class group sequence, we have

$$0 \to \frac{(O_K/p)^\times}{\mathrm{im}\, O_K^\times} \to \mathrm{Cl}(K, p) \to \mathrm{Cl}(K) \to 0.$$

The functor sending an abelian group A to A/mA is right exact, so we get a new exact sequence

$$\frac{(O_K/p)^\times}{(O_K/p)^{\times m} \cdot \mathrm{im}\, O_K^\times} \to \frac{\mathrm{Cl}(K, p)}{m\mathrm{Cl}(K, p)} \to \frac{\mathrm{Cl}(K)}{m\mathrm{Cl}(K)} \to 0.$$

This gives the bound

$$\begin{aligned}[K^{(m)}(p) : K] &= \left|\frac{\mathrm{Cl}(K, p)}{m\mathrm{Cl}(K, p)}\right| \le \left|\frac{(O_K/p)^\times}{(O_K/p)^{\times m} \cdot \mathrm{im}\, O_K^\times}\right| \cdot \left|\frac{\mathrm{Cl}(K)}{m\mathrm{Cl}(K)}\right| \\ &= \left|\frac{(O_K/p)^\times}{(O_K/p)^{\times m} \cdot \mathrm{im}\, O_K^\times}\right| \cdot |\mathrm{Cl}(K)[m]|. \end{aligned} \tag{2·3}$$

Finally, since $pO_K = \mathfrak{q}\overline{\mathfrak{q}}$, we get an isomorphism

$$(O_K/p)^\times \cong (O_K/\mathfrak{q})^\times \times (O_K/\overline{\mathfrak{q}})^\times \cong \mathbb{F}_p^\times \times \mathbb{F}_p^\times.$$

Since $\mathbb{F}_p^\times$ is cyclic, this gives the upper bounds

$$\left|\frac{(O_K/p)^\times}{(O_K/p)^{\times m} \cdot \mathrm{im}\, O_K^\times}\right| \le \left|\frac{(O_K/p)^\times}{(O_K/p)^{\times m}}\right| \le m^2.$$

Combining this with (2·3) shows that the degree of $K^{(m)}(p)$ over K is at most $m^2 \cdot |\mathrm{Cl}(K)[m]|$, as desired.

LEMMA 2·8. *Let K be an imaginary quadratic field and let m be a prime. Let p be a prime that splits completely in the m-governing field of K. There are two possibilities for the standard (e, f, g)-decomposition of p in* $K^{(m)}(p)$ (Table 1):

Proof. Because p is unramified in K and tamely ramified in $K^{(m)}(p)/K$, and because tame ramification is cyclic, we have $e(p, K^{(m)}(p)/\mathbb{Q}) = m$. Since $f(p, K/\mathbb{Q}) = 1$, and since $\mathrm{Gal}(K^{(m)}(p)/K)$ is a vector space over $\mathbb{F}_m$, it follows that $f(p, K^{(m)}(p)/\mathbb{Q})$ is either 1 or m. By Lemma 2·7, we have

$$e(p, K^{(m)}(p)/\mathbb{Q}) f(p, K^{(m)}(p)/\mathbb{Q}) g(p, K^{(m)}(p)/\mathbb{Q}) = 2m^2 \cdot |\mathrm{Cl}(K)[m]|,$$

and the result follows.

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

LEMMA 2·9. *Let m be a prime. Suppose p splits completely in the m-governing field of a quadratic imaginary field K and in $H_K^{(m)}$. Then we have for any choice of $K^{(m)}(\overline{\mathfrak{q}})$*

$$f(p, K^{(m)}(p)/\mathbb{Q}) = 1 \iff f(\mathfrak{q}, K^{(m)}(\overline{\mathfrak{q}})/K) = 1.$$

Proof. Note that the compositum $K^{(m)}(\overline{\mathfrak{q}})H_K^{(m)}$ does not depend on the choice of $K^{(m)}(\overline{\mathfrak{q}})/K$ as it is the maximal m-elementary abelian extension of K unramified away from $\mathfrak{q}$. Since p is assumed to split completely in $H_K^{(m)}$, we conclude that $f(\mathfrak{q}, K^{(m)}(\overline{\mathfrak{q}})/K)$ is independent of this choice.

Since $f(p, K/\mathbb{Q}) = 1$, we have $f(p, K^{(m)}(p)/\mathbb{Q}) = f(\mathfrak{q}, K^{(m)}(p)/K)$. Because $K^{(m)}(p) = K^{(m)}(\mathfrak{q})K^{(m)}(\overline{\mathfrak{q}})H_K^{(m)}$ and because p splits completely in $H_K^{(m)}$, we conclude that

$$\begin{aligned} f(p, K^{(m)}(p)/\mathbb{Q}) = 1 &\iff f(\mathfrak{q}, K^{(m)}(p)/K) = 1 \\ &\iff f(\mathfrak{q}, K^{(m)}(\mathfrak{q})/K) = 1 \text{ and } f(\mathfrak{q}, K^{(m)}(\overline{\mathfrak{q}})/K) = 1. \end{aligned} \tag{2·4}$$

Since $e(\mathfrak{q}, K^{(m)}(\mathfrak{q})/K) = m$, the condition $f(\mathfrak{q}, K^{(m)}(\mathfrak{q})/K) = 1$ is automatically satisfied. Removing it from the equivalence (2·4) gives the lemma.

LEMMA 2·10. *Let K be an imaginary quadratic field and let $m \geq 3$ be any odd integer such that* $\gcd(m, w_K) = 1$. *Set $M := K(\zeta_m)$. Let $\mathcal{O}$ be an order in K. Let p be a prime that splits completely in the ring class field of $\mathcal{O}$ and the m-governing field of K, and let $\kappa \in \mathcal{O}$ with $p = \kappa\overline{\kappa}$. Let $\mathfrak{q} = (\kappa)$, $\mathfrak{p}$ a prime in M above $\mathfrak{q}$ and $[\mathfrak{p}] = (\overline{\kappa}/\mathfrak{p})_{M,m}$. Then we have for any choice of $K^{(m)}(\overline{\mathfrak{q}})$*

$$f(\mathfrak{q}, K^{(m)}(\overline{\mathfrak{q}})/K) = 1 \iff [\mathfrak{p}] = 1.$$

Proof. Let $G(\overline{\mathfrak{q}})$ be the full ray class group of modulus $\overline{\mathfrak{q}}$ above K and let $K(\overline{\mathfrak{q}})$ be the full ray class field of modulus $\overline{\mathfrak{q}}$ above K. If $\psi_{K(\overline{\mathfrak{q}})/K}$ is the Artin reciprocity map, there is a commutative diagram

$$\begin{array}{ccc} G(\overline{\mathfrak{q}}) & \xrightarrow{\psi_{K(\overline{\mathfrak{q}})/K}} & \mathrm{Gal}(K(\overline{\mathfrak{q}})/K) \\ \downarrow & & \downarrow \\ G(\overline{\mathfrak{q}})/G(\overline{\mathfrak{q}})^m & \longrightarrow & \mathrm{Gal}(K^{(m)}(\overline{\mathfrak{q}})H_K^{(m)}/K), \end{array}$$

where the horizontal arrows are isomorphisms. Let Cl_K be the class group of K. By [**9**, theorem 1.7, chapter V], there is a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (\mathcal{O}/\overline{\mathfrak{q}})^\times/\mathcal{O}^\times & \xrightarrow{\varphi} & G(\overline{\mathfrak{q}}) & \longrightarrow & \mathrm{Cl}_K & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & (\mathcal{O}/\overline{\mathfrak{q}})^\times/(\mathcal{O}/\overline{\mathfrak{q}})^{\times m} & \longrightarrow & G(\overline{\mathfrak{q}})/G(\overline{\mathfrak{q}})^m & \longrightarrow & \mathrm{Cl}_K/\mathrm{Cl}_K^m & \longrightarrow & 1 \end{array}$$

with exact horizontal rows. Here we used that $\mathcal{O}^\times \subseteq (\mathcal{O}/\overline{\mathfrak{q}})^{\times m}$, which follows from our assumption $\gcd(m, w_K) = 1$ as then every element of $\mathcal{O}^\times$ must be an mth power.

By definition, $\varphi(\kappa) = \mathfrak{q}$. Observe that p certainly splits in $H_K^{(m)}$, as $H_K^{(m)}$ is contained in the ring class field of $\mathcal{O}$. Therefore we conclude that

$$\begin{aligned} f(\kappa, K^{(m)}(\overline{\mathfrak{q}})/K) = 1 &\iff f(\kappa, K^{(m)}(\overline{\mathfrak{q}})H_K^{(m)}/K) = 1 \\ &\iff \kappa \text{ is an } m\text{th power modulo } \overline{\mathfrak{q}}. \end{aligned}$$

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

Now, κ is an mth power modulo $\overline{\mathfrak{q}}$ if and only if κ is an mth power modulo any prime in $\mathcal{O}_M$ above $\overline{\mathfrak{q}}$ if and only if

$$\left(\frac{\kappa}{\sigma(\mathfrak{p})}\right)_{M,m} = 1.$$

Since $\mathbb{Q}(\zeta_m)$ is the fixed field of σ, we have the equalities

$$1 = \left(\frac{\kappa}{\sigma(\mathfrak{p})}\right)_{M,m} \Longleftrightarrow 1 = \sigma\left(\frac{\kappa}{\sigma(\mathfrak{p})}\right)_{M,m} = \left(\frac{\sigma(\kappa)}{\sigma^2(\mathfrak{p})}\right)_{M,m} = \left(\frac{\sigma(\kappa)}{\mathfrak{p}}\right)_{M,m} = \left(\frac{\overline{\kappa}}{\mathfrak{p}}\right)_{M,m} = [\mathfrak{p}],$$

as desired.

3. *Analytic prerequisites*

In this section we set up the analytic machinery that we will use in the next two sections. Our approach is based on [5].

3·1. *A fundamental domain*

Given an integral ideal $\mathfrak{a}$ of M, there are many possible generators α of $\mathfrak{a}$. For our analytic purposes, it will be useful to pick these generators in a systematic way. To this end, we decompose $O_M^\times$ as $T \times \langle \epsilon \rangle$, where T is the torsion subgroup and where ϵ is a fundamental unit. We write V for the group generated by ϵ.

Using our fixed integral basis $\{\eta_1, \eta_2, \eta_3, \eta_4\}$ of M, we get an isomorphism, in the category of vector spaces, $\iota : \mathbb{Q}^4 \to M$ by sending $(a_1, \ldots, a_4)$ to $a_1\eta_1 + a_2\eta_2 + a_3\eta_3 + a_4\eta_4$. We also view $\mathbb{Q}^4$ as a subset of $\mathbb{R}^4$ in the natural way. For a subset S of $\mathbb{R}^4$ and an element $\alpha = a_1\eta_1 + a_2\eta_2 + a_3\eta_3 + a_4\eta_4 \in M$, we will abuse notation by writing $\alpha \in S$ to mean $(a_1, \ldots, a_4) \in S$. Given a subset S of $\mathbb{R}^4$ and a real number $X > 0$, we define $S(X)$ to be the subset of $(s_1, \ldots, s_4) \in S$ satisfying $f(s_1, \ldots, s_4) \leq X$, where f is the norm polynomial $f(X_1, \ldots, X_4) = N_{M/\mathbb{Q}}(\eta_1 X_1 + \eta_2 X_2 + \eta_3 X_3 + \eta_4 X_4) \in \mathbb{Z}[X_1, \ldots, X_4]$. We write $\mathcal{D}$ for the fundamental domain constructed in [5, section 3·3]. The main properties of this fundamental domain can be found in [5, lemma 3·5] that we summarise now.

LEMMA 3·1. *There exists a subset $\mathcal{D} \subseteq \mathbb{R}^4$ with the following properties*:

(i) *for all non-zero $\alpha \in O_M$, there exists a unique unit $v \in V$ with $v\alpha \in \mathcal{D}$. Moreover, we have $\{u \in O_M^\times : u\alpha \in \mathcal{D}\} = \{vt : t \in T\}$;*

(ii) *the set $\mathcal{D}(1)$ has a 3-Lipschitz parametrisable boundary. Furthermore, there exists a constant $C > 0$ such that the boundary of $\mathcal{D}(1)$ intersects every line in at most C points*;

(iii) *there exists a constant $C > 0$ such that for all $\alpha = a_1\eta_1 + a_2\eta_2 + a_3\eta_3 + a_4\eta_4 \in \mathcal{D}$ (with $a_i \in \mathbb{Z}$), we have $|a_i| \leq C|N_{M/\mathbb{Q}}(\alpha)|^{1/4}$.*

3·2. *Vinogradov's sieve*

We will now state the main sieve that we will use. This sieve was originally developed by Vinogradov in the context of representing odd integers as sums of three primes. Recall that $M := K(\zeta_3)$. From now on we shall abbreviate $N_{M/\mathbb{Q}}$ simply as N and our ideals will be ideals of O_M unless otherwise indicated.

In order to prove our later results, we will handle a slightly more general symbol than $[\mathfrak{p}]$. To this end, fix an ideal $\mathfrak{M}$ of M and an invertible element $\mu \in O_M/\mathfrak{M}O_M$. We introduce

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

the function $r_i(\mathfrak{a}, \mu, \mathfrak{M})$ for $i = 1, \dots, h$, which is the indicator function of $\mathfrak{a}\mathfrak{p}_i$ having a generator α satisfying $\alpha \equiv \mu \bmod \mathfrak{M}$; recall that $\mathfrak{p}_i$ is one of our fixed representatives for $\mathrm{Cl}(M)$. We shall treat μ and $\mathfrak{M}$ as fixed throughout the paper, and we shall abbreviate $r_i(\mathfrak{a}) := r_i(\mathfrak{a}, \mu, \mathfrak{M})$. We will assume throughout the paper that $\mathfrak{M}$ is divisible by f, see equation (2·1).

PROPOSITION 3·2. *For every $\epsilon > 0$, there exists a constant $C > 0$ such that*

$$\left| \sum_{\substack{N(\mathfrak{a}) \leq X \\ \mathfrak{m} \mid \mathfrak{a}}} r_i(\mathfrak{a})[\mathfrak{a}] \right| \leq C X^{1-\frac{1}{24}+\epsilon}$$

uniformly for all non-zero integral ideals $\mathfrak{m}$ of O_M and all $X \geq 2$.

Proof. The proof of this proposition is postponed until Section 4.

PROPOSITION 3·3. *For every $\epsilon > 0$, there exists a constant $C > 0$ such that*

$$\left| \sum_{N(\mathfrak{m}) \leq M} \sum_{N(\mathfrak{n}) \leq N} \alpha_{\mathfrak{m}} \beta_{\mathfrak{n}} r_i(\mathfrak{m}\mathfrak{n})[\mathfrak{m}\mathfrak{n}] \right| \leq C(M+N)^{\frac{1}{24}} (MN)^{1-\frac{1}{24}+\epsilon}$$

uniformly for all $M, N \geq 2$ and all sequences of complex numbers $|\alpha_{\mathfrak{m}}| \leq 1$ and $|\beta_{\mathfrak{n}}| \leq 1$.

Proof. The proof of this proposition is postponed until Section 5.

Once Propositions 3·2 and 3·3 are proven, Vinogradov's sieve for number fields gives the following result.

THEOREM 3·4. *For every $\epsilon > 0$, there exists a constant $C > 0$ such that*

$$\left| \sum_{N(\mathfrak{p}) \leq X} r_i(\mathfrak{p})[\mathfrak{p}] \right| \leq C X^{1-\frac{1}{3136}+\epsilon}$$

for all $X \geq 2$.

Proof. Propositions 3·2 and 3·3 together with Vinogradov's sieve for number fields as presented in [**2**, proposition 5·2] yield

$$\left| \sum_{N(\mathfrak{a}) \leq X} r_i(\mathfrak{a})[\mathfrak{a}] \Lambda(\mathfrak{a}) \right| \leq C X^{1-\frac{1}{3136}+\epsilon},$$

where Λ is the natural generalisation of the von Mangoldt function to number fields. The theorem is then a direct consequence of partial summation.

4. *Sums of type* I

This section is entirely devoted to the proof of Proposition 3·2. Our proof follows among the same lines as [**5**, section 4] and [**2**, section 6]. From now on we fix a non-zero integral ideal $\mathfrak{m}$ of O_M. Let $\mathfrak{M}$ be an ideal of O_M divisible by f and let μ be an element of O_M coprime to $\mathfrak{M}$. Recall that we introduced the function $r_i(\mathfrak{a})$ for $i = 1, \dots, h$, which is the

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

indicator function of $\mathfrak{a}\mathfrak{p}_i$ having a generator α satisfying $\alpha \equiv \mu \bmod \mathfrak{M}$ (recall that $\mathfrak{p}_i$ is one of our fixed representatives for $\mathrm{Cl}(M)$). We set

$$F = 2^4 \cdot 3^{3h+4} \cdot N(\mathfrak{M}) \cdot \Delta(M/\mathbb{Q}),$$

where $\Delta(M/\mathbb{Q})$ is the absolute discriminant. Each non-zero ideal has exactly 6 or 12 generators in $\mathcal{D}$, which is exactly the size of the torsion subgroup T. Further splitting the sum into progressions modulo F, we unwrap the sum as

$$\begin{aligned}\sum_{\substack{N(\mathfrak{a})\le X\\ \mathfrak{m}\mid\mathfrak{a}}} r_i(\mathfrak{a})[\mathfrak{a}] &= \frac{1}{|T|}\sum_{\substack{\alpha\in\mathcal{D}(XN(\mathfrak{p}_i))\\ \alpha\equiv 0 \bmod \mathfrak{m}\mathfrak{p}_i}} r_i((\alpha)/\mathfrak{p}_i)[(\alpha)/\mathfrak{p}_i]\\ &= \frac{1}{|T|}\sum_{\rho \bmod F}\sum_{\substack{\alpha\in\mathcal{D}(XN(\mathfrak{p}_i))\\ \alpha\equiv 0 \bmod \mathfrak{m}\mathfrak{p}_i\\ \alpha\equiv\rho \bmod F}} r_i((\alpha)/\mathfrak{p}_i)[(\alpha)/\mathfrak{p}_i],\end{aligned}$$

where our first identity is justified due to the change of variables $\mathfrak{a}\mathfrak{p}_i = (\alpha)$. We claim that

$$[(\alpha)/\mathfrak{p}_i] = [(\alpha)] \cdot \gamma_\rho \tag{4·1}$$

for all $\alpha \equiv \rho \bmod F$, where γ_ρ is some fixed number in $\{1, \zeta_3, \zeta_3^2, 0\}$ depending only on ρ and i. To prove the claim, first note that the claim holds if $\sigma(\mathfrak{p}_i)\sigma\tau(\mathfrak{p}_i)$ is not a principal ideal of K as we may simply take $\gamma_\rho = 0$. Henceforth we assume that $\sigma(\mathfrak{p}_i)\sigma\tau(\mathfrak{p}_i)$ is principal and generated by some element $g \in O_K$, and we may similarly assume that α is coprime to 3. Recalling the identity (2·2), we see that

$$\begin{aligned}[(\alpha)/\mathfrak{p}_i] &= \left(\frac{\sigma(\alpha)\sigma\tau(\alpha)/g}{(\alpha)/\mathfrak{p}_i}\right)_{M,3} = \left(\frac{\sigma(\alpha)\sigma\tau(\alpha)g^2}{(\alpha)\mathfrak{p}_i^2}\right)_{M,3}\\ &= [(\alpha)]\left(\frac{g}{\alpha}\right)^2_{M,3}\left(\frac{\sigma(\alpha)\sigma\tau(\alpha)}{\mathfrak{p}_i}\right)^2_{M,3}\left(\frac{g^2}{\mathfrak{p}_i^2}\right)_{M,3}.\end{aligned} \tag{4·2}$$

In the first line of the above display, we have used that α is coprime to f (as $\mathfrak{M}$ is divisible by f by assumption), and hence to $N_{M/\mathbb{Q}}(\mathfrak{p}_i)$, and that $\mathfrak{p}_i$ is an unramified prime of degree 1 so that $\mathfrak{p}_i$ is coprime to g. Applying Proposition 2·1 to $(g^2/\alpha)_{M,3}$, it follows that each of the individual symbols in (4·2) depends only on ρ and i. Hence the claim follows.

We also note that $r_i((\alpha)/\mathfrak{p}_i)$ depends only on $\alpha \bmod F$. Prompted by these calculations, we define for each $\rho \bmod F$ and each ideal $\mathfrak{m}$

$$A(X,\rho) = \sum_{\substack{\alpha\in\mathcal{D}(X)\\ \alpha\equiv 0 \bmod \mathfrak{m}\\ \alpha\equiv\rho \bmod F}} [(\alpha)].$$

By the above manipulations it suffices to estimate each $A(X,\rho)$ individually. Furthermore, we may assume that $\gcd(3,\rho) = (1)$ as otherwise the symbol $[(\alpha)]$ is constantly zero.

Recalling that $\eta_1 = 1$ by convention and writing $\mathbb{M} = \mathbb{Z}\eta_2 + \mathbb{Z}\eta_3 + \mathbb{Z}\eta_4$ allows us to decompose $O_M = \mathbb{Z} \oplus \mathbb{M}$. Therefore every $\alpha \in O_M$ can uniquely be written as

$$\alpha = a + \beta, \qquad a \in \mathbb{Z}, \beta \in \mathbb{M}.$$

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

This transforms the sum $A(X, \rho)$ as

$$A(X,\rho) = \sum_{\substack{a+\beta \in \mathcal{D}(X) \\ a+\beta \equiv 0 \bmod \mathfrak{m} \\ a+\beta \equiv \rho \bmod F}} \left(\frac{\sigma(a+\beta)}{a+\beta}\right)_{M,3} \left(\frac{\sigma\tau(a+\beta)}{a+\beta}\right)_{M,3}$$

due to equation (2·2). Our aim is now to rewrite the cubic residue symbols. We have

$$\left(\frac{\sigma(a+\beta)}{a+\beta}\right)_{M,3} = \left(\frac{a+\sigma(\beta)}{a+\beta}\right)_{M,3} = \left(\frac{\sigma(\beta)-\beta}{a+\beta}\right)_{M,3},$$

and similarly for the other cubic residue symbol. If $\sigma(\beta)-\beta = 0$ or if $\sigma\tau(\beta)-\beta = 0$, then our cubic residue symbols are constantly 0 and we may safely remove such β from consideration. In all other cases, we are thus incentivised to factor $\sigma(\beta)-\beta$ and $\sigma\tau(\beta)-\beta$. Define $\mathfrak{c}$ to be the largest divisor of $\sigma(\beta)-\beta$ coprime to F and define $\mathfrak{c}'$ to be the largest divisor of $\sigma\tau(\beta)-\beta$ coprime to F. We claim that

$$\left(\frac{\sigma(\beta)-\beta}{a+\beta}\right)_{M,3} = \mu_1 \cdot \left(\frac{a+\beta}{\mathfrak{c}}\right)_{M,3}, \qquad \left(\frac{\sigma\tau(\beta)-\beta}{a+\beta}\right)_{M,3} = \mu_2 \cdot \left(\frac{a+\beta}{\mathfrak{c}'}\right)_{M,3} \tag{4·3}$$

for some numbers $\mu_1, \mu_2 \in \{1, \zeta_3, \zeta_3^2, 0\}$ depending on ρ and β but not on a.

We will prove the claim for $(\sigma(\beta)-\beta)/a+\beta)_{M,3}$, the other residue symbol can be treated similarly. We choose a factorisation

$$(\sigma(\beta)-\beta) = (t_3^3)\mathfrak{c}\mathfrak{t}_1\mathfrak{t}_2$$

with the properties:

(1) $\mathfrak{t}_1 \mid F^\infty$ and is coprime to 3;
(2) $\mathfrak{t}_2 \mid 27^h$, where we recall that h denotes the class number of K, and $t_3 \mid 3^\infty$.

We emphasise that such a factorization always exists although may not be unique. We denote by $\mathfrak{C}$, $\mathfrak{T}_1$ and $\mathfrak{T}_2$ the fixed inverses in the class group of respectively $\mathfrak{c}$, $\mathfrak{t}_1$ and $\mathfrak{t}_2$ that we have chosen in Subsection 2.3. Then we have $\mathfrak{c}\mathfrak{C} = (g_0)$, $\mathfrak{t}_1\mathfrak{T}_1 = (g_1)$ and $\mathfrak{t}_2\mathfrak{T}_2 = (g_2)$. Because $\mathfrak{c}\mathfrak{t}_1\mathfrak{t}_2$ is principal, it follows that $\mathfrak{C}\mathfrak{T}_1\mathfrak{T}_2 = (g_3)$ must also be principal. For a good choice of generators g_i, it follows that

$$\sigma(\beta)-\beta = t_3^3 g_0 g_1 g_2 g_3^{-1}.$$

We conclude that

$$\left(\frac{\sigma(\beta)-\beta}{a+\beta}\right)_{M,3} = \left(\frac{g_0g_1g_2g_3^{-1}}{a+\beta}\right)_{M,3} = \left(\frac{g_0g_1g_2g_3^2}{a+\beta}\right)_{M,3} = \left(\frac{g_0g_1g_3^2}{a+\beta}\right)_{M,3} \left(\frac{g_2}{a+\beta}\right)_{M,3},$$

where we used that $a+\beta$ is coprime to $3f$. Since $(g_2) = \mathfrak{t}_2\mathfrak{T}_2$ divides $F/27$, Proposition 2·1 shows that the last symbol depends only on ρ and β. For the other symbol, we also apply Proposition 2·1 to obtain

$$\left(\frac{g_0g_1g_3^2}{a+\beta}\right)_{M,3} = \mu_3 \cdot \left(\frac{a+\beta}{g_0g_1g_3^2}\right)_{M,3}$$

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

for some number $\mu_3 \in \{1, \zeta_3, \zeta_3^2\}$ depending on ρ and β but not on a. We finally observe that

$$\left(\frac{a+\beta}{g_0 g_1 g_3^2}\right)_{M,3} = \left(\frac{a+\beta}{\mathfrak{c}}\right)_{M,3} \left(\frac{a+\beta}{\mathfrak{t}_1 \mathfrak{T}_2^2}\right)_{M,3}.$$

Since the last factor only depends on ρ and β, this proves our claim (4·3). We record our progress by applying the triangle inequality to deduce that

$$|A(X,\rho)| \leq \sum_{\beta \in \mathbb{M}} |T(X,\rho,\beta)|,$$

where

$$T(X,\rho,\beta) := \sum_{\substack{a \in \mathbb{Z} \\ a+\beta \in \mathcal{D}(X) \\ a+\beta \equiv 0 \bmod \mathfrak{m} \\ a+\beta \equiv \rho \bmod F}} \left(\frac{a+\beta}{\mathfrak{c}}\right)_{M,3} \left(\frac{a+\beta}{\mathfrak{c}'}\right)_{M,3}.$$

We will treat β as fixed and work towards estimating each $T(X,\rho,\beta)$ individually. It is at this stage that we bring the material from Subsection 2.4 into play. To this end, we remark that $\mathfrak{c}'$ is in fact the extension of an ideal of $\mathbb{Q}(\sqrt{3d})$. Here we use that $\mathfrak{c}'$ is coprime to F and thus the discriminant of M and that $\mathfrak{c}'$ is the largest such divisor of $\sigma\tau(\beta) - \beta$. From now on we shall view $\mathfrak{c}'$ as an ideal of $O_{\mathbb{Q}(\sqrt{3d})}$. We factor it as

$$\mathfrak{c}' O_{\mathbb{Q}(\sqrt{3d})} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$$

for prime ideals $\mathfrak{p}_i$ of $O_{\mathbb{Q}(\sqrt{3d})}$, so that

$$\left(\frac{a+\beta}{\mathfrak{c}' O_M}\right)_{M,3} = \prod_{i=1}^{k} \left(\frac{a+\beta}{\mathfrak{p}_i O_M}\right)_{M,3}^{e_i}.$$

Observe that the ideals $\mathfrak{p}_i$ are coprime to F by construction and hence unramified in the extension $M/\mathbb{Q}(\sqrt{3d})$. We now claim that

$$\left(\frac{a+\beta}{\mathfrak{p}_i O_M}\right)_{M,3} = \mathbf{1}_{\gcd(a+\beta, \mathfrak{p}_i) = (1)}. \tag{4·4}$$

Since $\mathfrak{p}_i$ divides $\mathfrak{c}'$ and since $\mathfrak{c}'$ divides $\sigma\tau(\beta) - \beta$, it follows that $\sigma\tau(a+\beta) \equiv a+\beta \bmod \mathfrak{p}_i O_M$. Therefore Lemma 2·6 allows us to replace $a+\beta$ by some $\beta' \in O_{\mathbb{Q}(\sqrt{3d})}$. Then Lemma 2·4 gives the claim in case $\mathfrak{p}_i$ splits in M. Instead suppose that $\mathfrak{p}_i$ stays inert in M. If we write p_i for the unique prime of $\mathbb{Z}$ below $\mathfrak{p}_i$, we certainly find that $p \equiv 2 \bmod 3$. In this case the claim is a consequence of Lemma 2·5.

Having proved our claim, we perform a similar operation on the other cubic residue symbol. This residue symbol shall not disappear, but we will be able to "lower it" to $\mathbb{Q}(\zeta_3)$. This is the crucial step in making our results unconditional compared to [**2**] despite working in a field of degree 4.

Arguing as before, we may view $\mathfrak{c}$ as the extension of an ideal of $\mathbb{Z}[\zeta_3]$, and by abuse of notation we shall view $\mathfrak{c}$ as an ideal of $\mathbb{Z}[\zeta_3]$ from now on. In this case we factor $\mathfrak{c}\mathbb{Z}[\zeta_3] = \mathfrak{g}\mathfrak{q}$,

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

where $\mathfrak{q}$ has squarefree norm, $\mathfrak{g}$ has squarefull norm and $\gcd(N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\mathfrak{g}), N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\mathfrak{q})) = 1$. Furthermore, observe that $\mathfrak{q}$ and $\mathfrak{g}$ are both coprime to F, so all prime divisors of $\mathfrak{q}$ and $\mathfrak{g}$ stay unramified in $M/\mathbb{Q}(\zeta_3)$. So far we have shown that

$$\left(\frac{a+\beta}{\mathfrak{c}O_M}\right)_{M,3} = \left(\frac{a+\beta}{\mathfrak{g}O_M}\right)_{M,3}\left(\frac{a+\beta}{\mathfrak{q}O_M}\right)_{M,3}.$$

Lemma 2·6 and the Chinese remainder theorem allow us to replace β by some $\beta' \in \mathbb{Z}[\zeta_3]$. Combining Lemma 2·4 and Lemma 2·5 yields

$$\left(\frac{a+\beta'}{\mathfrak{q}O_M}\right)_{M,3} = \left(\frac{a+\beta'}{\mathfrak{q}}\right)^2_{\mathbb{Z}[\zeta_3],3}, \tag{4·5}$$

as any prime $\mathfrak{p}$ in $\mathbb{Z}[\zeta_3]$ that stays inert in M satisfies $p \equiv 1 \bmod 3$ (writing $p := \mathfrak{p} \cap \mathbb{Z}$). Finally, as $q := N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\mathfrak{q})$ is squarefree, the Chinese remainder theorem guarantees the existence of some rational integer b with $\beta' \equiv b \bmod \mathfrak{q}$.

Thanks to equations (4·4) and (4·5), we have thus arrived at

$$T(X,\rho,\beta) = \sum_{\substack{a\in\mathbb{Z}\\ a+\beta\in\mathcal{D}(X)\\ a+\beta\equiv 0 \bmod \mathfrak{m}\\ a+\beta\equiv\rho \bmod F}} \left(\frac{a+\beta}{\mathfrak{g}O_M}\right)_{M,3}\cdot\left(\frac{a+b}{\mathfrak{q}}\right)^2_{\mathbb{Z}[\zeta_3],3}\cdot \mathbf{1}_{\gcd(a+\beta,\mathfrak{c}')=(1)}.$$

Following the proof on [**5**], we fix a modulo the radical g_0 of g and detect the condition $\mathbf{1}_{\gcd(a+\beta,\mathfrak{c}')=(1)}$ using the Mobius function. Continuing in the footsteps of [**5**], we apply the triangle inequality

$$|T(X,\rho,\beta)| \leq \sum_{a_0 \bmod g_0}\sum_{\mathfrak{d}\mid \mathfrak{c}'O_M} |T(X,\rho,\beta,a_0,\mathfrak{d})|,$$

where

$$T(X,\rho,\beta,a_0,\mathfrak{d}) := \sum_{\substack{a\in\mathbb{Z}\\ a+\beta\in\mathcal{D}(X)\\ a+\beta\equiv 0 \bmod \mathfrak{m}\\ a+\beta\equiv\rho \bmod F\\ a\equiv a_0 \bmod g_0\\ a+\beta\equiv 0 \bmod \mathfrak{d}}} \left(\frac{a+b}{\mathfrak{q}}\right)^2_{\mathbb{Z}[\zeta_3],3}.$$

Since squaring a cubic residue symbol is the same as conjugating it, we may now remove the square factor without changing the absolute value of $T(X,\rho,\beta,a_0,\mathfrak{d})$. After doing so, the sum $T(X,\rho,\beta,a_0,\mathfrak{d})$ has the same shape as [**5**, equation (4·2)]. Having successfully applied our field lowering technique, the remainder of the proof is identical to [**5**, p. 7422-7424].

5. *Sums of type* II

This section is entirely devoted to the proof of Proposition 3·3. This will be relatively straightforward, as the required tools have already been developed in the literature. This was started in [**5**, proposition 3·6], which is unfortunately not applicable here as the symbol is required to take values in $\{\pm 1, 0\}$. Smith [**14**] developed a very general large sieve that is

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

completely explicit in its dependence on the underlying number field. Another interesting recent result in this direction can be found in recent work of Santens [**12**]. Here we shall appeal to [**7**, proposition 4·3].

In the notation of [**7**], we shall use [**7**, proposition 4·3] with the integer M on [**7**, p. 11] equal to F, with the number field K equal to our $M = K(\zeta_3)$, with n equal to 4, with $\ell = 3$, with $t_1 = t_2 = 1$, with the function γ equal to

$$\gamma(w,z) := \left(\frac{\sigma(w)}{z}\right)_{M,3}\left(\frac{\sigma(z)}{w}\right)_{M,3}\left(\frac{\sigma\tau(w)}{z}\right)_{M,3}\left(\frac{\sigma\tau(z)}{w}\right)_{M,3}$$

and with A_{bad} the set of squarefull integers. Then we can take C_1 to be an absolute constant ($C_1 = 100$ suffices) and $C_2 = 1/2$. We now check that this data satisfies the conditions (P1)-(P4) form [**7**, p. 11-12].

Condition (P1) is a consequence of Proposition 2·1. Condition (P2) follows from the definition of the cubic residue symbol. Condition (P4) is readily verified by counting squarefull integers in the usual way. Finally, (P3) follows from the Chinese remainder theorem and orthogonality of characters. Applying [**7**, proposition 4·3], we exhibit, for any given $\epsilon > 0$, the existence of a constant $C(\epsilon) > 0$ satisfying the inequality

$$\sum_{\substack{w\in\mathcal{D}(X)\\ w\equiv\delta_1 \bmod F}}\sum_{\substack{z\in\mathcal{D}(Y)\\ z\equiv\delta_2 \bmod F}}\alpha_w\beta_z\gamma(w,z) \le C(\epsilon)(X+Y)^{\frac{1}{24}}(XY)^{1-\frac{1}{24}+\epsilon} \tag{5·1}$$

for all α_w, β_z of magnitude bounded by 1.

With this calculated, recall that our aim is to demonstrate the bound

$$\left|\sum_{N(\mathfrak{m})\le M}\sum_{N(\mathfrak{n})\le N}\alpha_{\mathfrak{m}}\beta_{\mathfrak{n}}r_i(\mathfrak{m}\mathfrak{n})[\mathfrak{m}\mathfrak{n}]\right| \le C(M+N)^{\frac{1}{24}}(MN)^{1-\frac{1}{24}+\epsilon}.$$

Let us first deal with the case that $\mathfrak{m}$ and $\mathfrak{n}$ are both principal. Observe that every principal ideal has exactly $|T|$ generators in $\mathcal{D}$ by Lemma 3·1, so our sum becomes

$$\frac{1}{|T|^2}\sum_{w\in\mathcal{D}(M)}\sum_{z\in\mathcal{D}(N)}\alpha_w\beta_z r_i(wz)[wz]. \tag{5·2}$$

We note that $r_i(wz)$ depends only on wz mod F and that

$$[(wz)] = \gamma(w,z)\left(\frac{\sigma(w)}{w}\right)_{M,3}\left(\frac{\sigma(z)}{z}\right)_{M,3}\left(\frac{\sigma\tau(w)}{w}\right)_{M,3}\left(\frac{\sigma\tau(z)}{z}\right)_{M,3}.$$

Absorbing the last four cubic residue symbols in the coefficients α_w, β_z and splitting the sum over congruence classes modulo F shows that we can bound the expression (5·2) by at most F^8 sums appearing in the inequality (5·1).

This finishes the proof of Proposition 3·3 when the ideals $\mathfrak{m}$, $\mathfrak{n}$ of that proposition are restricted to principal ideals. The general case is handled by appealing to (4·1) and reducing to the case of principal ideals.

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

6. *Proof of main theorems*

In this section, we gather our previous results to prove our main theorems.

6·1. *Proof of Theorem* 1·2

Define $\mathcal{I}$ to be the set of indices $1 \leq i \leq h$ such that our fixed generator $\mathfrak{p}_i$ of $\mathrm{Cl}(M)$ has principal norm in K. Then Theorem 1·2 is an immediate consequence of Theorem 3·4 by taking $\mathfrak{M} = fO_M$ and summing over all $\mu \in (O_M/\mathfrak{M}O_M)^\times$ and all $i \in \mathcal{I}$.

6·2. *Proof of Corollary* 1·3

We take $\mathcal{I}$ as above, and we write $\tilde{f}$ for the conductor of $\mathcal{O}$. We also take $\mathfrak{M} = f\tilde{f}O_M$. The first part of Corollary 1·3 follows from Proposition 2·3 and Theorem 3·4 by summing over all $i \in \mathcal{I}$ and summing over the relevant $\mu \in (O_M/f\tilde{f}O_M)^\times$.

The second part of Corollary 1·3 follows by enlarging $\mathfrak{M}$ and choosing μ appropriately to account for the additional splitting condition.

6·3. *Proof of Theorem* 1·4

The first part of Theorem 1·4 is an entirely algebraic statement which is proven by combining Lemma 2·9 and Lemma 2·10. The last part of Theorem 1·4 is a consequence of Theorem 3·4.

6·4. *Proof of Corollary* 1·5

We shall now give the necessary background in Galois representations to relate Corollary 1·5 to Corollary 1·3.

Proof of Corollary 1·5. For any elliptic curve E, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ℓ^∞-torsion points of E gives rise to a Galois representation ρ ramified at finitely many places. By [**13**, theorem V·2·3·1], at each unramified place p, the error term $a_{\mathfrak{P}}(E)$ coincides with the trace of the image under ρ of any Frobenius lift at p. Therefore Corollary 1·5 is a consequence of Corollary 1·3.

Acknowledgements. The authors are thankful to Ravi Ramakrishna and Fabien Pazuki for helpful conversations. The authors are also indebted to the anonymous referee for their careful reading of the manuscript. Koymans gratefully acknowledges the support of Dr. Max Rössler, the Walter Haefner Foundation and the ETH Zürich Foundation. Uttenthal was supported by a research grant (VIL54509) from Villum Fonden.

REFERENCES

[1] D. A. COX. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication* (John Wiley and Sons, Inc., 1989).
[2] J. B. FRIEDLANDER, H. IWANIEC, B. MAZUR and K. RUBIN. The spin of prime ideals. *Invent. Math.* **193** (2013), 697–749.
[3] G. GRAS and A. MUNNIER. *Extensions cycliques T-totalement ramifiées*, Théorie des nombres, Années 1996/97–1997/98 (Publ. Math. UFR *Sci*. Tech. Besançon, Univ. Franche-Comté, Besançon, 1999), p. 16.
[4] F. HAJIR, C. MAIRE and R. RAMAKRISHNA. On tame $\mathbb{Z}/p\mathbb{Z}$-extensions with prescribed ramification. *Canad. Math. Bull.* **67** (1) (2024), 40–48.
[5] P. KOYMANS and D. MILOVIC. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \bmod 4$. *Internat. Math. Res. Not.*, no. 23 (2019), 7406–7427.
[6] P. KOYMANS and D. MILOVIC. Joint distribution of spins. *Duke Math. J.* **170** (8) (2021), 1723–1755.

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press

[7] P. KOYMANS and N. ROME. Weak approximation on the norm one torus. *Compositio Math.* **160** (6) (2024), 1304-1348.
[8] J. MERIKOSKI. A cubic analogue of the Friedlander–Iwaniec spin over primes. *Math. Z.* **300** (2022), 2809–2835.
[9] J.S. MILNE. *Class field theory (v4.03)*, (2020). Available at jmilne.org/math/, pp. 287+viii.
[10] M. PICCOLO. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-3p})$ for primes p congruent to 1 modulo 4. *Acta Arith.* **202** (2022), 1–20.
[11] R. RAMAKRISHNA. Deforming an even representation. II. Raising the level. *J. Number Theory* **72** (1) (1998), 92–109.
[12] T. SANTENS. Diagonal quartic surfaces with a Brauer–Manin obstruction. *Compositio Math.* **159** (4) (2023), 659–710.
[13] J. H. SILVERMAN. *The Arithmetic of Elliptic Curves*, 2nd ed. Graduate Texts in Math. **106** (Springer, 1986).
[14] A. SMITH. The distribution of ℓ^∞-Selmer groups in degree ℓ twist families I, *Preprint*: ArXiv: 2207.05674 (2022).
[15] O. TAUSSKY. Prof. David Hilbert, For.Mem.R.S.. *Nature*, no. 3850, Obituaries (August 14, 1943), p. 182.
[16] T. WESTON. Power residues of Fourier coefficients of modular forms. Canad. J. Math. **57** (5) (2005), 1102–1120.
[17] T. WESTON and E. ZAUROVA. Power residues of Fourier coefficients of elliptic curves with complex multiplication. *Internat. J. Number Theory* **5** (1) (2009), 109–124.

https://doi.org/10.1017/S0305004125000428 Published online by Cambridge University Press