Mathematische Zeitschrift

Check for
updates

A cubic analogue of the Friedlander–Iwaniec spin over primes

Jori Merikoski[1]

Abstract

In 1998 Friedlander and Iwaniec proved that there are infinitely many primes of the form $a^2 + b^4$. To show this they used the Jacobi symbol to define the spin of Gaussian integers, and one of the key ingredients in the proof was to show that the spin becomes equidistributed along Gaussian primes. To generalize this we define the cubic spin of ideals of $\mathbb{Z}[\zeta_{12}] = \mathbb{Z}[\zeta_3, i]$ by using the cubic residue character on the Eisenstein integers $\mathbb{Z}[\zeta_3]$. Our main theorem says that the cubic spin is equidistributed along prime ideals of $\mathbb{Z}[\zeta_{12}]$. The proof of this follows closely along the lines of Friedlander and Iwaniec. The main new feature in our case is the infinite unit group, which means that we need to show that the definition of the cubic spin on the ring of integers lifts to a well-defined function on the ideals. We also explain how the cubic spin arises if we consider primes of the form $a^2 + b^6$ on the Eisenstein integers.

Contents

✉ Jori Merikoski
  jori.merikoski@maths.ox.ac.uk

[1] Mathematical Institute, University of Oxford, Andrew Wiles Building Radcliffe Observatory Quarter (550), Woodstock Road, Oxford OX2 6GG, UK

1 Introduction

Friedlander and Iwaniec [1] famously showed that there are infinitely many prime numbers represented by $a^2 + b^4$. Remarkable here is that numbers of this form are very sparse, that is, the number of such integers up to x is of order $x^{3/4}$. Other similar results are Heath-Brown's proof that there are infinitely many primes of the form $a^3 + 2b^3$ [6], the generalization of Heath-Brown and Moroz of this to binary cubic forms [8], the extension of this by Maynard to general incomplete norm forms [11], and the result of Heath-Brown and Li [7] that the Friedlander–Iwaniec result holds also with b restricted to prime values.

If a prime p is of the form $a^2 + b^4$, then $p = \pi\overline{\pi}$ for some Gaussian prime $\pi = b^2 + ia$, so that the arithmetic in the work of Friedlander and Iwaniec really lies in $\mathbb{Z}[i]$. For a Gaussian integer $z = r + is$ with r odd, define the quadratic spin as

$$[z]_2 := \left(\frac{s}{r} \right)_2,$$

where $(s/r)_2$ is the Jacobi symbol. One of the key ingredients in the proof of Friedlander and Iwaniec is to show that the spin is equidistributed along Gaussian primes [1, Theorem 2], which they obtained in the form

$$\sum_{\substack{p=r^2+s^2\leq x \\ 2\nmid r}} \left(\frac{s}{r} \right)_2 \ll x^{1-1/77}. \tag{1.1}$$

This has been generalized by Milovic to show equidistribution of $(v/u)_2$ over primes of the form $p = u^2 - 2v^2$, which corresponds to the above with $\mathbb{Z}[\sqrt{2}]$ in place of $\mathbb{Z}[i]$ [14, Theorem 2].

It is natural to ask if the argument can be extended to produce primes of the form $a^2 + b^6$. Friedlander and Iwaniec have solved the ternary divisor problem for this sequence [3], and under the assumption of the existence of exceptional Dirichlet characters they have shown that there are infinitely many primes of this form [2].

sAt the moment there seems to be two major obstacles to solving the problem of primes of the form $a^2 + b^6$. Firstly, the sequence of integers is now too sparse to replicate the steps in [1, Sects. 5–9]. The second problem is structural. Recall that the proof of (1.1) relies on the law of quadratic reciprocity. With the sequence $a^2 + b^6$ we end up with cubic residues which unfortunately do not satisfy a suitable reciprocity law on $\mathbb{Z}$.

The second obstacle can be overcome if we extend the whole set-up from $\mathbb{Z}$ to the Eisenstein integers $\mathbb{Z}[\zeta_3]$, where the cubic residue character does satisfy a reciprocity law (see Lemma 4). Unfortunately the first issue remains and we are not able to detect primes of $\mathbb{Z}[\zeta_3]$ of the form $a^2 + b^6$ with $a, b \in \mathbb{Z}[\zeta_3]$ (see Sect. 9 for more details). However, we can still obtain the analogue of (1.1) in this situation and thus make partial progress on this problem. The Gaussian integers now correspond to the ring $\mathbb{Z}[\zeta_{12}] = \mathbb{Z}[\zeta_3, i]$ of integers of the twelfth cyclotomic extension, since the relative norm is $N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_3)}(r + is) = r^2 + s^2$ for $r, s \in \mathbb{Q}(\zeta_3)$.

We say that $z \in \mathbb{Z}[\zeta_{12}]$ is primary if $z \equiv \pm 1 \pmod 3$. For any $(z, 3) = 1$ there exists a unit μ such that μz is primary. For a primary number $z = r + is \in \mathbb{Z}[\zeta_{12}]$ we define the cubic spin

$$[z]_3 := \left[\frac{s}{r} \right]_3,$$

where $[s/r]_3$ is the cubic residue character on $\mathbb{Z}[\zeta_3]$ (see Sect. 2 for details). We extend this to the ideals $\mathfrak{a}$ of $\mathbb{Z}[\zeta_{12}]$ by defining $[\mathfrak{a}]_3 := [z]_3$ if z is a primary generator of $\mathfrak{a}$ with $(r, s) = 1$ and set $[\mathfrak{a}]_3 = 0$ otherwise. In Sect. 3 we will show that this definition does not depend on the choice of the primary associate z (note that by Dirichlet's unit theorem there are infinitely many possible choices). Our main theorem says that the values of the cubic spin are equidistributed along prime ideals of $\mathbb{Z}[\zeta_{12}]$.

Theorem 1 *We have*

$$\sum_{N_{\mathbb{Q}(\zeta_{12})}\,\mathfrak{p}\leq x} [\mathfrak{p}]_3 \ll x^{1-1/143}.$$

Similarly as in [1, Theorem 2], the exponent 1/143 is not the best that could be obtained and we have opted for simplicity in the proof over optimality.

The above cubic spin and the spin of Friedlander and Iwaniec [1] should not be confused with the spin of a prime ideal as defined by Friedlander, Iwaniec, Mazur, and Rubin [4].

Note that for a given prime $\mathfrak{p} = (r + is)$ all of its Galois conjugates appear in the sum, which means that the sum is real. Indeed, for $r + is$ primary we have

$$\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})} [\sigma(r+is)]_3 = \left[\frac{s}{r}\right]_3 + \left[\frac{-s}{r}\right]_3 + \left[\frac{\bar{s}}{\bar{r}}\right]_3 + \left[\frac{-\bar{s}}{\bar{r}}\right]_3 = 4\,\mathrm{Re}\left(\left[\frac{s}{r}\right]_3\right)$$

by using the properties $[\bar{s}/\bar{r}]_3 = \overline{[s/r]_3}$ and $[-s/r]_3 = [s/r]_3$.

Note also that for $\pi = r^2 + s^2$ with $r + is$ primary we have by cubic reciprocity (Lemma 4)

$$\left[\frac{s}{r}\right] = \left[\frac{s^2}{r}\right]^2 = \left[\frac{\pi}{r}\right]^2 = \left[\frac{r}{\pi}\right]^2, \tag{1.2}$$

ssince $r + is$ being primary implies that r and π are primary in $\mathbb{Z}[\zeta_3]$. Thus, our main theorem implies that r is a cube modulo primes π asymptotically one third of the time (to prove this, expand $1_{r\equiv t^3 \pmod{\pi}} = (1 + [r/\pi] + [r/\pi]^2)/3$ and note that $\sum[\mathfrak{p}]_3^2 = \sum\overline{[\mathfrak{p}]_3}$).

Corollary 2 *We have*

$$\sum_{\substack{N_{\mathbb{Q}(\zeta_3)}\pi\leq x \\ \pi=r^2+s^2, \\ r\equiv\pm1 \pmod{3},\, 3|s}} 1_{r\equiv t^3 \pmod{\pi}} = \frac{1}{3} \sum_{\substack{N_{\mathbb{Q}(\zeta_3)}\pi\leq x \\ \pi=r^2+s^2, \\ r\equiv\pm1 \pmod{3},\, 3|s}} 1 + O(x^{1-1/143}).$$

Remark 1 Since we prove that $[\mathfrak{a}]_3$ is independent of the choice of the primary generator $z = r + is$, this means by (1.2) that for primes $\pi = r^2 + s^2$ the property that $r \equiv t^3 \pmod{\pi}$ is independent of the representation $\pi = r^2 + s^2$ where $r + is$ is primary, so that the sum in the above corollary is well-defined. The corollary may be viewed as an approximation to the problem of primes of the form $t^6 + s^2$ on $\mathbb{Z}[\zeta_3]$ – instead of r being a perfect cube, it is a cube modulo $\pi = r^2 + s^2$.

For any integer $n \geq 1$ define

$$\lambda_3(n) := \sum_{N_{\mathbb{Q}(\zeta_{12})}\,\mathfrak{a}=n} [\mathfrak{a}]_3.$$

For rational primes we get the following corollary of Theorem 1 (the error term we get from the proof of Theorem 1 is actually $O_\epsilon(x^{1-1/142+\epsilon})$ so that the same error term holds for the corollary below).

Corollary 3 *We have*

$$\sum_{n \leq x} \Lambda(n)\lambda_3(n) \ll x^{1-1/143}.$$

Remark 2 The proof of Theorem 1 relies mainly on the law of cubic reciprocity. Thus, it seems plausible that the result can be generalized as follows. If an algebraic number field K contains a primitive mth root of unity, then we can define the mth power residue character on K which satisfies a reciprocity law (see [13, Chapter VIII, Theorem 5.11], for instance). Given a quadratic extension L/K we can then define a spin at elements of $\mathcal{O}_L$. It seems plausible that the argument could be generalized to obtain equidistribution of the spin along principal prime ideals of L. We hope to attack this question in a future article. Probably some assumptions are required here. At least in the simplest case of $K = \mathbb{Q}(\zeta_m)$ with m odd prime and $L = K[i]$ many parts of the argument seem to generalize nicely.

Remark 3 In [1, Sect. 23] Friedlander and Iwaniec write "We suspect, but have not examined thoroughly, that $\lambda(n)$ are related to the Fourier coefficients of some kind of metaplectic Eisenstein series or a cusp form, by analogy to the Hecke eigenvalues (16.30) which generate a modular form of integral weight." Similarly, we expect that $\lambda_3(n)$ can be interpreted in terms of automorphic forms. Working out the details of this would be useful with a view towards the generalization outlined in the previous remark.

Remark 4 We suspect that our main theorem has some applications to elliptic curves over $\mathbb{Z}[\zeta_3]$ but we do not have anything particularly interesting. For example, if $\pi = r^2 + s^2$ is a prime and $r \equiv t^3 \pmod{\pi}$, then Corollary 2 provides us with a large family of elliptic curves $E : Y^2 = X^3 + 3t^2 X \pm 2s$ with bad reduction at some large prime $\pi = \pi(E)$.

1.1 A brief sketch of the Friedlander–Iwaniec argument

We present here a non-rigorous sketch of the proof of (1.1) which appears in [1, Sects. 19–26]. Recall that the claim is that

$$\sum_{\substack{z \in \mathbb{Z}[i] \\ |z|^2 = p \leq x}} [z]_2 \ll x^{1-1/77},$$

where $[r + is]_2 = (s/r)_2$ is the usual Jacobi symbol. The summation needs to be restricted to odd r but let us ignore this in the notation to simplify the presentation. Then by a sieve argument (essentially Vaughan's identity) the task is reduced to bounding Type I sums

$$\sum_{|w|^2 \sim M} \alpha_w \sum_{|z|^2 \sim N} [wz]_2 \tag{1.3}$$

and Type II sums

$$\sum_{|w|^2 \sim M} \alpha_w \sum_{|z|^2 \sim N} \beta_z [wz]_2, \tag{1.4}$$

where α_w and β_z are arbitrary bounded coefficients and $MN = x$ with sufficiently flexible ranges for M and N.

For $w = u + iv$ with $(u, v) = 1$, let $\omega \equiv -vu^{-1} \pmod{u^2 + v^2}$, where u^{-1} denotes the multiplicative inverse, so that $\omega^2 \equiv -1 \pmod{u^2 + v^2}$. Similarly as in [1, Sect. 19],

for any $z = r + is$ we define

$$\left(\frac{z}{w}\right)_2 := \left(\frac{r + \omega s}{u^2 + v^2}\right)_2.$$

Since $\omega^2 \equiv -1 \pmod{u^2 + v^2}$, this symbol is completely multiplicative in the upper variable and is therefore a quadratic character modulo $u^2 + v^2$. We also have $(z/w_1)_2(z/w_2)_2 = (z/w_1 w_2)_2$ provided that $(w_1, \overline{w_2}) = 1$. The general multiplicativity rule in the lower part is not much more complicated, but to simplify let us pretend that the symbol is completely multiplicative also in the lower varliable.

The key lemma is [1, Lemma 20.1], which morally states that the quadratic spin is twisted multiplicative in the sense that

$$[wz]_2 = \mathcal{E}[w]_2[z]_2\left(\frac{z}{w}\right)_2$$

for some simple sign factor $\mathcal{E}$. The proof of this relies on quadratic reciprocity multiple times. To simplify the presentation we pretend that this holds with $\mathcal{E} = 1$. Then bounding the Type I and Type II sums is reduced to (absorbing factors into the coefficients α_w and β_w)

$$\sum_{|w|^2 \sim M} \alpha_w \sum_{|z|^2 \sim N} [z]_2\left(\frac{z}{w}\right)_2 \quad \text{and} \quad \sum_{|w|^2 \sim M} \alpha_w \sum_{|z|^2 \sim N} \beta_z\left(\frac{z}{w}\right)_2.$$

For the Type I sums (see [1, Sect. 22]) we fix w and write

$$\left| \sum_{|z|^2 \sim N} [z]_2\left(\frac{z}{w}\right)_2 \right| \le \sum_{r \ll \sqrt{N}} \left| \sum_{s^2 \sim N - r^2} \left[\frac{s}{r}\right]_2 \left(\frac{r + s\omega}{u^2 + v^2}\right)_2 \right|$$

$$= \sum_{r \ll \sqrt{N}} \left| \sum_{s \in I(r)} \left(\frac{s}{r(u^2 + v^2)}\right)_2 \right|$$

by making making the change of variables $s \mapsto s + \omega r$, where $I(r)$ denotes an interval of length $\ll \sqrt{N}$. The sum over s can be bounded using the Pólya-Vinogradov inequality for short character sums, which yields a non-trivial bound for the Type I sums (1.3) in the range $M \le x^{1/3 - \eta}$ for any $\eta > 0$.

To handle the Type II sums (see [1, Sect. 21]) we use Cauchy–Schwarz to morally get

$$\sum_{|w|^2 \sim M} \alpha_w \sum_{|z|^2 \sim N} \beta_z\left(\frac{z}{w}\right)_2 \ll N^{1/2}\left(\sum_{|w_1|^2, |w_2|^2 \sim M} \alpha_{w_1}\alpha_{w_2} \sum_{|z|^2 \sim N} \left(\frac{z}{w_1 w_2}\right)_2\right)^{1/2}.$$

Since $(z/w_1 w_2)_2$ is a quadratic character modulo $|w_1 w_2|^2$, the sum over z is very small unless $|w_1 w_2|^2$ is a perfect square (at least for N large compared to $|w_1 w_2|^2 \asymp M^2$). The part where $|w_1 w_2|^2$ is a perfect square is a very narrow subset of the variables, which gives a non-trivial bound for the Type II sums. This bound can be amplified by a suitable application of Hölder's inequality and by the reciprocity $(z/w)_2 = (w/z)_2$. We get a non-trivial bound for the Type II sums (1.4) in the full range $x^\eta \ll M, N \ll x^{1-\eta}$.

1.2 Structure of the article

The proof of Theorem 1 follows the same lines as the proof of [1, Theorem 2]. In Sect. 2 we recall the law of cubic reciprocity and prove that the cubic spin $[z]_3$ satisfies a twisted

multiplicativity relation (Lemma 5). This relation is the key ingredient in all of the arguments that follow. In Sect. 3 we recall basic facts about $\mathbb{Q}(\zeta_{12})$ and show that the definition of the spin $[\mathfrak{a}]_3 = [z]_3$ is independent of the choice of primary generator z of $\mathfrak{a}$ (also for this we need Lemma 5).

In Sect. 4 we use Buchstab's identity to obtain a decomposition of the prime sum into sums of Type I and Type II. We could also use similar arguments as in [1] to this end. In Sect. 5 we explain how to choose unique primary generators for the ideals of $\mathfrak{a}$ in a consistent manner.

After these steps the arugment is essentially same as in [1] with only minor modifications. In Sects. 7 and 8 we compute the Type I and Type II sums, respectively, which by Sect. 4 completes the proof of Theorem 1. For this we need a version of the Poisson summation on $\mathbb{Z}[\zeta_3]$, which is given in Sect. 6. The reason why the exponent in Theorem 1 is worse than that in [1, Theorem 2] is solely because in the Type I sums we essentially get a contribution from the error term in a lattice point counting problem on $\mathbb{Z}[\zeta_3]$.

Lastly, in Sect. 9 we illustrate non-rigorously how the cupic spin arises from the problem of primes of the type $\alpha^2 + \beta^6$ on $\mathbb{Z}[\zeta_3]$. The arguments follow the same lines as in [1]. We also explain why the density issue prevents us from completing the goal of detecting primes of this form.

1.3 Notations

For functions f and g, we write $f \ll g$ or $f = \mathcal{O}(g)$ if there is a constant C such that $|f| \leq C|g|$. The notation $f \asymp g$ means $g \ll f \ll g$. The constant may depend on some parameter, which is indicated in the subscript (e.g. $\ll_\epsilon$). We write $f = o(g)$ if $f/g \to 0$ for large values of the variable. For variables we write $n \sim N$ meaning $N < n \leq 2N$.

For two functions f and g with $g \geq 0$, it is convenient for us to denote $f(N) \lll g(N)$ if $f(N) \ll_\epsilon N^\epsilon g(N)$. A typical bound we use is $\tau_k(n) \lll 1$, where τ_k is the k-fold divisor function. For multivariable functions such as sums over two variables we write

$$\sum_{\substack{m \sim M \\ n \sim N}} f(m, n) \lll \sum_{\substack{m \sim M \\ n \sim N}} g(m, n)$$

to mean

$$\sum_{\substack{m \sim M \\ n \sim N}} f(m, n) \ll_\epsilon (M + N)^\epsilon \sum_{\substack{m \sim M \\ n \sim N}} g(m, n).$$

We say that an arithmetic function f is divisor bounded if $|f(n)| \ll \tau_k(n)$ for some k.

For a statement E we denote by 1_E the characteristic function of that statement. For a set A we use 1_A to denote the characteristic function of A.

We let $e(x) := e^{2\pi i x}$ and $e_q(x) := e(x/q)$ for any integer $q \geq 1$. We abbreviate modular arithmetic such as $a \equiv b \pmod{c}$ by $a \equiv b\,(c)$. For any $(a, b) = 1$ we let $a^{-1}\,(b)$ denote the multiplicative inverse, so that $aa^{-1} \equiv 1\,(b)$.

We abbreviate the norm maps as follows. For any $a = a^{(1)} + a^{(2)}\zeta_3 \in \mathbb{Z}[\zeta_3]$, $a^{(j)} \in \mathbb{Z}$, and $\zeta = r + is \in \mathbb{Z}[\zeta_{12}]$, $r, s \in \mathbb{Z}[\zeta_3]$ we set

$$N_3(a) := N_{\mathbb{Q}(\zeta_3)}(a) = (a^{(1)})^2 - a^{(1)}a^{(2)} + (a^{(2)})^2 = |a|^2,$$

$$N_{12/3}(\zeta) := N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_3)}(\zeta) = r^2 + s^2, \quad \text{and} \quad N_{12} := N_{\mathbb{Q}(\zeta_{12})} = N_3 \circ \mathbb{N}_{12/3}.$$

2 Cubic reciprocity

In this section we recall basic properties of the Eisenstein integers $\mathbb{Z}[\zeta_3]$ and the cubic residue character (cf. [10, Chapter 7], for instance). We also prove a twisted multiplicativity rule for the cubic spin $[z]_3$ (Lemma 5) by using the cubic reciprocity law. To simplify the notation we will abbreviate modular arithmetic such as $a \equiv b \pmod{c}$ by $a \equiv b \, (c)$.

The unit group of $\mathbb{Z}[\zeta_3]$ is the group of sixth roots of unity $\{\pm 1, \pm \zeta_3, \pm \zeta_3^2\}$. We say that an integer $a \in \mathbb{Z}[\zeta_3]$ is primary if $a \equiv \pm 1 \, (3)$. Equivalently, $a = a^{(1)} + a^{(2)}\zeta_3$ with $a^{(j)} \in \mathbb{Z}$ is primary if $3 | a^{(2)}$ and $a^{(1)} \equiv \pm 1 \, (3)$. For any $(a, 3) = 1$ there exists a unit μ such that $\mu a \equiv 1 \, (3)$.

Any rational prime $p \equiv 1 \, (3)$ splits as $p = \pi \bar{\pi}$ for a prime $\pi \in \mathbb{Z}[\zeta_3]$. Then for any $a \in \mathbb{Z}[\zeta_3]$, $\pi \nmid a$, we have by Fermat's Little Theorem

$$a^{p-1} \equiv 1 \, (\pi).$$

Since $p \equiv 1 \, (3)$, we see that $a^{(p-1)/3} \equiv \zeta_3^k \, (\pi)$ for some $k \in \{0, 1, 2\}$, so that we may define the cubic residue character modulo π

$$\left[\frac{a}{\pi} \right]_3 := \zeta_3^k.$$

If $\pi | a$ we set $[a/\pi]_3 := 0$. The rational primes $q \equiv 2 \, (3)$ are inert and we define $[a/q]_3 := 1$ if $q \nmid a$ and $[a/q]_3 := 0$ if $q | a$. For any unit μ of $\mathbb{Z}[\zeta_3]$ we set $[a/\mu]_3 := 1$, and for the prime $1 - \zeta_3$ we set $[a/(1 - \zeta_3)]_3 := 1$ (recall that $3 = -\zeta_3^2(1 - \zeta_3)^2$ is the only prime that ramifies). Then for any prime $\tau \in \mathbb{Z}[\zeta_3]$ the congruence $x^3 \equiv a \, (\tau)$ has a non-zero solution if and only if $[a/\tau]_3 = 1$.

For any non-zero $\lambda \in \mathbb{Z}[\zeta_3]$ we have a unique factorization

$$\lambda = \pm \zeta_3^k (1 - \zeta_3)^\ell \pi_1^{\alpha_1} \cdots \pi_m^{\alpha_m} q_1^{\beta_1} \cdots q_n^{\beta_n},$$

where $\pi_j \equiv 1 \, (3)$, and $q_j \equiv 2 \, (3)$ are rational primes. Therefore, we may extend $[\cdot/\pi]_3$ to all of $\mathbb{Z}[\zeta_3]$ multiplicatively

$$\left[\frac{a}{\lambda} \right]_3 := \left[\frac{a}{\pi_1} \right]_3^{\alpha_1} \cdots \left[\frac{a}{\pi_k} \right]_3^{\alpha_k}.$$

It is then clear that this is completely multiplicative in both variables. From here on we simplify notations by ignoring the subscript 3, that is, we write $[a/b] := [a/b]_3$.

For any $a, b \in \mathbb{Z}[\zeta_3]$ we write $(a, b) = 1$ if a and b are coprime. For any $(a, b) = 1$ we let $\epsilon(a, b)$ denote the cubic root of unity such that

$$\left[\frac{a}{b} \right] = \epsilon(a, b) \left[\frac{b}{a} \right],$$

Note that for any $a, b, c \in \mathbb{Z}[\zeta_3]$ with $(a, bc) = 1$ we have multiplicativity in the sense that

$$\epsilon(a, bc) = \epsilon(a, b)\epsilon(a, c) \quad \text{and} \quad \epsilon(bc, a) = \epsilon(b, a)\epsilon(c, a).$$

Note also that $\epsilon(a, b) = \epsilon(a, b)^{-1} = \epsilon(b, a)^2$.

By [10, Theorem 7.8] we have the following cubic reciprocity law (which can also be found in [13, Chapter VIII, Example 5.13]).

Lemma 4 (Cubic reciprocity). *Let $a, b \in \mathbb{Z}[\zeta_3]$ be coprime. If a and b are primary, then $\epsilon(a, b) = 1$. If $a = a^{(1)} + a^{(2)}\zeta_3$ is primary, then depending on the sign of $a^{(1)} \equiv \pm 1 \pmod 3$ we have*

$$\epsilon(\zeta_3, a) = \zeta_3^{(1 \pm (-a^{(1)} - a^{(2)}))/3}, \quad \epsilon(1 - \zeta_3, a) = \zeta_3^{(\pm a^{(1)} - 1)/3}, \quad \epsilon(3, a) = \zeta_3^{\pm a^{(2)}/3},$$

so that for any $c \in \mathbb{Z}[\zeta_3]$ we have

$$\epsilon(\zeta_3, a + 9c) = \epsilon(\zeta_3, a) \quad \text{and} \quad \epsilon(1 - \zeta_3, a + 9c) = \epsilon(1 - \zeta_3, a).$$

We say that $z \in \mathbb{Z}[\zeta_{12}]$ is primary if $z \equiv \pm 1$ (3). For a primary $z = r + is \in \mathbb{Z}[\zeta_{12}]$ we define

$$[z] := [z]_3 = \left[\frac{s}{r} \right].$$

We will extend this definition to ideals of $\mathbb{Z}[\zeta_{12}]$ in Sect. 3. We say that $w = u + iv \in \mathbb{Z}[\zeta_{12}]$ is primitive if $(u, v) = 1$. For $w \in Z[\zeta_{12}]$ primary primitive, set $\omega \equiv -vu^{-1} \pmod{u^2 + v^2}$, where u^{-1} is the multiplicative inverse modulo $u^2 + v^2$. Analogously to the Dirichlet symbol defined in [1, Sect. 19], we define

$$\left(\frac{z}{w} \right) := \left[\frac{r + \omega s}{u^2 + v^2} \right]. \tag{2.1}$$

Since $\omega^2 \equiv -1$ $(u^2 + v^2)$, this is completely multiplicative in the upper variable, so that this is an extension of the character $[r/(u^2 + v^2)]$ from $\mathbb{Z}[\zeta_3]$ to $\mathbb{Z}[\zeta_{12}]$.

Similarly as [1, Lemma 20.1] follows from the quadratic reciprocity, the cubic reciprocity law implies that the cubic spin $[z]$ is multiplicative up to the symbol (z/w). The analogous result on $\mathbb{Z}[\sqrt{2}]$ in the work of Milovic is [14, Proposition 8].

Lemma 5 *Let $w = u + iv, z = r + is \in \mathbb{Z}[\zeta_{12}]$ be primary with w primitive. Then*

$$[wz] = [w][z]\left(\frac{z}{w} \right).$$

Proof First note that since w and z are primary, it follows that all of u, r, wz, and $ur - vs$ are primary, and $3|v$ and $3|s$. If $(u, v) \neq 1$ or $(r, s) \neq 1$, then the claim is trivial since then both sides vanish. Assume then that $(u, v) = (r, s) = 1$. Let $r_0 = (r, v)$ be primary, and denote $r = r_0 r_1$, $v = r_0 v_1$, so that $(r_1, v_1) = 1$ (since r is primary we have $(3, r_0) = 1$ and we may pick a primary representative for r_0). By using $s \equiv ur_1 v_1^{-1} (ur_1 - v_1 s)$ we get

$$
\begin{aligned}
[wz] &= \left[\frac{us + vr}{ur - vs} \right] = \left[\frac{us}{r_0} \right]\left[\frac{us + vr}{ur_1 - v_1 s} \right] = \left[\frac{u}{r_0} \right]\left[\frac{s}{r_0} \right]\left[\frac{u^2 r_1 v_1^{-1} + vr}{ur_1 - v_1 s} \right] \\
&= \left[\frac{u}{r_0} \right]\left[\frac{s}{r_0} \right]\left[\frac{r_1 v_1^{-1}}{ur_1 - v_1 s} \right]\left[\frac{u^2 + v^2}{ur_1 - v_1 s} \right] \\
&= \left[\frac{u}{r_0} \right]^2 \left[\frac{s}{r_0} \right]\left[\frac{r_1 v_1^{-1}}{ur_1 - v_1 s} \right]\left[\frac{u}{r_0} \right]^2 \left[\frac{u^2 + v^2}{ur_1 - v_1 s} \right] \\
&= \left[\frac{u}{r_0} \right]^2 \left[\frac{s}{r_0} \right]\left[\frac{r_1 v_1^{-1}}{ur_1 - v_1 s} \right]\left[\frac{u^2 + v^2}{r_0} \right]\left[\frac{u^2 + v^2}{ur_1 - v_1 s} \right] \\
&= \left[\frac{s}{r_0} \right]\left[\frac{r_1}{ur_1 - v_1 s} \right] \cdot \left[\frac{u}{r_0} \right]^2 \left[\frac{v_1}{ur_1 - v_1 s} \right]^2 \cdot \left[\frac{u^2 + v^2}{ur - vs} \right].
\end{aligned}
$$

We now compute the above three factors separately.

We have

$$\begin{bmatrix} s \\ r_0 \end{bmatrix}\begin{bmatrix} r_1 \\ ur_1 - v_1 s \end{bmatrix} = \begin{bmatrix} s \\ r_0 \end{bmatrix}\begin{bmatrix} ur_1 - v_1 s \\ r_1 \end{bmatrix} = \begin{bmatrix} s \\ r_0 \end{bmatrix}\begin{bmatrix} v_1 s \\ r_1 \end{bmatrix} = \begin{bmatrix} v_1 \\ r_1 \end{bmatrix}[z]$$

by Lemma 4 since $ur_1 - v_1 s$ and r_1 are both primary.

By a similar argument the second factor is

$$\begin{bmatrix} u \\ r_0 \end{bmatrix}^2 \begin{bmatrix} v_1 \\ ur_1 - v_1 s \end{bmatrix}^2 = \begin{bmatrix} u \\ r_0 \end{bmatrix}^2 \begin{bmatrix} ur_1 - v_1 s \\ v_1 \end{bmatrix}^2 \epsilon(v_1, ur_1 - v_1 s)^2$$

$$= \begin{bmatrix} u \\ r_0 \end{bmatrix}^2 \begin{bmatrix} ur_1 \\ v_1 \end{bmatrix}^2 \epsilon(v_1, ur_1 - v_1 s)^2$$

$$= \begin{bmatrix} u \\ v \end{bmatrix}^2 \begin{bmatrix} r_1 \\ v_1 \end{bmatrix}^2 \epsilon(v_1, ur_1 - v_1 s)^2$$

$$= [w]^2 \begin{bmatrix} r_1 \\ v_1 \end{bmatrix}^2 \epsilon(v_1, ur_1 - v_1 s)^2 \epsilon(u, v)^2.$$

For the third factor, since u, $u^2 + v^2$, and $ur - vs$ are primary, we have by two applications of Lemma 4

$$\begin{bmatrix} u^2 + v^2 \\ ur - vs \end{bmatrix} = \begin{bmatrix} ur - vs \\ u^2 + v^2 \end{bmatrix} = \begin{bmatrix} u \\ u^2 + v^2 \end{bmatrix}\left(\frac{z}{w}\right) = \begin{bmatrix} u^2 + v^2 \\ u \end{bmatrix}\left(\frac{z}{w}\right) = [w]^2\left(\frac{z}{w}\right).$$

Combining all we have $[wz] = \mathcal{E}[w][z](\frac{z}{w})$ for

$$\mathcal{E} = \begin{bmatrix} v_1 \\ r_1 \end{bmatrix} \cdot \begin{bmatrix} r_1 \\ v_1 \end{bmatrix}^2 \epsilon(v_1, ur_1 - v_1 s)^2 \epsilon(u, v)^2$$

$$= \epsilon(v_1, r_1)\epsilon(v_1, ur_1 - v_1 s)^2 \epsilon(v, u)$$

Let $v_1 = \pm\zeta_3^k(1-\zeta_3)^\ell\lambda$ where λ is primary. Then, since $9 | v_1 s$, we see from the supplementary laws in Lemma 4 (note also that $\epsilon(\lambda, ur_1 - v_1 s) = 1 = \epsilon(\lambda, ur_1)$ since $ur_1 - v_1 s$ and ur_1 are primary)

$$\epsilon(v_1, ur_1 - v_1 s) = \epsilon(\zeta_3, ur_1 - v_1 s)^k \epsilon(1 - \zeta_3, ur_1 - v_1 s)^\ell \epsilon(\lambda, ur_1 - v_1 s)$$

$$= \epsilon(\zeta_3, ur_1)^k \epsilon(1 - \zeta_3, ur_1)^\ell \epsilon(\lambda, ur_1) = \epsilon(v_1, ur_1)$$

$$= \epsilon(v_1, u)\epsilon(v_1, r) = \epsilon(r_0, u)^2 \epsilon(v, u)\epsilon(v_1, r) = \epsilon(v, u)\epsilon(v_1, r)$$

since r_0 and u are primary. Hence, we get $\mathcal{E} = \epsilon(v_1, r_1)\epsilon(v, u)^2 \epsilon(v_1, r_1)^2 \epsilon(v, u) = 1.$ □

Remark 5 It is perhaps surprising that our Lemma 5 is much simpler than the corresponding results in the quadratic case [1, Lemma 20.1] and [14, Proposition 8], where the equalities hold only up to a simple factor. The main reason for this seems to be that -1 is always a cube so that $[-1/a] = 1$ for all $a \in \mathbb{Z}[\zeta_3]$, a fact that we used in the proof.

We will abbreviate the norm maps as follows. For any $a = a^{(1)} + a^{(2)}\zeta_3 \in \mathbb{Z}[\zeta_3]$ and $\zeta = r + is \in \mathbb{Z}[\zeta_{12}], r, s \in \mathbb{Z}[\zeta_3]$ we set

$$N_3(a) := N_{\mathbb{Q}(\zeta_3)}(a) = (a^{(1)})^2 - a^{(1)}a^{(2)} + (a^{(2)})^2 = |a|^2,$$

$$N_{12/3}(\zeta) := N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_3)}(\zeta) = r^2 + s^2, \quad \text{and} \quad N_{12} := N_{\mathbb{Q}(\zeta_{12})} = N_3 \circ N_{12/3}.$$

The symbol (z/w) in Lemma 5 is completely multiplicative in the upper variable. Similar to [1, Sects. 19 and 21], to handle Type II sums we need a multiplier rule in the lower variable also, which is given by the following.

Lemma 6 *Let $w_1, w_2 \in \mathbb{Z}[\zeta_{12}]$ be primary primitive and let $\zeta = r + is \in \mathbb{Z}[\zeta_{12}]$ be primary. Set*

$$q_j = N_{12/3}(w_j), \quad e := (w_1, \sigma(w_2^2)), \quad and \quad d := N_{12/3}(e),$$

where σ is the conjugation $\sigma(a + ib) = a - ib$. Then for some root $\omega^2 + 1 \equiv 0 \ (q_1 q_2^2)$ we have

$$\left(\frac{\zeta}{w_1}\right)\left(\frac{\zeta}{w_2}\right)^2 = \left[\frac{r - \omega s}{d}\right]\left[\frac{r + \omega s}{q_1 q_2^2/d}\right].$$

Proof We can write $\zeta = az$, where $a \in \mathbb{Z}[\zeta_3]$ and z is primary primitive. Since both sides are completely multiplicative, it suffices to prove the claim separately for $a \in \mathbb{Z}[\zeta_3]$ and for $z \in \mathbb{Z}[\zeta_{12}]$ primary primitive.

For any $a \in \mathbb{Z}[\zeta_3]$ we have by definition

$$\left(\frac{a}{w_1}\right)\left(\frac{a}{w_2}\right)^2 = \left[\frac{a}{q_1}\right]\left[\frac{a}{q_2^2}\right] = \left[\frac{a}{d}\right]\left[\frac{a}{q_1 q_2^2/d}\right].$$

For $z = r + is$ primary primitive we get from Lemma 5 a reciprocity law $(z/w) = (w/z)$ for any primary primitive w. Note that by definition $w_1 w_2^2/d$ is primary primitive. Therefore, we get by reciprocity (note that $r^2 + s^2$ and d are primary)

$$\left(\frac{z}{w_1}\right)\left(\frac{z}{w_2}\right)^2 = \left(\frac{w_1}{z}\right)\left(\frac{w_2^2}{z}\right) = \left(\frac{d}{z}\right)\left(\frac{w_1 w_2^2/d}{z}\right) = \left[\frac{d}{N_{12/3}(z)}\right]\left(\frac{w_1 w_2^2/d}{z}\right)$$

$$= \left[\frac{r^2 + s^2}{d}\right]\left[\frac{r + \omega s}{q_1 q_2^2/d^2}\right] = \left[\frac{r - \omega s}{d}\right]\left[\frac{r + \omega s}{q_1 q_2^2/d}\right],$$

since $r^2 + s^2 \equiv (r + \omega s)(r - \omega s) \ (d)$. □

Remark 6 In [1, Sect. 19] we have for primary $z = r + is, w = u + iv \in \mathbb{Z}[i]$ with w primitive

$$\left(\frac{z}{w}\right)_2 := \left(\frac{r + \omega s}{u^2 + v^2}\right)_2 = \left(\frac{ur - vs}{u^2 + v^2}\right)_2 = \left(\frac{\operatorname{Re} wz}{|w|}\right)_2.$$

In our case the middle equality does not hold but we have for $z = r + is, w = u + iv \in \mathbb{Z}[\zeta_3]$ primary

$$\left(\frac{ur - vs}{u^2 + v^2}\right) = \left(\frac{u}{u^2 + v^2}\right)\left(\frac{r + \omega s}{u^2 + v^2}\right) = [w]^2\left(\frac{z}{w}\right)$$

by reciprocity if w is primary primitive. Lack of this alternative representation does not hinder us in any way.

3 The twelfth cyclotomic extension

So far we have defined $[z]$ only for primary $z \in \mathbb{Z}[\zeta_{12}]$. In this section we extend the definition to ideals of $\mathbb{Z}[\zeta_{12}]$.

Table 1 Values of $\epsilon_0^k \zeta_{12}^\ell$. Note that for $z \in \mathbb{Z}[\zeta_{12}]$ if $z \equiv \pm 1, \pm i$ (3), then both of the coefficients of $\sqrt{3}/2$ and $i\sqrt{3}/2$ are divisible by 3

ℓ	k 0	1	2
1	$\frac{1}{2} + \frac{i}{2} + \frac{\sqrt{3}}{2} + \frac{i\sqrt{3}}{2}$	$\frac{1}{2} + i + \frac{i\sqrt{3}}{2}$	$\frac{-1}{2} + i + \frac{i\sqrt{3}}{2}$
2	$2i + i\sqrt{3}$	$-1 + \frac{3i}{2} - \frac{\sqrt{3}}{2} - i\sqrt{3}$	$\frac{-3}{2} + i - \sqrt{3} + \frac{i\sqrt{3}}{2}$
3	$\frac{-5}{2} + \frac{5i}{2} - \frac{3\sqrt{3}}{2} + \frac{3i\sqrt{3}}{2}$	$\frac{-7}{2} + i - 2\sqrt{3} + \frac{i\sqrt{3}}{2}$	$\frac{-7}{2} - i - 2\sqrt{3} - \frac{i\sqrt{3}}{2}$
4	$-7 - 4\sqrt{3}$	$-6 - \frac{7i}{2} - \frac{7\sqrt{3}}{2} - 2i\sqrt{3}$	$\frac{-7}{2} - 6i - 2\sqrt{3} - \frac{7i\sqrt{3}}{2}$
5	$\frac{-19}{2} - \frac{19i}{2} - \frac{11\sqrt{3}}{2} - \frac{11i\sqrt{3}}{2}$	$\frac{-7}{2} - 13i - 2\sqrt{3} - \frac{15i\sqrt{3}}{2}$	$\frac{7}{2} - 13i + 2\sqrt{3} - \frac{15i\sqrt{3}}{2}$

The only entry satisfying this is $\epsilon_0^3 = \frac{-5}{2} + \frac{5i}{2} - \frac{3\sqrt{3}}{2} + \frac{3i\sqrt{3}}{2}$, but we have $\epsilon_0^3 = 5 - 2i - 3(1 + i)\zeta_3 \equiv 2 - 2i \not\equiv \pm 1, \pm i$ (3), so that none of the values in the table are $\equiv \pm 1, \pm i$ (3)

The unit group of $\mathbb{Z}[\zeta_{12}]$ is generated by ζ_{12} and the fundamental unit (cf. [10, Chapter 7.4])

$$\epsilon_0 := \frac{1 + \sqrt{3}}{1 - i} = 1 + \zeta_3 - i\zeta_3.$$

For every $z \in \mathbb{Z}[\zeta_{12}]$ coprime to 3 there exists a unit μ such that $\mu z \equiv 1$ (3) (cf. [10, Exercise 7.4]). The next lemma shows that the subgroup of primary units is $\{\pm (i\epsilon_0^6)^k : k \in \mathbb{Z}\}$.

Lemma 7 We have $-i\epsilon_0^6 \equiv 1$ (3). Furthermore, $k = 6$ is the smallest positive exponent such that $\epsilon_0^k \equiv \zeta_{12}^\ell$ (3) for some integer ℓ, so that as a set

$$(\mathbb{Z}[\zeta_{12}]/3\mathbb{Z}[\zeta_{12}])^\times = \{\zeta_{12}^\ell \epsilon_0^k, \ k \in \{0, 1, \ldots, 5\}\}.$$

Also, we have

$$[\pm i\epsilon_0^6] = 1.$$

Proof By direct computation we see that

$$i\epsilon_0^6 = 26 + i(15 + 30\zeta_3) \equiv 2 \ (3),$$

and that for $1 \le k \le 5$ and for all ℓ we have $\epsilon_0^k \zeta_{12}^\ell \not\equiv \pm 1$ (3) (see Table 3). Note that to check this it suffices to verify that for all $1 \le k \le 5$ and $0 \le \ell \le 2$ we have $\epsilon_0^k \zeta_{12}^\ell \not\equiv \pm 1, \pm i$ (3).

Since every number coprime to 3 is congruent to some unit modulo 3, this implies the claimed structure for $(\mathbb{Z}[\zeta_{12}]/3\mathbb{Z}[\zeta_{12}])^\times$. By the definition of $[z]$ we get

$$[i\epsilon_0^6] = \left[\frac{15 + 30\zeta_3}{26}\right] = \left[\frac{15}{26}\right]\left[\frac{1 + 2\zeta_3}{26}\right] = \left[\frac{\zeta_3}{26}\right]\left[\frac{1 - \zeta_3}{26}\right] = \zeta_3^{(1+26)/3}\zeta_3^{(-1-26)/3} = 1$$

by the supplementary laws in Lemma 4, and since $[m/n] = 1$ for all $m, n \in \mathbb{Z}$ with $n \neq 0$. □

As a corollary we see that $[z]$ does not depend on which primary associate we choose.

Lemma 8 If z and z' are primary associates, then $[z] = [z']$.

Proof There is some unit μ such that $z = \mu z'$. Since z and z' are primary, also μ must be primary. By Lemma 7 we see that $\mu = \pm(i\epsilon_0^6)^k$ for some $k \in \mathbb{Z}$. Hence, by Lemma 5

$$[z] = [\mu z'] = [\mu][z']\left(\frac{z'}{\mu}\right).$$

By definition

$$\left(\frac{z'}{\mu}\right) = \left[\frac{r' + \omega s'}{N_{12/3}(\mu)}\right] = 1$$

since $N_{12/3}(\mu)$ is a unit in $\mathbb{Z}[\zeta_3]$, and similarly we see that

$$[\mu] = [\pm(i\epsilon_0^6)^k] = [i\epsilon_0^6]^k = 1$$

by using the last part of Lemma 7. □

Since $\mathbb{Z}[\zeta_{12}]$ is a principal ideal domain, by the above lemma the following definition is appropriate.

Definition 1 For any ideal $\mathfrak{a}$ of $\mathbb{Z}[\zeta_{12}]$, we define

$$[\mathfrak{a}] := [z] = \left[\frac{s}{r}\right]$$

if $\mathfrak{a}$ is generated by $z = r + is$ and z is primary.

Remark 7 We also define $[z]$ for non-primary $z = r + is$ by $[z] := [s/r]$. Then we have $[z] = \nu(z)[(z)]$ where $\nu(z)$ depends only on the residue class z (3). We will not need it in the following but it might be interesting to give a simple closed formula for $\nu(z)$.

Remark 8 It is natural that we need the reciprocity laws to prove that the spin is well-defined on ideals. After all, the cubic reciprocity can be restated as a transformation rule for $[z]$ under multiplication of z by a root of unity. This is because for $z = r + is$

$$[iz] = [-s + ir] = \left[\frac{r}{s}\right] = \epsilon(r, s)[z], \quad \text{and} \quad [\zeta_3 z] = \left[\frac{\zeta_3 s}{\zeta_3 r}\right] = \left[\frac{\zeta_3}{r}\right]\left[\frac{s}{r}\right] = \epsilon(\zeta_3, r)[z],$$

which by considering $z_1 = r + i(1 - \zeta_3)$ and $z_2 = r + i3$ covers also the supplementary laws.

4 Sieve argument

In this section we prove Theorem 1. We apply a sieve argument in $\mathbb{Z}[\zeta_{12}]$ to decompose our sum into Type I and Type II sums. The argument is essentially same as in Harman's sieve method [5]. We could use [4, Proposition 5.2] directly but we give our on proof based on Buchstab's identity since it does not take much effort to inclue it here.

For two functions f and g with $g \geq 0$, it is convenient for us to denote $f(N) \lll g(N)$ if $f(N) \ll_\epsilon N^\epsilon g(N)$. A typical bound we use is $\tau_k(n) \lll 1$, where τ_k is the k-fold divisor function. For multivariable functions such as sums over two variables we write

$$\sum_{\substack{m \sim M \\ n \sim N}} f(m, n) \lll \sum_{\substack{m \sim M \\ n \sim N}} g(m, n)$$

to mean

$$\sum_{\substack{m \sim M \\ n \sim N}} f(m, n) \ll_\epsilon (M + N)^\epsilon \sum_{\substack{m \sim M \\ n \sim N}} g(m, n).$$

We say that an arithmetic function f is divisor bounded if $|f(n)| \ll \tau_k(n)$ for some k.

For the sieve we require the following arithmetic information, which is proved in Sects. 7 and 8.

Proposition 9 (Type I sums) *Let $\alpha_{\mathfrak{d}}$ be divisor bounded. Then*

$$\sum_{N_{12}(\mathfrak{d}) \leq D} \alpha_{\mathfrak{d}} \sum_{N_{12}(\mathfrak{n}) \sim x/N_{12}(\mathfrak{d})} [\mathfrak{d}\mathfrak{n}] \lll x^{11/12} D^{13/12}$$

Proposition 10 (Type II sums) *Let $\alpha_{\mathfrak{m}}$ and $\beta_{\mathfrak{n}}$ be divisor bounded coefficients. Then*

$$\sum_{N_{12}(\mathfrak{m}) \sim M} \sum_{N_{12}(\mathfrak{n}) \sim N} \alpha_{\mathfrak{m}} \beta_{\mathfrak{n}} [\mathfrak{m}\mathfrak{n}] \lll M N^{9/10} + M^{9/10} N.$$

Remark 9 Note that $[\mathfrak{a}] = 0$ if $\mathfrak{a}$ is not primitive. Thus, we may assume that the coefficients α and β in the above are supported on primitive ideals.

Remark 10 Our Type I information is very weak but this is compensated by the fact that the Type II bound is non-trivial as soon as $M \gg x^{\eta}$ or $N \gg x^{\eta}$.

Define

$$P_{12}(Y) := \prod_{N_{12}(\mathfrak{p}) < Y} \mathfrak{p}.$$

Note that the norm map induces a partial ordering on the set of ideals, and that for every prime ideal there are at most four prime ideals of the same norm. For any ideal $\mathfrak{d} \subseteq \mathbb{Z}[\zeta_{12}]$ we set

$$S(\mathcal{A}_{\mathfrak{d}}, Y) := \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{d}\mathfrak{n}) \sim x}} 1_{(\mathfrak{n}, P_{12}(Y))=1} [\mathfrak{d}\mathfrak{n}].$$

Proof of Theorem 1 Let $Z = x^{\gamma}$ for some $\gamma \in (0, 1/2)$ which we will optimize later on. By Buchstab's identity

$$S(\mathcal{A}, 2\sqrt{x}) = S(\mathcal{A}, Z) - \sum_{Z \leq N_{12}(\mathfrak{p}) < 2\sqrt{x}} S(\mathcal{A}_{\mathfrak{p}}, N_{12}(\mathfrak{p})) + O(E) =: S_1(\mathcal{A}) - S_2(\mathcal{A}) + O(E),$$

where the error term E consists of that part in $S_2(\mathcal{A})$ where the implicit variable $\mathfrak{n}$ is divisible by another prime ideal of same norm $N_{12}(\mathfrak{p})$ (we could also handle this part by fixing a complete ordering for prime ideals $\mathfrak{p}$ but then we would later have to remove cross-conditions coming from this). We have trivially

$$E \leq \sum_{Z \leq N_{12}(\mathfrak{p}) < 2\sqrt{x}} \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{n}) \sim x}} 1_{N_{12}(\mathfrak{p})^2 | N_{12}(\mathfrak{n})} \lll \sum_{Z \leq k < 2\sqrt{x}} \sum_{n \sim x} 1_{k^2 | n} \lll x Z^{-1}.$$

For the second sum we have (writing $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$)

$$S_2(\mathcal{A}) = \sum_{Z \leq N_{12}(\mathfrak{p}) < 2\sqrt{x}} \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{p}\mathfrak{n}) \sim x}} 1_{(\mathfrak{n}, P_{12}(N_{12}(\mathfrak{p})))=1} [\mathfrak{p}\mathfrak{n}]$$

$$= \sum_{k \ll 1} \sum_{Z \leq N_{12}(\mathfrak{p}) < 2\sqrt{x}} \sum_{\substack{N_{12}(\mathfrak{p}) < N_{12}(\mathfrak{p}_1) < \cdots < N_{12}(\mathfrak{p}_k) \\ N_{12}(\mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_k) \sim x}} [\mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_k] + O(\tilde{E})$$

$$\lll x Z^{-1/10} + x Z^{-1} \tag{4.1}$$

by Proposition 10 once we remove the cross-conditions $N_{12}(\mathfrak{p}) < N_{12}(\mathfrak{p}_1)$ and $N_{12}(\mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_k)$ $\sim x$ by Perron's formula (cf. for instance [5, Chapter 3.2], this works essentially the same in our situation since we apply it to the real quantities $N_{12}(\mathfrak{p}_j)$). Here the error term $\tilde{E}$ consists of the part where $\mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_k$ is divisible by a square, so that we have $\tilde{E} \ll xZ^{-1}$ by a similar argument as with E above.

For the first sum $S_1(\mathcal{A})$ we use the Möbius function to expand the condition $(\mathfrak{n}, P_{12}(Z)) = 1$ to get

$$
\begin{aligned}
S_1(\mathcal{A}) &= \sum_{\mathfrak{d} \mid P_{12}(Z)} \mu(\mathfrak{d}) \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{d}\mathfrak{n}) \sim x}} [\mathfrak{d}\mathfrak{n}] \\
&= \sum_{\substack{\mathfrak{d} \mid P_{12}(Z) \\ N_{12}(\mathfrak{d}) < Z}} \mu(\mathfrak{d}) \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{d}\mathfrak{n}) \sim x}} [\mathfrak{d}\mathfrak{n}] + \sum_{\substack{\mathfrak{d} \mid P_{12}(Z) \\ N_{12}(\mathfrak{d}) \geq Z}} \mu(\mathfrak{d}) \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{d}\mathfrak{n}) \sim x}} [\mathfrak{d}\mathfrak{n}] =: S_{11}(\mathcal{A}) + S_{12}(\mathcal{A})
\end{aligned}
$$

For the first sum we apply Proposition 9 to get

$$
S_{11} = \sum_{\substack{\mathfrak{d} \mid P_{12}(Z) \\ N_{12}(\mathfrak{d}) < Z}} \mu(\mathfrak{d}) \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{d}\mathfrak{n}) \sim x}} [\mathfrak{d}\mathfrak{n}] \lll x^{11/12} Z^{13/12}. \tag{4.2}
$$

For the second sum we write $\mathfrak{d} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ for $N_{12}(\mathfrak{p}_1) \leq \cdots \leq N_{12}(\mathfrak{p}_k) < Z$. Since there are at most four prime ideals of the same norm and $\mathfrak{d}$ is square free, by the greedy algorithm there is a unique $\ell \leq k$ such that $\mathfrak{d} = \mathfrak{d}_1 \mathfrak{d}_2$ with

$$
\mathfrak{d}_1 = \mathfrak{p}_1 \cdots \mathfrak{p}_\ell, \qquad \mathfrak{d}_2 = \mathfrak{p}_{\ell+1} \cdots \mathfrak{p}_k,
$$
$$
N_{12}(\mathfrak{d}_1) \in [Z, Z^5], \quad N_{12}(\mathfrak{d}_1') < Z, \qquad N_{12}(\mathfrak{p}_\ell) < N_{12}(\mathfrak{p}_{\ell+1}),
$$

where $\mathfrak{d}_1' := \mathfrak{p}_1 \cdots \mathfrak{p}_{\ell-j}$ if j is the largest number such that $N_{12}(\mathfrak{p}_{\ell-j+1}) = N_{12}(\mathfrak{p}_\ell)$ (that is, we apply the greedy algorithm for groups of at most four prime ideals of the same norm). Hence, the second sum $S_{12}(\mathcal{A})$ can be partitioned as

$$
\sum_{k \ll \log x} (-1)^k \sum_{\ell \leq k} \sum_{\substack{N_{12}(\mathfrak{d}_1) \in [Z, Z^5] \\ N_{12}(\mathfrak{d}_1') < Z \\ \mathfrak{d}_1 = \mathfrak{p}_1 \cdots \mathfrak{p}_\ell \text{ square free} \\ N_{12}(\mathfrak{p}_1) \leq \cdots \leq N_{12}(\mathfrak{p}_\ell) < Z}} \sum_{\substack{\mathfrak{d}_2 = \mathfrak{p}_{\ell+1} \cdots \mathfrak{p}_k \text{ square free} \\ N_{12}(\mathfrak{p}_\ell) < N_{12}(\mathfrak{p}_{\ell+1}) \leq \cdots \leq N_{12}(\mathfrak{p}_k) < Z}} \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{d}_1) N_{12}(\mathfrak{d}_2\mathfrak{n}) \sim x}} [\mathfrak{d}_1 \mathfrak{d}_2 \mathfrak{n}].
$$

The cross-conditions $N_{12}(\mathfrak{p}_\ell) < N_{12}(\mathfrak{p}_{\ell+1})$ and $N_{12}(\mathfrak{d}_1) N_{12}(\mathfrak{d}_2\mathfrak{n}) \sim x$ can now be removed by Perron's formula, so that by Proposition 10 we get

$$
\sum_{\substack{\mathfrak{d} \mid P(Z) \\ N_{12}(\mathfrak{d}) \geq Z}} \mu(\mathfrak{d}) \sum_{\substack{\mathfrak{n} \\ N_{12}(\mathfrak{d}\mathfrak{n}) \sim x}} [\mathfrak{d}\mathfrak{n}] \lll \frac{x}{Z} Z^{9/10} + Z^5 \left(\frac{x}{Z^5} \right)^{9/10}. \tag{4.3}
$$

Combining the bounds (4.1), (4.2), and (4.3), and choosing $Z := x^{5/71}$ (note that then $Z^5 < x^{1/2}$) to optimize we get

$$
S(\mathcal{A}, 2\sqrt{x}) \lll xZ^{-1/10} + x^{11/12} Z^{13/12} \ll_\epsilon x^{1-1/142+\epsilon} \ll x^{1-1/143}.
$$

$\square$

5 Fixing primary generators

For the proofs of our arithmetic information (Propositions 9 and 10) we need to fix primary generators of ideals of $\mathbb{Z}[\zeta_{12}]$ in a consistent manner, and in such a way that the resulting conditions do not cause problems later on. Luckily fixing an embedding of $\mathbb{Z}[\zeta_{12}]$ in $\mathbb{C}$ along with Lemma 7 allows us to do just this. We choose the embedding which maps ζ_{12} to $e^{2\pi i/12} \in \mathbb{C}$. For any $z = r + is \in \mathbb{Z}[\zeta_{12}]$, $r, s \in \mathbb{Z}[\zeta_3]$ we let $|z| := |r + is|$ denote the norm of the complex number $r + is \in \mathbb{C}$. Note that then

$$|\epsilon_0| = \left|\frac{1 + \sqrt{3}}{1 - i}\right| = (1 + \sqrt{3})/\sqrt{2} > 1.$$

Lemma 11 *For every ideal $\mathfrak{a}$ coprime to 3 there exists a unique generator $z = r + is \in \mathbb{Z}[\zeta_{12}]$ of $\mathfrak{a}$ such that $z \equiv 1$ (3) and*

$$N_{12}(z)^{1/4} \leq |z| < N_{12}(z)^{1/4}|\epsilon_0|^6. \tag{5.1}$$

Furthermore, for such a $z = r + is$ we have $|r|, |s| \ll |z|$.

Proof If $z_0 \equiv 1$ (3) is a generator of $\mathfrak{a}$, then by Lemma 7 the associates of z_0 which are $\equiv 1$ (3) are precisely $(-i\epsilon_0^6)^k z_0$ with $k \in \mathbb{Z}$. Clearly there is a unique k such that $z = (-i\epsilon_0^6)^k z_0$ satisfies (5.1). From (5.1) it follows that

$$|r^2 + s^2|^{1/2} \asymp |r + is|,$$

so that $|r - is| \asymp |r + is|$ which implies $|r|, |s| \ll |z|$. □

In the summations we will denote this condition by $\sum^{\wedge}$, so that we may write, for example,

$$\sum_{N_{12}(z)\sim N}^{\wedge} [z] = \sum_{\substack{N_{12}(z)\sim N \\ z\equiv 1 \ (3) \\ N_{12}(z)^{1/4}\leq|z|<N_{12}(z)^{1/4}|\epsilon_0|^6}} [z] = \sum_{N_{12}(\mathfrak{n})\sim N} [\mathfrak{n}]. \tag{5.2}$$

6 Truncated Poisson summation formula on $\mathbb{Z}[\zeta_3]$

In the proofs of Propositions 9 and 10 we will need a version of the Poisson summation formula on $\mathbb{Z}[\zeta_3]$. For the lemma we fix an embedding identifying ζ_3 with $e^{2\pi i/3} \in \mathbb{C}$, so that any element of $\mathbb{Z}[\zeta_3]$ is viewed as a complex number. For $z \in \mathbb{C}$ denote

$$z = z^{(1)} + \zeta_3 z^{(2)}$$

with $z^{(1)}, z^{(2)} \in \mathbb{R}$. For $q \in \mathbb{Z}[\zeta_3] \setminus \{0\}$, $\beta \in \mathbb{C}$, and $h_1, h_2 \in \mathbb{Z}$ we define (denoting $e_q(x) := e^{2\pi ix/q}$)

$$\psi_q^{(h_1,h_2)}(\beta) := e_{N_3(q)}(h_1(\beta\bar{q})^{(1)} + h_2(\beta\bar{q})^{(2)}),$$

so that $\psi_q^{(h_1,h_2)}$ is an additive character of $\mathbb{Z}[\zeta_3]/q\mathbb{Z}[\zeta_3]$ (here $\bar{q}$ denotes the complex conjugate).

Lemma 12 (Truncated Poisson summation formula on $\mathbb{Z}[\zeta_3]$). *Fix $\beta, q \in \mathbb{Z}[\zeta_3]$ and $x_0, y_0 \in \mathbb{R}$. For $K > 1$ let*

$$G_K(x, y) := G\left(\frac{x - x_0}{K}, \frac{y - y_0}{K}\right)$$

for some fixed compactly supported C^∞-smooth function $G : \mathbb{R}^2 \to \mathbb{C}$. We define $G_K : \mathbb{C} \to \mathbb{C}$ by setting $G_K(\alpha) := G_K(\alpha^{(1)}, \alpha^{(2)})$. Then for any $C, \epsilon > 0$ with $H := K^{\epsilon/2} N_3(q)^{1/2}/K$ we have

$$\sum_{\substack{\alpha \in \mathbb{Z}[\zeta_3] \\ \alpha \equiv \beta \ (q)}} G_K(\alpha) = \frac{1}{N_3(q)} \sum_{\alpha \in \mathbb{Z}[\zeta_3]} G_K(\alpha) + \frac{K^\epsilon}{H^2} \sum_{\substack{|h_1|,|h_2| \leq H \\ (h_1,h_2) \neq (0,0)}} c_{h_1,h_2} \psi_q^{(h_1,h_2)}(-\beta) + O_{G,C,\epsilon}(K^{-C})$$

for some bounded coefficients $c_{h_1,h_2} = c_{h_1,h_2,G,K,q}$ satisfying $|c_{h_1,h_2}| \ll_G 1$.

Proof Recall that for $\alpha, q \in \mathbb{Z}[\zeta_3]$ we have

$$\alpha q = \alpha^{(1)} q^{(1)} - \alpha^{(2)} q^{(2)} + \zeta_3(\alpha^{(2)} q^{(1)} + \alpha^{(1)} q^{(2)} - \alpha^{(2)} q^{(2)}).$$

Substituting $\alpha \mapsto \alpha q + \beta$, we get by two applications of the usual Poisson summation formula (denoting $x := x_1 + \zeta_3 x_2 \in \mathbb{C}$)

$$\sum_{\substack{\alpha \in \mathbb{Z}[\zeta_3] \\ \alpha \equiv \beta \ (q)}} G_K(\alpha) = \sum_{\alpha \in \mathbb{Z}[\zeta_3]} G_K(\alpha q + \beta) = \sum_{\alpha \in \mathbb{Z}[\zeta_3]} G_K((\alpha q)^{(1)} + \beta^{(1)}, (\alpha q)^{(2)} + \beta^{(2)})$$

$$= \sum_{\alpha^{(1)}, \alpha^{(2)} \in \mathbb{Z}} G_K(\alpha^{(1)} q^{(1)} - \alpha^{(2)} q^{(2)} + \beta^{(1)}, \alpha^{(2)} q^{(1)} + \alpha^{(1)} q^{(2)} - \alpha^{(2)} q^{(2)} + \beta^{(2)})$$

$$= \sum_{h_1,h_2} \iint G_K(x_1 q^{(1)} - x_2 q^{(2)} + \beta^{(1)}, x_2 q^{(1)}$$
$$+ x_1 q^{(2)} - x_2 q^{(2)} + \beta^{(2)}) e(h_1 x_1 + h_2 x_2) dx_1 dx_2$$

$$= \sum_{h_1,h_2} \iint G_K((xq)^{(1)} + \beta^{(1)}, (xq)^{(2)} + \beta^{(2)}) e(h_1 x_1 + h_2 x_2) dx_1 dx_2$$

$$= \sum_{h_1,h_2} \iint G_K(xq + \beta) e(h_1 x_1 + h_2 x_2) dx_1 dx_2,$$

where xq is computed as a multiplication of two complex numbers, so that

$$xq = (xq)^{(1)} + \zeta_3(xq)^{(2)}.$$

We make the change of variables

$$x_j \mapsto x_j K/N_3(q)^{1/2} - (\beta\bar{q})^{(j)}/N_3(q) \quad \text{for} \quad j \in \{1, 2\}$$

so that $xq + \beta$ is mapped to

$$\left(x_1 K/N_3(q)^{1/2} + \zeta_3 x_2 K/N_3(q)^{1/2} - \beta\bar{q}/N_3(q) \right) \cdot q + \beta = \frac{K}{N_3(q)^{1/2}} xq.$$

We get

$$\sum_{\substack{\alpha \in \mathbb{Z}[\zeta_3] \\ \alpha \equiv \beta \ (q)}} G_K(\alpha) = \frac{K^2}{N_3(q)} \sum_{h_1,h_2} c_{h_1,h_2} \psi_q^{(h_1,h_2)}(-\beta),$$

where

$$c_{h_1,h_2} := \iint G_K\left(\frac{K}{N_3(q)^{1/2}} xq \right) e\left(\frac{K(h_1 x_1 + h_2 x_2)}{N_3(q)^{1/2}} \right) dx_1 dx_2$$

$$= \iint G\left(\frac{(xq)^{(1)}}{N_3(q)^{1/2}} - \frac{x_0}{K}, \frac{(xq)^{(2)}}{N_3(q)^{1/2}} - \frac{y_0}{K}\right) e\left(\frac{K(h_1x_1 + h_2x_2)}{N_3(q)^{1/2}}\right) dx_1 dx_2$$

$$= \psi_q^{(h_1,h_2)}(x_0 + \zeta_3 y_0) \iint G\left(\frac{(xq)^{(1)}}{N_3(q)^{1/2}}, \frac{(xq)^{(2)}}{N_3(q)^{1/2}}\right) e\left(\frac{K(h_1x_1 + h_2x_2)}{N_3(q)^{1/2}}\right) dx_1 dx_2$$

by making the translation (denoting $z_0 := (x_0 + \zeta_3 y_0)$)

$$x \mapsto x + \frac{1}{K N_3(q)^{1/2}} z_0 \bar{q},$$

that is,

$$x_j \mapsto x_j + \frac{1}{K N_3(q)^{1/2}} (z_0 \bar{q})^{(j)}.$$

For all h_1, h_2 we have the trivial estimate $|c_{h_1,h_2}| \leq c_{0,0} \ll_G 1$ (note that $x \mapsto xq/N_3^{1/2}(q)$ is a rotation in $\mathbb{C}$ so that $c_{0,0}$ is independent of q). As usual, $h_1 = h_2 = 0$ gives us the main term, since by another double application of Poisson summation

$$\frac{K^2}{N_3(q)} c_{0,0} = \frac{K^2}{N_3(q)} \iint G\left(\frac{(xq)^{(1)}}{N_3(q)^{1/2}}, \frac{(xq)^{(2)}}{N_3(q)^{1/2}}\right) dx_1 dx_2 = \frac{K^2}{N_3(q)} \iint G(x_1, x_2) dx_1 dx_2$$

$$= \frac{1}{N_3(q)} \iint G_K(x_1, x_2) dx_1 dx_2 = \frac{1}{N_3(q)} \sum_{\alpha \in \mathbb{Z}[\zeta_3]} G_K(\alpha) + O_C(K^{-C}).$$

For $|h_1| > H$ or $|h_2| > H$ we can iterate integration by parts to show that the contribution from this part is $\ll_{C,\epsilon} K^{-C}$. □

7 Type I sums

Using the notation of Sect. 5, for any primary $w \in \mathbb{Z}[\zeta_{12}]$ define

$$\mathcal{K}_w(N) := \sum_{N_{12}(z) \sim N}^{\wedge} [wz]$$

In this section we show (analogously to [1, Proposition 22.1]) the following proposition, which implies Proposition 9.

Proposition 13 *We have*

$$\mathcal{K}_w(N) \lll N^{11/12} N_{12}(w)^{1/6}$$

For the proof we need a generalization of the Pólya-Vinogradov estimate for short character sums. Unfortunately on $\mathbb{Z}[\zeta_3]$ we do not quite have the usual square-root bound since the estimate relies on the error term in counting lattice points; on a number field of degree d and a primitive non-principal character χ modulo $\mathfrak{q}$ Landau's generalization gives

$$\sum_{N(\mathfrak{a}) \leq x} \chi(\mathfrak{a}) \ll (N\mathfrak{q})^{1/(d+1)} (\log N(\mathfrak{q}))^d x^{(d-1)/(d+1)}.$$

However, for a smoothed version we have the Pólya–Vinogradov estimate in the usual form. Also, since we require the bound not only for short sums near 0 but in more general small sets, the smoothed version is more convenient for us. Unfortunately in our application we need to transition from a smoothed version to a sharp cut-off, which causes us to lose a power of x compared to the results in [1].

Lemma 14 *Fix $\beta, q \in \mathbb{Z}[\zeta_3]$ and $x_0, y_0 \in \mathbb{R}$. For $K \gg 1$ let*

$$G_K(x, y) := G\left(\frac{x - x_0}{K}, \frac{y - y_0}{K}\right)$$

for some fixed compactly supported C^∞-smooth function G. For $\alpha \in \mathbb{Z}[\zeta_3]$, let $G_K(\alpha) := G_K(\alpha^{(1)}, \alpha^{(2)})$. If $q \in \mathbb{Z}[\zeta_3]$ is primary primitive and not a perfect cube, then

$$\sum_{s \equiv t \ (3)} G_K(s)\left[\frac{s}{q}\right] \ll \sqrt{N_3(q)}.$$

Proof By Lemma 12 we have

$$\sum_{s \equiv t \ (3)} G_K(s)\left[\frac{s}{q}\right] = \frac{1}{9} \sum_{\psi \in \widehat{\mathbb{Z}[\zeta_3]/3\mathbb{Z}[\zeta_3]}} \psi(-t) \sum_{\beta \ (3q)} \psi(\beta)\left[\frac{\beta}{q}\right] \sum_{s \equiv \beta \ (3q)} G_K(s)$$

$$\ll \max_{\psi, h_1, h_2} \sum_{\beta \ (3q)} \left[\frac{\beta}{q}\right] \psi_{3q}^{(h_1, h_2)}(-\beta) \psi(\beta) \ll \sqrt{N_3(q)}$$

by the standard bound for Gauss sums on $\mathbb{Z}[\zeta_3]/3q\mathbb{Z}[\zeta_3]$ (proved by exactly the same argument as in the classical case on $\mathbb{Z}$). Note that the main term (corresponding to $(h_1, h_2) = (0, 0)$) is 0 by orthogonality of multiplicative characters. $\square$

Proof of Proposition 13 By Lemma 5, if $q := N_{12/3}(w)$, then for some $\omega^2 + 1 \equiv 0 \ (q)$ denoting $z = r + is, r, s \in \mathbb{Z}[\zeta_3]$

$$\mathcal{K}_w(N) \ll \sum_{N_{12}(z) \sim N}^{\wedge} \left[\frac{s}{r}\right]\left[\frac{r + \omega s}{q}\right].$$

Shifting s by ωr to get $[(r + \omega(s + r\omega))/q] = [\omega/q][s/q]$, we see by Lemma 11 that

$$\mathcal{K}_w(N) \ll \sum_{N_3(r) \ll 2\sqrt{N}} \left| \sum_{\substack{s \in I(r) \\ s \equiv \omega r \ (3)}} \left[\frac{s}{rq}\right] \right|,$$

where $I(r)$ is the domain in $\mathbb{C}$ defined by the conditions

$$|r + i(s - \omega r)||r - i(s - \omega r)| \sim N^{1/2} \qquad \text{and}$$

$$|r - i(s - \omega r)| \leq |r + i(s - \omega r)| < |r - i(s - \omega r)||\epsilon_0|^{12}$$

(so that $I(r)$ is contained in the annulus $|s - r(i - \omega)| \asymp N^{1/4}$). If rq is a perfect cube we use the trivial bound. In the remaining part we use a smooth finer-than-dyadic decomposition. Let $K > 1$ be a parameter to be optimized later. There exists a smooth partition of unity

$$\sum_{n \in \mathbb{Z}} F(x - n) = 1 \quad \text{for all} \quad x \in \mathbb{R}$$

for a certain fixed compactly supported C^∞-smooth function F. By scaling and squaring we get a smooth partition

$$\sum_{(n_1, n_2) \in \mathbb{Z}^2} F\left(\frac{x - n_1 K}{K}\right) F\left(\frac{y - n_2 K}{K}\right) = 1 \quad \text{for all} \quad (x, y) \in \mathbb{R}^2.$$

.

Using this we can to partition $I(r)$ into smoothed boxes of side-length $\asymp K$, obtaining $\ll N^{1/2}/K^2$ such boxes weighted with functions G_K as in Lemma 14. On the boundary of $I(r)$ we use the trivial bound K^2 and the fact that there are $\ll N^{1/4}/K$ boxes that intersect with the boundary, so that

$$
\mathcal{K}_w(N) \ll \sum_{\substack{N_3(r) \leq 2\sqrt{N} \\ rq=t^3}} \sqrt{N} + \sum_{N_3(r) \leq 2\sqrt{N}} N^{1/4}K + \sum_{\substack{N_3(r) \leq 2\sqrt{N} \\ rq \neq t^3}} \frac{N^{1/2}}{K^2} \max_{G_K} \left| \sum_{s \equiv \omega r \,(3)} G_K(s) \left[\frac{s}{rq}\right] \right|
$$

for any $K \ll N^{1/4}$. By Lemma 14 we have

$$
\sum_{s \equiv \omega r \,(3)} G_K(s) \left[\frac{s}{rq}\right] \ll \sqrt{N_3(rq)}
$$

assuming that rq is not a perfect cube. Hence,

$$
\mathcal{K}_w(N) \ll \sum_{\substack{N_3(r) \leq 2\sqrt{N} \\ rq=t^3}} \sqrt{N} + \sum_{N_3(r) \leq 2\sqrt{N}} N^{1/4}K + \sum_{N_3(r) \leq 2\sqrt{N}} \frac{N^{1/2}}{K^2} \sqrt{N_3(rq)}
$$

$$
\ll \sum_{\substack{n \leq 2\sqrt{N} \\ nm=t^3}} \sqrt{N} + N^{3/4}K + \frac{N^{5/4}N_3(rq)^{1/2}}{K^2} \ll N^{2/3} + N^{3/4}K + \frac{N^{5/4}N_3(q)^{1/2}}{K^2}.
$$

Choosing $K = N^{1/6}N_3(q)^{1/6} \ll N^{1/4}$ to optimize the bound we get

$$
\mathcal{K}_w(N) \ll N^{11/12}N_3(q)^{1/6}.
$$

Note that if $K = N^{1/6}N_3(q)^{1/6} \gg N^{1/4}$ then this bound is trivial. $\qquad \square$

8 Type II sums

The goal of this section is to prove Proposition 10. It turns out that the arguments in [1, Sect. 21] generalize to our case essentially verbatim. Our slightly better exponent is thanks to a small technical refinement (using a smooth weight) which is actually necessary in our situation.

By using Lemma 5 and the notation of Sect. 5, the claim is reduced to bounding (absorbing $[z]$ and $[w]$ into the coefficients)

$$
Q(M, N) := \sum_{N_{12}(w) \sim M}^{\wedge} \sum_{N_{12}(z) \sim N}^{\wedge} \alpha_w \beta_z \left(\frac{z}{w}\right),
$$

where α_w and β_z are supported on primitive numbers. First we require the following preliminary bound for $Q(M, N)$ (compare to [1, Lemma 21.2]).

Lemma 15 *We have*

$$
Q(M, N) \ll M^5 + M^{1/2}N.
$$

Proof We may assume that $N > M^{4+\eta}$ for some small $\eta > 0$, since otherwise by a trivial bound

$$
Q(M, N) \ll MN \leq M^{5+\eta}.
$$

By Cauchy-Schwarz and by Lemma 11 we have

$$Q(M, N) \ll N^{1/2} \left(\sum_{N_{12}(z) \sim N}^{\wedge} \left| \sum_{N_{12}(w) \sim M}^{\wedge} \alpha_w \left(\frac{z}{w} \right) \right|^2 \right)^{1/2}$$

$$\leq N^{1/2} \left(\sum_{w_1, w_2}^{\wedge} \alpha_{w_1} \overline{\alpha}_{w_2} \sum_{\substack{z=r+is \\ r \equiv 1 \, (3), \, 3|s}} F_{\sqrt{N}}(r) F_{\sqrt{N}}(s) \left(\frac{z}{w_1} \right) \left(\frac{z}{w_2} \right)^2 \right)^{1/2}$$

where $F_{\sqrt{N}}(r) = F(N_3(r)/\sqrt{N})$ for a fixed compactly supported C^∞-smooth function F so that $F_{\sqrt{N}}(r) F_{\sqrt{N}}(s)$ is a smooth majorant for the original summation range. Let $q := N_{12/3}(w_1 w_2) = u^2 + v^2$ with $(u, v) = 1$. Note that $(3, q) = 1$ since -1 is not a square in $\mathbb{Z}[\zeta_3]/(1 - \zeta_3)\mathbb{Z}[\zeta_3]$. Splitting the sum over z into residue classes modulo $3q$ we get for some constant c_0

$$\sum_{\substack{z=r+is \\ r \equiv 1 \, (3), \, 3|s}} F_{\sqrt{N}}(r) F_{\sqrt{N}}(s) \left(\frac{z}{w_1} \right) \left(\frac{z}{w_2} \right)^2$$

$$= \sum_{\substack{\zeta = r_0 + i s_0 \in \mathbb{Z}[\zeta_{12}]/3q\mathbb{Z}[\zeta_{12}] \\ r_0 \equiv 1 \, (3), \, 3|s_0}} \left(\frac{\zeta}{w_1} \right) \left(\frac{\zeta}{w_2} \right)^2 \sum_{\substack{r, s \in \mathbb{Z}[\zeta_3] \\ (r,s) \equiv (r_0, s_0) \, (3q)}} F_{\sqrt{N}}(r) F_{\sqrt{N}}(s)$$

$$= \left(\frac{c_0^2 N}{N_3(3q)^2} + O_C(X^{-C}) \right) \sum_{\substack{\zeta = r_0 + i s_0 \in \mathbb{Z}[\zeta_{12}]/3q\mathbb{Z}[\zeta_{12}] \\ r_0 \equiv 1 \, (3), \, 3|s_0}} \left(\frac{\zeta}{w_1} \right) \left(\frac{\zeta}{w_2} \right)^2$$

by Lemma 12 since $N_3(q) \ll M^2 < X^{-\eta} \sqrt{N}$. Recall the notation of Lemma 6, that is,

$$q_j = N_{12/3}(w_j), \quad e := (w_1, \sigma(w_2^2)), \quad \text{and} \quad d := N_{12/3}(e),$$

where σ is the conjugation $\sigma(a + ib) = a - ib$. By Lemma 6 we have (writing $x := r_0 - \omega s_0$, $y := r_0 + \omega s_0$)

$$\sum_{\substack{\zeta = r_0 + i s_0 \in \mathbb{Z}[\zeta_{12}]/3q\mathbb{Z}[\zeta_{12}] \\ r_0 \equiv 1 \, (3), \, 3|s_0}} \left(\frac{\zeta}{w_1} \right) \left(\frac{\zeta}{w_2} \right)^2 = \sum_{\substack{r_0, s_0 \in \mathbb{Z}[\zeta_3]/3q\mathbb{Z}[\zeta_3] \\ r_0 \equiv 1 \, (3), \, 3|s_0}} \left[\frac{r_0 - \omega s_0}{d} \right] \left[\frac{r_0 + \omega s_0}{q_1 q_2^2/d} \right]$$

$$= \sum_{\substack{x \in \mathbb{Z}[\zeta_3]/3q\mathbb{Z}[\zeta_3] \\ x \equiv 1 \, (3)}} \left[\frac{x}{d} \right] \sum_{\substack{y \in \mathbb{Z}[\zeta_3]/3q\mathbb{Z}[\zeta_3] \\ y \equiv 1 \, (3)}} \left[\frac{y}{q_1 q_2^2/d} \right]$$

$$= N_3(q) \sum_{\substack{x \in \mathbb{Z}[\zeta_3]/3d\mathbb{Z}[\zeta_3] \\ x \equiv 1 \, (3)}} \left[\frac{x}{d} \right] \sum_{\substack{y \in \mathbb{Z}[\zeta_3]/(3q/d)\mathbb{Z}[\zeta_3] \\ y \equiv 1 \, (3)}} \left[\frac{y}{q_1 q_2^2/d} \right] = 0$$

unless both of d and $q_1 q_2^2/d$ are perfect cubes in which case we get

$$N_3(q) \varphi(N_3(d)) \varphi(N_3(q/d)) \leq N_3(q)^2.$$

To see this, recall that $(3, q) = 1$ and note that $[y/(q_1 q_2^2/d)]$ is a cubic character modulo q/d. Hence, we get

$$Q(M, N)^2 \lll N^2 \sum_{\substack{q_1, q_2 \in \mathbb{Z}[\zeta_3] \\ q_1 q_2^2 = t^3 \\ N_3(q_1), N_3(q_2) \leq 2M}} 1.$$

We have

$$\sum_{\substack{q_1, q_2 \in \mathbb{Z}[\zeta_3] \\ q_1 q_2^2 = t^3 \\ N_3(q_1), N_3(q_2) \leq 2M}} 1 \lll \sum_{\substack{m_1, m_2 \leq 2M \\ m_1 m_2^2 = c^3}} 1 = \sum_{d \leq 2M} \sum_{\substack{m_1, m_2 \leq 2M/d \\ (m_1, m_2) = 1 \\ m_1 = c_1^3, m_2 = c_2^3}} 1 \ll M^{2/3} \sum_{d \leq 2M} d^{-2/3} \ll M,$$

so that for $N > X^\eta M^4$

$$Q(M, N) \lll M^{1/2} N.$$

□

Remark 11 Note that the modulus $q_1 q_2^2$ being a cube is morally the same as $q_1 q_2$ being a square which explains why we get the same term $M^{1/2} N$ as in [1, Lemma 21.2].

Lemma 15 is non-trivial as soon as $N \gg M^4 \gg 1$. Similarly as in [1], we now use Hölder's inequality to extend this range so that we can handle the range $M \asymp N$. We get

$$Q^k(M, N) \lll M^{k-1} \sum_w^\wedge \left| \sum_z^\wedge \beta_z \left(\frac{z}{w} \right) \right|^k = M^{k-1} \tilde{Q}(M, N^k),$$

where $\tilde{Q}$ is of similar form as Q except that α_w is replaced by some coefficients $\tilde{\alpha}_w$ with $|\tilde{\alpha}_w| \leq 1$ and β_z is replaced by the divisor bounded coefficient

$$\tilde{\beta}_z = \sum_{z_1 \cdots z_k = z}^\wedge \beta_{z_1} \cdots \beta_{z_k}$$

where now each z_1 satisfies the conditions of Lemma 11 separately. Applying Lemma 15 to $\tilde{Q}(M, N^k)$ we get

$$Q(M, N) \lll M^{1+4/k} + M^{1-1/2k} N.$$

Similarly as in [1], we will use reciprocity below to get a symmetric bound. Hence, the most difficult range will be $M = N$. To optimize the bound we choose $k = 5$ to get

$$Q(M, N) \lll M^{9/5} + M^{9/10} N \lll M^{9/10} N$$

if $M \leq N$. Since by Lemma 5 $(z/w) = (w/z)$ for primitive primary z and w, the form $Q(M, N)$ is symmetric and we get

$$Q(M, N) \lll M N^{9/10} + M^{9/10} N.$$

□

Remark 12 The reason our bound is superior to that in [1, Proposition 21.3] is that we used the smooth function $F_{\sqrt{N}}(r)$ instead of a sharp cut-off $N_3(r) \leq \sqrt{N}$ in the proof of Lemma 15. This allows us to improve the term $M^2 N^{3/4}$ appearing in Lemma [1, Lemma 21.2] to M^5. Obviously the same refinement can be implemented to improve their bound to the same form.

9 Connection to primes of the form $\alpha^2 + \beta^6$ on $\mathbb{Z}[\zeta_3]$

It is tempting to ask if the method of Friedlander and Iwaniec can be extended to produce primes of the form $a^2 + b^6$ on $\mathbb{Z}$ (cf. [12, Remarque 4.20]). Unfortunately there seems to be two large obstacles to this. Firstly, the sequence is too sparse for replicating the steps in [1, Sects. 5–9]. The second problem is structural—the proofs in [1] rely on the law of quadratic reciprocity in multiple places, while for cubic residues we do not have a suitable reciprocity law on $\mathbb{Z}$. To mend this we need to transfer the whole set-up to $\mathbb{Z}[\zeta_3]$. Unfortunately the first problem persist (cf. the paragraph around (9.4) below).

In this section we explain how the sum in Theorem 1 arises if we consider primes of the form $\alpha^2 + \beta^6$ on $\mathbb{Z}[\zeta_3]$, which was the original motivation for this manuscript. All of the discussion presented here is non-rigorous and for the sake of illustration we omit all of the technical issues that arise in [1]. The argument follows exactly the same lines as in [1].

Note that if $z \in \mathbb{Z}[\zeta_3]$ is the sum of two squares, it has infinitely many such representations. To make the analogy with the Friedlander-Iwaniec Theorem precise we consider primary primes $\pi = \beta^3 + i\alpha$ on $\mathbb{Z}[\zeta_{12}]$ with the restriction

$$N_{12}(\beta^3 + i\alpha)^{1/4} \leq |\beta^3 + i\alpha| < N_{12}(\beta^3 + i\alpha)^{1/4}|\epsilon_0|^6 \tag{9.1}$$

as in Sect. 5. Note that this implies that $|\alpha| \ll x^{1/4}$ and $|\beta| \ll x^{1/12}$ if $N_{12}(\pi) \ll x$.

The number of ideals $\mathfrak{a}$ with $N_{12}\mathfrak{a} \leq x$ that have such a generator $\beta^3 + i\alpha$ is

$$\sum_{N_{12}\mathfrak{a} \leq x} \sideset{}{^\wedge}\sum_{\substack{y = \beta^3 + i\alpha \\ (y) = \mathfrak{a}}} 1 \asymp x^{2/3},$$

which is very sparse (the inability of the Friedlander-Iwaniec method to handle sets of density $< x^{-1/3}$ is also noted by Helfgott [9]). Due to this we are not able to handle the Type II sums, as we shall see soon below (see (9.4)). However, it should be possible to obtain an approximation to this problem by considering primes of the form $\alpha^2 + \lambda^2 \beta^6$ where λ runs over elements of small norm $N_3(\lambda) \leq x^\delta$, to show that for some fairly small $\delta > 0$ we get a lower bound of the correct order of magnitude for the number of such primes. For this the sieve of Friedlander and Iwaniec needs to be replaced by Harman's sieve (see [11] for a version of this on Number fields).

Remark 13 Restricting to generators satisfying (9.1) does not decrease the density essentially. Most of the integers $\beta^3 + i\alpha \in \mathbb{Z}[\zeta_{12}]$ with $|\alpha^2 + \beta^6|^2 \leq x$ come from the part $|\alpha| \ll x^{1/4}$ and $|\beta| \ll x^{1/12}$. To see this note that we have $|\beta^3 + i\alpha||\beta^3 - i\alpha| \leq x^{1/2}$. Suppose that $|\beta^3 + i\alpha|$ and $|\beta^3 - i\alpha|$ are not of similar size, say, $|\beta^3 - i\alpha| \asymp Y$ for some $1 \ll Y \ll x^{1/4}$. For any given β there are roughly Y^2 choices of α that satisfy $|\beta^3 - i\alpha| \asymp Y$. But then $|\beta^3 + i\alpha| \ll x^{1/2}/Y$ is morally the same as $|\beta| \ll x^{1/6}/Y^{1/3}$, so that there are roughly $x^{1/3}/Y^{2/3}$ choices for β and we get

$$|\{\alpha, \beta \in \mathbb{Z}[\zeta_3] : |\alpha^2 + \beta^6|^2 \leq x, \ |\beta^3 - i\alpha| \asymp Y\}| \asymp Y^2 \cdot x^{1/3}/Y^{2/3} = x^{1/3}Y^{4/3},$$

which is much less than $x^{2/3}$ if Y is much smaller than $x^{1/4}$. Heuristically the same holds also for $Y < 1$, since the probability of finding a lattice point $i\alpha$ near β^3 is proportional to the area Y^2. Thus, we cannot increase the density by considering all generators $\beta^3 + i\alpha$ instead of just those satisfying (9.1).

Using a sieve argument the main problem is to handle Type II sums of the form

$$S_1 := \sum_{N_{12}\mathfrak{m}\sim M} \alpha_\mathfrak{m} \sum_{N_{12}\mathfrak{n}\sim N} \beta_\mathfrak{n} \sum_{\substack{y=\beta^3+i\alpha \\ (y)=\mathfrak{mn}}}^{\wedge} 1,$$

where $MN = x$, and α and β are bounded coefficients with β behaving like a Möbius function in terms of a Siegel–Walfisz type condition. The goal then is to show that $S_1 \ll_C x^{2/3} \log^{-C} x$.

We now pick a primary generator z of $\mathfrak{n}$ according to Sect. 5, and then pick a generator $\sigma(w)$ of $\mathfrak{m}$ such that $y = \sigma(w)z$. The cross-condition

$$N_{12}(w)^{1/4} N_{12}(z)^{1/4} \leq |z||w| < N_{12}(w)^{1/4} N_{12}(z)^{1/4} |\epsilon_0|^6 \tag{9.2}$$

is easily removed by Perron's formula, so that we are essentially left with

$$S_2 := \sum_{N_{12}(w)\sim M}^{\wedge} \alpha_{\sigma(w)} \sum_{N_{12}(z)\sim N}^{\wedge} \beta_z \sum_{\sigma(w)z=\beta^3+i\alpha} 1$$

(note that (9.2) together with $|z| \asymp N_{12}(z)^{1/4}$ implies $|w| \asymp N_{12}(w)^{1/4}$ which is morally same as the condition implied by the $\wedge$ in the sum over w).

Applying the Cauchy–Schwarz inequality similarly as in [1] we get $S_2 \ll M^{1/2} S_3^{1/2}$ for

$$S_3 := \sum_{z_1,z_2}^{\wedge} \beta_{z_1} \overline{\beta}_{z_2} \sum_w \sum_{\substack{\sigma(w)z_1=\beta_1^3+i\alpha_1 \\ \sigma(w)z_2=\beta_2^3+i\alpha_2}} F_M(w)$$

for some suitable smooth function F_M supported on $N_{12}(w) \asymp M$ and $|w| \asymp M^{1/4}$.

From the diagonal part $z_1 = z_2$ we get a contribution $(MN)^{2/3}$, which is sufficient for $S_1 \ll x^{2/3} \log^{-C} x$ as long as

$$N \gg x^{1/3} \log^C x. \tag{9.3}$$

In the off-diagonal the generic case is $(z_1, z_2) = 1$, and by the same argument as in [1, Sect. 6] we have

$$i\Delta w = \beta_1^3 z_2 - \beta_2^3 z_1,$$

where $z_j = r_j + i s_j$ and $\Delta := r_1 s_2 - r_2 s_1$. Thus, the off-diagonal part is

$$S_4 := \sum_{(z_1,z_2)=1}^{\wedge} \beta_{z_1}\overline{\beta}_{z_2} \sum_{\beta_1^3 z_2 \equiv \beta_2^3 z_1\,(\Delta)} F_M((\beta_1^3 z_2 - \beta_2^3 z_1)/i\Delta)$$

$$= \sum_{(z_1,z_2)=1}^{\wedge} \beta_{z_1}\overline{\beta}_{z_2} \sum_{\substack{\gamma_1,\gamma_2\,(\Delta) \\ \gamma_1^3 z_2 \equiv \gamma_2^3 z_1\,(\Delta)}} \sum_{(\beta_1,\beta_2)\equiv(\gamma_1,\gamma_2)\,(\Delta)} F_M((\beta_1^3 z_2 - \beta_2^3 z_1)/i\Delta).$$

Similarly to [1] we note that the congruence $\beta_1^3 z_2 \equiv \beta_2^3 z_1\,(\Delta)$ is in fact a $\mathbb{Z}[\zeta_3]$-rational congruence, since

$$z_2 z_1^{-1} \equiv \frac{r_1 r_2 + s_1 s_2}{r_1^2 + s_1^2}\,(\Delta).$$

Unfortunately here we run into a problem with the sparseness of our sequence (note that also in [1] for the Type II sums this is the only part of the argument affected by the sparsity).

We would like to apply Poisson summation (Lemma 12) to evaluate the smoothed sum over β_1, β_2. However, due to the diagonal contribution (9.3) we have essentially

$$N_3(\Delta) \approx N \gg x^{1/3} \log^C x$$

while the length of the sum is

$$N_3(\beta_j) \ll x^{1/6} \tag{9.4}$$

which is just narrowly too short (Poisson summation becomes ineffective if the length of the sum is less than square root of the size of the modulus). Due to this we are not able to evaluate the sum in any range of N. If we consider the aforementioned approximation version of the problem with $\alpha^2 + \lambda^2 \beta^6$ for $N_3(\lambda) \leq x^\delta$, then the diagonal part gives a restriction $N \gg x^{1/3 - 2\delta/3} \log^C x$ which gives some room to work with. We have been able to evaluate the sum over $\beta_1^3 \lambda_1 z_2 \equiv \beta_2^3 \lambda_2 z_1$ (Δ) in some ranges using a large sieve argument similar to that in Heath-Brown and Li [7] (although the argument required here is much more intricate).

Remark 14 Since the argument falls short barely, there is some hope that with a delicate estimate we could handle Type II sums in some very narrow non-trivial range for $N = x^{1/3 + o(1)}$. This would suffice to break the parity barrier, that is, to show that there are infinitely many of $\alpha^2 + \beta^6$ are a product of exactly two primes (one of size M and the other of size N).

Assuming that the sum over β_1, β_2 could be computed, then the main term is essentially (up to a multiplicative factor and a smooth coefficient, and ignoring the fact that γ_j may have common factors with Δ)

$$S_5 := \sideset{}{^\wedge}\sum_{(z_1, z_2) = 1} \beta_{z_1} \overline{\beta}_{z_2} \sum_{\substack{(\omega, \Delta) = 1 \\ \omega^3 \equiv z_2 z_1^{-1} \, (\Delta)}} 1$$

(for the approximate version of the problem the congruence is $\omega^3 \equiv z_2 \lambda_1 z_1^{-1} \lambda_2^{-1}$ (Δ), which is morally the same). Here we need to show only a little bit of cancellation, that is, $S_5 \ll N^2 \log^{-C} x$. To evaluate the sum over cubic roots we make use of the Chinese Reminder Theorem and the cubic residue character to get (assuming Δ is square-free, primitive, and ignoring the fact that $3 | \Delta$)

$$\sum_{\substack{(\omega, \Delta) = 1 \\ \omega^3 \equiv z_2 z_1^{-1} \, (\Delta)}} 1 = \prod_{\pi | \Delta} \left(1 + \left[\frac{z_2 z_1^{-1}}{\pi} \right] + \left[\frac{z_2 z_1^{-1}}{\pi} \right]^2 \right)$$

$$= \sum_{\delta_1 \delta_2 | \Delta} \left[\frac{z_2 z_1^{-1}}{\delta_1} \right] \left[\frac{z_2 z_1^{-1}}{\delta_2} \right]^2 .$$

Thus, we essentially get (compare to $T(\beta)$ in [1, Sect. 10])

$$S_5 = \sum_{\delta_1, \delta_2} \sideset{}{^\wedge}\sum_{\substack{(z_1, z_2) = 1 \\ \Delta \equiv 0 \, (\delta_1 \delta_2)}} \beta_{z_1} \overline{\beta}_{z_2} \left[\frac{z_2 z_1^{-1}}{\delta_1} \right] \left[\frac{z_2 z_1^{-1}}{\delta_2} \right]^2 .$$

Similarly as in [1, Sect. 10], we now split the sum into three parts $U + V + W$ according to the size of $\delta_1 \delta_2$, where in U we have $N_3(\delta_1 \delta_2) \ll \log^C N$, in W we have $N_3(\delta_1 \delta_2) \gg N_3(\Delta) \log^{-C}$, and V is the remaining middle part.

For U we get the required cancellation from the β_z, which look like a Möbius function, by using a suitable Siegel–Walfisz type bound.

For V we have not checked in detail but we expect that the large sieve -type arguments in [1, Sects. 11–15] generalize to our case.

For W the generic case is $\delta_1\delta_2 = \Delta$. To handle this we need the following analogue of [1, Lemma 17.1], which we will prove at the end of this section.

Lemma 16 *For z_1, z_2, $\Delta = r_1s_2 - r_2s_1$ with z_1, z_2 primary and $z_1 \equiv z_2$ (9) we have*

$$\left[\frac{z_2z_1^{-1}}{\Delta}\right] = \left[\frac{s_1}{r_1}\right]^2\left[\frac{s_2}{r_2}\right].$$

To guarantee that $z_1 \equiv z_2$ (9) we have to split z into residue classes modulo 9 before the application of Cauchy–Schwarz.

Using this lemma the sum W is essentially reduced to

$$
\begin{aligned}
S_6 &:= \sum_{(z_1,z_2)=1}^{\wedge} \beta_{z_1}\overline{\beta}_{z_2} \sum_{\Delta=\delta_1\delta_2}\left[\frac{z_2z_1^{-1}}{\delta_1}\right]\left[\frac{z_2z_1^{-1}}{\delta_2}\right]^2 \\
&= \sum_{(z_1,z_2)=1}^{\wedge} \beta_{z_1}\overline{\beta}_{z_2}\left[\frac{z_2z_1^{-1}}{\Delta}\right]\sum_{\delta_2|\Delta}\left[\frac{z_2z_1^{-1}}{\delta_2}\right] \\
&= \sum_{(z_1,z_2)=1}^{\wedge} \beta_{z_1}\left[\frac{s_1}{r_1}\right]^2\overline{\beta}_{z_2}\left[\frac{s_2}{r_2}\right]\sum_{\delta_2|\Delta}\left[\frac{z_2z_1^{-1}}{\delta_2}\right].
\end{aligned}
$$

We now again partition the sum into three parts $W_1 + W_2 + W_3$ according to the size of δ_2.

In W_1 the generic case is $\delta_2 = 1$ and we get a sum

$$\sum_{(z_1,z_2)=1}^{\wedge} \beta_{z_1}\left[\frac{s_1}{r_1}\right]^2\overline{\beta}_{z_2}\left[\frac{s_2}{r_2}\right],$$

which can be bounded using similar arguments as in the proof of Theorem 1 (once we remove the condition $(z_1, z_2) = 1$ either by Möbius function or by the device in [1]), since the coefficients β_z have a Type I/Type II decomposition.

Similarly for W_3 the generic case is $\delta_2 = \Delta$ and we get by a second application of Lemma 16 a sum

$$\sum_{(z_1,z_2)=1}^{\wedge} \beta_{z_1}\left[\frac{s_1}{r_1}\right]\overline{\beta}_{z_2}\left[\frac{s_2}{r_2}\right]^2$$

which is of the same form as with W_1.

Finally for W_2 we note that this sum is essentially contained in the earlier sum V but with the coefficients β_z twisted by $[z]$ or $[z]^2$, so that the same argument as with V should take care of this part.

Proof of Lemma 16 The argument is essentially the same as the proof of [1, Lemma 17.1]. For simplicity we give the proof only in the case $(r_1, r_2) = 1$ (in the general case we have to juggle back and forth with the factor (r_1, r_2)). Since $[r_1^3/\Delta] = 1$, we have

$$\left[\frac{z_2z_1^{-1}}{\Delta}\right] = \left[\frac{(r_1^2 + s_1^2)^{-1}(r_1r_2 + s_1s_2)}{\Delta}\right] = \left[\frac{(r_1^2 + s_1^2)^{-1}(r_1r_2 + s_1s_2)r_1^3}{\Delta}\right].$$

We have

$$(r_1 r_2 + s_1 s_2)r_1^3 - (r_1^2 + s_2^2)r_1^2 r_2 = r_1^2 s_1 (r_1 s_2 - r_2 s_1) \equiv 0 \; (\Delta),$$

so that

$$(r_1^2 + s_1^2)^{-1}(r_1 r_2 + s_1 s_2)r_1^3 \equiv r_1^2 r_2 \; (\Delta).$$

Hence,

$$\left[\frac{z_2 z_1^{-1}}{\Delta}\right] = \left[\frac{r_1^2 r_2}{\Delta}\right] = \left[\frac{r_1}{\Delta}\right]^2 \left[\frac{r_2}{\Delta}\right] = \left[\frac{\Delta}{r_1}\right]^2 \left[\frac{\Delta}{r_2}\right]$$

by the supplementary laws in Lemma 4, since $z_1 \equiv z_2$ (9). Therefore,

$$\left[\frac{z_2 z_1^{-1}}{\Delta}\right] = \left[\frac{r_1 s_2 - r_2 s_1}{r_1}\right]^2 \left[\frac{r_1 s_2 - r_2 s_1}{r_2}\right] = \left[\frac{-r_2 s_1}{r_1}\right]^2 \left[\frac{r_1 s_2}{r_2}\right] = \left[\frac{s_1}{r_1}\right]^2 \left[\frac{s_2}{r_2}\right],$$

since by Lemma 4 for r_1 and r_2 primary

$$\left[\frac{-r_2}{r_1}\right]^2 \left[\frac{r_1}{r_2}\right] = \left[\frac{r_2}{r_1}\right]^2 \left[\frac{r_1}{r_2}\right] = \left[\frac{r_1}{r_2}\right]^3 = 1.$$

$\square$

References

1. Friedlander, J., Iwaniec, H.: The polynomial $X^2 + Y^4$ captures its primes. Ann. of Math. (2) **148**(3), 945–1040 (1998)
2. Friedlander, J.B., Iwaniec, H.: The illusory sieve. Int. J. Number Theory **1**(4), 459–494 (2005)
3. Friedlander, J.B., Iwaniec, H.: A polynomial divisor problem. J. Reine Angew. Math. **601**, 109–137 (2006)
4. Friedlander, J.B., Iwaniec, H., Mazur, B., Rubin, K.: The spin of prime ideals. Invent. Math. **193**(3), 697–749 (2013)
5. Harman, G.: Prime-detecting sieves. London Mathematical Society Monographs Series, vol. 33. Princeton University Press, Princeton, NJ (2007)
6. Heath-Brown, D.R.: Primes represented by $x^3 + 2y^3$. Acta Math. **186**(1), 1–84 (2001)
7. Heath-Brown, D.R., Li, X.: Prime values of $a^2 + p^4$. Invent. Math. **208**(2), 441–499 (2017)
8. Heath-Brown, D.R., Moroz, B.Z.: Primes represented by binary cubic forms. Proc. Lond. Math. Soc. (3) **84**(2), 257–288 (2002)
9. Helfgott, H.A.: The parity problem for reducible cubic forms. J. Lond. Math. Soc. (2) **73**(2), 415–435 (2006)
10. Lemmermeyer, F.: Reciprocity laws. Springer Monographs in Mathematics. Springer-Verlag, Berlin. From Euler to Eisenstein (2000)
11. Maynard, J.: Primes represented by incomplete norm forms. Forum Math. Pi **8**, e3 (2020)

12. Michel, P.: Progrès récents du crible et applications (d'après Duke, Fouvry, Friedlander, Iwaniec). Number 252, pages Exp. No. 842, 4, 185–209. Séminaire Bourbaki. Vol. 1997/98 (1998)
13. Milne, J.: Class field theory, 2020. URL (Accessed 8.9.2020): https://www.jmilne.org/math/CourseNotes/cft.html
14. Milovic, D.: On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \ @mod 4$. Geom. Funct. Anal. **27**(4), 973–1016 (2017)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.