On the largest prime factor of quartic polynomial values: the cyclic and dihedral cases

Cécile Dartyge, James Maynard

On the largest prime factor of quartic polynomial values: the cyclic and dihedral cases

Cécile Dartyge and James Maynard

Abstract

Let $P(X) \in \mathbb{Z}[X]$ be an irreducible, monic, quartic polynomial with cyclic or dihedral Galois group. We prove that there exists a constant $c_P > 0$ such that for a positive proportion of integers n, $P(n)$ has a prime factor $\geq n^{1+c_P}$.

Contents

1 Introduction

Let $P(X) \in \mathbb{Z}[X]$ be an irreducible degree polynomial with $d \geq 2$. Assuming that there is no local obstruction, it is widely believed [17] that P should take on infinitely many prime values, but unfortunately this conjecture remains completely open for all non-linear polynomials P.

As an approximation to this problem, one can look for integers n for which $P(n)$ has a large prime factor. For general polynomials P, the best known bound is due to Tenenbaum [18], who shows that there are infinitely many integers n such that $P(n)$ has a prime factor of size at least $n \exp((\log n)^\alpha)$ for any $\alpha < 2 - \log 4$. When the degree of P is 5 or more, this is the best known result, but for some low degree polynomials, one can produce bounds which are much stronger.

Hooley [9] proved the first result of this kind, showing that the largest prime factor $P^+(n^2+1)$ of n^2+1 satisfies $P^+(n^2+1) > n^{11/10}$ infinitely often. The exponent $11/10$ has been improved by Deshouillers and Iwaniec [5], next by La Bretèche and Drappeau [2] and the current record due to Merikoski [15] is that $P^+(n^2+1) > n^{1.279}$ infinitely often. Heath-Brown [8] showed that $P^+(n^3+2) > n^{1+10^{-303}}$ infinitely often. Irving [10] proved fifteen years later that exponent $1+10^{-303}$ can be replaced by $1+10^{-52}$. It seems plausible that the underlying methods could be adapted to more general degree 2 or degree 3 polynomials.

For degree 4 polynomials, results can currently only be obtained when the Galois group G of $P(X)$ takes a simple form. When $P(X) = X^4 - X^2 + 1$, the twelfth cyclotomic polynomial, Dartyge [4] proved that there are infinitely many n such that $P^+(n^4-n^2+1) > n^{1+10^{-26531}}$. La Bretèche [1] generalised this result to quartic irreducible even monic polynomials with Galois group isomorphic to the Klein group $V := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For such

polynomials P, he proved that there exists $c_P > 0$ such that $P^+(P(n)) > n^{1+c_P}$ for a positive proportion of integers n. It seems plausible that the methods of [1] and [4] may be adapted for some more general quartic polynomials, but the condition that the Galois group is V is crucial to the method.

In this work we obtain results for irreducible quartic polynomials with Galois group isomorphic to the cyclic group $C_4 := \mathbb{Z}/4\mathbb{Z}$ or the dihedral group $D_4 = \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/4\mathbb{Z}$. Our method doesn't work for polynomials with Galois group A_4 or S_4 which are the most frequent Galois groups for quartic irreducible polynomials. However, the fifth cyclotomic polynomial $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, $X^4 - 5X^2 + 5$, $X^4 + 13X + 39$ are examples of polynomials with cyclic Galois group and X^4+2, X^4+3X+3, $X^4 - 5X^2 + 3$ are polynomials with Galois group D_4. (cf. [3] for other examples of quartic polynomials with dihedral or cyclic Galois group).

Theorem 1.1. *Let $P(X)$ be a monic quartic irreducible polynomial with Galois group C_4 or D_4. Then there exists a constant $c_P > 0$ such that for $x > x_0(P)$, we have*

$$|\{x < n \leq 2x : P^+(P(n)) \geq x^{1+c_P}\}| \gg x.$$

The key new technical innovation behind our proof of Theorem 1.1 is to incorporate 'Type II' or 'bilinear' information into the method of detecting large prime factors; previous approaches had relied solely on 'Type I' information. This Type II information allows us to handle polynomials with Galois groups C_4 or D_4 which were out of reach of the Type I approach. In principle one could hope to handle the remaining possibilities A_4 or S_4 to cover all Galois groups by a similar procedure, but we do not know how to handle the relevant Type II estimates in this case, and so our paper is limited to C_4 and D_4. Following the approaches of Heath-Brown [8], Dartyge [4] and La Bretèche [1], the key to obtaining estimates like Theorem 1.1 is showing that a certain multivariate polynomial q associated to $P(X)$ has a convenient prime factorisation for a positive proportion of its values.

For quartic $P(X)$, this associated polynomial $q = q(a_1, a_2, a_3)$ is a ternary sextic form. If P has a Galois group V, then $q(a_1, a_2, a_3) = q_1(a_1, a_2, a_3)q_2(a_1, a_2, a_3)q_3(a_1, a_2, a_3)$ is a product of 3 ternary quadratic forms, and the methods of [4] and [1] could then produce many suitable prime factorisations by showing equidistribution of q_1 and q_2 in suitable arithmetic progressions[1]. (This is why we refer to their methods as 'Type I' methods.) When P has a larger Galois group, then the form $q(a_1, a_2, a_3)$ is the product of a quartic and a quadratic (if $G = C_4$ or D_4) or is an irreducible sextic (if $G = A_4$ or S_4). Unfortunately one cannot obtain a suitable factorisation by just considering analogous equidistribution in arithmetic progressions in these cases, since one would need to work with moduli which are too large for equidistribution to occur.

We find that if $G = C_4$ or D_4, the ternary quartic factor of q has the additional algebraic structure of being an 'incomplete norm form'.

[1] Similarly, in the work of Heath-Brown [8] dealing with cubic $P(X)$, the associated form q is a binary cubic, and it suffices to just obtain distribution estimates for q in arithmetic progressions

Maynard [14] produced various Type II estimates which were used to count prime values of incomplete norm forms. By adapting the ideas underlying these estimates to our situation we are able to show that q has a convenient prime factorisation for a positive proportion of its values. This part corresponds to Theorem 4.1 announced in Section 4.

Combining this result with the previous machinery (suitably generalised to our situation) then yields Theorem 1.1.

1.1 Outline of the proof of Theorem 1.1

The proof of Theorem 1.1 takes three key steps. Step 1 is an argument due to Heath-Brown [8] (see also [6]), which reduces the problem to showing the existence of many integers where $P(n)$ has an unusually large friable part (i.e. a part without large prime factor).

Step 2 follows and generalises [8, 4, 1] and shows that by using the q-analogue of Van der Corput's method, it suffices to show that a certain ternary form $q(a_1, a_2, a_3)$ associated to P takes many values with a suitable prime factorisation. This step makes use of the fact that P is a quartic polynomial. The key new ingredient in our work is Step 3, where we establish that $q(a_1, a_2, a_3)$ takes on many values with the suitable prime factorisation when P has Galois group C_4 or D_4. For this final step we incorporate ideas of Maynard [14] on prime values of incomplete norm forms.

Step 1: Reduction to many integers with large friable part.

Let $r_1 \in \overline{\mathbb{Q}}$ be a root of $P(n)$, $K = \mathbb{Q}(r_1)$ and $N_P = N_{K/\mathbb{Q}}$ the associated norm. Then we see that $N_P(n - r_1) = P(n)$, and so we are interested in counting integers n such that the ideal $(n - r_1)$ has a prime ideal factor of large norm. In particular,

$$\sum_{\substack{n\in[x,2x]\\ P^+(P(n))\geq x^{1+\eta}}} 1 = \sum_{\substack{n\in[x,2x]\\ \exists \mathfrak{p}|(n-r_1):\, N_P(\mathfrak{p})\geq x^{1+\eta}}} 1 \gg \frac{1}{\log x} \sum_{n\in[x,2x]} \sum_{\substack{\mathfrak{p}^e|(n-r_1)\\ N_P(\mathfrak{p})\geq x^{1+\eta}}} \log N_P(\mathfrak{p}).$$

By inclusion-exclusion and the fact that $\sum_{\mathfrak{p}^e|(n-r_1)} \log \mathfrak{p} = \log P(n)$, we have that the double sum on the right hand side is given by

$$\sum_{n\in[x,2x]} \log P(n) - \sum_{n\in[x,2x]} \sum_{\substack{\mathfrak{p}^e|(n-r_1)\\ N_P(\mathfrak{p})\leq 2x}} \log N_P(\mathfrak{p}) - \sum_{n\in[x,2x]} \sum_{\substack{\mathfrak{p}^e|(n-r_1)\\ 2x<N_P(\mathfrak{p})<x^{1+\eta}}} \log N_P(\mathfrak{p}).$$

Since $P(n) \asymp n^4$, the first sum is $(4 + o(1))x \log x$. Swapping the order of summation and applying the Prime Ideal Theorem shows that the second sum is $(1 + o(1))x \log x$. Let $\mathcal{A}$ be the set of integers n with $\sum_{\mathfrak{p}|(n-r_1), N_P(\mathfrak{p})\leq 2x} \log N_P(\mathfrak{p}) \geq (1 + \delta_0) \log x$. We split the third sum according to whether $n \in \mathcal{A}$ or not. Therefore the above expression is

$$(3 + o(1))x \log x - \sum_{\substack{n\in[x,2x]\\ n\in\mathcal{A}}} \sum_{\substack{\mathfrak{p}^e|(n-r_1)\\ 2x<N_P(\mathfrak{p})<x^{1+\eta}}} \log N_P(\mathfrak{p}) - \sum_{\substack{n\in[x,2x]\\ n\notin\mathcal{A}}} \sum_{\substack{\mathfrak{p}^e|(n-r_1)\\ 2x<N_P(\mathfrak{p})<x^{1+\eta}}} \log N_P(\mathfrak{p}).$$

If $n \in \mathcal{A}$ then since prime ideals with $N_P(\mathfrak{p}) \leq 2x$ contribute at least $(1 + \delta_0) \log x$ to $\sum_{\mathfrak{p}|(n-r_1)} \log N_P(\mathfrak{p}) = (4 + o(1)) \log x$, the contribution

from prime ideals with $N_P(\mathfrak{p}) > 2x$ must be $\leq (3 - \delta_0 - o(1)) \log x$. If $n \notin \mathcal{A}$ then we note from size considerations there can be at most 3 prime ideals with $N_P(\mathfrak{p}) \geq 2x$ dividing $(n - r_1)$, and so the inner sum over $\mathfrak{p}$ is at most $3(1 + \eta) \log x$. Substituting these bounds into the above, we find

$$\sum_{n \in [x,2x]} \sum_{\substack{\mathfrak{p}^e | (n-r_1) \\ N_P(\mathfrak{p}) \geq x^{1+\eta}}} \log N_P(\mathfrak{p}) \geq \delta_0 \# \mathcal{A} \log x - (3\eta + o(1)) x \log x.$$

In particular, if $\#\mathcal{A} \gg x$ then choosing $\eta = \delta_0 \#\mathcal{A}/(4x)$ shows that the left hand side is $\gg x \log x$. Thus it suffices to show

$$\#\Big\{ n \in [x, 2x] : \prod_{\substack{\mathfrak{p}^e | (n-r_1) \\ N_P(\mathfrak{p}) \leq x}} N_P(\mathfrak{p}) \geq x^{1+\delta_0} \Big\} \gg x.$$

Step 2: Reduction to values of a polynomial with convenient factorisation.

By concentrating on multiples of friable principle ideals $\mathfrak{J} = (a_0 + a_1 r_1 + a_2 r_1^2 + a_3 r_1^3)$ of norm $\asymp x^{1+\delta_0}$, where r_1 is a root of P, we find it suffices to show there is some dense set $\mathcal{A} \subset \mathbb{Z}^4 \cap [1, x^{(1+\delta_0)/4}]$ such that

$$\sum_{(a_0,a_1,a_2,a_3) \in \mathcal{A}} \sum_{\substack{n \in [x,2x] \\ (a_0 + a_1 r_1 + a_2 r_1^2 + a_3 r_1^3) | (n - r_1)}} 1 \gg x.$$

The condition $(a_0+a_1r_1+a_2r_1^2+a_3r_1^3)|(n-r_1)$ is equivalent to a congruence condition $n \equiv k_{\mathbf{a}} \pmod{N_P(a_0+a_1r_1+a_2r_1^2+a_3r_1^3)}$, and so by completion of sums and swapping the order of summation, it suffices to obtain a power-saving in the exponential sums (for small integers $h \neq 0$ and with the standard notation $\mathrm{e}(t) = \exp(2i\pi t)$)

$$\sum_{a_0,a_1,a_2,a_3 \in \mathcal{A}} \mathrm{e}\Big(\frac{h k_{a_0,a_1,a_2,a_3}}{N_P(a_0 + a_1 r_1 + a_2 r_1^2 + a_3 r_1^3)} \Big).$$

This is complicated by the fact that the variables a_0, a_1, a_2, a_3 appear in both the numerator and denominator. However, for quartic P we find that there are polynomials $B_{14}(a_0, a_1, a_2, a_3), B_{13}(a_0, a_1, a_2, a_3)$ and $q(a_1, a_2, a_3)$ with no common factor such that

$$\mathrm{e}\Big(\frac{h k_{a_0,a_1,a_2,a_3}}{N_P(a_0 + a_1 r_1 + a_2 r_2 + a_3 r_3)} \Big) \approx \mathrm{e}\Big(\frac{h B_{13}(a_0, a_1, a_2, a_3) \overline{B_{14}(a_0, a_1, a_2, a_3)}}{q(a_1, a_2, a_3)} \Big),$$

and now the denominator is independent of a_0. We wish to obtain a power-saving estimate for the sum over a_0, but this is complicated by the fact that the modulus of the expression $q(a_1, a_2, a_3) \asymp x^{6(1+\delta_0)/4}$ is much larger than the length $x^{(1+\delta_0)/4}$ of summation of a_0. To estimate such short exponential sums, we can use the q-analogue of Van der Corput's method provided the modulus $q(a_1, a_2, a_3)$ consists only of small prime factors.

Thus our task has reduced to showing that for a positive proportion of integers $a_1, a_2, a_3 \in [1, x^{(1+\delta_0)/4}]$ we can ensure that the polynomial

$q(a_1, a_2, a_3)$ has a convenient prime factorisation. Specifically, we will require that

$$q(a_1, a_2, a_3) = d_0 d_1 \cdots d_r \tag{1.1}$$

where $d_0 < x^{2-\varepsilon}$, $\max(d_1, \ldots, d_r) \leq x^{1-\varepsilon}$, $\min(d_0, \ldots, d_r) \geq x^{\varepsilon}$ for some fixed $\varepsilon > 0$.

Step 3: Counting factorisations of incomplete norm forms

So far we have followed a similar approach to the works [4, 1]. If the Galois group of P is the Klein group, then it turns out that the polynomial $q(a_1, a_2, a_3)$ is the product of three quadratic polynomials. By considering the distribution in suitable residue classes one can then guarantee that each quadratic has a suitable factor, and so $q(a_1, a_2, a_3)$ then has a suitable prime factorisation.

When the Galois group of P is C_4 or D_4, it turns out that $q(a_1, a_2, a_3) = q_1(a_1, a_2, a_3)q_2(a_1, a_2, a_3)$ is the product of a quartic polynomial and a quadratic polynomial. Unfortunately the fact that one factor is quartic means that one cannot guarantee a suitable prime factorisation by looking at variables in residue classes to reasonably small moduli. The difficulty here is that $q_1(a_1, a_2, a_3) \approx (\max_i a_i)^4$, so the size of the values considered are very large compared to the size of the variables a_i. Indeed, it is not known that an arbitrary ternary quartic form q_1 takes infinitely many values compatible with the factorisation (1.1).

Fortunately in our problem the form q_1 is not arbitrary, and in fact we can show that q_1 corresponds to an incomplete norm form of a number field. More precisely, we prove that there exist a number field K of degree 4 over $\mathbb{Q}$ depending only on P and some elements $\nu_1, \nu_2, \nu_3 \in K$ such that $q_1(a_1, a_2, a_3) = N_{K/\mathbb{Q}}(\sum_{i=1}^{3} a_i \nu_i)$.

Maynard [14] gave asymptotic formulae for the number of primes represented by incomplete norm forms; that is primes p such that $p = N(a_1 + a_2\omega + \cdots + a_{n-k}\omega^{n-k-1})$ where $a_1, \ldots, a_{n-k}$ are integers, ω is a root of monic and irreducible polynomial $f \in \mathbb{Z}[X]$ of degree $n \geq 4k$ and N is a norm of the corresponding number field. For $k = 1$ and $n = 4$ this result counts values quartic norms in 3 variables with a particular type of prime factorisation. We adapt the methods of [14] to our situation to count representations of the type (1.1). Unfortunately we require various additional technical conditions (such as a localized version of Maynard's estimates where the variables lie in suitable arithmetic progressions), which means that large parts of [14] have to be generalised to our specific situation. Once suitable technical estimates have been obtained, we find (1.1) is satisfied for a positive proportion of a_1, a_2, a_3, as required.

2 Acknowledgements

CD was supported by ANR grant ANR-20-CE91-0006. JM is supported by a Royal Society Wolfson Merit Award, and this project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 851318). Part of this work was conducted while JM was visiting the Institute for Advanced Study in Princeton.

CD and JM would like to thank the anonymous referees for their careful reading of the manuscript and several helpful comments.

3 Initial steps

Following the argument of Heath-Brown sketched as 'step 1' in our outline, we have the following result.

Lemma 3.1. *Let $P \in \mathbb{Z}[X]$ be an irreducible quartic and monic polynomial of degree 4 with root r_1, and let*

$$\mathcal{E}(\delta) := \{X < n \leq 2X : \prod_{\substack{\mathfrak{p}^e | (n-r_1) \\ N_P(\mathfrak{p}) \leq x}} N_P(\mathfrak{p}) \geq X^{1+\delta}\}. \tag{3.1}$$

If $\delta_0, \delta_1 > 0$ are such that for all X large enough in terms of δ_0, δ_1, P we have $|\mathcal{E}(\delta_0)| > \delta_1 X$, then we have for sufficiently large X

$$|\{n \in]X, 2X] : P^+(P(n)) \gg X^{1+\frac{\delta_0\delta_1}{3}}\}| \geq (\delta_1\delta_0^2 + o(1))X.$$

Proof. This is essentially [8, Lemma 2], (or [1, Lemme 4.1]) after noting that $\sum_{p|P(n), p\leq z} \log p \geq \sum_{\mathfrak{p}|(n-r_1), N_P(\mathfrak{p})\leq z} \log N_P(\mathfrak{p})$. □

Thus it suffices to show that $|\mathcal{E}(\delta_0)| \gg X$ for some small absolute constant $\delta_0 > 0$. To do this we will choose a set of ideals $\mathcal{J}$ (the explicit, technical choice is made in Section 6) such that

$$\prod_{\substack{\mathfrak{p}^e | \mathfrak{J} \\ N_P(\mathfrak{p}) \leq X}} N_P(\mathfrak{p}) \geq X^{1+\delta_0} \qquad \forall \mathfrak{J} \in \mathcal{J}. \tag{3.2}$$

Let $\mathcal{J}_2 := \{\mathfrak{J} \in \mathcal{J} : P^-(N_P(\mathfrak{J})) \geq X^{\theta_0}\}$ for some small absolute constant $\theta_0 > 0$. Then we see that for any $n \in [X, 2X]$ there are at most $2^{4\theta_0^{-1}}$ ideals $\mathfrak{J} \in \mathcal{J}_2$ with $\mathfrak{J}|(n - r_1)$, since $(n - r_1)$ can have at most $4\theta^{-1}$ prime ideal factors with norm bigger than X^{θ_0}. We then see that

$$\begin{aligned} |\mathcal{E}(\delta_0)| &\geq |\{X < n \leq 2X : \exists\ \mathfrak{J} \in \mathcal{J}_2 \text{ such that } \mathfrak{J}|(n - r_1)\}| \\ &\geq \frac{\sum_{\mathfrak{J}\in\mathcal{J}_2} |\mathcal{E}_{\mathfrak{J}}|}{\sup_{X\leq n\leq 2X} |\{\mathfrak{J} \in \mathcal{J}_2 : \mathfrak{J}|(n - r)\}|} \\ &\gg \sum_{\substack{\mathfrak{J}\in\mathcal{J} \\ P^-(N_P(\mathfrak{J}))\geq X^{\theta_0}}} |\mathcal{E}_{\mathfrak{J}}|, \end{aligned}$$

where $\mathcal{E}_{\mathfrak{J}} := \{X < n \leq 2X : \mathfrak{J}|(n - r_1)\}$. Every ideal $\mathfrak{J}$ has at most α_0^{-1} representations as $\mathfrak{J} = KL$ for K a prime ideal with $N_P(K) \in [X^{4\alpha_0}, X^{5\alpha_0}]$. Thus we see that

$$|\mathcal{E}(\delta_0)| \gg \sum_{K\in\mathcal{K}} \sum_{\substack{P^-(N_P(L))\geq X^{\theta_0} \\ KL\in\mathcal{J}}} |\mathcal{E}_{KL}|,$$

where

$$\mathcal{K} := \Big\{K \text{ prime ideal, } N_P(K) \in [X^{4\alpha_0}, X^{5\alpha_0}]\Big\}. \tag{3.3}$$

We apply a linear sieve of level $X^{3\theta_0}$ to bound the condition $P^-(N_P(L)) \geq X^{\theta_0}$ from below, giving

$$|\mathcal{E}(\delta_0)| \gg \sum_{K\in\mathcal{K}} \sum_{KL\in\mathcal{J}} \left(\sum_{d|N_P(L)} \lambda_d^- \right) |\mathcal{E}_{KL}|$$

where λ_d^- are the usual Rosser-Iwaniec lower bound linear sieve weights ([12] and [11]) supported on $d < X^{3\theta_0}$ with $p|d \Rightarrow p \leq X^{\theta_0}$. We see that if X is large enough $\mathcal{E}_{\mathfrak{J}}$ has density $\rho_P(N_P(\mathfrak{J}))/N_P(\mathfrak{J})$, where

$$\varrho_P(\mathfrak{I}) := \mathrm{card}\{0 \leq n < N_P(\mathfrak{I}) : n \equiv r_1 \pmod{\mathfrak{I}}\}. \tag{3.4}$$

With this in mind, we define the error $R_{\mathfrak{J}}$ in the approximation by

$$R_{\mathfrak{J}} := |\mathcal{E}_{\mathfrak{J}}| - X \frac{\varrho_P(N_P(\mathfrak{J}))}{N_P(\mathfrak{J})}. \tag{3.5}$$

Thus

$$|\mathcal{E}_1| \gg XS_0 + S_1,$$

where

$$\begin{aligned} S_0 &:= \sum_{K\in\mathcal{K}} \sum_{KL\in\mathcal{J}(K)} \left(\sum_{d|N_P(L)} \lambda_d^- \right) \frac{\varrho_P(KL)}{N_P(KL)}, \\ S_1 &:= \sum_{K\in\mathcal{K}} \sum_{KL\in\mathcal{J}(K)} \left(\sum_{d|N_P(L)} \lambda_d^- \right) R_{KL}. \end{aligned} \tag{3.6}$$

To obtain Theorem 1.1 we see it suffices to prove the following two key propositions.

Proposition 3.2 (Estimate for S_0)**.** *Let θ_0 be sufficiently small, and $\mathcal{J}$ be the set of ideals described in Section 6. Then we have*

$$S_0 \gg 1.$$

Proposition 3.3 (Estimate for S_1)**.** *Let θ_0 be sufficiently small, and $\mathcal{J}$ be the set of ideals described in Section 6. Then we have*

$$S_1 = o(X).$$

Together these propositions rely heavily on our key technical result, Theorem 4.1. Section 7 is devoted to establishing Proposition 3.3, which uses the fact that $\mathcal{J}$ is a set of ideals with small prime factors to bound the relevant exponential sums. Section 8 is devoted to establishing Proposition 3.2 assuming Theorem 4.1. The rest of the paper is then devoted to establishing Theorem 4.1, which asserts that $\mathcal{J}$ is a set of nonzero density.

4 Localised divisors of values of incomplete norm forms

As described in the outline, the key to the proof of Theorem 1.1 is to show that for a positive proportion of a_1, a_2, a_3 (in a box like $[A, 2A]^3$)

an auxiliary polynomial $q(a_1, a_2, a_3) = q_1(a_1, a_2, a_3)q_2(a_1, a_2, a_3)$ takes values where $P^+(q_2(a_1, a_2, a_3)) < A^{2-\epsilon}$ and $P^+(q_1(a_1, a_2, a_3)) < A^{1-\epsilon}$. The term q_2 will be a quadratic form, and so $P^+(q_2(a_1, a_2, a_3)) < A^{2-\epsilon}$ if $p|q_2(a_1, a_2, a_3)$ for some $p \in [A^{2\epsilon}, A^{3\epsilon}]$, which occurs if a_1, a_2, a_3 lie in suitable residue classes $\pmod p$. Thus it suffices to show that there are the expected number of (a_1, a_2, a_3) such that $P^+(q_1(a_1, a_2, a_3)) < A^{1-\epsilon}$ and (a_1, a_2, a_3) lies in a suitable residue class modulo p on average over $p \in [A^{2\epsilon}, A^{3\epsilon}]$. Since q_1 will be an incomplete norm form for a quartic extension, we see that we are therefore counting friable values of an incomplete norm form (with some additional congruence constraints). The aim of this section is to introduce the notation to state Theorem 4.1, and then to explain how this technical statement relates to our specific problem by giving a suitable asymptotic for such friable values of auxiliary forms.

Let K be a quartic extension of $\mathbb{Q}$ with a $\mathbb{Z}$-basis $\{\nu_1, \nu_2, \nu_3, \nu_4\}$ for $\mathcal{O}_K$ such that $\nu_1 = 1$ and $K = \mathbb{Q}(\nu_2)$. Given a large value X, we wish to count the number of (a_1, a_2, a_3) in a small box such that $N_{K/\mathbb{Q}}(a_1\nu_1+a_2\nu_2+a_3\nu_3)$ has only small prime factors, and such that an auxiliary quadratic form $f(a_1, a_2, a_3)$ is a multiple of some fairly small $p \in [X^\tau, X^{\tau'}]$.

With this in mind, we consider the box $\mathcal{X}$ given by

$$\mathcal{X} := \prod_{i=1}^{3} [X_i, X_i(1 + \eta_1)[, \tag{4.1}$$

where $\eta_1 \in \mathbb{R}$ and $X_1, X_2, X_3 \in \mathbb{Z}$ are parameters satisfying

$$\eta_1 := (\log X)^{-100}, \tag{4.2}$$

$$X_1, X_2, X_3 \in [\eta_1 X, X], \tag{4.3}$$

$$N_{K/\mathbb{Q}}(X_1\nu_1 + X_2\nu_2 + X_3\nu_3) \geq \eta_1^{1/10} \max_i(X_i^4). \tag{4.4}$$

We are then interested in the sets

$$\begin{aligned} \mathcal{A} &:= \{(a_1, a_2, a_3) \in \mathbb{Z}^3 \cap \mathcal{X}\}, \\ \mathcal{A}(\mathbf{u}_0, m, p) &:= \{(a_1, a_2, a_3) \in \mathcal{A} : \mathbf{a} \equiv \mathbf{u}_0 \pmod m,\ p|f(a_1, a_2, a_3)\}, \\ \mathcal{A}_d(\mathbf{u}_0, m, p) &:= \{(a_1, a_2, a_3) \in \mathcal{A}(\mathbf{u}_0, m, p) : d|N_{K/\mathbb{Q}}(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)\}. \end{aligned} \tag{4.5}$$

Since we wish to count points when $N_{K/\mathbb{Q}}(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$ has small prime factors, we will count how often $d|N_{K/\mathbb{Q}}(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$ for an integer d of the form $d = q_1 \cdots q_\ell$ where each q_i is a prime localised to lie in an interval $[X^{\theta_j}, X^{\theta'_j}]$ for some fixed constants θ_i, θ'_i. We will require θ_j, θ'_j satisfy the following conditions.

- (Non-trivial intervals counting primes which are not too large)

$$\delta < \theta_i < \theta'_i < 1 - \delta \quad \forall\, 1 \leq i \leq \ell. \tag{4.6}$$

- (q_{1j} are distinct primes)

$$[\theta_i, \theta'_i] \cap [\theta_j, \theta'_j] = \emptyset \quad \forall\, 1 \leq i < j \leq \ell. \tag{4.7}$$

- ($\prod_{j=1}^{\ell} q_{1j}$ is not too large to divide N)

$$\sum_{i=1}^{\ell} \theta_i' < 4 - \delta. \tag{4.8}$$

- (Impossible for q_{1j}^2 to divide $N(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$)

$$\theta_j + \sum_{i=1}^{\ell} \theta_i > 4 + \delta \quad \forall\, 1 \le j \le \ell. \tag{4.9}$$

- (The product of the first q_{1i} is of controlled size) There exists $\ell' \in [1, \ell - 1]$ such that

$$1 + \delta < \sum_{i=1}^{\ell'} \theta_i < \sum_{i=1}^{\ell'} \theta_i' < 2 - \delta. \tag{4.10}$$

The conditions (4.6)-(4.9) are minor constraints to avoid some technical issues and to ensure that we expect that $d|N_{K/\mathbb{Q}}(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$ can actually occur; these constraints could be significantly weakened at the cost of some effort. The condition (4.10) is a technical condition which is vital for our method.

To avoid some further technical issues we will focus on the case when the quadratic form f is irreducible but not geometrically irreducible, and so the condition $f(a_1, a_2, a_3)$ becomes a product of two linear factors over $\mathbb{F}_p$ after restricting p to an arithmetic progression. Again, this setup could be relaxed at the cost of additional technical effort, but is the situation that arises when dealing with Theorem 1.1. It would be also interesting to have a more general result for incomplete norm forms and ternary forms f.

Finally we are in a position to state our counting result.

Theorem 4.1 (localised factors of values of incomplete norm forms)**.** *Let $f(X_1, X_2, X_3) \in \mathbb{Z}[X_1, X_2, X_3]$ be a homogeneous quadratic polynomial which splits into two distinct linear factors*

$$f(X_1, X_2, X_3) = L_1(X_1, X_2, X_3)L_2(X_1, X_2, X_3)$$

over a suitable extension of $\mathbb{Q}$. Let $D_f \in \mathbb{N}$ such that if $p \equiv 1 \pmod{D_f}$ then the $\mathbb{F}_p$-reduction of the two linear forms $L_1(X_1, X_2, X_3)$, $L_2(X_1, X_2, X_3)$ are in $\mathbb{F}_p[X_1, X_2, X_3]$.

Let K be a quartic extension of $\mathbb{Q}$ with $\{\nu_1, \nu_2, \nu_3, \nu_4\}$ being a $\mathbb{Z}$-basis for $\mathcal{O}_K$ such that $\nu_1 = 1$ and $K = \mathbb{Q}(\nu_2)$. Let X_1, X_2, X_3 satisfy (4.3) *and* (4.4)*. Let $\ell, \ell' \in \mathbb{N}$ such that $1 \le \ell' < \ell$ and $\theta_1, \theta_1', \dots, \theta_\ell, \theta_\ell'$ be reals satisfying* (4.6)-(4.10)*. Let $0 < \tau < \tau'$ satisfy*

$$\tau' < \min\Big(\frac{4 - 2\theta_1' - \ldots - 2\theta_{\ell'}'}{100}, \frac{\theta_1 + \cdots + \theta_{\ell'} - 1}{100}\Big). \tag{4.11}$$

Let $\mathcal{A}_d(\mathbf{u}, m, p)$ be as given by (4.5)*.*

Then for any choice of $\mathbf{u}_0 \pmod m$ *and* $K > 0$*, we have*

$$\sum_{\substack{p\in[X^\tau,X^{\tau'}]\\ p\equiv 1 \pmod{D_f}}} \sum_{\substack{q_1,\dots,q_\ell \text{ prime}\\ q_j\in[X^{\theta_j},X^{\theta_j'}]\,\forall 1\le j\le \ell}} |\mathcal{A}_{q_1\cdots q_\ell}(\mathbf{u}_0,m,p)|$$

$$= \eta_1^3 X_1X_2X_3 \frac{2\log(\frac{\tau'}{\tau})}{m^3\varphi(D_f)} \prod_{i=1}^{\ell} \log\Big(\frac{\theta_i'}{\theta_i}\Big) + O\Big(\frac{X_1X_2X_3}{(\log X)^K}\Big).$$

The implied constant depends on f, K, A, δ *and the* $\nu_i, \theta_i, \theta_i'$ *only.*

At first sight Theorem 4.1 looks like a Type I estimate since we are counting a_1, a_2, a_3 such that $N_{K/\mathbb{Q}}(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$ is a multiple of $q_1 \dots q_\ell$. However, since there are typically no values of a_1, a_2, a_3 such that this occurs (it is only a thin set of q_j's when there is a solution), we instead are required to view this as a Type II estimate counting $N_{K/\mathbb{Q}}(a_1\nu_1 + a_2\nu_2 + a_3\nu_3) = m_1m_2$ where $m_1 = q_1 \cdots q_{\ell'}$ is a product of ℓ' primes of constrained size and $m_2 = q_{\ell'+1} \cdots q_\ell r$ is the product of $\ell - \ell'$ primes and some other integer r.

4.1 Application to Theorem 1.1

If P is an irreducible monic quartic polynomial, then (generalising previous works) there is an auxilliary sextic form $q(a_1, a_2, a_3)$ such that provided q takes suitably friable values a positive proportion of the time, then we can use exponential sum methods to establish Theorem 1.1. If P has Galois group C_4 or D_4, then it turns out that the roots r_1, r_2, r_3, r_4 of P can be ordered such that $r_1r_2 + r_3r_4 \in \mathbb{Z}$ (c.f. Lemma 5.9), and that q factorises as q_1q_2 for a quartic form q_1 and a quadratic form q_2 (c.f. Lemma 5.10) which split completely in the splitting field of P.

Moreover, we find that for the quartic extension $K := \mathbb{Q}(r_1 + r_3)$ of $\mathbb{Q}$, the form q_1 satisfies

$$q_1(a_1, a_2, a_3) = \pm N_{K/\mathbb{Q}}(a_1 + a_2(r_1 + r_3) + a_3(r_1^2 + r_1r_3 + r_3^2)),$$

and so takes the shape of an incomplete norm form (c.f. Proposition 5.11).

The quadratic q_2 takes the form

$$\begin{aligned} q_2(a_1, a_2, a_3) = [a_1 + (r_1 + r_2)a_2 + (r_1^2 + r_1r_2 + r_2^2)a_3] \\ \times [a_1 + (r_3 + r_4)a_2 + (r_3^2 + r_3r_4 + r_4^2)a_3]. \end{aligned} \tag{4.12}$$

Since the two polynomials $P_1(X) := (X - (r_1 + r_2))(X - (r_3 + r_4))$ and $P_2(X) := (X - (r_1^2 + r_1r_2 + r_2^2))(X - (r_3^2 + r_3r_4 + r_4^2))$ are in $\mathbb{Z}[X]$[2], $r_1 + r_2$ and $r_1^2 + r_1r_2 + r_2^2$ are of degree at most 2 over $\mathbb{Q}$. Let Δ_1 and Δ_2 be the discriminant of these two polynomials and

$$D_{q_2} := \begin{cases} [8, \Delta_1, \Delta_2] & \text{if } \Delta_1\Delta_2 \neq 0, \\ [8, \Delta_1 + \Delta_2] & \text{otherwise.} \end{cases} \tag{4.13}$$

[2]We can check that $P_1(X) + (r_1r_2 + r_3r_4)$ and $P_2(X) + (r_1r_2 + r_3r_4)(X + \sum_{i<j} r_ir_j)$ have coefficients which are symmetric integer polynomials in the r_i, and so are in $\mathbb{Z}[X]$. Since $r_1r_2 + r_3r_4 \in \mathbb{Z}$, it follows that $P_1(X)$ and $P_2(X)$ are in $\mathbb{Z}[X]$.

Since P is irreducible of degree 4, we don't have $\Delta_1 = \Delta_2 = 0$.[3] If $p \equiv 1 \pmod{D_{q_2}}$ and $\Delta_1\Delta_2 \neq 0$, then $(\Delta_1/p) = (\Delta_2/p) = 1$ where (n/p) is the Legendre symbol. Thus the polynomials P_1 and P_2 modulo p factor into products of two degree one polynomials. The linear factors of q_2 in (4.12) have their coefficients in $\mathbb{F}_p$. We also verify that it is still the case when $p \equiv 1 \pmod{D_{q_2}}$ and $\Delta_1\Delta_2 = 0$.

Then $N_{K/\mathbb{Q}}(\sum_{i=1}^4 a_i\nu_i)$ is a quartic form in the integer variables a_1, a_2, a_3, a_4, and we have for all $a_1, a_2, a_3, a_4 \in \mathbb{Z}$

$$N_{K/\mathbb{Q}}\Big(\sum_{i=1}^4 a_i\nu_i\Big) = \prod_{i=1}^4 \Big(\sum_{j=1}^4 a_j\sigma_i(\nu_j)\Big),$$

where $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ are the different embeddings of $K/\mathbb{Q}$.

Given an irreducible quartic polynomial $P \in \mathbb{Z}[X]$ with Galois group C_4 or D_4 it is the case (see Lemma 5.9) that the distinct roots r_1, r_2, r_3, r_4 of P can be ordered such that $r_1r_2 + r_3r_4 \in \mathbb{Q}$. We are interested in the auxiliary polynomial q_2 (see (5.25)), given by

To ensure that $q_1(a_1, a_2, a_3) = N_{K/\mathbb{Q}}(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$ is composed only of suitably small prime factors, we will look for a_1, a_2, a_3 such that

$$q_{11}q_{12}q_{13}q_{14}\dots q_{1\ell} | N_{K/\mathbb{Q}}(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$$

for some suitable primes $q_{11}, q_{12}, q_{13}, q_{14}, \dots, q_{1\ell} < X^{1-\delta}$ with $\prod_{j=1}^{\ell} q_{1j} > X^{3+\delta}$. In the application to Theorem 1.1, we will only need the case $\ell = 6$, but the proof in this particular case is exactly the same as in the general case.

5 Algebraic properties of auxilliary polynomials

5.1 Ideals

Let r_1 be a root of P. We define for any ideal $\mathfrak{I}$ of $\mathbb{Z}[r_1]$ the function

$$\varrho_P(\mathfrak{I}) = \mathrm{card}\{0 \leq n < N_P(\mathfrak{I}) : n \equiv r_1 \pmod{\mathfrak{I}}\},$$

where $N_P = N_{\mathbb{Q}(r_1)/\mathbb{Q}}$ is the norm on $\mathbb{Q}(r_1)$. If $\mathfrak{I}$ is principal, $\mathfrak{I} = (\alpha)$, we will write simply $\varrho_P(\alpha)$ in place of $\varrho_P((\alpha))$.

Lemma 5.1. *Let $\mathfrak{I}$ be an ideal of $\mathcal{O}_{\mathbb{Q}(r_1)}$ such that $(N_P(\mathfrak{I}), \mathrm{Disc}\,(P)) = 1$. If the equation $n \equiv r_1 \pmod{\mathfrak{I}}$ has a solution with $n \in \mathbb{Z}$ then $\mathfrak{I}$ is a product of prime ideals whose norm is a prime number. Furthermore $\mathfrak{I}$ can't be divisible by two different prime ideals with the same norm. Conversely, if $\mathfrak{I}$ satisfies these different conditions then this congruence admits some solutions and $\varrho_P(\mathfrak{I}) = 1$. Finally if $\mathfrak{I}$ is an ideal such that $\varrho_P(\mathfrak{I}) = 1$ then for $m \in \mathbb{Z}$, $\mathfrak{I}|m \Leftrightarrow N_P(\mathfrak{I})|m$.*

Proof. This is [1, Lemma 3.1]. The particular case $P = \Phi_{12}$ is handled in [4, Lemma 3.1]. □

[3] If $\Delta_1 = \Delta_2 = 0$ then the roots of $r_1 + r_2$ and r_1r_2 are in $\mathbb{Q}$. This contradicts the fact that $[\mathbb{Q}(r_1) : \mathbb{Q}] = 4$.

5.2 The roots of P modulo m

In this part only we suppose that $P(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in \mathbb{Z}[X]$ is monic, irreducible of degree n. In our problem, the degree of P is 4 but the argument of this part is valid for all irreducible and monic polynomials and might be used in other contexts. Throughout the rest of the paper we fix a root r_1 of P.

For $\alpha \in \mathbb{Z}[r_1]$, we write $\alpha = a_0 + a_1 r_1 + a_2 r_1^2 + a_3 r_1^3 + \cdots + a_{n-1} r_1^{n-1}$. Let $m_\alpha : \mathbb{Q}(r_1) \to \mathbb{Q}(r_1)$ be the multiplication-by-α map: $m_\alpha(x) = \alpha x$. Let M_α be the matrix of m_α with respect to the basis $\{1, r_1, r_1^2, r_1^3, \ldots, r_1^{n-1}\}$ and $N_P(\alpha) = N_{\mathbb{Q}(r_1)/\mathbb{Q}}(\alpha)$ its determinant. For $P(X) = X^4 + 2$ the corresponding matrix is

$$\begin{pmatrix} a_0 & -2a_3 & -2a_2 & -2a_1 \\ a_1 & a_0 & -2a_3 & -2a_2 \\ a_2 & a_1 & a_0 & -2a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix}.$$

More generally since $r_1^n = -c_0 - c_1 r_1 - \cdots - c_{n-1} r_1^{n-1}$, we have

$$M_\alpha = \begin{pmatrix} a_0 & -c_0 a_{n-1} & * & \cdots & * \\ a_1 & a_0 - c_1 a_{n-1} & * & \cdots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_{n-2} - c_{n-1} a_{n-1} & * & \cdots & * \end{pmatrix}. \tag{5.1}$$

In this section we prove results analogous to [4, Lemma 4.1] or [1, Lemma 3.2]. As in these two papers, we let $B_{ij} = B_{ij}(\alpha)$ be the cofactor formed by taking the determinant of the $(n-1) \times (n-1)$ matrix formed by removing line i and column j from M_α and multiply it by $(-1)^{i+j}$. If $\alpha = a_0 + a_1 r_1 + \cdots + a_{n-1} r_1^{n-1}$ then B_{ij} is a polynomial in the a_i. By an abuse of notation we will sometimes use B_{ij} to refer to this polynomial, and sometimes the value attained at a particular point $(a_0, a_1, \ldots, a_{n-1})$. The intended usage should be clear from the context.

Lemma 5.2. *Let $\alpha = a_0 + a_1 r_1 + \cdots + a_{n-1} r_1^{n-1}$, with $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ be such that $(N_P(\alpha), B_{1n}\mathrm{Disc}(P)) = 1$. Then there exists an integer k_α, with $0 \leq k_\alpha < N_P(\alpha)$ such that we have*

$$n - r_1 \equiv 0 \pmod{(\alpha)} \Leftrightarrow n \equiv k_\alpha \pmod{N_P(\alpha)}.$$

This integer k_α satisfies the congruence

$$k_\alpha \equiv B_{2n}\overline{B_{1n}} \pmod{N_P(\alpha)}.$$

Furthermore, if $\mathfrak{J}$ is an ideal of $\mathbb{Z}[r_1]$ containing a principal ideal (α) with α as above then there exists a unique $k_\mathfrak{J}$ with $0 \leq k_\mathfrak{J} < N_P(\mathfrak{J})$ and

$$n - r_1 \in \mathfrak{J} \Leftrightarrow n \equiv k_\mathfrak{J} \pmod{N_P(\mathfrak{J})}.$$

Proof. The starting point is the following trivial observation: $\alpha r_1^j \in (\alpha)$ for all $j = 0, 1, 2, 3, \ldots, n-1$. Let $(m_{i,j})_{1 \leq i,j \leq n}$ be the coefficients of M_α. We obtain the equations

$$m_{1,j} + m_{2,j} r_1 + \cdots + m_{n,j} r_1^{n-1} = 0 \pmod{(\alpha)}, \forall\, 1 \leq j \leq n.$$

This system can be represented as

$$\begin{pmatrix} m_{2,1} & m_{3,1} & \dots & m_{n,1} \\ m_{2,2} & m_{3,2} & \dots & m_{n,2} \\ \vdots & \vdots & \dots & \vdots \\ m_{2,n} & m_{3,n} & \dots & m_{n,n} \end{pmatrix} \begin{pmatrix} r_1 \\ r_1^2 \\ \vdots \\ r_1^{n-1} \end{pmatrix} = \begin{pmatrix} -m_{1,1} \\ -m_{1,2} \\ \vdots \\ -m_{1,n} \end{pmatrix} \pmod{(\alpha)} \quad (5.2)$$

If we remove the i-th line in this system and apply Cramer's rule, we find

$$r_1 \det \begin{pmatrix} m_{2,1} & m_{3,1} & \dots & m_{n,1} \\ \vdots & \vdots & \dots & \vdots \\ m_{2,i-1} & m_{3,i-1} & \dots & m_{n,i-1} \\ m_{2,i+1} & m_{3,i+1} & \dots & m_{n,i+1} \\ \vdots & \vdots & \dots & \vdots \\ m_{2,n-1} & m_{3,n-1} & \dots & m_{n,n-1} \\ m_{2,n} & m_{3,n} & \dots & m_{n,n} \end{pmatrix} = \det \begin{pmatrix} -m_{1,1} & m_{3,1} & \dots & m_{n,1} \\ \vdots & \vdots & \dots & \vdots \\ -m_{1,i-1} & m_{3,i-1} & \dots & m_{n,i-1} \\ -m_{1,i+1} & m_{3,i+1} & \dots & m_{n,i+1} \\ \vdots & \vdots & \dots & \vdots \\ -m_{1,n-1} & m_{3,n-1} & \dots & m_{n,n-1} \\ -m_{1,n} & m_{3,n} & \dots & m_{n,n} \end{pmatrix} \pmod{(\alpha)}. \quad (5.3)$$

The transpose of the matrix on the left is the submatrix of M_α obtained by removing the first line and the i^{th} column. The matrix on the right is the submatrix of M_α obtained by removing the second line and the i^{th} column and by multiplying all elements of the first column by -1.

We recall that the B_{ij}, $1 \leq i, j \leq n$, are the cofactors of M_α, so that

$$M_\alpha^{-1} = \frac{1}{N_P(\alpha)} \begin{pmatrix} B_{11} & B_{21} & \dots & B_{n1} \\ B_{12} & B_{22} & \dots & B_{n2} \\ \vdots & \vdots & \dots & \vdots \\ B_{1n} & B_{2n} & \dots & B_{nn} \end{pmatrix}. \quad (5.4)$$

With this notation, (5.3) becomes

$$(-1)^{i+1} B_{1i} r_1 \equiv -(-1)^{i+2} B_{2i} \pmod{(\alpha)}.$$

In particular, this gives

$$B_{1i} r_1 \equiv B_{2i} \pmod{(\alpha)}. \quad (5.5)$$

By Lemma 5.1 (and the assumption $(N(\alpha), \mathrm{Disc}\,(P)) = 1$), if an integer is congruent to 0 (mod (α)) then it is divisible by $N_P(\alpha)$. Therefore considering $i = n$ now gives the claim of the first part of Lemma 5.2.

For the second part when $J|(\alpha)$, thus it suffices to take $k_J \in [0, N_P(J)]$ such that $k_J \equiv k_\alpha \pmod{N_P(J)}$. The claim now follows from (5.5). □

We end this subsection by observing some connection between the cofactors B_{1i} and B_{2j} with $1 \leq i, j \leq n$. Since $(m_\alpha)^{-1} = m_{\alpha^{-1}}$, we have

$$\alpha^{-1} = \frac{1}{N_P(\alpha)} (B_{11} + B_{12} r_1 + \dots + B_{1n} r_1^{n-1}),$$

and the columns of M_α^{-1} satisfy the same relations (5.1) as the one in M_α. By the relations (5.1) for $M_{\alpha^{-1}}$, we see that

$$\begin{pmatrix} B_{21} \\ B_{22} \\ \vdots \\ B_{2(n-1)} \\ B_{2n} \end{pmatrix} = \begin{pmatrix} -c_0 B_{1n} \\ B_{11} - c_1 B_{1n} \\ \vdots \\ B_{1(n-2)} - c_{n-2} B_{1n} \\ B_{1(n-1)} - c_{n-1} B_{1n} \end{pmatrix}. \tag{5.6}$$

In particular the last line implies that

$$B_{2n} = B_{1(n-1)} - c_{n-1} B_{1n}. \tag{5.7}$$

For $n = 4$, and $c_3 = 0$, we recover the formula $B_{14} r_1 \equiv B_{24} = B_{13} \pmod{(\alpha)}$, proved in [1] and in [4].

5.3 Elimination of a_0

The aim of this subsection is to approximate the fraction $k_\mathfrak{J}/N_P(\alpha)$ by a fraction whose denominator depends only on a_1, a_2, a_3. Now and for the rest of this paper we restrict our attention to P having degree 4. In this subsection we prove the analogue of [1, Lemma 3.3], or [4, Lemma 6.2]. A natural way to proceed is to work with some resultants of the different forms defined previously.

Lemma 5.3. *There is a homogeneous polynomial $q_3 = q_3(a_1, a_2, a_3)$ in a_1, a_2, a_3 such that*

$$B_{24} B_{13} - B_{14} B_{23} = q_3 N_P(\alpha). \tag{5.8}$$

Proof. We note that the argument giving (5.5) holds for any $\alpha \neq 0$. Applying this with $i = 3, 4$, $n = 4$ we find

$$r_1 B_{13} B_{24} \equiv r_1 B_{14} B_{23} \pmod{N_P(\alpha)}.$$

Since this holds for all a_0, a_1, a_2, a_3, we deduce that there exists a form $q_3 = q_3(a_0, a_1, a_2, a_3)$ such that whenever $(N_P(\alpha), \mathrm{Disc}\,(P)) = 1$ we have[4]

$$B_{24} B_{13} - B_{14} B_{23} = q_3 N_P(\alpha). \tag{5.9}$$

Since both sides are polynomials, this must actually hold for all α (including $(N_P(\alpha), \mathrm{Disc}\,(P)) \neq 1$.) Therefore we just need to show that q_3 actually doesn't depend on a_0. $N_P(\alpha)$ has degree 4 in a_0 while the polynomials B_{ij}, $i \neq j$ are of degree 2 in a_0, and so by equating the coefficients of a_0^4 we see that q_3 must not depend on a_0. □

Remark. *One can explicitly compute q_3 in terms of the coefficients c_i of P; it is given by*

$$q_3(a_1, a_2, a_3) = a_2^2 - a_1 a_3 - c_3 a_2 a_3 + c_2 a_3^2. \tag{5.10}$$

When $c_3 = 0$ this coincides with the form $-q_4$ given in [1, equation (2.7)].

[4] In [1] and [4] this form corresponds to the form q_4.

Remark. *Lemma 5.3 makes important use of the fact that P is a quartic polynomial. For polynomials P of degree $d > 4$ the form q_3 would have degree $d-4$ in a_0, and so would be no longer independent of a_0.*

Following the notation of [1] and [4], we write Resultant$(P_1, P_2; x)$ for the resultant of the polynomials P_1, P_2 with respect to the variable x. We will be interested by the two following resultants

$$\begin{aligned} R &:= R(a_1, a_2, a_3) = \text{Resultant}(B_{14}, N_P(\alpha); a_0) \\ R_0 &:= R_0(a_1, a_2, a_3) = \text{Resultant}(B_{13}, B_{14}; a_0) \end{aligned} \tag{5.11}$$

Lemma 5.4. *With the previous notation we have*

$$q_3^2 R = R_0^2.$$

Proof. The proof of Lemma 5.4 is the same as that of [1, Lemma 2.1]. Since B_{14} is of degree 2 in a_0, we have

$$q_3^2 R = \text{Resultant}(B_{14}, q_3 N_P(\alpha); a_0) = \text{Resultant}(B_{14}, B_{24}B_{13} - B_{14}B_{23}; a_0).$$

But $B_{24} = B_{13} - c_3 B_{14}$ and B_{13} is also of degree 2 in a_0. We deduce that

$$q_3^2 R = \text{Resultant}(B_{14}, B_{13}^2; a_0) = R_0^2.$$

This ends the proof of Lemma 5.4. □

We see that the polynomial q_3 divides R_0, and so we can write

$$R_0 = q q_3 \tag{5.12}$$

for some homogeneous polynomial $q = q(a_1, a_2, a_3)$. Moreover, since R_0 is the resultant of B_{13} and B_{14}, there are two polynomials U and $V \in \mathbb{Z}[a_0, a_1, a_2, a_3]$ such that

$$U B_{13} + V B_{14} = q q_3. \tag{5.13}$$

We are now ready to state the main result of this section. It is analogous to [4, Lemma 6.2] or [1, Lemma 3.3].

Lemma 5.5. *Suppose a_0, a_1, a_2, a_3 are such that $(B_{14}(a_0, a_1, a_2, a_3), q(a_1, a_2, a_3)) = 1$. Then $(N_P(\alpha), B_{14}(a_0, a_1, a_2, a_3)) = 1$ and for $h \in \mathbb{Z}$ we have*

$$\mathrm{e}\Big(\frac{-hk_\alpha}{N_P(\alpha)}\Big) = \mathrm{e}\Big(\frac{-hU(a_0, a_1, a_2, a_3)\overline{B_{14}(a_0, a_1, a_2, a_3)}}{q(a_1, a_2, a_3)} + hR(a_0, a_1, a_2, a_3)\Big),$$

where $U = U(a_0, a_1, a_2, a_3)$ is defined by (5.13) *and R is given by*

$$R(a_0, a_1, a_2, a_3) = \frac{U}{qB_{14}} - \frac{B_{24}}{N_P(\alpha)B_{14}}.$$

Proof. To simplify notation, for the proof let $q, q_3, U, B_{14}, B_{14}, B_{23}, B_{24}, N_P(\alpha)$ denote the values of the polynomials evaluated at a_0, a_1, a_2, a_3.

Since q divides the resultant R defined in (5.11), if q is coprime with B_{14}, we have $(N_P(\alpha), B_{14}) = 1$. By Lemma 5.2,

$$\mathrm{e}\Big(\frac{k_\alpha}{N_P(\alpha)}\Big) = \mathrm{e}\Big(\frac{B_{24}\overline{B_{14}}}{N_P(\alpha)}\Big).$$

We use the Bézout relation

$$\frac{\bar{u}}{v}+\frac{\bar{v}}{u}\equiv\frac{1}{uv}\ (\mathrm{mod}\ 1)\quad \text{for } (u,v)=1, \tag{5.14}$$

and the fact that $(N_P(\alpha),B_{14})=1$. This yields the formula

$$\mathrm{e}\Big(\frac{k_\alpha}{N_P(\alpha)}\Big)=\mathrm{e}\Big(-\frac{B_{24}\overline{N_P(\alpha)}}{B_{14}}+\frac{B_{24}}{B_{14}N_P(\alpha)}\Big). \tag{5.15}$$

Combining (5.7), (5.8) and (5.13), we obtain

$$\begin{aligned}UN_P(\alpha)q_3&=U[B_{13}(B_{13}-c_3B_{14})-B_{14}B_{23}]\\&=U(B_{13}^2-B_{14}(B_{23}+c_3B_{13}))\\&=B_{13}(q_3q-VB_{14})-UB_{14}(B_{23}+c_3B_{13})).\end{aligned}$$

This rearranges to give

$$(UN_P(\alpha)-qB_{13})q_3=B_{14}(-VB_{13}-U(B_{23}+c_3B_{13})).$$

Since q_3 and B_{14} are coprime, we deduce that

$$UN_P(\alpha)-qB_{13}\equiv 0\ (\mathrm{mod}\ B_{14}). \tag{5.16}$$

Since $B_{24}\equiv B_{13}\ (\mathrm{mod}\ B_{14})$, we obtain

$$B_{24}\overline{N_P(\alpha)}\equiv B_{13}\overline{N_P(\alpha)}\ (\mathrm{mod}\ B_{14})\equiv U\bar{q}\ (\mathrm{mod}\ B_{14}).$$

We insert this in (5.15) and apply (5.14) one more time. This gives the desired result. □

5.4 Explicit computations of B_{13}, B_{14}, U, V.

We have used SAGE to explicitly compute the polynomials q, B_{13}, B_{14}, U and V. The cofactors B_{13} and B_{14} are of degree 2 in a_0

$$\begin{aligned}B_{13}=&-a_2a_0^2+\Big(a_1^2+c_3a_1a_2+(-c_3^2+c_2)a_2^2+(-2c_2)a_1a_3\\&\quad+(c_3^3-c_2c_3+c_1)a_2a_3+(-c_2c_3^2+c_2^2+c_1c_3-c_0)a_3^2\Big)a_0\\&+(-c_3)a_1^3+c_3^2a_1^2a_2+(-c_2c_3)a_1a_2^2+(c_1c_3-c_0)a_2^3\\&+(-c_3^3+2c_2c_3)a_1^2a_3+(c_2c_3^2-3c_1c_3+2c_0)a_1a_2a_3\\&+(-c_1c_3^2+2c_0c_3)a_2^2a_3+(-c_2^2c_3+2c_1c_3^2-2c_0c_3)a_1a_3^2\\&+(c_1c_2c_3-c_0c_3^2-c_0c_2)a_2a_3^2+(-c_1^2c_3+c_0c_2c_3+c_0c_1)a_3^3,\end{aligned} \tag{5.17}$$

$$\begin{aligned}B_{14}=&-a_3a_0^2+\Big(2a_1a_2-c_3a_2^2-c_3a_1a_3+c_3^2a_2a_3+(-c_2c_3+2c_1)a_3^2\Big)a_0\\&-a_1^3+c_3a_1^2a_2-c_2a_1a_2^2+c_1a_2^3+(-c_3^2+2c_2)a_1^2a_3+(c_2c_3-3c_1)a_1a_2a_3\\&+(-c_1c_3+c_0)a_2^2a_3+(-c_2^2+2c_1c_3-c_0)a_1a_3^2\\&+(c_1c_2-c_0c_3)a_2a_3^2+(-c_1^2+c_0c_2)a_3^3.\end{aligned} \tag{5.18}$$

The quantities U and V are of degree 1 in a_0. In some step we will need the explicit formula for the coefficient in a_0 in U and in V

$$\begin{aligned}
U =& a_0\Big(-a_1^2a_3^2 + 2a_1a_2^2a_3 - 2c_3a_1a_2a_3^2 + 2c_2a_1a_3^3 - c_3a_2^3a_3 + \\
&\qquad (2c_3^2 - c_2)a_2^2a_3^2 + (-c_3^3 + c_1)a_2a_3^3 + (c_2c_3^2 - c_2^2 - c_1c_3 + c_0)a_3^4\Big) \\
&+ 3a_1^3a_2a_3 - 2c_3a_1^3a_3^2 - 4a_1^2a_2^3 + 4c_3a_1^2a_2^2a_3 \\
&+ (c_3^2 - 6c_2)a_1^2a_2a_3^2 + (-c_3^3 + 3c_2c_3 + 2c_1)a_1^2a_3^3 \\
&+ 4c_3a_1a_2^4 + (-9c_3^2 + 3c_2)a_1a_2^3a_3 + (6c_3^3 + c_2c_3 - 3c_1)a_1a_2^2a_3^2 \\
&+ (-c_3^4 - 5c_2c_3^2 + 3c_2^2 + 2c_1c_3 + c_0)a_1a_2a_3^3 + (c_2c_3^3 + c_1c_3^2 - 4c_1c_2 - c_0c_3)a_1a_3^4 - c_3^2a_2^5 \\
&+ (3c_3^3 - c_2c_3 - c_1)a_2^4a_3 + (-3c_3^4 + 5c_1c_3 - 2c_0)a_2^3a_3^2 \\
&+ (c_3^5 + 3c_2c_3^3 - 2c_2^2c_3 - 7c_1c_3^2 + c_1c_2 + 4c_0c_3)a_2^2a_3^3 \\
&+ (-2c_2c_3^4 + c_2^2c_3^2 + 3c_1c_3^3 + 2c_1c_2c_3 - 2c_0c_3^2 - c_1^2 - 2c_0c_2)a_2a_3^4 \\
&+ (c_2^2c_3^3 - c_2^3c_3 - 3c_1c_2c_3^2 + 2c_1c_2^2 + c_1^2c_3 + 2c_0c_2c_3 - c_0c_1)a_3^5, \quad (5.19)
\end{aligned}$$

$$\begin{aligned}
V =& a_0\Big(a_1^2a_2a_3 - 2a_1a_3^3 + 2c_3a_1a_2^2a_3 - 2c_2a_1a_2a_3^2 + c_3a_2^4 \\
&\qquad + (-2c_3^2 + c_2)a_2^3a_3 + (c_3^3 - c_1)a_2^2a_3^2 + (-c_2c_3^2 + c_2^2 + c_1c_3 - c_0)a_2a_3^3\Big) \\
&- a_1^4a_3 + a_1^3a_2^2 - 2c_3a_1^3a_2a_3 + 4c_2a_1^3a_3^2 + 2c_3a_1^2a_2^3 + (-c_3^2 - 4c_2)a_1^2a_2^2a_3 \\
&+ (-c_3^3 + 5c_2c_3)a_1^2a_2a_3^2 + (2c_2c_3^2 - 6c_2^2 - 2c_1c_3 + 2c_0)a_1^2a_3^3 + (-3c_3^2 + c_2)a_1a_2^4 \\
&+ (6c_3^3 - c_2c_3 - c_1)a_1a_2^3a_3 + (-3c_3^4 - 7c_2c_3^2 + 5c_2^2 + 6c_1c_3 - 5c_0)a_1a_2^2a_3^2 \\
&+ (7c_2c_3^3 - 4c_2^2c_3 - 5c_1c_3^2 + 5c_0c_3)a_1a_2a_3^3 + (-4c_2^2c_3^2 + 4c_3^2 + 4c_1c_2c_3 - 4c_0c_2)a_1a_3^4 \\
&+ (c_3^3 - c_2c_3 + c_1)a_2^5 + (-3c3^4 + 4c_2c_3^2 - c_2^2 - 3c_1c_3 + 2c_0)a_2^4a_3 \\
&+ (3c_3^5 - 3c_2c_3^3 + c_1c_3^2 + c_1c_2 - 2c_0c_3)a_2^3a_3^2 \\
&+ (-c_3^6 - 2c_2c_3^4 + 5c_2^2c_3^2 + 3c_1c_3^3 - 2c_2^3 - 4c_1c_2c_3 - 2c_0c_3^2 + 4c_0c_2)a_2^2a_3^3 \\
&+ (2c_2c_3^5 - 3c_2^2c_3^3 - 2c_1c_3^4 + c_2^3c_3 + c_1c_2c_3^2 + 2c_0c_3^3 + c_1^2c_3 - 2c_0c_2c_3 - c_0c_1)a_2a_3^4 \\
&+ (-c_2^2c_3^4 + 2c_2^3c_3^2 + 2c_1c_2c_3^3 - c_2^4 - 2c_1c_2^2c_3 - c_1^2c_3^2 - 2c_0c_2c_3^2 + 2c_0c_2^2 + 2c_0c_1c_3 - c_0^2)a_3^5. \\
& \qquad (5.20)
\end{aligned}$$

We don't write the expression for q because it would take more than one page and we won't need to know its precise shape during the proof. Let $U = a_0U_1 + U_0$, $V = a_0V_1 + V_0$. Then U_1 satisfies:

$$\begin{aligned}
U_1 &= -a_1^2a_3^2 + 2a_1a_2^2a_3 - 2c_3a_1a_2a_3^2 + 2c_2a_1a_3^3 - c_3a_2^3a_3 + \\
&\qquad (2c_3^2 - c_2)a_2^2a_3^2 + (-c_3^3 + c_1)a_2a_3^3 + (c_2c_3^2 - c_2^2 - c_1c_3 + c_0)a_3^4 \\
&= a_3\Big(-a_1^2a_3 + 2a_1a_2^2 - 2c_3a_1a_2a_3 + 2c_2a_1a_3^2 - c_3a_2^3 + \\
&\qquad (2c_3^2 - c_2)a_2^2a_3 + (-c_3^3 + c_1)a_2a_3^2 + (c_2c_3^2 - c_2^2 - c_1c_3 + c_0)a_3^3\Big). \\
& \qquad (5.21)
\end{aligned}$$

We observe that

$$a_2U_1 + a_3V_1 = 0. \qquad (5.22)$$

5.5 Factorisation of q

Lemma 5.6. *Let $P \in \mathbb{Z}[X]$ be an irreducible monic quartic polynomial and r_1, r_2, r_3, r_4 its roots. Let R and R_0 be the two resultants introduced in (5.11). Let $a(r) := a_0 + a_1 r + a_2 r^2 + a_3 r^3$. Then there exists $t_P \in \mathbb{Q}^*$ such that*

$$R(a_1, a_2, a_3) = t_P \prod_{1 \le i < j \le 4} (a(r_i) - a(r_j))^2.$$

Furthermore, the resultant R_0 is divisible by

$$\prod_{1 \le i < j \le 4} (a(r_i) - a(r_j)).$$

Proof. This is [1, Lemme 7.1] in the special case of quartic polynomials. □

Lemma 5.7. *The coefficient t_P in Lemma 5.6 is given by*

$$t_P = \prod_{1 \le i < j \le 4} \frac{1}{(r_i - r_j)^2}.$$

Proof. The proof follows the argument of La Bretèche and Mestre, but for completeness we repeat the main steps.

We note that $N_P(\alpha)$ is the determinant of the linear map $g_a : \overline{\mathbb{Q}}[X]/P(X) \to \overline{\mathbb{Q}}[X]/P(X)$ given by $g_a(H(X)) = a(X)H(X)$ where $a(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3$. Let $L_1(X), \dots, L_4(X)$ be the Lagrange interpolation polynomials for the roots $r_1, \dots, r_4$ of P. Thus $L_i(x) = \prod_{j \ne i}(x - r_j)/(r_i - r_j)$ and in particular $L_i(r_j) = 1$ if $i = j$, 0 if $i \ne j$. Then for all $i = 1, 2, 3, 4$,

$$g_a(L_i(X)) = a(X)L_i(X) = \sum_{j=1}^{4} a(r_j)L_j(X)L_i(X) = a(r_i)L_i(X),$$

in $\overline{\mathbb{Q}}[X]/(P)$, since $P(X) | L_i(X)L_j(X)$ if $i \ne j$ and $P(X) | (L_i^2(X) - L_i(X))$. Thus the matrix of g_a with respect to the basis $\{L_1(X), L_2(X), L_3(X), L_4(X)\}$ is diagonal with coefficients $a(r_1), a(r_2), a(r_3), a(r_4)$ on the diagonal.

Let T be the matrix of the polynomials $L_1(X), L_2(X), L_3(X), L_4(X)$ with respect to the standard basis $\{1, X, X^2, X^3\}$. Then the matrix of $N_P(\alpha)g_a^{-1}$ with respect to the standard basis is $N_P(\alpha)M_\alpha^{-1}$ with M_α^{-1} given by (5.4). Thus have

$$\begin{pmatrix} B_{11} & B_{21} & B_{31} & B_{41} \\ B_{12} & B_{22} & B_{32} & B_{42} \\ B_{13} & B_{23} & B_{33} & B_{34} \\ B_{14} & B_{24} & B_{34} & B_{44} \end{pmatrix} = T \begin{pmatrix} \prod_{j \ne 1} a(r_j) & 0 & 0 & 0 \\ 0 & \prod_{j \ne 2} a(r_j) & 0 & 0 \\ 0 & 0 & \prod_{j \ne 3} a(r_j) & 0 \\ 0 & 0 & 0 & \prod_{j \ne 4} a(r_j) \end{pmatrix} T^{-1}. \tag{5.23}$$

The form $N_P(\alpha) = \prod_{i=1}^4 a(r_i)$ is quartic and monic in a_0. If we write $B_{14} = B_{14}(a_0)$ as an element of $\mathbb{Z}[a_1, a_2, a_3][a_0]$, the resultant R satisfies

$$R = \prod_{i=1}^{4} B_{14}(d_i),$$

where $d_i = -a_1 r_i - a_2 r_i^2 - a_3 r_i^3$ for $i = 1, 2, 3, 4$ are the roots of $y \mapsto N_P(y + a_1 r_1 + a_2 r_1^2 + a_3 r_1^3)$. Let $P_i(X) := d_i + a_1 X + a_2 X^2 + a_3 X^3$. Formula (5.23) with d_1 in place of a_0, gives

$$\begin{pmatrix} B_{11}(d_1) & B_{21}(d_1) & B_{31}(d_1) & B_{41}(d_1) \\ B_{12}(d_1) & B_{22}(d_1) & B_{32}(d_1) & B_{42}(d_1) \\ B_{13}(d_1) & B_{23}(d_1) & B_{33}(d_1) & B_{34}(d_1) \\ B_{14}(d_1) & B_{24}(d_1) & B_{34}(d_1) & B_{44}(d_1) \end{pmatrix} = T \begin{pmatrix} \prod_{\ell \neq 1} P_1(r_\ell) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} T^{-1}.$$

We have similar formulas for the polynomials P_2, P_3, P_4. The first column of the matrix of the left corresponds to the coordinates in the standard basis of the image of the constant polynomial 1 by the map $N_P(\alpha) g_\alpha^{-1}$. The decomposition of the polynomial 1 in the Lagrange basis is $1 = L_1(X) + L_2(X) + L_3(X) + L_4(X)$. The first column of the left matrix is then

$$\begin{pmatrix} B_{11}(d_1) \\ B_{12}(d_1) \\ B_{13}(d_1) \\ B_{14}(d_1) \end{pmatrix} = T \begin{pmatrix} \prod_{\ell \neq 1} P_1(r_\ell) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = T \begin{pmatrix} \prod_{j=2}^4 P_1(r_j) \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

In particular we deduce that $B_{14}(d_1)$ is the coefficient of X^3 in the polynomial $\prod_{j=2}^4 P_1(r_j) L_1(X)$. Since $L_1(X) = \prod_{j=2}^4 (X - r_j)/(r_1 - r_j)$, we get

$$B_{14}(d_1) = \frac{\prod_{j=2}^4 P_1(r_j)}{\prod_{j=2}^4 (r_1 - r_j)} = -\prod_{i=2}^4 \frac{a(r_j) - a(r_1)}{r_j - r_1}.$$

In the same way we prove for $i = 2, 3, 4$:

$$B_{14}(d_i) = \frac{\prod_{j \neq i} P_i(r_j)}{\prod_{j \neq i}^4 (r_i - r_j)} = -\prod_{j \neq i} \frac{a(r_j) - a(r_i)}{r_j - r_i}.$$

This completes the proof of Lemma 5.7. □

Remark. *Lemma 5.7 is stated for quartic polynomials but is in fact also valid for irreducible polynomials of degree $n \geq 2$. For these polynomials, if the resultant is between $N_P(\alpha)$ and the cofactor B_{1n}, then $t_P^{-1} = (-1)^n \prod_{1 \leq i < j \leq n} (r_i - r_j)^2$. For the resultant between $N_P(\alpha)$ and $B_{1\ell}$ for some $1 \leq \ell \leq n-1$, we may also have for t_P an explicit but more complicated formula, involving the coefficients of X^ℓ in the Lagrange interpolation polynomials associated with the roots $r_1, \ldots, r_n$ of $P(X)$.*

Lemma 5.8. *The polynomial $q(a_1, a_2, a_3) \in \mathbb{Q}[a_1, a_2, a_3]$ satisfies*

$$q = \pm \prod_{1 \leq i < j \leq 4} \frac{a(r_i) - a(r_j)}{r_i - r_j},$$

where $a(r) := a_0 + a_1 r + a_2 r^2 + a_3 r^3$.

Proof. This follows immediately from putting together Lemmas 5.6, 5.4 and 5.7. □

5.6 The factor q_1 as a an incomplete norm form

A key point in the work of [4] and [1] is that the form q may be factored as a product of 3 quadratic forms whenever P has a suitably small Galois group. In this section, we prove that if $G = C_4$ or D_4 then q is a product of two forms $q = q_1 q_2$, where q_1 has degree 4, q_2 has degree 2 and q_1 is related to a norm form of a certain number field.

Lemma 5.9. *Let $P(X) \in \mathbb{Z}[X]$ be a monic quartic with Galois group C_4 or D_4. Then there is an ordering of the roots r_1, r_2, r_3, r_4 of P such that*

$$r_1 r_2 + r_3 r_4 \in \mathbb{Z}.$$

Proof. We recall the notation $P(X) = X^4 + c_3 X^3 + c_2 X^2 + c_1 X + c_0$. The cubic resolvent of P is

$$\begin{aligned} R_3(X) &= (X - (r_1 r_2 + r_3 r_4))(X - (r_1 r_3 + r_2 r_4))(X - (r_1 r_4 + r_2 r_3)) \\ &= X^3 - c_2 X^2 + (c_3 c_1 - 4c_0)X - (c_3^2 c_0 + c_1^2 - 4c_2 c_0), \end{aligned}$$

which clearly lies in $\mathbb{Z}[X]$. By Gauss' lemma, any rational root of $R(x)$ must then lie in $\mathbb{Z}$. We therefore see that the claim of the lemma is equivalent to $R_3(X)$ having a root in $\mathbb{Q}$ when $P(X)$ has Galois group $G = C_4$ or D_4. This fact (often stated in the form that the splitting field of $R_3(X)$ is a degree 2 extension) is a standard fact about cubic resolvants; see for example the web page of K. Conrad [3] or the book of Jensen, Ledet and Yui [13] for some nice expositions on the Galois group of quartic polynomials. □

Remark. *The resolvent $R_3(X)$ has a unique rational root when the Galois group is C_4 or D_4. When the Galois group is the Klein group, all roots of $R_3(X)$ are in $\mathbb{Q}$ and when the Galois group is alternating or symmetric (A_4 or S_4), no root of $R_3(X)$ is rational (cf. [3] or [13]).*

Lemma 5.10. *Let $P(X)$ have Galois group C_4 or D_4. Then the form $q \in \mathbb{Q}[a_1, a_2, a_3]$ has the factorisation*

$$q = \pm q_1 q_2$$

where $q_1 \in \mathbb{Q}[a_1, a_2, a_3]$ has degree 4 and $q_2 \in \mathbb{Q}[a_1, a_2, a_3]$ has degree 2. These are explicitly given by

$$q_1 = \frac{(a(r_1) - a(r_3))(a(r_1) - a(r_4))(a(r_2) - a(r_3))(a(r_2) - a(r_4))}{(r_1 - r_3)(r_1 - r_4)(r_2 - r_3)(r_2 - r_4)}, \tag{5.24}$$

and

$$q_2 = \frac{(a(r_1) - a(r_2))(a(r_3) - a(r_4))}{(r_1 - r_2)(r_3 - r_4)}, \tag{5.25}$$

where $a(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3$ and r_1, r_2, r_3, r_4 are the roots of $P(X)$, ordered such that $r_1 r_2 + r_3 r_4 \in \mathbb{Q}$.

Proof. We recall from Lemma 5.8 that the explicit formulae (5.24) and (5.25) give a factorisation $q = \pm q_1 q_2$ over $\overline{\mathbb{Q}}$. Thus we wish to show that

in fact $q_1, q_2 \in \mathbb{Q}[a_1, a_2, a_3]$, so that this is also a factorisation over $\mathbb{Q}$. A direct computation gives for all $1 \leq i < j \leq 4$:

$$\frac{a(r_i) - a(r_j)}{r_i - r_j} = a_1 + a_2(r_i + r_j) + a_3(r_i^2 + r_i r_j + r_j^2). \tag{5.26}$$

If $G = C_4$ then $G = \langle \sigma \rangle$ for some 4-cycle σ. Then we can label the roots such that σ is the permutation $\sigma = (r_1 r_3 r_2 r_4)$. With this choice of root ordering, we have $\sigma(r_1 r_2 + r_3 r_4) = r_1 r_2 + r_3 r_4$. Since $\sigma(q_1) = q_1$ and $\sigma(q_2) = q_2$, we have that $r_1 r_2 + r_3 r_4$, q_1 and q_2 are fixed by all of $G = \{Id, \sigma, \sigma^2, \sigma^3\}$, and so $r_1 r_2 + r_3 r_4 \in \mathbb{Q}$ and $q_1, q_2 \in \mathbb{Q}[a_1, a_2, a_3]$, giving the result in this case.

If $G = D_4$, then $G = \langle \sigma, \tau \rangle$ where τ is a transposition and σ a 4-cycle. We can label the roots such that $\tau = (r_3 r_4)$. This implies that $\sigma(r_3) \neq r_4$, since otherwise we could suppose that $\sigma = (r_3 r_4 r_1 r_2)$ and G would contains the following subset of 9 permutations :

$$\{Id, \tau, \sigma, \sigma^2, \sigma^3, \sigma\tau, (\sigma\tau)^2, \tau\sigma, (\tau\sigma)^2\} = \{Id, (r_3 r_4), (r_1 r_2 r_3 r_4), (r_1 r_3)(r_2 r_4), \\ (r_1 r_4 r_3 r_2), (r_1 r_2 r_3), (r_1 r_3 r_2), (r_1 r_2 r_4), (r_1 r_4 r_2)\},$$

which is not possible since $|G| = 8$. We prove in the same way that $\sigma(r_4) \neq r_3$. We can thus label the roots of P so that $\sigma(r_3) = r_2$. This implies that $\sigma(r_4) = r_1$, $\sigma(r_2) = r_4$ and $\sigma(r_1) = r_3$, that is $\sigma = (r_1 r_3 r_2 r_4)$. Again we observe that $r_1 r_2 + r_3 r_4 \in \mathbb{Q}$ since it is fixed by σ and τ.

Since $\tau(q_1) = q_1 = \sigma(q_1)$ and $\tau(q_2) = q_2 = \sigma(q_2)$ we also observe that $q_1, q_2 \in \mathbb{Q}[a_1, a_2, a_3]$ in this case. This completes the proof. □

The main result of this section is the following proposition.

Proposition 5.11. *Let $P(X) \in \mathbb{Z}[X]$ be irreducible, monic, quartic with Galois group C_4 or D_4. Let r_1, r_2, r_3, r_4 be the roots of P ordered such that $r_1 r_2 + r_3 r_4 \in \mathbb{Q}$ and let $K := \mathbb{Q}(r_1 + r_3)$. Then the form q_1 defined in* (5.24) *satisfies*

$$q_1(a_1, a_2, a_3) = \pm N_{K/\mathbb{Q}}(a_1 + a_2(r_1 + r_3) + a_3(r_1^2 + r_1 r_3 + r_3^2)).$$

Proof. We consider the cases when $G = C_4$ and $G = D_4$ separately.
Case 1: $G = C_4$. Let $G = \langle \sigma \rangle$ with $\sigma = (r_1 r_3 r_2 r_4)$ and $r_1 r_2 + r_3 r_4 \in \mathbb{Q}$. We see that

$$q_1 = \prod_{i=0}^{3} \sigma^i \Big(\frac{a(r_1) - a(r_3)}{r_1 - r_3} \Big) = N_{\mathbb{Q}(r_1)/\mathbb{Q}}(a_1 + a_2(r_1 + r_3) + a_3(r_1^2 + r_1 r_3 + r_3^2)).$$

To finish the proof, it remains to prove that $\mathbb{Q}(r_1 + r_3) = \mathbb{Q}(r_1)$ is the splitting field of P. Since it is obviously contained in the splitting field, we just need to verify the field is not fixed by σ^2. But $c_3 = -(r_1 + r_2 + r_3 + r_4) = -(r_1 + r_3) - \sigma^2(r_1 + r_3)$ so if $\mathbb{Q}(r_1 + r_3)$ is fixed by σ^2 then $\mathbb{Q}(r_1 + r_3) = \mathbb{Q}$. But in this case $r_1 + r_3 = \sigma(r_1 + r_3) = r_3 + r_2$, so the roots would not be distinct, which contradicts our assumption. Thus $\mathbb{Q}(r_1 + r_3) = \mathbb{Q}(r_1)$ as desired.

Case 2: $G = D_4$. Let $G = \langle \sigma, \tau \rangle$ with σ as above and $\tau = (r_3 r_4)$. We work with the permutation $\sigma\tau = (r_1 r_3)(r_2 r_4)$. Let L be the splitting field

of $P(X)$ and $K_0 = \{x \in L : \sigma\tau(x) = x\}$. Then L/K_0 is a Galois extension of degree 2 and $[K_0 : \mathbb{Q}] = 4$. We observe that $r_1 + r_3$, $\frac{a(r_1)-a(r_3)}{r_1-r_3} \in K_0$.

Now, by looking the orbit of $\{1, 3\}$ under the subgroup of S_4 generated by $\{(1324), (34)\}$, we see that

$$N_{L/\mathbb{Q}}\Big(\frac{a(r_1) - a(r_3)}{r_1 - r_3}\Big) = q_1^2$$

and

$$N_{L/K_0}\Big(\frac{a(r_1) - a(r_3)}{r_1 - r_3}\Big) = \Big(\frac{a(r_1) - a(r_3)}{r_1 - r_3}\Big)^2,$$

since $\frac{a(r_1)-a(r_3)}{r_1-r_3} \in K_0$. By the transitive property of the norms,

$$N_{L/\mathbb{Q}}\Big(\frac{a(r_1) - a(r_3)}{r_1 - r_3}\Big) = N_{K_0/\mathbb{Q}}\Big(N_{L/K_0}\Big(\frac{a(r_1) - a(r_3)}{r_1 - r_3}\Big)\Big) = N_{K_0/\mathbb{Q}}\Big(\frac{a(r_1) - a(r_3)}{r_1 - r_3}\Big)^2.$$

We deduce that $q_1 = \pm N_{K_0/\mathbb{Q}}\Big(\frac{a(r_1)-a(r_3)}{r_1-r_3}\Big)$.

As in the case (i), to finish the proof it remains to check that $\mathbb{Q}(r_1 + r_3) = K_0$. We have already seen that $\mathbb{Q}(r_1 + r_3) \subset K_0$, and so it suffices to show $[\mathbb{Q}(r_1 + r_3) : \mathbb{Q}] = 4$. This follows from an identical argument to that of case 1 because the intermediate extension between K_0 and $\mathbb{Q}$ is the subfield of K_0 fixed by $\sigma^2 = (r_1r_2)(r_3r_4)$. □

We will apply Theorem 4.1 with $K = \mathbb{Q}(r_1 + r_3)$ and $\nu_1 = 1$, $\nu_2 = r_1 + r_3$, $\nu_3 = r_1^2 + r_3^2 + r_1r_3$. In the next lemma, we verify that these 3 vectors ν_1, ν_2, ν_3 are linearly independent over $\mathbb{Q}$ (even though the situation would be simpler if there was a linear dependence).

Lemma 5.12. *With the previous notation,* $1, r_1 + r_3, r_1^2 + r_3^2 + r_1r_3$ *are linearly independent over* $\mathbb{Q}$.

Proof. In the proof of Proposition 5.11, we have seen that $r_1 + r_3 \notin \mathbb{Q}$, and so certainly 1 and $r_1 + r_3$ are linearly independent. Suppose that there exists $u, v \in \mathbb{Q}$ such that $r_1^2 + r_3^2 + r_1r_3 = u + v(r_1 + r_3)$. If we apply $\sigma^2 = (r_1r_2)(r_3r_3)$ to this expression, we find $r_2^2 + r_4^2 + r_2r_4 = u + v(r_2 + r_4)$. Summing this two equations gives

$$\sum_{i=1}^{4} r_i^2 + r_1r_3 + r_2r_4 = 2u + v(r_1 + r_2 + r_3 + r_4).$$

This contradicts the fact that $r_1r_3 + r_2r_4 \notin \mathbb{Q}$ (since $\sum_i r_i, \sum_i r_i^2 \in \mathbb{Q}$). □

5.7 On the solutions of some congruence equations with B_{14} and q

In this section we compute the number of solutions of various equations involving the factors q_1, q_2 and the cofactors B_{13}, B_{14}. These preliminary lemmas will be applied in several places in the proof of Theorem 1.1.

Some parts of this section are similar to [1, Lemma 3.9] or [4, Section 13], but both of these previous approaches relied on the condition $G = (\mathbb{Z}/2\mathbb{Z})^2$ which we do not assume, and so we require a slightly different approach.

Let δ_P be the discriminant of the splitting field of P.

Lemma 5.13. *Suppose that* $(p, a_3\delta_P \operatorname{Disc} P) = 1$ *and* $a_2 \in \mathbb{Z}$. *Let* $Q_p(a_2, a_3)$ *denote the number of integers* a_1 *with* $0 \le a_1 < p$ *such that*

$$q_1(a_1, a_2, a_3) \equiv q_2(a_1, a_2, a_3) \equiv 0 \pmod{p}. \tag{5.27}$$

Then

$$Q_p(a_2, a_3) = \begin{cases} 1, & \text{if } P((a_2 - c_3a_3)\overline{a_3}) \equiv 0 \pmod{p}; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let L be the splitting field of P and $\mathcal{O}_L$ its ring of integers. Since $(p, \delta_P) = 1$, p is not ramified in $\mathcal{O}_L$ and so its decomposition into prime ideals is $p\mathcal{O}_L = \prod_{i=1}^{s} \mathfrak{P}_i$ with $N_L(\mathfrak{P}_i) = p^t$ for some integers s, t with $st = [L : \mathbb{Q}]$. Formulas (5.24), (5.25), (5.26) give us the factorisation of the polynomials q_1 and q_2 over $\mathcal{O}_L$. The condition $q_1(a_1, a_2, a_3) \equiv q_2(a_1, a_2, a_3) \equiv 0 \pmod{p}$ is equivalent to one of the factors of q_1 and one of the factors of q_2 vanishing $\pmod{\mathfrak{P}_m}$ for each $1 \le m \le s$.

First we suppose that (5.27) has a solution. Thus for all $1 \le m \le s$, there exists $(i, j) \in \{(1,3), (1,4), (2,3), (2,4)\}$ and $(k, \ell) \in \{(1,2), (3,4)\}$ such that

$$\begin{cases} a_1 + a_2(r_i + r_j) + a_3(r_i^2 + r_ir_j + r_j^2) & \equiv 0 \pmod{\mathfrak{P}_m}, \\ a_1 + a_2(r_k + r_\ell) + a_3(r_k^2 + r_kr_\ell + r_\ell^2) & \equiv 0 \pmod{\mathfrak{P}_m}. \end{cases}$$

Eliminating a_1, we find

$$a_2(r_i + r_j - r_k - r_\ell) \equiv a_3(r_k^2 + r_kr_\ell + r_\ell^2 - r_i^2 - r_ir_j - r_j^2) \pmod{\mathfrak{P}_m}.$$

For notational simplicity we concentrate on the case $i = k = 1$, $j = 3$, $\ell = 2$; the other cases are entirely analogous (noting that $\{i, j\} \cap \{k, \ell\} \neq \emptyset$). We obtain

$$(r_3 - r_2)a_2 \equiv a_3(r_2 - r_3)(r_1 + r_2 + r_3) \pmod{\mathfrak{P}_m}.$$

Since $p \nmid \operatorname{Disc}(P)$ and $(r_3 - r_2) | \operatorname{Disc}(P)$, we see that $r_3 - r_2 \not\equiv 0 \pmod{\mathfrak{P}_m}$, and so (recalling $c_3 = -r_1 - r_2 - r_3 - r_4 \in \mathbb{Z}$) we have $a_2 \equiv a_3(c_3 + r_4) \pmod{\mathfrak{P}_m}$. This implies that $r_4 \equiv (a_2 - a_3c_3)\overline{a_3} \pmod{\mathfrak{P}_m}$ and so

$$P((a_2 - a_3c_3)\overline{a_3}) \equiv 0 \pmod{\mathfrak{P}_m}.$$

Since this argument is valid for all m, we find that $P((a_2 - a_3c_3)\overline{a_3}) \equiv 0 \pmod{p}$. Thus if $P((a_2 - c_3a_3)\overline{a_3}) \not\equiv 0 \pmod{p}$ then $Q_p(a_2, a_3) = 0$.

Now we suppose that $P((a_2 - c_3a_3)\overline{a_3}) \equiv 0 \pmod{p}$. Then there exists $j \in \{1, 2, 3, 4\}$ such that $r_j \equiv (a_2 - a_3c_3)\overline{a_3} \pmod{p}$. We may suppose that $j = 4$; the other cases are analogous. We see that this implies that $a_2 \equiv a_3(-r_1 - r_2 - r_3) \pmod{p}$ and that $r_4 \in \mathbb{Z} + p\mathcal{O}_L$. Moreover, we check that

$$a_2(r_1 + r_3) + a_3(r_1^2 + r_1r_3 + r_3^2) = a_3(-c_2 - c_3r_4 - r_4^2) \pmod{p},$$
$$a_2(r_1 + r_2) + a_3(r_1^2 + r_1r_2 + r_2^2) = a_2(r_1 + r_3) + a_3(r_1^2 + r_1r_3 + r_3^2) \pmod{p}.$$

Thus the system (5.27) admits the solution $a_1 = -(a_2(r_1 + r_3) + a_3(r_1^2 + r_1r_3 + r_3^2)) \pmod{p}$, noting this is in $\mathbb{Z} + p\mathcal{O}_L$. Thus $Q_p(a_2, a_3) \ge 1$.

Moreover, there are no other solutions modulo p, because the previous computations showed that for any $\{i,j,k,\ell\} = \{1,2,3,4\}$, if we have

$$\begin{cases} a_1 + a_2(r_i + r_j) + a_3(r_i^2 + r_i r_j + r_j^2) = 0 \pmod{\mathfrak{P}_m}, \\ a_1 + a_2(r_i + r_k) + a_3(r_i^2 + r_i r_k + r_k^2) = 0 \pmod{\mathfrak{P}_m}, \end{cases}$$

then we must have $(a_2 - c_3 a_3)\overline{a_3} = r_\ell \pmod{\mathfrak{P}_m}$. But the roots r_1, r_2, r_3, r_4 are distinct modulo p when $(p, \operatorname{Disc} P) = 1$, and so we must have $\ell = 4$. Thus the only solution is $a_1 \equiv -a_2(r_i + r_j) - a_3(r_i^2 + r_i r_j + r_j^2) \pmod{p}$ (noting that these are the same for all choices of $\{i,j,k\} = \{1,2,3\}$). Thus $Q_p(a_2, a_3) = 1$ when $P((a_2 - c_3 a_3)\overline{a_3}) \equiv 0 \pmod{p}$. □

Recall that B_{14}, B_{13} are cubic forms in a_0, a_1, a_2, a_3 given explicitly by (5.17) and (5.18). For later estimates, we need to understand the number of solutions in a_0 of the equations $B_{14} \equiv 0 \pmod{p}$ or $B_{13} \equiv 0 \pmod{p}$. Since B_{14} has degree 2 in a_0, we can get an explicit formula for its roots in $\overline{\mathbb{F}_p}$ with the discriminant.

Lemma 5.14. *Let $\Delta_{14} \in \mathbb{Z}[a_1, a_2, a_3]$ be the discriminant of B_{14} viewed as a polynomial in a_0. Then*

$$\Delta_{14} = -q_3 h, \tag{5.28}$$

where h is given by

$$\begin{aligned} h(a_1, a_2, a_3) &= -4a_1^2 + 4c_3 a_1 a_2 + (-3c_3^2 + 4c_2)a_1 a_3 - c_3 a_2^2 + (c_3^3 - 4c_1)a_2 a_3 \\ &\quad + (-c_2 c_3^2 + 4c_1 c_3 - 4c_0)a_3^2 \\ &= (r_1 + r_2 - r_3 - r_4)^2 q_3(a_1, a_2, a_3) - q_2(a_1, a_2, a_3). \end{aligned}$$

We remind the reader that q_3 is the form defined in (5.10) and q_2 is the form given by (4.12).

Proof. This follows from explicit computation using the formula for the discriminant of a quadratic. □

We recall that we have ordered the roots of P, r_1, r_2, r_3, r_4 so that $r_1 r_2 + r_3 r_4 \in \mathbb{Q}$.

Lemma 5.15. *Let $t_1 := r_1 r_2 + r_3 r_4$ and $t_2 := (r_1 + r_2)(r_3 + r_4)$. Then $t_1, t_2 \in \mathbb{Z}$.*

Proof. First we note that t_2 is fixed by the permutations $(r_1 r_3 r_2 r_4)$ and $(r_3 r_4)$, so $t_2 \in \mathbb{Q}$. Let $R(X)$ be a cubic resolvent associated to P, given by (see [3])

$$\begin{aligned} R(X) :=& (X - (r_1 + r_2)(r_3 + r_4))(X - (r_1 + r_3)(r_2 + r_4))(X - (r_1 + r_4)(r_2 + r_3)) \\ &= X^3 - 2c_2 X^2 + (c_2^2 + c_3 c_1 - 4c_0)X + (c_3^2 c_0 + c_1^2 - c_3 c_2 c_1). \end{aligned}$$

Then we see that $R(X) \in \mathbb{Z}[X]$ and it is a well-known fact that when P has Galois group C_4 or D_4, $R(X)$ has a unique root over $\mathbb{Q}$, which must be t_2. Since $R(X)$ is monic we see that $t_2 \in \mathbb{Z}$. Since $t_1 + t_2 = c_2 \in \mathbb{Z}$ we see that $t_1 \in \mathbb{Z}$. □

Remark. *(i) If $t_2 = 0$, that is $(r_1 + r_2)(r_3 + r_4) = 0$, then we have in fact $r_1 + r_2 = r_3 + r_4 = 0$ since $\sigma(r_1 + r_2) = r_3 + r_4$. This implies that $c_3 = 0 = c_1$. This situation is analogous to [1, Lemma 3.9] (or also [4, Lemmas 13.2 and 13.3] for the polynomial $X^4 - X^2 + 1$.)*

(ii) We have $t_1 \neq 0$, since otherwise we would have $r_1 - r_2 = \pm(r_3 - r_4)$. If we compose with the embedding $\tau = (r_3 r_4)$, we find $r_1 - r_2 = r_3 - r_4 = 0$ which is not possible.

Lemma 5.16. *Let $a_1, a_2, a_3 \in \mathbb{Z}$ be such that $(q(a_1, a_2, a_3), q_3(a_1, a_2, a_3)) = 1$ and $q(a_1, a_2, a_3)$ is squarefree. Let $t_2 = (r_1 + r_2)(r_3 + r_4) \in \mathbb{Z}$.*

Let p be a prime with $p | q(a_1, a_2, a_3)$ and $p \nmid a_2 a_3 \delta_P \operatorname{Disc} P$.

(i). If $p | q_1(a_1, a_2, a_3)$ or $p \nmid c_3^2 - 4t_2$, then

$$|\{0 \leq a_0 < p : B_{14}(a_0, a_1, a_2, a_3) \equiv 0 \pmod{p}\}| = 2.$$

(ii). If $p | q_2(a_1, a_2, a_3)$ and $p | c_3^2 - 4t_2$ then

$$|\{0 \leq a_0 < p : B_{14}(a_0, a_1, a_2, a_3) \equiv 0 \pmod{p}\}| = 1.$$

(iii). We have

$$|\{0 \leq a_0 < p : B_{13}(a_0, a_1, a_2, a_3) \equiv B_{14}(a_0, a_1, a_2, a_3) \equiv 0 \pmod{p})\}| = 1.$$

Proof. We recall from (5.11) and (5.12) that $q | R_0$, the resultant of B_{13} and B_{14} viewed as polynomials in a_0. Therefore since $p | q(a_1, a_2, a_3)$, we have that $p | R_0(a_1, a_2, a_3)$, and so the two quadratic polynomials in a_0, B_{13} and B_{14} have a common root in some finite extension of $\mathbb{F}_p$.

If this common root is not in $\mathbb{F}_p$ then its conjugate is also a common root of B_{13} and B_{14}, and so we would have $R_0(a_1, a_2, a_3) = q(a_1, a_2, a_3) q_3(a_1, a_2, a_3) \equiv 0 \pmod{p^2}$. But this is impossible since we assume that $q(a_1, a_2, a_3)$ is squarefree and coprime to $q_3(a_1, a_2, a_3)$ with $p | q(a_1, a_2, a_3)$. Therefore the common root must lie in $\mathbb{F}_p$. This proves assertion (iii).

Since the common root of B_{13} and B_{14} is in $\mathbb{F}_p$ and B_{14} is quadratic, both the roots of B_{14} (seen as a polynomial in a_0) are in $\mathbb{F}_p$. Thus the number of $0 \leq a_0 < p$ with $B_{14} \equiv 0 \pmod{p}$ is 1 when $p | \Delta_{14}$ and 2 otherwise.

If $p | q_2$, by Lemma 5.14, $p | \Delta_{14}$ if and only if $p | (r_1 + r_2 - r_3 - r_4)^2$. This gives the assertion (i) and (ii) in the case $p | q_2$ because $(r_1 + r_2 - r_3 - r_4)^2 = c_3^2 - 4t_2$.

We now consider the case $p | q_1$. Let L be the splitting field of P, $\mathcal{O}_L$ its integer ring and $p\mathcal{O}_L = \prod_{m=1}^{s} \mathfrak{P}_m$, the decomposition of p in $\mathcal{O}_L$. Then for all m there exists $(i, j) \in \{(1, 3), (1, 4), (2, 3), (2, 4)\}$ such that $a_1 \equiv -a_2(r_i + r_j) - a_3(r_i^2 + r_i r_j + r_j^2) \pmod{\mathfrak{P}_m}$. We may suppose that $i = 1$ and $j = 3$, the other cases being similar. Substituting $-a_2(r_1 + r_3) - a_3(r_1^2 + r_1 r_3 + r_3^2)$ for a_1 in the expression for h in Lemma 5.14, gives

$$\begin{aligned} h(a_1, a_2, a_3) \equiv -(a_3(r_1 + r_2 + r_3) + a_2)(a_3(r_1 + r_3 + r_4) + a_2) \\ \times (r_1 - r_2 + r_3 - r_4)^2 \pmod{\mathfrak{P}_m}. \end{aligned} \tag{5.29}$$

We have that $a_3(r_1 + r_2 + r_3) + a_2 \not\equiv 0 \pmod{\mathfrak{P}_m}$. If this were not the case we would have $a_3(-c_3 - r_4) + a_2 \equiv 0 \pmod{\mathfrak{P}_m}$, and then

$P((a_2 - a_3c_3)\overline{a_3}) = 0 \pmod p$. By Lemma 5.13 we would have $p|(q_1, q_2)$ which is not possible when q is squarefree. Similarly $a_3(r_1+r_3+r_4)+a_2 \not\equiv 0 \pmod{\mathfrak{P}_m}$.

Thus $\Delta_{14} \equiv 0 \pmod{\mathfrak{P}_m}$ if and only if $r_1 - r_2 + r_3 - r_4 \equiv 0 \pmod{\mathfrak{P}_m}$ for all m. But this is equivalent to $r_1 - r_2 + r_3 - r_4 \equiv 0 \pmod p$, and so $\gamma(r_1 - r_2 + r_3 - r_3) \equiv 0 \pmod p$ for all embeddings γ. Applying this with $\gamma = \iota, \tau$ we see that $p|\Delta_{14}$ if and only if $r_1 \equiv r_2 \pmod p$, which is impossible since $p \nmid \operatorname{Disc}(P)$. Thus when $p|q_1$ we have $p \nmid \Delta_{14}$, and so B_{14} has two roots $\pmod p$. □

Lemma 5.17. *Let $a_0, a_1, a_2, a_3, p \in \mathbb{Z}$ be such that $(q(a_1, a_2, a_3), q_3(a_1, a_2, a_3)) = 1$, $q(a_1, a_2, a_3)$ is squarefree and $p|(q(a_1, a_2, a_3), B_{14}(a_0, a_1, a_2, a_3))$. Then we have*

$$p|N_P(\alpha) \Leftrightarrow p|B_{13}(a_0, a_1, a_2, a_3).$$

where $\alpha = a_0 + a_1r_1 + a_2r_1^2 + a_3r_1^3$.

Proof. This is a variant of [4, Lemma 13.3] (or [1, Section 6.1]). By (5.6) and (5.8), we have

$$(B_{13} - c_3B_{14})B_{13} - B_{14}(B_{12} - c_2B_{14}) = q_3N_P(\alpha).$$

The Lemma follows from this formula since $(p, q_3(a_1, a_2, a_3)) = 1$. □

6 The set of ideals $\mathcal{J}$

In this section we define a set $\mathcal{J}$ of principle ideals which correspond to the forms q_1 and q_2 having a convenient prime factorisation. This will have a slightly technical definition to ensure that it is compatible with later arguments.

It is known (see [14, Lemma 4.2]) that there is a fundamental domain $\mathcal{D}_P$ of the units action group such that if $\alpha = a_0+a_1r_1+a_2r_1^2+a_3r_1^3 \in \mathcal{D}_P$, then $\max(|a_0|, |a_1|, |a_2|, |a_3|) \ll N_P(\alpha)^{1/4}$ and so $|\sigma(\alpha)| \ll N_P(\alpha)^{1/4}$ for all embeddings σ. We recall that the forms $q_1(a_1, a_2, a_3)$ and $q_2(a_1, a_2, a_3)$ are defined by (5.24) and (5.25), the polynomials $P_1(X) := (X - (r_1 + r_2))(X-(r_3+r_4))$ and $P_2(X) := (X-(r_1^2+r_1r_2+r_2^2))(X-(r_3^2+r_3r_4+r_4^2))$ with discriminants Δ_1 and Δ_2 respectively, D_{q_2} from (4.13), and δ_P is the discriminant of the splitting field of P. With this notation we introduce a constant q_0 depending only on the polynomial P

$$q_0 = 512(1 + c_3^2 + |c_2| + |t_1| + |t_2|)\delta_P \operatorname{Disc} P, \tag{6.1}$$

where t_1 and t_2 are the integers defined in Lemma 5.15. The set $\mathcal{J}$ will depend on various auxiliary absolute constants

$$\alpha_0, \theta_{11}, \dots, \theta_{16}, \theta_{21}, \tau_{11}, \dots, \tau_{16}, \tau_{21} \in (0, 1).$$

These constants will be required to satisfy various inequalities, specifically

$$[\theta_{ij}, \theta_{ij}+\tau_{ij}] \cap [\theta_{i'j'}, \theta_{i'j'}+\tau_{i'j'}] = \emptyset \quad \text{for } (i,j) \neq (i',j'), \tag{6.2}$$

$$0 < \theta_{1j} < \theta_{1j} + \tau_{1j} < 7/32 \text{ for all } 1 \leq j \leq 6, \tag{6.3}$$

$$\alpha_0 < \frac{1}{2^{15}}, \tag{6.4}$$

$$\sum_{j=1}^{6} (\theta_{1j} + \tau_{1j}) < 1 + \alpha_0/2, \tag{6.5}$$

$$\theta_{11}, \theta_{12}, \theta_{13}, \theta_{14}, \theta_{15}, \theta_{16}, \theta_{21} > 1 + \alpha_0 - \sum_{j=1}^{6} \theta_{1j}, \tag{6.6}$$

$$\frac{1+\alpha_0}{4} < \theta_{11} + \theta_{12} + \theta_{13} < \frac{2+\alpha_0}{4} - \tau_{11} - \tau_{12} - \tau_{13}, \tag{6.7}$$

$$\theta_{21} + \tau_{21} < \frac{2+\alpha_0}{200} - \frac{\sum_{i=1}^{3}(\theta_{1i}+\tau_{1i})}{50}, \tag{6.8}$$

$$\theta_{21} + \tau_{21} < \Big(\frac{4(\theta_{11}+\theta_{12}+\theta_{13})}{1+\alpha_0} - 1\Big)\frac{2+\alpha_0}{800}. \tag{6.9}$$

There is reasonable flexibility in how we might choose these constants (and the above constraints could likely be weakened significantly), but for concreteness, we can chose the following explicit values of these variables:
$\alpha_0 = 0.00001$, $\theta_{11} = 0.1398$, $\theta_{12} = 0.1401$, $\theta_{13} = 0.1402$,
$\theta_{14} = 0.21$, $\theta_{15} = 0.19$, $\theta_{16} = 0.1799$, $\theta_{21} = 0.001$,
$\tau_{ij} = 0.0000001$ for all $(i,j) \in I_{\mathcal{C}}$.

Now we are ready to define the set $\mathcal{J}$. The set $\mathcal{J}$ is the set of all principal ideals (α) of $\mathcal{O}_{\mathbb{Q}(r_1)}$ with generator $\alpha = a_0 + a_1 r_1 + a_2 r_1^2 + a_3 r_1^3$ where $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4 \cap \mathcal{D}_P$, satisfying the conditions (C1), (C2), (C3), (C4) and (C5) below.

(C1) $q(a_1, a_2, a_3)$ is squarefree.

(C2) *Size conditions:* We have

$$\begin{aligned} q(a_1,a_2,a_3) &\geq X^{3/2}, \\ |B_{14}(a_0,a_1,a_2,a_3)| &\geq X^{3/4}, \\ N_P(\alpha) &\in [X^{1+\alpha_0/2}, X^{1+\alpha_0}]. \end{aligned}$$

(C3) *Factorisation conditions on α:* There exists ideals K, L such that $(\alpha) = KL$ with K a prime ideal satisfying

$$X^{4\alpha_0} < N_P(K) \leq X^{5\alpha_0}. \tag{6.10}$$

(C4) *Factorisations conditions of auxiliary polynomials:* The values of the forms $q_1(a_1, a_2, a_3)$ and $q_2(a_1, a_2, a_3)$ evaluated at a_1, a_2, a_3 can be factored as:

$$\begin{aligned} q_1(a_1,a_2,a_3) &= \prod_{j=1}^{7} q_{1j}, \\ q_2(a_1,a_2,a_3) &= q_{21}q_{22} \text{ with } q_{21} \equiv 1 \pmod{D_{q_2}}, \end{aligned} \tag{6.11}$$

where $q_{21},\ q_{11}, q_{12}, q_{13}, q_{14}, q_{15}, q_{16}$ are prime numbers satisfying

$$q_{ij} \in [X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}]$$

for all $(i,j) \in \{(1,1),(1,2),(1,3),(1,4),(1,5),(2,1)\}$, and where q_{22}, q_{16} are integers (not necessarily prime) with

$$P^-(q_{22}), P^-(q_{17}) > q_0$$

where q_0 is given by (6.1).

(C5) *Coprimality conditions:*

(a) $(a_2, a_3) = 30$ and $a_2, a_3 \equiv 30 \pmod{900}$, $a_1 \equiv 1 \pmod{30}$.
(b) $(N_P(\alpha), q_0) = 1$.
(c) $(q(a_1,a_2,a_3), q_3(a_1,a_2,a_3)) = 1$.
(d) $(q(a_1,a_2,a_3), B_{14}(a_0,a_1,a_2,a_3)) = 1$.
(e) $(q(a_1,a_2,a_3), a_2a_3) = 1$.

With this definition of $\mathcal{J}$, we can verify the property (3.2) if δ_0 is chosen small enough.

Lemma 6.1. *We have that for all $\mathfrak{J} \in \mathcal{J}$*

$$\prod_{\substack{\mathfrak{p}^e \| \mathfrak{J} \\ N_P(\mathfrak{p}) \le X}} N_P(\mathfrak{p}) \ge X^{1+\alpha_0/2}.$$

Proof. This is a consequence of (C2) which forces $N_P(\alpha) \ge X^{1+\alpha_0/2}$ and (C3), which forces all ideal factors of (α) to have norm at most $\max(X^{5\alpha_0}, X^{1-3\alpha_0}) < X$. (We note that (6.4) implies that $19\alpha_0 < 1$). □

The next Lemma says that the congruence $n \equiv r_1 \pmod{\mathfrak{J}}$ can be solved when $\mathfrak{J} \in \mathcal{J}$. We recall that ϱ_P is defined in (3.4).

Lemma 6.2. *For all $\mathfrak{J} \in \mathcal{J}$ we have $\varrho_P(\mathfrak{J}) = 1$.*

Proof. Let $\mathfrak{J} \in \mathcal{J}$. There exists $\alpha = a_0 + a_1 r_1 + a_2 r_1^2 + a_3 r_1^3$ with $(a_0,a_1,a_2,a_3) \in \mathbb{Z}^4 \cap \mathcal{D}_P$ satisfying (C1),(C2),(C3),(C4),(C5) and such that $\mathfrak{J} = (\alpha)$. By Lemma 5.5 and (C5)(d), $(N_P(\mathfrak{J}), B_{14}(a_0,a_1,a_2,a_3)) = 1$. The condition (C5)(b) and Lemmas 5.2 and 5.1 imply then that $\varrho_P(\mathfrak{J}) = 1$. □

Remark. *As mentioned in Section 3, we will work with the set $\mathcal{J}_2$ which is the set of $\mathfrak{J} \in \mathcal{J}$ such that $P^-(N_P(\mathfrak{J})) > X^{\theta_0}$. This condition implies (C5)(b).*

We see from condition $(C2)$ that if $\mathfrak{a} \in \mathcal{J}$ then $\mathfrak{a} = (a_0 + a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$ for some $\mathbf{a} \in \mathbb{Z}^4$ which lies in the region

$$\begin{aligned}\mathcal{R} := \Big\{ \mathbf{a} \in \mathbb{R}^4 \cap \mathcal{D}_P :\ & 7X^{1+\alpha_0/2} < \widetilde{N}(a_0,a_1,a_2,a_3) \le X^{1+\alpha_0}, \\ & |B_{14}(a_0,a_1,a_2,a_3)| \ge X^{3/4},\ |q(a_1,a_2,a_3)| \ge X^{3/2} \Big\}.\end{aligned} \tag{6.12}$$

Here we have written $\widetilde{N}_P$ as the extension of $N_P(\alpha)$ to $\mathbb{R}^4$;

$$\widetilde{N}(a_1,a_2,a_3,a_4) := \prod_{i=1}^{4}\Big(\sum_{j=1}^{4} a_j\sigma_i(\nu_j)\Big). \tag{6.13}$$

By our choice of $\mathcal{D}_P$ we see that if $\mathbf{a}\in\mathcal{R}$ then $|a_i| \ll X^{(1+\alpha_0)/4}$ for all $i\in\{1,2,3,4\}$. For notational convenience we set $I_{\mathcal{C}}$ to be the set

$$I_{\mathcal{C}} := \{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(2,1)\}, \tag{6.14}$$

so that condition $(C4)$ forces $q_{ij}\in[X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}]$ for all $(i,j)\in I_{\mathcal{C}}$, for example.

7 Proof of Proposition 3.3: The term S_1

In this section we establish Proposition 3.3 by bounding the sum S_1 defined by (3.6). The overall approach is similar to previous works. First we reduce to controlling exponential sums, then remove the a_0-dependence in the denominator of the phase which means that we can apply the q-analogue of Van der Corput's method whenever the denominator of the phase takes a suitably friable form.

Lemma 7.1 (Reduction to exponential sums)**.** *Let S_1 be as given by (3.6), and $\eta_0,\alpha_0,\theta_0>0$ be such that*

$$\alpha_0<\eta_0<1-\frac{9}{4}\alpha_0, \qquad 12\theta_0+19\alpha_0<1.$$

Then for $X\geq 2$, $H=X^{\eta_0}$ we have

$$S_1 \ll (\log H)\sum_{K\in\mathcal{K}}\sum_{\substack{A\\ N_P(A)|\mathcal{P}(X^{\theta_0})\\ N_P(A)\leq X^{3\theta_0}}}\sum_{h\leq H^2}\frac{|E_1(X,h;KA)|+|E_2(X,h;KA)|}{h+h^2/H}+o(X), \tag{7.1}$$

where for $\ell\in\{1,2\}$

$$E_\ell(X,h;KA) := \sum_{\substack{(\alpha)\in\mathcal{J}\\ KA|(\alpha)}} \mathrm{e}\Big(\frac{h\ell X}{N_P(\alpha)}-\frac{hU\overline{B_{14}}}{q}\Big).$$

Proof. This is [1, Lemma 5.1]. □

To show that S_1 is small, our task is therefore reduced to showing cancellation in the exponential sums E_ℓ. Lemma 5.5 allows us to put the exponential phase into a form where we can then apply the q-analogue of Van der Corput's method. The bounds from this method are summarised in the following lemma.

Lemma 7.2 (q-Van der Corput for short exponential sums)**.** *Let $k,D\geq 1$, $\varepsilon>0$. Let $f,g,v\in\mathbb{Z}[X]$ of degree $\leq D$ and $r=r_0\cdots r_k$ be squarefree such that $P^-(r)>2^kD$. Suppose that for every $p|r$ there is no polynomial $w\in\mathbb{Z}[X]$ of degree $\leq k+1$ such that $f(X)\equiv w(X)g(X)\pmod p$. Moreover,*

suppose that $v(X)$ is not the zero polynomial $\pmod p$ *for any* $p|r$. *Then for* $A, B, h \geq 1$ *we have*

$$\sum_{\substack{A<n\leq A+B\\(v(n)\overline{g(n)},r)=1}} \mathrm{e}\left(\frac{hf(n)\overline{g(n)}}{r}\right) \ll_{k,D,\varepsilon} r^{\varepsilon} B\Big[\Big(\frac{\Delta}{r_0}\Big)^{1/2^{k+1}} + \Big(\frac{r_0}{\Delta B^2}\Big)^{1/2^{k+1}} + \sum_{j=1}^{k}\Big(\frac{r_{k+1-j}}{B}\Big)^{1/2^j}\Big],$$

where $\Delta := (r_0, h)$.

Proof. This is [1, Lemme 3.10] (a small variation of [8, Theorem 2]). □

To apply this lemma, the denominator $q(a_1, a_2, a_3)$ in our exponential phase must have a good factorisation. We will apply Theorem 4.1 to show that for a positive proportion of (a_1, a_2, a_3) the denominator $q = q(a_1, a_2, a_3)$ has such a factorisation. We want the $\mathrm{e}(hU\overline{B_{14}}/q)$ factor to oscillate suitably to give this cancellation via Lemma 7.2. The following lemma will ensure that this factor is not degenerate.

Lemma 7.3. *Let* $U = a_0U_1 + U_0$, $V = a_0V_1 + V_0$ *as in* (5.21) *and in* (5.22). *If* $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ *are such that* $(a_0 + a_1r_1 + a_2r_1^2 + a_3r_1^3) \in \mathcal{J}$, *then*

$$(U_0(a_1, a_2, a_3), U_1(a_1, a_2, a_3), q(a_1, a_2, a_3)) = 1.$$

Proof. Imagine for a contradiction that $p|q(a_1, a_2, a_3), U_0(a_1, a_2, a_3), U_1(a_1, a_2, a_3)$. Condition (C4) implies that $q(a_1, a_2, a_3)$ has no prime factors smaller that q_0, so certainly $p > 2$. Then $U(a_0', a_1, a_2, a_3) = 0 \pmod p$ for all a_0', and so the equation $UB_{13} + VB_{14} = qq_3$ (5.13) simplifies to give

$$V(a_0', a_1, a_2, a_3)B_{14}(a_0', a_1, a_2, a_3) \equiv 0 \pmod p$$

for all a_0'. Condition (C5)(d) then implies that $B_{14}(a_0', a_1, a_2, a_3)$ does not identically vanish $\pmod p$, so $V_1(a_1, a_2, a_3) = V_0(a_1, a_2, a_3) = 0 \pmod p$.

By conditions (C1) and (C5)(c), a_1, a_2, a_3 satisfy the hypotheses of Lemma 5.16. But this implies that there is a choice of a_0' such that $B_{14}(a_0', a_1, a_2, a_3) = B_{13}(a_0', a_1, a_2, a_3) = 0 \pmod p$. Evaluating (5.13) at a_0', a_1, a_2, a_3 then implies that

$$q(a_1, a_2, a_3)q_3(a_1, a_2, a_3) \equiv 0 \pmod{p^2}.$$

This is impossible since $(q(a_1, a_2, a_3), q_3(a_1, a_2, a_3)) = 1$ and $q(a_1, a_2, a_3)$ is squarefree by conditions (C5)(c) and (C1). This gives the result. □

Finally, we need a short lemma to show that we can restrict attention to $q(a_1, a_2, a_3)$ being not too small.

Lemma 7.4 (Bounding terms with $q_2(a_1, a_2, a_3)$ small)**.** *Let* $\tau_{20} > 0$ *and for* $\ell = 1, 2$, $E_\ell'(X, h; KA)$ *be the contribution in* $E_\ell(X, h; KA)$ *given by the* $(\alpha) \in \mathcal{J}$ *such that* $|q_2(a_1, a_2, a_3)| \leq X^{(1+\alpha_0)/2-\tau_{20}}$. *Then*

$$E_\ell'(X, h; KA) \ll \frac{X^{1+\alpha_0-\tau_{20}/2}}{N_P(KA)}.$$

Proof. If $E'_\ell(X,h;KA)=0$ then the result is trivial. If $E'_\ell(X,h;KA)\neq 0$ then there exists at least an ideal $(\tilde{\alpha})\in\mathcal{J}$ such that $N_P(AK)|(\tilde{\alpha})$. By the last assertion of Lemma 5.2, this implies that there exists an integer j such that $r_1\equiv j \pmod{KA}$. The condition $KA|(\alpha)$ is therefore equivalent to

$$a_0\equiv -a_1j-a_2j^2-a_3j^3 \pmod{N_P(AK)}.$$

Thus, for any given a_1,a_2,a_3 there are $O(X^{(1+\alpha_0)/4}/N_P(KA))$ terms a_0 in $E'_\ell(X,h;KA)$.

We recall that $q_2(a_1,a_2,a_3)=\prod_{i=0}^{1}L_i(a_1,a_2,a_3)$ with for $i=0,1$:

$$L_i(a_1,a_2,a_3)=a_1+(r_{1+2i}+r_{2+2i})a_2+(r_{1+2i}^2+r_{1+2i}r_{2+2i}+r_{2+2i}^2)a_3.$$

If $|q_2(a_1,a_2,a_3)|\leq X^{(1+\alpha_0)/2-\tau_{20}}$ then

$$\min_{i=0,1}|L_{2i}(a_1,a_2,a_3)|\ll X^{(1+\alpha_0)/4-\tau_{20}/2}. \tag{7.2}$$

For any given a_2,a_3, the number of a_1 satisfying (7.2) is $O(X^{(1+\alpha_0)/4-\tau_{20}/2})$. Since there are $O(X^{(1+\alpha_0)/2})$ choices of a_2,a_3, the total number of terms in $E'(X,h;KA)$ is $O(X^{1+\alpha_0-\tau_{20}/2})$. □

We are now able to bound S_1 suitably.

Proof of Proposition 3.3. First we wish to apply Lemma 7.1. By (6.4), we have $\alpha_0<1/20$, so the conditions of the lemma hold if η_0 is slightly larger than α_0 and θ_0 is sufficiently small. This gives

$$S_1\ll(\log H)\sum_{K\in\mathcal{K}}\sum_{\substack{A\\ N_P(A)|\mathcal{P}(X^{\theta_0})\\ N_P(A)\leq X^{3\theta_0}}}\sum_{h\leq H^2}\frac{|E_1(X,h;KA)|+|E_2(X,h;KA)|}{h+h^2/H}+o(X),$$

where

$$E_\ell(X,h;KA):=\sum_{\substack{(\alpha)\in\mathcal{J}\\ KA|(\alpha)}}\mathrm{e}\Big(\frac{h\ell X}{N_P(\alpha)}-\frac{hU\overline{B_{14}}}{q}\Big).$$

We write $E_\ell=E'_\ell+E_\ell$ where E'_ℓ is the contribution from terms in E_ℓ with $|q_2(a_1,a_2,a_3)|\leq Y$, and E''_ℓ is the contribution from terms with $|q_2(a_1,a_2,a_3)|>Y$. By Lemma 7.4, the contribution to S_1 from E'_ℓ is $O(X^{1-\epsilon+o(1)})$ provided

$$Y<X^{(1+\alpha_0)/2-4\eta_0-\epsilon}. \tag{7.3}$$

Therefore we concentrate on the contribution from E''_ℓ. As in the proof of Lemma 7.4, there exists an integer j such that the condition $KA|(\alpha)$ is equivalent to

$$a_0\equiv -a_1j-a_2j^2-a_3j^3 \pmod{N_P(AK)}. \tag{7.4}$$

Let $\tilde{a}_0=\tilde{a}_0(a_1,a_2,a_3;KA)$ be a solution of the congruence (7.4). We may write $a_0=\tilde{a}_0+mN_P(KA)$ with $m\in\mathcal{R}'(a_1,a_2,a_3)$ where

$$\mathcal{R}'(a_1,a_2,a_3):=\{m:(\tilde{a}_0+mN_P(KA),a_1,a_2,a_3)\in\mathcal{R}\}.$$

(We recall that $\mathcal{R}$ is the domain defined in (6.12).) This set $\mathcal{R}'(a_1,a_2,a_3)$ can be written as a finite union of intervals $I'(a_1,a_2,a_3)$.

Any a_0 of the above form ensures that conditions $(C2)$ and $(C3)$ are satisfied. Conditions (C1), (C4) and (C5) parts (a),(c),(e) don't depend on a_0. Thus we find

$$E''_\ell(X,h;KA) \ll \sum_{\substack{a_1,a_2,a_3 \ll X^{(1+\alpha_0)/4} \\ q_2(a_1a_2,a_3)>Y \\ (6.11)}} \Big| \sum_{\substack{m\in I'(a_1,a_2,a_3) \\ (N_P(\alpha),q_0)=(q,B_{14})=1}} \mathrm{e}\Big(\frac{h\ell X}{N_P(\alpha)} - \frac{hU\overline{B_{14}}}{q}\Big)\Big|.$$

Here by $\sum_{(6.11)}$ we mean that the summation is constrained by the factorisation condition (6.11) .

We now need to control the gcd between $N_P(KA)$ and q. We define $t=(N_P(KA),q)$ and $t'=q/t$. Since q is squarefree, $(t,t')=1$. We apply Bezout formula (5.14) to separate the congruence in t and in t' and use partial summation to remove the factor $e(h\ell X/N_P(\alpha))$. This gives for $\ell=1,2$, (as in [1, p. 239])

$$E''_\ell(X,h;KA) \ll X^{2\eta_0+\alpha_0/4} \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{C} \\ q_2(a_1,a_2,a_3)>Y \\ (6.11)}} \max_{B\ll \frac{X^{\frac{1+\alpha_0}{4}}}{N_P(KA)}} \Big| \sum_{\substack{m\le B \\ (g(m),t')=1}} \mathrm{e}\Big(\frac{h\bar{t}f(m)\overline{g(m)}}{t'}\Big)\Big|, \tag{7.5}$$

where $\mathcal{C}$ is the projection of $\mathcal{R}$ onto the final 3 coordinates and

$$f(m) := U(\tilde{a}_0 + mN_P(KA)), \quad g(m) := B_{14}(\tilde{a}_0 + mN_P(KA)).$$

We recall from (6.11) that for all a_1,a_2,a_3 under consideration $q(a_1,a_2,a_3)$ factors as $\prod_{i=1}^{7} q_{1i}\prod_{j=1}^{2} q_{2j}$ for some integers q_{ij} of constrained sizes. We now wish to apply Lemma 7.2, which requires that for all a_1,a_2,a_3 under consideration and all $p|q(a_1,a_2,a_3)$, there is no polynomial $w(X)\in\mathbb{Z}[X]$ of degree less than 10 such that $f(X)\equiv w(X)g(X) \pmod p$.

Let $p|q(a_1,a_2,a_3)$. By (C5)(e), a_3 is coprime with p, and so by (5.18), $B_{14} \pmod p$ is a polynomial of degree exactly two in a_0 since its lead coefficient is $-a_3$. By Lemma 7.3 , $(p, U_0(a_1,a_2,a_3), U_1(a_1,a_2,a_3)) = 1$, and so $U(a_0,a_1,a_2,a_3) \pmod p$ is not identically zero and has degree at most 1 in a_0. This implies that for all $p|q$, there is no polynomial $w\in\mathbb{Z}[X]$ such that $U(X,a_1,a_2,a_3)\equiv w(X)B_{14}(X,a_1,a_2,a_3) \pmod p$ and we can apply Lemma 7.2 with $k=8$. We take $r_0=q_{22}/(q_{22},t)$, $r_1=q_{21}/(q_{21},t)$, $r_2=q_{17}/(q_{17},t)$, $r_3=q_{16}/(q_{16},t)$, $\ldots$, $r_8=q_{11}/(q_{11},t)$. By (6.11) and (6.6), we observe that $q_{17}<q_{1j}$ for all $1\le j\le 6$. Let

$$\theta_{max}+\tau_{max} = \sup_{(i,j)\in I_{\mathcal{C}}} (\theta_{ij}+\tau_{ij}), \tag{7.6}$$

where we recall from (6.14) that

$$I_{\mathcal{C}} := \{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(2,1)\}.$$

Then the sum over m in (7.5) is bounded by

$$\Big| \sum_{\substack{m\le B\\ (g(m),t')=1}} \mathrm{e}\Big(\frac{h\bar{t}\overline{f(m)g(m)}}{t'}\Big)\Big|$$
$$\ll q^{\varepsilon}B\Big(\Big(\frac{(h,q)(q_{22},t)}{q_{22}}\Big)^{1/2^9}+\Big(\frac{q_{22}}{B^2}\Big)^{1/2^9}+\sup_{(i,j)\in I_{\mathcal{C}}}\Big(\frac{q_{ij}}{B}\Big)^{1/2^8}\Big).$$

We insert this bound into $E''_\ell(X,h;KA)$, and then subsitute this into S_1. Writing $q_{22}=X^{\theta_{22}}$, this gives

$$S_1 \ll X^{2\eta_0+1+\frac{5\alpha_0}{4}+\varepsilon}\big(X^{-\theta_{22}2^{-9}}+X^{(\theta_{22}-\frac{1+\alpha_0}{2}+6\theta_0+10\alpha_0)2^{-9}}$$
$$+X^{(\theta_{max}+\tau_{max}-\frac{1+\alpha_0}{4}+3\theta_0+5\alpha_0)2^{-8}}\big)+X^{1-\epsilon+o(1)}.$$

Thus we see that $S_1=o(X)$ provided

$$\begin{aligned} 2\eta_0+\frac{5\alpha_0}{4} &< \frac{\theta_{22}}{2^9}\\ \frac{\theta_{22}}{2^9} &< \frac{1}{2^9}\Big(\frac{1+\alpha_0}{2}-6\theta_0-10\alpha_0\Big)-2\eta_0-\frac{5\alpha_0}{4}\\ \frac{\theta_{max}+\tau_{max}}{2^8} &< \frac{1}{2^8}\Big(\frac{1+\alpha_0}{4}-3\theta_0-5\alpha_0\Big)-2\eta_0-\frac{5\alpha_0}{4}. \end{aligned}$$

We recall that $q_{22}=q_2(a_1,a_2,a_3)/q_{21}$, that $q_2(a_1,a_2,a_3)\in[Y,X^{(1+\alpha_0)/2}]$ and $q_{21}\in[X^{\theta_{21}},X^{\theta_{21}+\tau_{21}}]$. Thus on choosing $Y=X^{(1+\alpha_0)/4-4\eta_0-\epsilon}$ so (7.3) is satisfied, we see that the bound $S_1=o(X)$ holds provided

$$\begin{aligned} 2\eta_0+\frac{5\alpha_0}{4} &< \Big(\frac{1+\alpha_0}{4}-\theta_{21}-\tau_{21}-4\eta_0\Big)\frac{1}{2^9}\\ \frac{1}{2^9}\Big(\frac{1+\alpha_0}{4}-\theta_{21}\Big) &< \frac{1}{2^9}\Big(\frac{1+\alpha_0}{2}-6\theta_0-10\alpha_0\Big)-2\eta_0-\frac{5\alpha_0}{4}\\ \frac{\theta_{max}+\tau_{max}}{2^8} &< \frac{1}{2^8}\Big(\frac{1+\alpha_0}{4}-3\theta_0-5\alpha_0\Big)-2\eta_0-\frac{5\alpha_0}{4}. \end{aligned}$$

These follow from (6.3), (6.4) and (6.8) on taking θ_0 sufficiently small and η_0 sufficiently close to α_0. □

8 Proof of Proposition 3.2: The sum S_0

In this section we estimate the sum S_0 from (3.6) and establish Proposition 3.2 all under the assumption of Theorem 4.1.

8.1 The variable a_0 in S_0

With the notation $\alpha=a_0+a_1r_1+a_2r_1^2+a_3r_1^3$, we consider the subset $\mathcal{R}\in\mathbb{R}^4$ is defined by (6.12).

For S_0 we proceed in the same way as in [1], [4], [8] but with slight differences in some steps where a bound in $O(X^{\varepsilon})$ is not always sufficient.

Lemma 8.1 (Removing the variable a_0)**.** *Let $12\theta_0 + 22\alpha_0 < 1$. We have*

$$S_0 = \Big(\frac{4e^\gamma}{3}\log(5/4)\log 2 + o(1)\Big)\prod_{p<X_0^\theta}\Big(1-\frac{g(p)}{p}\Big)S_{01} + O(X^{-\alpha_0/5}),$$

where

$$S_{01} := \sum_{(a_1,a_2,a_3)\in\mathcal{C}\cap\mathcal{G}} I(a_1,a_2,a_3)h(q(a_1,a_2,a_3)), \tag{8.1}$$

$$g(p) := |\{\mathfrak{P} : N_P(\mathfrak{P}) = p\}|, \tag{8.2}$$

$$\mathcal{C} := \{(a_1,a_2,a_3)\in\mathbb{R}^3 : \exists a_0\in\mathbb{R}\ s.t.\ (a_0,a_1,a_2,a_3)\in\mathcal{R}\}, \tag{8.3}$$

$$\mathcal{G} := \{(a_1,a_2,a_3)\in\mathbb{Z}^3 : \exists a_0\in\mathbb{Z}\ s.t.\ (\alpha)\in\mathcal{J}\}, \tag{8.4}$$

$$h(q) := \mu^2(q)\prod_{p|q}\frac{(1-2/p)}{1-g(p)/p}\mathbf{1}_{P^-(q)>q_0}, \tag{8.5}$$

$$I(a_1,a_2,a_3) := \int_{a_0\in\mathcal{D}(a_1,a_2,a_3)}\frac{\mathrm{d}\,a_0}{\widetilde{N}_P(a_0,a_1,a_2,a_3)}, \tag{8.6}$$

$$\mathcal{D}(a_1,a_2,a_3) := \{a_0\in\mathbb{R} : (a_0,a_1,a_2,a_3)\in\mathcal{R}\}. \tag{8.7}$$

Here $\widetilde{N}_P(a_0,a_1,a_2,a_3)$ is the quartic form coinciding with $N_P(a_0+a_1r_1+a_2r_1^2+a_3r_1^3)$ on integers.

Proof. We want to isolate the variable a_0. We note that the condition $(\alpha)\in\mathcal{J}$ implies that $(q(a_1,a_2,a_3), B_{14}(a_0,a_1,a_2,a_3)) = 1$ and that $(a_0,a_1,a_2,a_3)\in\mathcal{R}$ but otherwise there are no further dependencies between a_0 and a_1,a_2,a_3. We use Möbius inversion to detect the condition $(q,B_{14})=1$ when evaluated at a_0,a_1,a_2,a_3. This give rise to a squarefree $r|(q,B_{14})$ which we decompose as $r = r_1'r_2'$ with $r_1'|N_P(KA)$ and $(r_2', N_P(KA)) = 1$. This yields

$$\begin{aligned} S_0 = \sum_{K\in\mathcal{K}}\sum_A \lambda^-_{N_P(A)} \sum_{(a_1,a_2,a_3)\in\mathcal{C}\cap\mathcal{G}} \sum_{\substack{r_1'|N_P(KA)\\ r_1'|q(a_1,a_2,a_3)}} \mu(r_1') \\ \times \sum_{\substack{r_2'|q(a_1,a_2,a_3)\\ (r_2',N_P(KA))=1}} \mu(r_2') \sum_{\tilde{a}_0\in S(r_1',r_2')} \sum_{\substack{a_0\in\mathcal{D}(a_1,a_2,a_3)\\ a_0\equiv\tilde{a}_0 \pmod{r_2'N_P(KA)}}} \frac{1}{N_P(\alpha)}, \end{aligned} \tag{8.8}$$

where $\mathcal{C}$, $\mathcal{G}$ are as in (8.3) and (8.4)

$$S(r_1',r_2') := \{0\le a_0\le r_2'N_P(KA) : r_1'r_2'|B_{14}(a_0,a_1,a_2,a_3),\ KA|(\alpha)\}. \tag{8.9}$$

(We have suppressed the dependence of $S(r_1',r_2')$ on a_1,a_2,a_3 for notational convenience.) The inner sum over a_0 is now over points in an interval with a congruence constraint, and so by partial summation (and recalling from (6.12) that $N_P(\alpha)\gg X^{1+\alpha_0/2}$ for all $\mathbf{a}\in\mathcal{R}$), we obtain

$$\sum_{\substack{a_0\in\mathcal{D}(a_1,a_2,a_3)\\ a_0\equiv\tilde{a}_0 \pmod{r_2'N_P(KA)}}} \frac{1}{N_P(\alpha)} = \frac{I(a_1,a_2,a_3)}{r_2'N_P(AK)} + O\Big(\frac{1}{X^{1+\alpha_0/2}}\Big). \tag{8.10}$$

The $O(X^{-(1+\alpha_0/2)})$ error term in (8.10) contributes to S_0 a total

$$\ll \frac{1}{X^{1+\alpha_0/2-o(1)}} \sum_{N_P(K)\ll X^{5\alpha_0}} \sum_{N_P(A)\le X^{3\theta_0}} \sum_{(a_1,a_2,a_3)\in\mathcal{C}} 1 \ll X^{-1/4+3\theta_0+21\alpha_0/4+o(1)}.$$

(Recall that if $\mathbf{a}\in\mathcal{R}$ then $\|\mathbf{a}\|_\infty \ll X^{(1+\alpha_0)/4}$ by our choice of fundamental domain). This is $O(X^{-\alpha_0/4+o(1)})$ if $12\theta_0+22\alpha_0<1$, as in the assumptions of the lemma.

Thus we are left to consider the contribution from the main term of (8.10), namely

$$\sum_{(a_1,a_2,a_3)\in\mathcal{C}} \sum_{K\in\mathcal{K}} \sum_{A} \lambda^-_{N_P(A)} \sum_{\substack{r_1'r_2'|q(a_1,a_2,a_3)\\ r_1'|N_P(KA)\\ (r_2',N_P(KA))=1}} \mu(r_1')\mu(r_2') \frac{|S(r_1',r_2')|I(a_1,a_2,a_3)}{r_2' N_P(AK)}. \tag{8.11}$$

By the Chinese Remainder Theorem, we have

$$|S(r_1',r_2')| = \prod_{p|r_2'N_P(KA)} |S(r_1',r_2',p)|, \tag{8.12}$$

where

$$|S(r_1',r_2',p)| := \begin{cases} |\{0\le a_0<p : p|(B_{14}(a_0,a_1,a_2,a_3),N_P(\alpha))\}|, & \text{if } p|r_1',\\ |\{0\le a_0<p : p|B_{14}(a_0,a_1,a_2,a_3)\}|, & \text{if } p|r_2',\\ |\{0\le a_0<p : p|N_P(\alpha)\}|, & \text{if } p|N_P(KA)/r_1'. \end{cases}$$

We compute $|S(r_1',r_2',p)|$ using Lemmas 5.16 and 5.17. Under the condition $P^-(q)>q_0$ we find

$$|S(r_1',r_2',p)| = \begin{cases} 2 & \text{if } p|r_2',\\ 1 & \text{if } p|N_P(KA). \end{cases}$$

Using this bound in (8.12) gives

$$|S(r_1',r_2')| = 2^{\omega(r_2')}.$$

Inserting this in the previous expression (8.11) for the main term of S_0, we see that the sum over r_1' is 1 if $(q(a_1,a_2,a_3),N_P(KA))=1$, and 0 otherwise. Thus the expression (8.11) simplifies to

$$\sum_{(a_1,a_2,a_3)\in\mathcal{C}} I(a_1,a_2,a_3)\Big(\sum_{r_2'|q(a_1,a_2,a_3)} \frac{\mu(r_2')2^{\omega(r_2')}}{r_2'}\Big) h_1(q(a_1,a_2,a_3)),$$

where

$$h_1(q) := \Bigg(\sum_{\substack{K\in\mathcal{K}\\ (N_P(K),q)=1}} \frac{1}{N_P(K)}\Bigg)\Bigg(\sum_{(N_P(A),q)=1} \frac{\lambda^-_{N_P(A)}}{N_P(A)}\Bigg).$$

Recalling that $\mathcal{K}$ is the set of prime ideals with norm between $X^{4\alpha_0}$ and $X^{5\alpha_0}$, we see that for $q \ll X^{O(1)}$

$$\sum_{\substack{K\in\mathcal{K}\\(N_P(K),q)=1}} \frac{1}{N_P(K)} = \log(5/4) + o(1),$$

$$\begin{aligned}\sum_{(N_P(A),q)=1} \frac{\lambda^-_{N_P(A)}}{N_P(A)} &= \sum_{\substack{d\le X^{3\theta_0}\\(d,q)=1}} \frac{\lambda^-_d g(d)}{d}\\ &= \Big(\frac{2e^\gamma \log 2}{3} + o(1)\Big) \prod_{p<X^{\theta_0}} \Big(1-\frac{g(p)}{p}\Big) \prod_{\substack{p\mid q\\ p\le X^{\theta_0}}} \Big(1-\frac{g(p)}{p}\Big)^{-1}.\end{aligned}$$

Here we used the fact that the linear sieve lower bound function evaluated at 3 is $2e^\gamma \log 2/3$. Putting these expressions together now gives the result. □

8.2 Splitting into small boxes

We see from condition (C2) that if $\mathfrak{a} \in \mathcal{J}$ then $\mathfrak{a} = (a_0+a_1r_1+a_2r_1^2+a_3r_1^3)$ for some $\mathbf{a} \in \mathbb{Z}^4$ which lies in the region $\mathcal{R}$ given by (6.12). We recall that $\eta_1 = (\log x)^{-100}$. We cover the region $\mathcal{R}$ by hyper-rectangles of type

$$\mathcal{H} =]A_0, A_0+\eta_1 A_0] \times]A_1, A_1(1+\eta_1)] \times]A_2, A_2(1+\eta_1)] \times]A_3, A_3(1+\eta_1)]. \tag{8.13}$$

The number of such hyper-rectangles is $O(\eta_1^{-4})(\log X)^4 = O(\eta_1^{-5})$.

Furthermore the contribution to S_{01} from hyper-rectangles such that $\min(|A_i|) \le X^{1/4-7\alpha_0/8}$ is $O(X^{1-\alpha_0/8+\varepsilon})$ which is sufficiently small.

We will say that $\mathcal{H}$ is a 'good' hyper-rectangle if $\mathcal{H} \subset \mathcal{R}$ and

$$\begin{aligned}&\min(|A_0|,|A_1|,|A_2|,|A_3|) \ge X^{1/4-7\alpha_0/8},\\ &\min(|A_0|,|A_1|,|A_2|,|A_3|) \ge \eta_1 \max(|A_0|,|A_1|,|A_2|,|A_3|),\\ &q_1(A_1,A_2,A_3) \ge \eta_1^{1/10} \max(|A_1|,|A_2|,|A_3|)^4.\end{aligned} \tag{8.14}$$

If $\mathcal{H}$ is not 'good' then we say $\mathcal{H}$ is 'bad'. We note that the second and third assertions in this definition corresponds to the conditions (4.3) and (4.4).

We denote by $\mathscr{H}_{\mathcal{R}}$ the set of all good hyper-rectangles. To each hyper-rectangle $\mathcal{H}$ we associate its projection to $\mathbb{R}^3$ by ignoring a_0:

$$\mathcal{H}' =]A_1, A_1(1+\eta_1)] \times]A_2, A_2(1+\eta_1)] \times]A_3, A_3(1+\eta_1)]. \tag{8.15}$$

Lemma 8.2 (Splitting into small boxes)**.** *Let S_{01} be as in Lemma 8.1. We have that*

$$S_{01} \gg \sum_{\mathcal{H}\in\mathscr{H}_{\mathcal{R}}} \frac{A_0\eta_1}{\widetilde{N}_P(A_0,A_1,A_2,A_3)} S_{02}(\mathcal{H}),$$

where

$$S_{02}(\mathcal{H}) := \sum_{\substack{q_{ij}\in[X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]\\(i,j)\in I_{\mathcal{C}}\\ q_{21}\equiv 1 \pmod{D_{q_2}}}} \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{H}'\\ \prod_{j=1}^{6} q_{1j}\mid q_1(a_1,a_2,a_3)\\ q_{21}\mid q_2(a_1,a_2,a_3)\\ (q(a_1,a_2,a_3),q_3(a_1,a_2,a_3))=1\\ (q,a_2a_3)=1\\ (a_2,a_3)=30,\ a_1\equiv 1 \pmod{30}\\ a_2,a_3\equiv 30 \pmod{900}}} h(q(a_1,a_2,a_3)).$$

We recall from (6.13) that $\widetilde{N}_P(a_0,a_1,a_2,a_3)$ is the quartic form coinciding with $N_P(a_0+a_1r_1+a_2r_1^2+a_3r_1^3)$ on integers.

Proof. By splitting the sum over a_1,a_2,a_3 and the integral over a_0 into the hyperrectangles $\mathcal{H}$, and then restricting only to good hyperrectangles for a lower bound, we find

$$S_{01} \geq \sum_{\mathcal{H}\in\mathscr{H}_{\mathcal{R}}} S'_{01}(\mathcal{H}),$$

where

$$S'_{01}(\mathcal{H}) := \sum_{(a_1,a_2,a_3)\in\mathcal{C}\cap\mathcal{H}'\cap\mathcal{G}} h(q(a_1,a_2,a_3))I_{\mathcal{H}}(a_1,a_2,a_3),$$

$$I_{\mathcal{H}}(a_1,a_2,a_3) := \int_{A_0}^{A_0(1+\eta_1)} \frac{\mathrm{d}\,a_0}{\widetilde{N}_P(a_0,a_1,a_2,a_3)} = \frac{A_0\eta_1(1+o(1))}{\widetilde{N}_P(A_0,A_1,A_2,A_3)}.$$

We recall from (6.11) that if $(a_1,a_2,a_3)\in\mathcal{G}$ then $q_1(a_1,a_2,a_3)$ and $q_2(a_1,a_2,a_3)$ factor as $\prod_{i=1}^{6} q_{1i}$ and $q_{21}q_{22}$ respectively with $q_{21},q_{11},q_{12},q_{13},q_{14},q_{15}$ primes satisfying $q_{ij}\geq X^{\theta_{ij}}$. In particular, we see that for any choice of a_1,a_2,a_3 there are $O(1)$ choices of q_{ij} such that $q_i(a_1,a_2,a_2)=\prod_j q_{ij}$. Thus, summing over these representations, we find

$$S_{01}(\mathcal{H}) \gg \frac{A_0\eta_1}{\widetilde{N}_P(A_0,A_1,A_2,A_3)} S_{02}(\mathcal{H}),$$

say, with $S_{02}(\mathcal{H})$ as given by the lemma and $I_{\mathcal{C}}$ defined in (6.14). This gives the result. □

8.3 Preparation for the application of Theorem 4.1

Following [1, Section 6.2] or [4, Section 15], we do several manipulations in order to take care of the different coprimality conditions and the multiplicative weight $h(q)$. In our situation it is important that we are slightly more careful than these previous works. We do not impose congruence conditions to moduli larger than $(\log X)^{O(1)}$ since this would cause issues related to Siegel zeros (the argument of the previous papers would introduce a congruence constraint of modulus X^{t_0} for some $t_0>0$). This means we need to be careful not to lose the fact that when $(a_0,a_1,a_2,a_3)\in\mathcal{H}$, the a_i are in small intervals. Let

$$Z := (\log X)^{\lambda_0}, \qquad Z' := X^{\alpha_0/10000}, \tag{8.16}$$

where α_0 is the constant used to define the set $\mathcal{K}$ (which will be chosen sufficiently small later on) and λ_0 is a fixed constant (which will be chosen sufficiently large). From the bound (8.14), we certainly note that since $\alpha_0 < 1$ we have

$$Z^{1000} < Z'^{100} < \min(A_0, A_1, A_2, A_3). \tag{8.17}$$

For brevity we will write

$$N_{\mathcal{H}} = \widetilde{N}_P(A_0, A_1, A_2, A_3). \tag{8.18}$$

Lemma 8.3 (Removing the condition $(q, q_3) = 1$)**.** *Let $S_{02}(\mathcal{H})$ be as in Lemma 8.2. Then we have*

$$S_{02}(\mathcal{H}) = S_{03}(\mathcal{H}) + O\Big(\frac{\eta_1^3 A_1 A_2 A_3}{Z^{3/4}}\Big),$$

where

$$S_{03}(\mathcal{H}) := \sum_{d \le Z} \mu(d) \sum_{\substack{q_{ij} \in [X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}] \\ (i,j) \in I_{\mathcal{C}} \\ q_{21} \equiv 1 \pmod{D_{q_2}}}} \sum_{\substack{(a_1,a_2,a_3) \in \mathcal{H}' \\ \prod_{j=1}^6 q_{1j} | q_1(a_1,a_2,a_3) \\ q_{21} | q_2(a_1,a_2,a_3) \\ d | q(a_1,a_2,a_3) \\ d | q_3(a_1,a_2,a_3) \\ (q(a_1,a_2,a_3), q_3(a_1,a_2,a_3)) = 1 \\ (q, a_2 a_3) = 1 \\ (a_2,a_3) = 30,\ a_1 \equiv 1 \pmod{30} \\ a_2, a_3 \equiv 30 \pmod{900}}} h(q(a_1,a_2,a_3)).$$

Proof. First, we detect the condition $(q, q_3) = 1$ via Möbius inversion

$$S_{02}(\mathcal{H}) = \sum_{\substack{q_{ij} \in [X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}] \\ (i,j) \in I_{\mathcal{C}} \\ q_{21} \equiv 1 \pmod{D_{q_2}}}} \sum_{\substack{(a_1,a_2,a_3) \in \mathcal{H}' \\ \prod_{j=1}^6 q_{1j} | q_1(a_1,a_2,a_3) \\ q_{21} | q_2(a_1,a_2,a_3) \\ (q(a_1,a_2,a_3), q_3(a_1,a_2,a_3)) = 1 \\ (q, a_2 a_3) = 1 \\ (a_2,a_3) = 30,\ a_1 \equiv 1 \pmod{30} \\ a_2, a_3 \equiv 30 \pmod{900}}} h(q(a_1,a_2,a_3)) \sum_{\substack{d | q(a_1,a_2,a_3) \\ d | q_3(a_1,a_2,a_3)}} \mu(d).$$

We split $S_{02}(\mathcal{H})$ into three sums,

$$S_{02}(\mathcal{H}) = S_{03}(\mathcal{H}) + U_{21}(\mathcal{H}) + U_{22}(\mathcal{H}),$$

where $S_{03}(\mathcal{H})$ is the contribution of the terms in $S_{02}(\mathcal{H})$ with $d \le Z$, $U_{21}(\mathcal{H})$ is the contribution from $Z < d \le Z'$ and $U_{22}(\mathcal{H})$ is the contribution from $d > Z'$. We note that $S_{03}(\mathcal{H})$ is as given in the lemma, so we are left to bound $U_{21}(\mathcal{H})$ and $U_{22}(\mathcal{H})$.

First we bound U_{21}. Recall that $q_3(a_1, a_2, a_3) = -a_1 a_3 + a_2^2 - c_3 a_2 a_3 - c_2 a_3^2$, so the condition $q_3 \equiv 0 \pmod d$ implies that $a_1 \equiv \overline{a_3}(a_2^2 - c_3 a_2 a_3 - c_2 a_3^2) \pmod d$. (We restrict ourselves to $(a_3, q(a_1, a_2, a_3)) = 1$ so $(a_3, d) = 1$.) Inserting this into the condition $q(a_1, a_2, a_3) \equiv 0 \pmod d$ and multiplying by a_3^6 gives $Q(a_2, a_3) := q(a_2^2 - c_3 a_2 a_3 - c_2 a_3^2, a_2 a_3, a_3^2) \equiv 0 \pmod d$, for a polynomial $Q(a_2, a_3)$ which is of degree 12 in a_2 (and non-zero). For any given a_3 the number of roots of $Q(a_2, a_3) \pmod d$ is $O(12^{\omega(d)})$. For any choice of a_1, a_2, a_3 under consideration, there are $O(1)$ choices of primes $q_{ij} \in [X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}]$ with $q_{ij} | q_1(a_1, a_2, a_3) q_2(a_1, a_2, a_3)$. Thus,

letting $b(a_2,a_3)=\overline{a_3}(a_2^2-c_3a_2a_3-c_2a_3^2)$, and noting $Z'<A_i^{0.99}$ (recall (8.17)), we deduce

$$U_{21}(\mathcal{H}) \ll \sum_{Z<d\le Z'} \sum_{a_3\in[A_3,A_3(1+\eta_1)]} \sum_{\substack{a_2\in[A_2,A_2(1+\eta_1)]\\ Q(a_2,a_3)\equiv 0 \pmod d}} \sum_{\substack{a_1\in[A_1,A_1(1+\eta_1)]\\ a_1\equiv b(a_2,a_3) \pmod d}} 1$$
$$\ll A_1A_2A_3\eta_1^3 \sum_{Z<d<Z'} \frac{12^{\omega(d)}}{d^2} \ll A_1A_2A_3\eta_1^3 Z^{-3/4}.$$

We now consider U_{22}. Since $Q(a_2,a_3)\equiv 0 \pmod d$, if $Q(a_2,a_3)\neq 0$ there are $O(X^\epsilon)$ choices of d given a_2,a_3. We have $Q(a_2,a_3)=0$ if and only if $\exists (i,j)$ such that

$$(a_2^2-c_3a_2a_3-c_2a_3^2)+(r_i+r_j)a_2a_3+a_3^2(r_i^2+r_ir_j+r_j^2)=0,$$

which rearranges to

$$a_2^2+a_2a_3(r_i+r_j-c_3)+a_3^2(r_i^2+r_ir_j+r_j^2-c_2)=0.$$

Since $a_3\neq 0$, a_2/a_3 is a root of $X^2+(r_i+r_j-c_3)X+r_i^2+r_ir_j+r_j^2-c_2$ and there are at most two such roots. Thus for each choice of a_2 there are at most 2 choices of a_3 such that $Q(a_2,a_3)=0$. Moreover, in this case we still have $d|q_3(a_1,a_2,a_3)\neq 0$, so there are $O(X^\epsilon)$ choices of d given a_1,a_2,a_3. We deduce that (using $Z'\ll A_1,A_3$)

$$U_{22}(\mathcal{H}) \ll \sum_{d>Z'} \mu^2(d) \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{H}'\\ Q(a_2,a_3)\neq 0\\ a_1\equiv b(a_2,a_3) \pmod d}} 1 + \sum_{d>Z'} \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{H}'\\ Q(a_2,a_3)=0\\ d|q_3(a_1,a_2,a_3)}} \mu^2(d)$$
$$\ll \sum_{a_2\in[A_2,A_2(1+\eta_1)]} \sum_{\substack{a_3\in[A_3,A_3(1+\eta_1)]\\ Q(a_2,a_3)\neq 0}} \sum_{\substack{d>Z'\\ d|Q(a_2,a_3)\\ \mu^2(d)=1}} \sum_{\substack{a_1\in[A_1,A_1(1+\eta_1)]\\ a_1\equiv b(a_2,a_3) \pmod d}} 1$$
$$+ \sum_{a_1\ll A_1,a_2\ll A_2} \sum_{\substack{0<a_3\ll A_3\\ Q(a_2,a_3)=0}} \sum_{d|q_3(a_1,a_2,a_3)} 1$$
$$\ll \frac{A_1}{Z'} \sum_{\substack{a_2\in[A_2,A_2(1+\eta_1)]\\ a_3\in[A_3,A_3(1+\eta_1)]\\ Q(a_2,a_3)\neq 0}} \tau(Q(a_2,a_3)) + A_1A_2X^\varepsilon \ll \frac{A_1A_2A_3X^\varepsilon}{Z'}.$$

This gives the result. □

Lemma 8.4 (Removing the condition $(q,a_2a_3)=1$)**.** *Let $S_{03}(\mathcal{H})$ be as given in Lemma 8.3. Then we have*

$$S_{03}(\mathcal{H}) = S_{04}(\mathcal{H}) + O\Big(\frac{\eta_1^3A_1A_2A_3}{Z^{1/2}}\Big),$$

where

$$S_{04}(\mathcal{H}) := \sum_{\substack{d\le Z\\ s_2s_3\le Z}} \mu(d)\mu(s_2s_3) \sum_{\substack{q_{ij}\in[X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]\\ \forall\,(i,j)\in I_{\mathcal{C}}\\ q_{21}\equiv 1 \pmod{D_{q_2}}}} \sum_{\substack{(a_1,s_2a_2',s_3a_3')\in\mathcal{H}'\\ \prod_{j=1}^6 q_{1j}|q_1(a_1,s_2a_2',s_3a_3')\\ q_{21}|q_2(a_1,s_2a_2',s_3a_3')\\ [d,s_2s_3]|q(a_1,s_2a_2',s_3a_3')\\ d|q_3(a_1,a_2,a_3)\\ (s_2a_2',s_3a_3')=30,\ a_1\equiv 1 \pmod{30}\\ s_2a_2',s_3a_3'\equiv 30 \pmod{900}}} h(q(a_1,s_2a_2',s_3a_3')).$$

Proof. We remove the condition $(a_2a_3, q(a_1,a_2,a_3)) = 1$ via Mobius inversion, giving

$$S_{03}(\mathcal{H}) = \sum_{d\le Z}\mu(d)\sum_{\substack{q_{ij}\in[X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]\\(i,j)\in I_{\mathcal{C}}\\ q_{21}\equiv 1 \pmod{D_{q_2}}}}\ \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{H}'\\ \prod_{j=1}^6 q_{1j}\mid q_1(a_1,a_2,a_3)\\ q_{21}\mid q_2(a_1,a_2,a_3)\\ (a_2,a_3)=30,\ a_1\equiv 1 \pmod{30}\\ a_2,a_3\equiv 30 \pmod{900}\\ d\mid q_3(a_1,a_2,a_3)}}\ \sum_{\substack{s\mid a_2a_3\\ [d,s]\mid q(a_1,a_2,a_3)}}\mu(s)h(q(a_1,a_2,a_3)).$$

We write s as $s = s_2s_3$ with $s_2|a_2$ and $s_3|a_3$, and write $a_2 = s_2a_2'$, $a_3 = s_3a_3'$. Let $U_3(\mathcal{H})$ denote the contribution given by the $s > Z$ and $S_{04}(\mathcal{H})$ the remaining contribution with $s \le Z$. Thus we are left to bound $U_3(\mathcal{H})$.

Since each $q_i(a_1, s_2a_2', s_3a_3')$ has a finite number of prime factors in $[X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}]$, there are $O(1)$ choices of the q_{ij}, so

$$U_3(\mathcal{H}) \ll \sum_{d\le Z}\mu^2(d)\sum_{Z<s_2s_3\ll N_{\mathcal{H}}^{1/4}}\mu^2(s_2s_3)\sum_{\substack{(a_1,s_2a_2',s_3a_3')\in\mathcal{H}'\\ [d,s]\mid q(a_1,a_2's_2,a_3's_3)\\ d\mid q_3(a_1,a_2's_2,a_3's_3)}}1.$$

The form q is monic of degree 6 in a_1 (by (5.24), (5.25)) and $[d, s_2s_3]$ is squarefree, so given s_2, s_3, a_2', a_3' there are $O(6^{\omega([d,s_2s_3])})$ choices of $a_1 \pmod{[d, s_2s_3]}$ such that $q(a_1, a_2's_2, a_3's_3) = 0 \pmod{[d, s_2s_3]}$. Since $(a_1, a_2's_2, a_3's_3) \in \mathcal{H}'$ we obtain

$$\begin{aligned}U_3(\mathcal{H}) &\ll \sum_{d<Z}\mu^2(d)\sum_{Z<s_2s_3\ll N_{\mathcal{H}}^{1/4}}\mu^2(s_2s_3)6^{\omega([s_2s_3,d])}\Big(\frac{\eta_1A_2}{s_2}+1\Big)\Big(\frac{\eta_1A_3}{s_3}+1\Big)\Big(\frac{\eta_1A_1}{[s_2s_3,d]}+1\Big)\\ &\ll ZN_{\mathcal{H}}^{1/4+\varepsilon} + ZN_{\mathcal{H}}^{1/4+\varepsilon}(|A_1|+|A_2|+|A_3|) + \frac{A_1A_2A_3\eta_1^2}{\min(A_1,A_2,A_3)}ZX^{\varepsilon}\\ &\quad + \eta_1^3A_1A_2A_3\sum_{d<Z}\sum_{s>Z}\frac{6^{\omega([d,s])}}{s[s,d]}.\end{aligned}$$

This final term is seen to be $O(\eta_1^3A_1A_2A_3(\log Z)^{O(1)}/Z)$. Since $\max(A_1, A_2, A_3) \ll N_{\mathcal{H}}^{1/4}$ and $Z = (\log X)^{O(1)}$, this gives

$$U_3(\mathcal{H}) \ll \frac{\eta_1^3A_1A_2A_3}{Z^{1/2}} + N_{\mathcal{H}}^{1/2+\epsilon}.$$

This gives the result. □

Lemma 8.5 (Simplifying the function h)**.** *Let $S_{04}(\mathcal{H})$ be as in Lemma 8.4. Then we have*

$$S_{04}(\mathcal{H}) = S_{05}(\mathcal{H}) + O\Big(\frac{\eta_1^3A_1A_2A_3}{Z}\Big),$$

where

$$S_{05}(\mathcal{H}) := \sum_{\substack{u\le Z^{20}\\ d\le Z\\ s_2s_3\le Z}}\mu(d)\mu(s_2s_3)\ell(u)\sum_{\substack{q_{ij}\in[X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]\\ \forall\,(i,j)\in I_{\mathcal{C}}\\ q_{21}\equiv 1 \pmod{D_{q_2}}}}\ \sum_{\substack{(a_1,s_2a_2',s_3a_3')\in\mathcal{H}'\\ \prod_{j=1}^6 q_{1j}\mid q_1(a_1,s_2a_2',s_3a_3')\\ q_{21}\mid q_2(a_1,s_2a_2',s_3a_3')\\ [d,s_2s_3,u]\mid q(a_1,s_2a_2',s_3a_3')\\ d\mid q_3(a_1,a_2,a_3)\\ (s_2a_2',s_3a_3')=30,\ a_1\equiv 1 \pmod{30}\\ s_2a_2',s_3a_3'\equiv 30 \pmod{900}}}1,$$

and ℓ is the multiplicative function defined by

$$\ell(p^\nu) := \begin{cases} \frac{g(p)-2}{p-g(p)}, & \text{if } p > q_0 \text{ and } \nu = 1, \\ -1, & \text{if } 7 \le p \le q_0 \text{ and } \nu = 1, \\ -h(p), & \text{if } \nu = 2, \\ 0, & \text{if } \nu \ge 3, \end{cases}$$

with q_0 given by (6.1).

Proof. Recalling (8.5), we see that $h = \mathbf{1} * \ell$ where ℓ is as given by the lemma. In particular,

$$h(q(a_1, s_2a_2', s_3a_3')) = \sum_{u \mid q(a_1, s_2a_2', s_3a_3')} \ell(u).$$

Since $a_1 \equiv 1 \pmod{30}$ and $30 \mid (a_2, a_3)$, $(u, 30) = 1$. We substitute this into our definition of $S_{04}(\mathcal{H})$, and consider separately the contribution $S_{05}(\mathcal{H})$ from $u < Z^{20}$ and the contribution $U_4(\mathcal{H})$ from $u > Z^{20}$.

Since $\ell(u) = 0$ when there exists p such that $p^3 \mid u$, we may write $u = v^2w$ with $\mu^2(vw) = 1$. Since $U_4(\mathcal{H})$ has $u > Z^{20}$, it suffices to separately bound the contribution of terms $U_{41}(\mathcal{H})$ with $w > Z^{10}$ and the contribution $U_{42}(\mathcal{H})$ of terms with $v^2 > Z^{10} \ge w$.

First we bound $U_{41}(\mathcal{H})$ with $w > Z^{10}$. Since $q_0 > 10$, we see that $|\ell(u)| \le 10^{\omega(vw)}/w$. Following an entirely analogous argument to our bound for $U_2(\mathcal{H})$ in Lemma 8.3, we can find that

$$\begin{aligned} U_{41}(\mathcal{H}) &\ll Z \sum_{\substack{s_2s_3 < Z \\ \mu^2(s_2s_3)=1}} \sum_{\substack{w \ge Z^{10} \\ wv^2 \mid q}} \mu^2(vw) \frac{(60)^{\omega(vw)}}{w} \Big(\frac{\eta_1 A_1}{wv^2} + 1 \Big) \frac{\eta_1^2 A_2 A_3}{s_2 s_3} \\ &\ll A_2A_3X^\varepsilon + \eta_1^3 A_1A_2A_3 (\log X) Z^{-3} \ll \frac{A_1A_2A_3}{Z}. \end{aligned}$$

Thus we are left to bound $U_{42}(\mathcal{H})$ involving terms with $v \ge Z^5$. We see

$$U_{42}(\mathcal{H}) \le V'(\mathcal{H}) + \sum_{(i,j) \in I_{\mathcal{C}}} V_{ij}(\mathcal{H}),$$

where $V_{ij}(\mathcal{H})$ denotes those terms with $q_{ij} \mid v$ for some $q_{ij} \in [X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}]$, and $V'(\mathcal{H})$ denotes those terms with $(\prod_{(i,j)\in I_{\mathcal{C}}} q_{ij}, v) = 1$ for all $q_{ij} \in [X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}]$, $(i,j) \in I_{\mathcal{C}}$.

First we consider $V_{21}(\mathcal{H})$. By (6.6), we have $\sum_{i=1}^6 \theta_{1i} + \theta_{21} > 1 + \alpha_0$. We recall $q_1(a_1, a_2a_3) \ll X^{1+\alpha_0}$ for all $(a_1, a_2, a_3) \in \mathcal{H}$ and that $\prod_{j=1}^6 q_{1j} \mid q_1(a_1, a_2, a_3)$ with $\prod_{j=1}^6 q_{1j} \gg X^{\sum_{j=1}^6 \theta_{1j}}$. Therefore we must have that $(q_{21}, q_1(a_1, a_2, a_3)) = 1$. Since $\alpha_0 < 1/19$ by (6.4) and $q_{21}^2 \le X^{2\theta_{21}+2\tau_{21}} \le X^{1/4-7\alpha_0/8} \le \min(A_1, A_2, A_3)$ by (6.8) and (8.14), we deduce that

$$\begin{aligned} V_{21}(\mathcal{H}) &\ll X^\varepsilon \sum_{q_{21} \in [X^{\theta_{21}}, X^{\theta_{21}+\tau_{21}}]} \sum_{\substack{(a_1,a_2,a_3) \in \mathcal{H}' \\ q_{21}^2 \mid q_2(a_1,a_2,a_3)}} 1 \\ &\ll X^{-\theta_{21}+\varepsilon} A_1A_2A_3. \end{aligned}$$

We now consider $V_{1j}(\mathcal{H})$. As with $V_{21}(\mathcal{H})$, we can't have $q_{1j}^2|q_1(a_1,a_2,a_3)$ by size considerations and (6.6). Therefore if $q_{1i}^2|q(a_1,a_2,a_3)$ then $q_{1i}|(q_1(a_1,a_2,a_3),q_2(a_1,a_2,a_3))$, and so Lemma 5.13 shows that $P((a_2-c_3a_3)\overline{a_3})\equiv 0 \pmod{q_{1i}}$. Again, we have that $q_{1j}\leq \min(A_1,A_2,A_3)$. Thus we have

$$\begin{aligned}V_{1i}(\mathcal{H}) &\ll X^{\varepsilon}\sum_{q_{1i}\in[X^{\theta_{1i}},X^{\theta_{1i}+\tau_{1i}}]}\sum_{\substack{(a_2,a_3)\in[A_2,A_2(1+\eta_1)]\times[A_3,A_3(1+\eta_1)]\\ P((a_2-c_3a_3)\overline{a_3})\equiv 0 \pmod{q_{1i}}}}\sum_{\substack{a_1\in[A_1,A_1(1+\eta_1)]\\ q_{1i}|q_1(a_1,a_2,a_3)}}1\\ &\ll X^{-\theta_{1i}+\varepsilon}A_1A_2A_3.\end{aligned}$$

Finally, we are left to bound $V'(\mathcal{H})$. Each v counted in $V'(\mathcal{H})$ may factored as $v=v_1v_2v_3$, with

$$v_1:=\prod_{\substack{p|v\\ p^2|q_1(a_1,a_2,a_3)}}p,\qquad v_2:=\prod_{\substack{p|v/v_1\\ p^2|q_2(a_1,a_2,a_3)}}p,\qquad v_3:=\frac{v}{v_1v_2}.$$

Since v was squarefree, we see that v_1,v_2,v_3 are pairwise coprime and squarefree.

By Lemma 5.13 again, $P((a_2-c_3a_3)\overline{a_3})\equiv 0 \pmod{v_3}$. In $V'(\mathcal{H})$, v is coprime with all the q_{ij}, and so for any $a_1,a_2,a_3\in\mathcal{H}$

$$v_1^2v_3\ll\frac{q_1(a_1,a_2,a_3)}{\prod_{j=1}^5 q_{1j}}\ll X^{1+\alpha_0-\sum_{j=1}^5\theta_{1j}}<\eta_1A_2, \tag{8.19}$$

$$v_2^2v_3\ll\frac{q_2(a_1,a_2,a_3)}{q_{21}}\ll X^{(1+\alpha_0)/2-\theta_{21}}. \tag{8.20}$$

Thus we have

$$V'(\mathcal{H})\ll\sum_{\substack{s,d<Z\\ \mu^2(d)\mu^2(s)=1}}\sum_{w<Z^{10}}\frac{10^{\omega(w)}}{w}\sum_{\substack{v_1v_2v_3>Z^5\\ \mu^2(wv_1v_2v_3)=1}}\sum_{\substack{a_2\in[A_2,A_2(1+\eta_1)]\\ a_3\in[A_3,A_3(1+\eta_1)]\\ P((a_2-c_3a_3)\overline{a_3})\equiv 0 \pmod{v_3}}}\sum_{\substack{a_1\in[A_1,A_1(1+\eta_1)]\\ v_1^2v_3|q_1(a_1,a_2,a_3)\\ v_2^2v_3|q_2(a_1,a_2,a_3)}}1.$$

Let $d_1\in\mathbb{Z}[a_2,a_3]$ denote the discriminant of q_1 (viewing q_1 as a polynomial in a_1), and $d_2\in\mathbb{Z}[a_2,a_3]$ denote the discriminant of q_2. By Lemma 5.13, we see that the inner sum restricts a_1 to one of $O(6^{\omega(v_1v_2v_3)})$ residue classes modulo $v_1^2v_2^2v_3/(v_1,d_1(a_2,a_3))(v_2,d_2(a_2,a_3))$. Thus

$$\sum_{\substack{a_1\in[A_1,A_1(1+\eta_1)]\\ v_1^2v_3|q_1(a_1,a_2,a_3)\\ v_2^2v_3|q_2(a_1,a_2,a_3)}}1\ll 6^{\omega(v_1v_2v_3)}\Big(\frac{\eta_1A_1(v_1,d_1(a_2,a_3))(v_2,d_2(a_2,a_3))}{v_1^2v_2^2v_3}+1\Big). \tag{8.21}$$

Let $I_1=\{(1,3),(1,4),(2,3),(2,4)\}$ be the set of the indexes (i,j) such that (r_i,r_j) is involved in the factorisation of q_1. We note that

$$d_1(a_2,a_3)=\prod_{\substack{(i,j),(k,l)\in I_1\\ (i,j)\neq(k,l)}}(a_2(r_i+r_j-r_k-r_\ell)+a_3(r_i^2+r_ir_j+r_j^2-r_k^2-r_\ell^2-r_kr_\ell))$$

$$d_2(a_2,a_3)=-(a_2(r_1+r_2-r_3-r_4)+a_3(r_1^2+r_1r_2+r_2^2-r_3^2-r_3r_4-r_4^2))^2.$$

We remark that the coefficient in a_2^{12} in d_1 is non zero because we can't have $r_i + r_j - r_k - r_l = 0$ for two different $(i,j),(k,\ell) \in I_1$. The case $\{i,j\} \cap \{k,\ell\} \neq \emptyset$ is clear, the other case was noticed in Remark (ii) after the proof of Lemma 5.15.

For d_2, it may be the case that $r_1 + r_2 - r_3 - r_4 = 0$. However in this case we can't also have $r_1^2 + r_1 r_2 + r_2^2 - r_3^2 - r_3 r_4 - r_4^2 = 0$ since this would imply that $r_1 + r_2 = r_3 + r_4$ and $r_1 r_2 = r_3 r_4$ which is not possible when the roots of P are distinct. Thus either the coefficient of a_2 in d_2 is non-zero or the coefficient of a_3 is non-zero.

To estimate the sum over v_1, v_2, v_3, a_2, a_3 of the terms with $d_1(a_2,a_3), d_2(a_2,a_3)$ in (8.21), we write $w_i = (v_i, d_i(a_2,a_3))$ for $i = 1, 2$ and next forget the coprimality between v_i/w_i and $d_i(a_2,a_3)/w_i$. This sum is thus bounded by

$$\sum_{\substack{v_1v_2v_3 \geq Z^5 \\ v_1^2 v_3 \leq X^{1+\alpha_0-\sum_{j=1}^6 \theta_{1j}} \\ v_2^2 v_3 \leq X^{(1+\alpha_0)/2-\theta_{21}} \\ \mu^2(v_1v_2v_3)=1}} \frac{6^{\omega(v_1v_2v_3)}}{v_1^2 v_2^2 v_3} \sum_{\substack{w_1 | v_1 \\ w_2 | v_2}} w_1 w_2 \sum_{\substack{a_2 \in [A_2, A_2(1+\eta_1)] \\ a_3 \in [A_3, A_3(1+\eta_1)] \\ d_1(a_2,a_3) \equiv 0 \pmod{w_1} \\ d_2(a_2,a_3) \equiv 0 \pmod{w_2} \\ P((a_2 - c_3 a_3)\overline{a_3}) \equiv 0 \pmod{v_3}}} 1.$$

If the coefficient in a_2^2 in $d_2(a_2,a_3)$ is non zero, then the inner sum over a_2, a_3 is

$$\ll \eta_1 A_3 \Big(1 + \frac{\eta_1 A_2}{w_1 w_2 v_3}\Big) 12^{\omega(w_1w_2v_3)},$$

otherwise the condition $w_2 | d_2(a_2,a_3)$ is equivalent to $w_2 | d_P a_3$ for some $d_P \in \mathbb{Z}$ depending only of P (we recall that w_2 is square free) and thus the inner sum over a_2, a_3 is bounded by

$$\ll \Big(1 + \frac{\eta_1 A_3}{w_2}\Big)\Big(1 + \frac{\eta_1 A_2}{w_1 v_3}\Big) 12^{\omega(v_1v_2v_3)} \ll 12^{\omega(w_1w_2v_3)} \Big(1 + \frac{\eta_1 A_3}{w_2} + \frac{\eta_1 A_2}{w_1 v_3} + \frac{\eta_1^2 A_2 A_3}{w_1 w_2 v_3}\Big).$$

Finally we obtain that

$$\begin{aligned} V'(\mathcal{H}) &\ll Z^2 (\log Z)^{10} \sum_{\substack{v_1v_2v_3 \geq Z^5 \\ v_1^2 v_3 \leq X^{1+\alpha_0-\sum_{j=1}^6 \theta_{1j}} \\ v_2^2 v_3 \leq X^{(1+\alpha_0)/2-\theta_{21}} \\ \mu^2(v_1v_2v_3)=1}} 6^{\omega(v_1v_2v_3)} \Big[\eta_1^2 A_2 A_3 \\ &\quad + \sum_{\substack{w_1 | v_1 \\ w_2 | v_2}} \frac{12^{\omega(w_1w_2v_3)} \eta_1 A_1 w_1 w_2}{v_1^2 v_2^2 v_3^2} \Big(\eta_1 A_3 + \frac{\eta_1 A_2}{w_1 v_3} + \frac{\eta_1^2 A_2 A_3}{w_1 w_2 v_3}\Big)\Big] \\ &\ll Z^{-3} (\log Z)^{10} \eta_1^3 A_1 A_2 A_3 + Z^3 \frac{A_1 A_2 A_3}{\min(A_1, A_2, A_3)} X^{3(1+\alpha_0)/4 - \sum_{(i,j) \in I_{\mathcal{C}}} \theta_{ij}/2}. \end{aligned}$$

By (8.14) and (6.6) we see that $X^{3(1+\alpha_0)/4-\sum_{ij \in I_{\mathcal{C}}} \theta_{ij}/2} \leq \min(A_1, A_2, A_3) X^{-\epsilon}$. Putting everything together then gives the result. □

Lemma 8.6 (Removing $(a_2,a_3)/30 = 1$)**.** *Let $S_{05}(\mathcal{H})$ be as given in Lemma 8.5. Then we have*

$$S_{05}(\mathcal{H}) = S_{06}(\mathcal{H}) + O\Big(\frac{\eta_1^3 A_1 A_2 A_3}{Z}\Big),$$

where

$$S_{06}(\mathcal{H}) := \sum_{\substack{t\le Z^{50}\\ u\le Z^{20}\\ d\le Z\\ s_2s_3\le Z\\ (t,30)=1}} \mu(d)\mu(s_2s_3)\ell(u)\mu(t) \sum_{\substack{q_{ij}\in[X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]\\ \forall\,(i,j)\in I_{\mathcal{C}}\\ q_{21}\equiv 1 \pmod{D_{q_2}}}} \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{H}'\\ \prod_{j=1}^6 q_{1j}\mid q_1(a_1,a_2,a_3)\\ q_{21}\mid q_2(a_1,a_2,a_3)\\ [d,s_2s_3,u]\mid q(a_1,a_2,a_3)\\ d\mid q_3(a_1,a_2,a_3)\\ [t,s_2]\mid a_2\\ [t,s_3]\mid a_3\\ a_2,a_3\equiv 30 \pmod{900}\\ a_1\equiv 1 \pmod{30}}} 1.$$

Proof. Since we have $a_2, a_3 \equiv 30 \pmod{900}$, we can detect $(a_2, a_3)|30$ using Möbius inversion $\mathbf{1}_{(a_2,a_3)|30} = \sum_{\substack{t|(a_2,a_3)\\(t,30)=1}} \mu(t)$ and separately consider the contribution $S_{06}(\mathcal{H})$ from terms with $t \le Z^{50}$ and the contribution $U_5(\mathcal{H})$ from terms with $t > Z^{50}$. Since there are $O(1)$ choices of the q_{ij} given a choice of a_1, a_2, a_3, we see that

$$\begin{aligned} U_5(\mathcal{H}) &\ll \sum_{t>Z^{50}} \sum_{\substack{u\le Z^{20}\\ d,s_2s_3\le Z}} \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{H}'\\ t\mid(a_2,a_3)}} O(1)\\ &\ll Z^{30} \sum_{Z^{50}<t<\min(A_2,A_3)} \eta_1 A_1 \Big(\frac{\eta_1 A_2}{t}+1\Big)\Big(\frac{\eta_1 A_3}{t}+1\Big) \ll \frac{\eta_1^3 A_1A_2A_3}{Z}. \end{aligned}$$

This gives the result. □

8.4 Application of Theorem 4.1

Lemma 8.7 (Application of Theorem 4.1)**.** *Let $S_{06}(\mathcal{H})$ be as in Lemma 8.6. Then we have*

$$S_{06}(\mathcal{H}) \gg \eta_1^3 A_1A_2A_3.$$

Proof of Lemma 8.7 assuming Theorem 4.1. Recalling the definition of S_{06} from Lemma 8.6, we remark that the different conditions modulo 30 on a_1, a_2, a_3 imply that $(q(a_1, a_2, a_3), 30) = 1$ and thus we may impose that $(ds_2s_3tu, 30) = 1$. Splitting (a_1, a_2, a_3) into residue classes $\pmod{[t, u, d, s_2, s_3]}$, we see that

$$S_{06}(\mathcal{H}) = \sum_{\substack{t\le Z^{50}\\ u\le Z^{20}\\ d\le Z\\ s_2s_3\le Z\\ (ds_2s_3tu,30)=1}} \mu(d)\mu(s_2s_3)\ell(u)\mu(t) \sum_{\mathbf{u}_0\in\mathcal{S}(d,s_2,s_3,t,u)} S_{07}(\mathbf{u}_0,[d,s_2,s_3,t,u]), \tag{8.22}$$

where

$$S_{07}(\mathbf{u}_0,m) := \sum_{\substack{q_{ij}\in[X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]\\ \forall\,(i,j)\in I_{\mathcal{C}}\\ q_{21}\equiv 1 \pmod{D_{q_2}}}} \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{H}'\\ \prod_{j=1}^6 q_{1j}\mid q_1(a_1,a_2,a_3)\\ q_{21}\mid q_2(a_1,a_2,a_3)\\ (a_1,a_2,a_3)\equiv\mathbf{u}_0 \pmod{m}\\ a_2,a_3\equiv 30 \pmod{900},\ a_1\equiv 1 \pmod{30}}} 1,$$

$$\mathcal{S}(d,s_2,s_3,t,u) := \Big\{(u_1,u_2,u_3) \pmod{[d,s_2s_3,t,u]} :\ [d,s_2s_3,u]\mid q(u_1,u_2,u_3),\\ d\mid q_3(u_1,u_2,u_3),\ [s_2,t]\mid u_2,\ [s_3,t]\mid u_3\Big\}.$$

We now apply Theorem 4.1 on incomplete norms with $K = \mathbb{Q}(r_1 + r_3)$, $\nu_1 = 1$, $\nu_2 = r_1 + r_3$, $\nu_3 = r_1^2 + r_3^2 + r_1 r_3$ and ν_4 such that ν_4 is in the ring of integers of K and $(\nu_1, \nu_2, \nu_3, \nu_4)$ is a $\mathbb{Q}$-basis of K. By Theorem 4.1 (taking $X_i = A_i$, $\ell = 5$, $\ell' = 3$, $\theta_i = \theta_{1i}\frac{\log X}{\log A_1}$, $\theta_i' = (\theta_{1i} + \tau_{1i})\frac{\log X}{\log A_1}$, $\tau = \theta_{21}\frac{\log X}{\log A_1}$, $\tau' = (\theta_{21} + \tau_{21})\frac{\log X}{\log A_1}$), we have that

$$S_{07}(\mathbf{u}_0, m) = (1 + o(1))\frac{\eta_1^3 A_1 A_2 A_3}{30^5 m^3 \varphi(D_{q_2})} \prod_{(i,j)\in I_{\mathcal{C}}} \log\Big(1 + \tau_{ij}/\theta_{ij}\Big).$$

Here we have used the fact that (4.3) and (4.4) hold by (8.14). Similarly (4.6) holds by (6.3), (4.7) holds by (6.2), (4.8) holds by (6.5), (4.9) holds by (6.6), (4.10) holds by (6.7) and (4.11) holds by (6.8) and (6.9) and by noticing that $\frac{4}{1+\alpha_0} \le \frac{\log X}{\log A_1} \le \frac{4}{1+\alpha_0/2}$. Substituting this into our expression (8.22) for S_{06}, we find that

$$S_{06}(\mathcal{H}) = (1 + o(1))\frac{\eta_1^3}{30^5}\frac{A_1 A_2 A_3}{\varphi(D_{q_2})} \prod_{(i,j)\in I_{\mathcal{C}}} \log\Big(1 + \tau_{ij}/\theta_{ij}\Big) \sum_{m \le Z^{72}} \frac{L(m)}{m^3}, \tag{8.23}$$

where

$$L(m) := \sum_{\substack{d \le Z \\ s_2 s_3 \le Z \\ u \le Z^{20} \\ (ds_2 s_3 tu, 30) = 1 \\ t < Z^{50} \\ [d, s_2 s_3, t, u] = m}} \mu(d)\mu(s_2 s_3)\mu(t)\ell(u)|\mathcal{S}(d, s_2, s_3, t, u)|.$$

We wish to remove the upper bound constraints on d, s_2, s_3, u, t, m so we can understand $\sum_m L(m)/m^3$ via an Euler product. Let

$$L^*(m) := \sum_{\substack{[d,s,t,u] = m \\ (ds_2 s_3 tu, 30) = 1}} |\mu(d)\mu(s)\mu(t)\ell(u)| \sum_{s_2 s_3 = s} |\mathcal{S}(d, s_2, s_3, t, u)|,$$

$$\tilde{L}(m) := \sum_{\substack{[d,s,t,u] = m \\ (ds_2 s_3 tu, 30) = 1}} \mu(d)\mu(s)\mu(t)\ell(u) \sum_{s_2 s_3 = s} |\mathcal{S}(d, s_2, s_3, t, u)|,$$

which are multiplicative functions of m. We note that $L^*(m) \ge \max(|L(m)|, |\tilde{L}(m)|)$ for all m and that $\tilde{L}(m) = L(m)$ for $m \le Z$. From the support of μ, ℓ we have $L^*(p^k) = 0$ for $k \ge 3$. We easily check that $L^*(p) \le 2^5 p$ and $L^*(p^2) \le 3p^2$ for $p > q_0$ since $|\ell(p)| \le 2/(p-2)$ in this range. We deduce that $L^*(m)/m^3 \ll \tau(m)^5/m^2$. We note that $\tilde{L}(p^k) = 0$ for $k \ge 2$ and $2 \le p \le q_0$, and that $\tilde{L}(p^k) = 0$ for any $k \ge 1$ when $p = 2, 3, 5$. We find

$$\begin{aligned}\sum_{m \le Z^{72}} \frac{L(m)}{m^3} &= \sum_{m \le Z} \frac{\tilde{L}(m)}{m^3} + O\Big(\sum_{m > Z} \frac{L^*(m)}{m^3}\Big) \\ &= \sum_{m} \frac{\tilde{L}(m)}{m^3} + O\Big(\sum_{m > Z} \frac{\tau(m)^5}{m^2}\Big) \\ &= \prod_{7 \le p \le q_0} \Big(1 + \frac{\tilde{L}(p)}{p^3}\Big) \prod_{p > q_0} \Big(1 + \frac{\tilde{L}(p)}{p^3}\Big) + O\Big(\frac{1}{Z^{1/2}}\Big).\end{aligned}$$

From our bounds on L^* we see that $\prod_{p>q_0}(1+\tilde{L}(p)/p^3) \gg 1$ and the product over $p \le q_0$ converges. We wish to show that the product converges to a strictly positive constant, and so need to check that $1+\tilde{L}(p)/p^3$ doesn't vanish for some small prime p with $7 \le p \le q_0$. If $p|[d,s_2,s_3]$ then for $u=1$ or p, we have

$$|\mathcal{S}(d,s_2,s_3,u,1)| = |\mathcal{S}(d,s_2,s_3,u,p)|.$$

Since $\ell(p)+\ell(1)=0$ when $7 \le p \le q_0$, we deduce

$$\sum_{[d,s_2,s_3]=p} \sum_{[d,s_2,s_3,t,u]=p} \mu(d)\mu(s_2s_3)\mu(t)\ell(u)|\mathcal{S}(d,s_1,s_2,t,u)| = 0.$$

The value $\tilde{L}(p)$ is then

$$\tilde{L}(p) = 1-p-|\{(u_1,u_2,u_3) \pmod p : p|q(u_1,u_2,u_3)\}|.$$

Then

$$1+\tilde{L}(p)/p^3 \ge (p^3-6p^2-p+1)/p^3 > 0,$$

when $p \ge 7$. Thus $\sum_{m \le Z^{72}} L(m)/m^3 \gg 1$, and so substituting this into (8.23) and using the fact $\tau_{ij}/\theta_{ij} \gg 1$ we obtain the result. □

8.5 Proof of Proposition 3.2

Proof of Proposition 3.2 assuming Theorem 4.1. By Lemmas 8.1, 8.2, 8.3, 8.4, 8.5, 8.6 and 8.7 in turn, we see that

$$S_0 \gg \frac{1}{\log X} \sum_{\mathcal{H} \in \mathscr{H}_{\mathcal{R}}} \frac{A_0A_1A_2A_3\eta_1^4}{\widetilde{N}_P(A_0,A_1,A_2,A_3)} + O\Big(\frac{1}{Z^{1/2}}\Big).$$

(Note that in this application of Lemma 8.7 we are assuming Theorem 4.1, and that we have $12\theta_0+22\alpha_0<1$ required for Lemma 8.1 since we are taking θ_0 sufficiently small and assuming that α_0 satisfies (6.4).) We note that

$$\sum_{\mathcal{H} \in \mathscr{H}_{\mathcal{R}}} \frac{A_0A_1A_2A_3\eta_1^4}{\widetilde{N}_P(A_0,A_1,A_2,A_3)} = \sum_{\mathcal{H} \subset \mathcal{R}} \frac{A_0A_1A_2A_3\eta_1^4}{\widetilde{N}_P(A_0,A_1,A_2,A_3)} - \sum_{\substack{\mathcal{H} \subset \mathcal{R} \\ \mathcal{H} \text{ bad}}} \frac{A_0A_1A_2A_3\eta_1^4}{\widetilde{N}_P(A_0,A_1,A_2,A_3)}.$$

If $\mathcal{H}$ is bad, then $\max(A_1,A_2,A_3)^4\eta_1^{1/10} \ge q_1(A_1,A_2,A_3)$ or there exists $i \in \{0,1,2,3\}$ such that $|A_i| < \eta_1 \max(|A_0|,|A_1|,|A_2|,|A_3|)$. The first inequality implies that there exists $(i,j) \in I_{\mathcal{C}}$ such that

$$L_{i,j}(A_1,A_2,A_3) := |A_1+(r_i+r_j)A_2+(r_i^2+r_ir_j+r_j^2)A_3| \ll \eta_1^{1/40}\max(A_1,A_2,A_3).$$

Thus, by partial summation

$$\begin{aligned}\sum_{\substack{\mathcal{H} \subset \mathcal{R} \\ \mathcal{H} \text{ bad}}} \frac{A_0A_1A_2A_3\eta_1^4}{\widetilde{N}_P(A_0,A_1,A_2,A_3)} &\ll \sum_{(i,j)\in I_{\mathcal{C}}} \sum_{A=2^\ell \atop X^{1-\frac{7\alpha_0}{8}} \ll A \ll X^{\frac{1+\alpha_0}{4}}} \sum_{\substack{(a_0,a_1,a_2,a_3)\in\mathcal{R} \\ L_{i,j}(a_1,a_2,a_3)\le \eta_1^{1/40}A \\ \max(a_0,a_1,a_2,a_3)\ll A}} \frac{1}{A^4} \\ &\quad + \sum_{i=0}^{3} \sum_{A=2^\ell \atop X^{1-\frac{7\alpha_0}{8}} \ll A \ll X^{\frac{1+\alpha_0}{4}}} \sum_{\substack{(a_0,a_1,a_2,a_3)\in\mathcal{R} \\ a_i \le \eta_1 A \\ \max(a_0,a_1,a_2,a_3)\ll A}} \frac{1}{A^4} \\ &\ll \eta_1^{1/40}\log X.\end{aligned}$$

Similarly, we find by partial summation

$$\sum_{\mathcal{H}\subset\mathcal{R}} \frac{A_0A_1A_2A_3\eta_1^4}{\widetilde{N}_P(A_0,A_1,A_2,A_3)} = (1+o(1)) \sum_{(a_0,a_1,a_2,a_3)\in\mathcal{R}} \frac{1}{\widetilde{N}_P(a_0,a_1,a_2,a_3)}$$
$$\gg \log X.$$

Putting everything together now gives Proposition 3.2. □

Thus we are left to establish Theorem 4.1.

9 Incomplete norm forms

In this section we perform our initial reductions to reduce the proof of Theorem 4.1 to that of establishing Proposition 9.13 and Proposition 9.14. We roughly follow the argument of [14] in this section, but require a number of small technical modifications.

Let K be a quartic number field, $\mathcal{O}_K$ its integer ring, Cl_K its class group. Let $\nu_1,\nu_2,\nu_3,\nu_4 \in \mathcal{O}_K$ such that $\mathbf{v} = (\nu_1,\nu_2,\nu_3,\nu_4)$ is a $\mathbb{Q}$-basis of K. We suppose for convenience that $\nu_1 = 1$ and $K = \mathbb{Q}(\nu_2)$. We then define $\mathcal{O}_{\mathbf{v}} = \mathbb{Z}[\nu_1,\nu_2,\nu_3,\nu_4]$ the order generated by $\mathbf{v}$.

We let $N(\cdot) = N_K(\cdot)$ be the norm on K, and note that this is a different norm to N_P on $\mathbb{Q}(r_1)$ encountered earlier.

There exists an integral basis of $\mathcal{O}_K$, $\mathbf{w} = (\omega_1,\omega_2,\omega_3,\omega_4)$ and some integers w_{ij}, $1 \le i \le j \le 4$, such that

$$\nu_j = \sum_{i=1}^{j} w_{ij}\omega_i \quad (j = 1,2,3,4). \tag{9.1}$$

(cf. for example [16, Proposition 2.11]).

9.1 From $\mathcal{O}_K$ to $\mathcal{O}_{\mathbf{v}}$ and vice-versa

We denote by $L_{\mathbf{wv}} = (w_{ij})_{1\le i,j\le 4}$ the matrix of $\mathbf{v}$ in $\mathbf{w}$ so that for all $1 \le j \le 4$, $\nu_j = \sum_{i=1}^4 w_{ij}\omega_i$.

By (9.1) this matrix is upper triangular and the absolute value of its determinant is

$$W = |w_{11}w_{22}w_{33}w_{44}| \in \mathbb{Z}^* \tag{9.2}$$

Lemma 9.1. *For all $\alpha \in \mathcal{O}_K$, there exist $a_1,a_2,a_3,a_4 \in \mathbb{Z}$, with*

$$\alpha = \frac{1}{W}\sum_{i=1}^{4} a_i\nu_i$$

Conversely, there exists a subset $\mathcal{V}_0 \subset \{0,\dots,W-1\}^4$ such that for all $\mathbf{a} \in \mathbb{Z}^4$ we have

$$\frac{1}{W}\sum_{i=1}^{4} a_i\nu_i \in \mathcal{O}_K \Leftrightarrow \exists \mathbf{u} \in \mathcal{V}_0 : \mathbf{a} \equiv \mathbf{u} \pmod{W}.$$

Proof. Let $\alpha \in \mathcal{O}_K$. There exist $(a_1, a_2, a_3, a_4) \in \mathbb{Z}^4$ and $(a_1', a_2', a_3', a_4') \in \mathbb{Q}^4$ such that $\alpha = \sum_{i=1}^4 a_i\omega_i = \sum_{i=1}^4 a_i'\nu_i$. With our previous notation,

$$\begin{pmatrix} a_1' \\ a_2' \\ a_3' \\ a_4' \end{pmatrix} = (L_{\mathbf{wv}})^{-1} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}.$$

The matrix $(L_{\mathbf{wv}})^{-1}$ is of type $\frac{1}{W}(w_{ij}')_{1\le i,j\le 4}$ where the coefficients w_{ij}' are integers. This implies the first part of the lemma.

The second part of the lemma is also a direct consequence of the change of basis formula. With our previous notation we have

$$\sum_{j=1}^4 a_j\nu_j = \sum_{i=1}^4 \Big(\sum_{j=1}^4 w_{ij}a_j\Big)\omega_i.$$

Then for any $\mathbf{a} = (a_1, a_2, a_3, a_4) \in \mathbb{Z}^4$, $\frac{1}{W}\sum_{i=1}^4 a_i\nu_i \in \mathcal{O}_K$ if and only if for all $1 \le i \le 4$, we have

$$\sum_{j=1}^4 w_{ij}a_j \equiv 0 \pmod{W}.$$

The set $\mathcal{V}_0$ is the the subset of $\{0, \dots, W-1\}^4$ formed by all the solutions of these congruences. □

Lemma 9.2. *Let $\mathfrak{a}$ be a principal ideal. Then there is a generator α of $\mathfrak{a}$ such that*

$$|\alpha^\sigma| \ll N(\mathfrak{a})^{1/4}$$

for all embeddings $\sigma : K \hookrightarrow \mathbb{C}$. Furthermore there exists $W > 0$ depending only on $\mathbf{v}$ such that

$$\alpha = \frac{1}{W}\sum_{i=1}^4 a_i\nu_i$$

for some integers $a_i \ll N(\mathfrak{a})^{1/4}$.

Proof. The first part is a particular case of [14, Lemma 4.3]. The last part follows also from this lemma combined with Lemma 9.1. □

Lemma 9.3. *Let $\mathcal{C}$ be an hypercube of side length $\delta_0 B$ which contains a point $\mathbf{b}_0 \in \mathbb{Z}^4$ such that $\|\mathbf{b}_0\| \ll B$. We suppose that $\mathfrak{b}_0 = (W^{-1}\sum_{i=1}^4 (\mathbf{b}_0)_i\nu_i)$ is an integral ideal whose norm satisfies $N(\mathfrak{b}_0) = B_0^4 \gg B^4$. Let q such that $W|q$ and $10qW \le \delta_0 B$.*

Then there exists a set $\mathcal{W}(\mathbf{b}_0)$ of W^4 elements $\beta_0' \in \mathcal{O}_K$ with $\beta_0' = W^{-1}\sum_{i=1}^4 (\mathbf{b}_0')_i\nu_i$ and with $\mathbf{b}_0' \in \mathcal{C}$, such that for all $\mathbf{b} \in \mathcal{C}$, $\mathbf{b} \equiv \mathbf{b}_0 \pmod q$ if and only if $\beta = \frac{1}{W}\sum_{i=1}^4 b_i\nu_i \in \mathcal{O}_K$ and there exists $\beta_0' \in \mathcal{W}(\mathbf{b}_0)$ with $\beta \equiv \beta_0' \pmod q$.

Proof. This is variant of an argument used in the proof of [14, Lemma 9.4].

Let $\beta_0 := \frac{1}{W}\sum_{i=1}^4 (\mathbf{b}_0)_i\nu_i$. For all $\mathbf{v} = (v_1, \dots, v_4) \in \{0, \dots, W-1\}^4$, there exists $\mathbf{u} = \mathbf{u}(\mathbf{b}_0, \mathbf{v}) \in \mathbb{Z}^4$ such that $\mathbf{b}_0 + q(\mathbf{v} + W\mathbf{u}) \in \mathcal{C}$ since $qW \le \delta_0 B$, the side length of $\mathcal{C}$. We will prove that the set

$$\mathcal{W} := \Big\{\beta_0' = \frac{1}{W}\sum_{i=1}^4 b_i'\nu_i \text{ with } \mathbf{b}' = \mathbf{b}_0 + q(\mathbf{v} + W\mathbf{u}(\mathbf{b}_0, \mathbf{v})), \mathbf{v} \in \{0, \dots, W-1\}^4\Big\}$$

satisfies the conclusion of the lemma.

First we suppose that $\mathbf{b} \equiv \mathbf{b}_0 \pmod q$. This implies that there exist four integers m_1, m_2, m_3, m_4 such that $b_i = (\mathbf{b}_0)_i + qm_i$. We get

$$\beta := \frac{1}{W}\sum_{i=1}^4 \mathbf{b}_i\nu_i = \frac{1}{W}\sum_{i=1}^4 ((\mathbf{b}_0)_i + m_iq)\nu_i = \beta_0 + \frac{q}{W}\sum_{i=1}^4 m_i\nu_i.$$

Since $W|q$, this implies that $\beta \in \mathcal{O}_K$. If we choose $\beta_0' = \beta_0 + \frac{q}{W}\sum_{i=1}^4 v_i\nu_i +$ with $0 \le v_1, \dots, v_4 < W$ such that $v_i \equiv m_i \pmod W$ then we would have $\beta = \beta_0' + \frac{q}{W}\sum_{i=1}^4 (m_i - v_i + Wu_i)\nu_i$, and thus $\beta \equiv \beta_0' \pmod q$.

Now we prove the reciprocal assertion. We suppose that there exists $\beta_0' \in \mathcal{W}$ such that $\beta \equiv \beta_0' \pmod q$. Then $\beta = \beta_0' + q\gamma$ for some $\gamma \in \mathcal{O}_K$. There exists $g_1, g_2, g_3, g_4 \in \mathbb{Z}$ such that $\gamma = \frac{1}{W}\sum_{i=1}^4 g_i\nu_i$. For each $i = 1, 2, 3, 4$, we have $\frac{b_i}{W} = \frac{(\mathbf{b}_0)_i + q(v_i + Wu_i + g_i)}{W}$. This implies that $\mathbf{b} \equiv \mathbf{b}_0 \pmod q$. □

For any ideal $\mathfrak{d}$ of $\mathcal{O}_K$, we define the function $\varrho_{\mathbf{v}}$ by

$$\varrho_{\mathbf{v}}(\mathfrak{d}) := \frac{|\{\mathbf{a} \in [1, N(\mathfrak{d})]^3 : \mathfrak{d} | (a_1\nu_1 + a_2\nu_2 + a_3\nu_3)\}|}{N(\mathfrak{d})^2}. \tag{9.3}$$

This function satisfies the following properties.

Lemma 9.4. *1. For all degree one prime ideals $\mathfrak{p}$ with $(N(\mathfrak{p}), W) = 1$, we have $\varrho_{\mathbf{v}}(\mathfrak{p}) = 1$.*

2. We have

$$\Big|\Big\{\mathbf{x} \in [1, p^2]^3 : p^2 | N\Big(\sum_{i=1}^3 x_i\nu_i\Big)\Big\}\Big| \ll p^4.$$

3. For any ideal $\mathfrak{e}$ such that $N(\mathfrak{e})$ is a power of p, we have

$$\frac{\varrho_{\mathbf{v}}(\mathfrak{e})}{N(\mathfrak{e})} \ll \frac{1}{p^2}$$

unless $\mathfrak{e}$ is a degree 1 prime ideal above p.

4. For any ideals $\mathfrak{a}, \mathfrak{b}$, $\varrho_{\mathbf{v}}(\mathfrak{ab}) = \varrho_{\mathbf{v}}(\mathfrak{a})\varrho_{\mathbf{v}}(\mathfrak{b})$ if $(N(\mathfrak{a}), N(\mathfrak{b})) = 1$.

5. For $k \ge 3$, we have

$$\Big|\Big\{\mathbf{x} \in [1, p^k]^3 : p^k | N\Big(\sum_{i=1}^3 x_i\nu_i\Big)\Big\}\Big| \ll kp^{11k/4}.$$

Proof. The first four assertions are essentially given by [14, Lemma 7.7], except that they work with a basis $\nu_1, \nu_2, \nu_3, \nu_4$ in place of $1, \theta, \theta^2, \theta^3$ which has a negligible effect on the proof. Indeed, by (9.1) the $\mathbb{Q}$-vector space spanned by ν_1, ν_2, ν_3 is the same as the one spanned by $\omega_1, \omega_2, \omega_3$, and the change-of-basis matrix between the basis $\nu_1, \nu_2, \nu_3, \nu_4$ and $\omega_1, \omega_2, \omega_3, \omega_4$ has determinant W. Thus when $(N(\mathfrak{d}), W) = 1$ we have

$$\varrho_{\mathbf{v}}(\mathfrak{d}) = \frac{|\{\mathbf{a} \in [1, N(\mathfrak{d})]^3 : \mathfrak{d} | (a_1\omega_1 + a_2\omega_2 + a_3\omega_3)\}|}{N(\mathfrak{d})^2},$$

and so it is sufficient to prove these four statements with the basis $\mathbf{w}$ in place of $\mathbf{v}$. The proof is then the same as in [14].

We are left to establish assertion 5. Since $N(\nu_1) \neq 0$, for any choice of x_2, x_3, $g_{x_2,x_3}(x_1) := N(x_1\nu_1 + x_2\nu_2 + x_3\nu_3)$ is a non-zero polynomial of degree 4 in x_1. Thus, given x_2, x_3, if $N(x_1\nu_1 + x_2\nu_2 + x_3\nu_3) \equiv 0 \pmod{p^k}$, we see that $\|x_1 - \alpha\|_p \ll p^{-k/4}$ for one of the 4 roots α of g_{x_2,x_3} over $\overline{\mathbb{Q}_p}$. Thus there are $O(p^{3k/4})$ choices of $x_1 \in [1, p^k]$ for each choice of x_2, x_3. This gives the result. □

Let γ_K be the residue in $s = 1$ of ζ_K and we define $\tilde{\mathfrak{S}}$ to be the Euler product[5]

$$\tilde{\mathfrak{S}} := \prod_{\mathfrak{P}} \Big(1 - \frac{\varrho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\Big)\Big(1 - \frac{1}{N(\mathfrak{P})}\Big)^{-1}. \tag{9.4}$$

Lemma 9.5. *There exists a constant $c > 0$ such that for any ideal $\mathfrak{I}$ of $\mathcal{O}_K$, $m \in \mathbb{N}$, $R \geq 2$ we have*

$$\sum_{\substack{N(\mathfrak{d}) < R \\ (\mathfrak{d}, \mathfrak{I}) = 1 \\ (N(\mathfrak{d}), m) = 1}} \frac{\mu(\mathfrak{d})\varrho_{\mathbf{v}}(\mathfrak{d})}{N(\mathfrak{d})} \log \frac{R}{N(\mathfrak{d})} = \frac{\tilde{\mathfrak{S}}}{\gamma_K} \prod_{\mathfrak{P} | (m)\mathfrak{I}} \Big(1 - \frac{\varrho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\Big)^{-1} + O\Big(2^{4\omega((m)\mathfrak{I})} \exp(-c\sqrt{\log R})\Big).$$

Proof. The proof is exactly the same as in [14, Lemma 8.5]. [14, Lemma 8.5] states the result with $N(J)^{o(1)}$ in place of $2^{4\omega(J)}$, but following the proof we see that the error term can be taken as $\exp(-c\sqrt{\log R}) \prod_{\mathfrak{P} | J} (1 - \frac{1}{N(\mathfrak{P})^{3/4}})^{-1}$, which is clearly sufficient for our slightly stronger bound. □

Lemma 9.6. *For any $2 \leq R \leq x$ we have*

$$\sum_{N(\mathfrak{d}) \leq R} \mu^2(\mathfrak{d}) \sum_{N(\mathfrak{J}) \leq x} \frac{\varrho_{\mathbf{v}}(\mathfrak{d}\mathfrak{J})}{N(\mathfrak{d}\mathfrak{J})} \ll (\log x)^8.$$

Proof. By Rankin's trick, we have

$$\sum_{N(\mathfrak{d}) \leq R} \mu^2(\mathfrak{d}) \sum_{N(\mathfrak{J}) \leq x} \frac{\varrho_{\mathbf{v}}(\mathfrak{d}\mathfrak{J})}{N(\mathfrak{d}\mathfrak{J})} \leq \prod_{N(\mathfrak{P}) \leq x} \Big(1 + 2\sum_{k \geq 1} \frac{\varrho_{\mathbf{v}}(\mathfrak{P}^k)}{N(\mathfrak{P}^k)}\Big).$$

By Lemma 9.4, if $\mathfrak{P}$ is a degree 1 prime ideal above p then the term in parentheses is $1 + 2/p + O(1/p^2)$, and if $\mathfrak{P}$ is of degree more than 1 above p then this is $1 + O(1/p^2)$. The result now follows from the Prime Ideal Theorem. □

[5]This definition of $\tilde{\mathfrak{S}}$ is slightly different as the one given in [14]. In the present paper $\tilde{\mathfrak{S}}$ doesn't depend on some modulus q^* or m.

9.2 Multiplication in $\mathcal{O}_{\mathbf{v}}$

Definition. *For any vectors $\mathbf{d}, \mathbf{e} \in \mathbb{Z}^4 \setminus \{\mathbf{0}\}$, we define $\mathbf{d} \diamond \mathbf{e}$ as be the vector $\mathbf{b} \in \mathbb{Q}^4$ such that*

$$\sum_{i=1}^{4} b_i \nu_i = \sum_{i=1}^{4} d_i \nu_i \times \sum_{i=1}^{4} e_i \nu_i$$

For $1 \leq i \leq 4$ we denote by $(\mathbf{d} \diamond \mathbf{e})_i$ the coordinate b_i.

This operation is helpful to detect the elements of $\mathcal{O}_{\mathbf{v}}$ with a fourth coordinate equal to zero. The following lemma turns the problem of detecting this zero coordinate into a question about lattices.

Lemma 9.7. *For any $\mathbf{d} \in \mathbb{Z}^4 \setminus \{\mathbf{0}\}$ let $\Lambda_{\mathbf{d}}$ be the subset of $\mathbb{Z}^4$ defined by*

$$\Lambda_{\mathbf{d}} = \{\mathbf{e} \in \mathbb{Z}^4 : (\mathbf{d} \diamond \mathbf{e})_4 = 0\}.$$

Then $\Lambda_{\mathbf{d}}$ is a lattice of rank 3 and $\det(\Lambda_{\mathbf{d}}) \ll \|\mathbf{d}\|/D$,where D is the GCD of the components of $\mathbf{d}$.

Proof. The argument is essentially a special case of [14, Lemma 7.2] . We will expose it in a more pedestrian way. First we suppose that $D = 1$. For all $1 \leq i, j \leq 4$ there exist rational numbers $\lambda_{i,j,k}$, $1 \leq k \leq 4$ such that

$$\nu_i \nu_j = \sum_{k=1}^{4} \lambda_{ijk} \nu_k.$$

For all $\mathbf{d}, \mathbf{e} \in \mathbb{Z}^4$,

$$\sum_{i=1}^{4} (\mathbf{d} \diamond \mathbf{e})_i \nu_i = \sum_{k=1}^{4} \Big(\sum_{i,j=1}^{4} \lambda_{ijk} d_i e_j \Big) \nu_k$$

Identifying the fourth coordinate, we deduce for all $\mathbf{d} \in \mathbb{Z}^4 \setminus \{\mathbf{0}\}$,

$$\Lambda_{\mathbf{d}} = \Big\{ \mathbf{e} \in \mathbb{Z}^4 : \sum_{j=1}^{4} \Big(\sum_{i=1}^{4} \lambda_{ij4} d_i \Big) e_j = 0 \Big\}.$$

The terms $\sum_{i=1}^{4} \lambda_{ij4} d_i$, for $j = 1, 2, 3, 4$ correspond to the coefficients of the fourth row of the matrix in basis $\mathbf{v}$ of the multiplication by $d = d_1\nu_1 + d_2\nu_2 + d_3\nu_3 + d_4\nu_4$. Since $\mathbf{d} \neq \mathbf{0}$, this matrix is invertible and at least one of these coefficients is non zero. This shows that $\Lambda_{\mathbf{d}}$ has rank 3. By [7], the determinant of Λ_{d} is equal to the determinant of the dual lattice that is for us the lattice spanned by the vector

$$T(\mathbf{d}) := \begin{pmatrix} \sum_{i=1}^{4} \lambda_{i14} d_i \\ \sum_{i=1}^{4} \lambda_{i24} d_i \\ \sum_{i=1}^{4} \lambda_{i34} d_i \\ \sum_{i=1}^{4} \lambda_{i44} d_i \end{pmatrix}. \tag{9.5}$$

Since the components of this vector have size $O(\max_{1 \leq i \leq 4} |d_i|)$, $\det(\Lambda_d) \ll \|\mathbf{d}\|$. This ends the proof in the case $D = 1$. In the case $D > 1$, we observe that $\Lambda_{\mathbf{d}} = \Lambda_{\frac{\mathbf{d}}{D}}$, and we can apply the previous case.

□

Lemma 9.8. *For any $m \in \mathbb{N}$ and $X \geq 3$, we have*

$$\sum_{\max(|x_1|,|x_2|,|x_3|)\ll X} \tau\Big(\sum_{i=1}^{3} x_i\nu_i\Big)^m \ll X^3(\log X)^{O_m(1)}.$$

Proof. The proof is the same as that of [14, Lemma 4.2] which concerns the case $\nu_i = \theta^{i-1}$. The only place where this change could have an importance is for the bound of the sums with any $\mathfrak{d}$ such that $N(\mathfrak{d}) \ll X^{1/n}$

$$\sum_{\substack{\max(|x_1|,|x_2|,|x_3|)\ll X \\ \mathfrak{d}|(\sum_{i=1}^{3} x_i\nu_i)}} 1.$$

Since the ν_i are linear combinations of some θ^j, $j = 0, 1, 2, 3$ for θ such that $K = \mathbb{Q}(\theta)$, the condition $\mathfrak{d}|(\sum_{i=1}^{3} x_i\nu_i)$ can be split in the x_i into arithmetic progression $\pmod{N(\mathfrak{d})}$, and thus the argument of [14] combined with Lemma 9.4 apply also in our case. □

Lemma 9.9. *Let $\mathbf{d} \in \mathbb{Z}^4 \setminus \{\mathbf{0}\} \cap [-D, D]^4$ and $\Lambda_{\mathbf{d}}$ as in Lemma 9.7. Let $\mathbf{z}_1(\mathbf{d})$ denote a shortest non-zero vector in $\Lambda_{\mathbf{d}}$. Then we have $\|\mathbf{z}_1(\mathbf{d})\| \ll D^{1/3}$ and*

$$|\{\mathbf{d} \in [1, D]^4 : \|\mathbf{z}_1(\mathbf{d})\| \leq Z\}| \ll D^{3+o(1)}Z^3.$$

Furthermore we have

$$\sum_{\|\mathbf{d}\|\leq D} \frac{1}{\|\mathbf{z}_1(\mathbf{d})\|^2} \ll D^{10/3+o(1)}.$$

Proof. The proof is exactly the same as the proof of [14, Lemma 7.3] except that we have a slightly different definition for $\diamond$, and so require Lemmas 9.7 and 9.8 instead of [14, Lemma 4.2] and [14, Lemma 7.2]. □

Lemma 9.10. *Let $\mathfrak{d}$ be an ideal of $\mathcal{O}_K$ with $(N(\mathfrak{d}), q) = 1$. Let $\mathcal{R} \subset [-X, X]^3$ as in the Proposition 9.11 below. Then we have*

$$|\{\mathbf{a} \in \mathbb{Z}^3 \cap \mathcal{R} : \mathfrak{d}|\big(\sum_{i=1}^{3} a_i\nu_i\big),\ \mathbf{a} \equiv \mathbf{a}_0 \pmod q\}| = \frac{\varrho_{\mathbf{v}}(\mathfrak{d})\,\mathrm{vol}\,(\mathcal{R})}{N(\mathfrak{d})q^3} + O(N(\mathfrak{d})^4X^2).$$

Proof. The proof is identical as the proof of [14, Lemma 7.4] with $\mathbf{v}$ in place of $(1, \dots, \theta^{n-1})$. In fact, the arguments of [14] give a slightly stronger error term of $O(X^2\varrho_{\mathbf{v}}(N(\delta))(qN(\delta))^{-2} + \varrho_{\mathbf{v}}(N(\delta)))$. □

9.3 Sums of Type I

We now state a similar result to [14, Proposition 7.5]

Proposition 9.11. *Let $\mathcal{R} \subset [-X, X]^3$ be a region such that any line parallel to the coordinate axes intersects $\mathcal{R}$ in $O(1)$ intervals. For any given $\mathbf{u}_0 \in \mathbb{Z}^3$ and $q \leq \sqrt{X}$ we define*

$$\Gamma = \Big\{\sum_{i=1}^{3} a_i\nu_i : \mathbf{a} \in \mathbb{Z}^3 \cap \mathcal{R},\ \mathbf{a} \equiv \mathbf{u}_0 \pmod q\Big\}.$$

Let $\Gamma_{\mathfrak{d}} = \{\kappa \in \Gamma : \mathfrak{d}|(\kappa)\}$. Then we have

$$\sum_{\substack{N(\mathfrak{d})\in[D,2D]\\(N(\mathfrak{d}),q)=1}} \left| |\Gamma_{\mathfrak{d}}| - \frac{\varrho_{\mathbf{v}}(\mathfrak{d})\,\mathrm{vol}\,(\mathcal{R})}{q^3 N(\mathfrak{d})} \right| \ll X^2 q^{1+o(1)} D^{1/3+o(1)} + Dq^{4+o(1)}. \quad (9.6)$$

Proof. We follow the proof of [14, Proposition 7.5], but now we work with a general order $\mathcal{O}_{\mathbf{v}}$ in place of $\mathbb{Z}[\theta]$. This involves minor modifications at the beginning of the argument; the last steps require no modification. For brevity we emphasise just the key points requiring modification and only sketch the rest of the argument.

We split the summation on the ideals $\mathfrak{d}$ according to their class in Cl_K. Let $\mathcal{C}$ be a given class and consider the contribution of all the $\mathfrak{d} \in \mathcal{C}$. Since the $\mathfrak{d}$ in the summation in (9.6) are coprime with q, we can fix a representative integral ideal $\mathfrak{c} \in \mathcal{C}$ such that $(N(\mathfrak{c}), q) = 1$ and with $N(\mathfrak{c}) = q^{o(1)}$. The ideal $\mathfrak{d}\mathfrak{c}^{-1}(N(\mathfrak{c}))$ is a principal ideal of $\mathcal{O}_K$. By Lemma 9.2 we can find a generator of the form $\delta = \frac{1}{W}\sum_{i=1}^4 d_i\nu_i$ where the d_i are integers such that $|d_i| \ll D^{1/n}q^{o(1)}$. Then $\delta_{\mathfrak{c}} := \frac{1}{WN(\mathfrak{c})}\sum_{i=1}^4 d_i\nu_i$ is a generator of the principal fractional ideal $\mathfrak{d}\mathfrak{c}^{-1}$. In [14] it is proved that $|\sigma_0(\delta_{\mathfrak{c}})| \gg D^{1/4}q^{o(1)}$ for all embeddings σ_0.

Let $\alpha \in \Gamma_{\mathfrak{d}}$, so $(\alpha) = \mathfrak{a}'\mathfrak{d}$ for some integral ideal $\mathfrak{a}'$. Since $(\alpha) = \mathfrak{a}'\mathfrak{c}\mathfrak{d}\mathfrak{c}^{-1}$ and (α) and $\mathfrak{d}\mathfrak{c}^{-1} = (\delta_{\mathfrak{c}})$ are principal, $\mathfrak{a}'\mathfrak{c}$ is principal too, so $\mathfrak{a}'\mathfrak{c} = (\beta)$ for some generator $\beta \in \mathcal{O}_K$. By Lemma 9.1, we can take $\beta = \frac{1}{W}\sum_{i=1}^4 b_i\nu_i$ where $\mathbf{b} = (b_1, b_2, b_3, b_4) \in \mathbb{Z}^4$ satisfies $(\mathbf{b} \pmod W) \in \mathcal{V}_0$. Then $(\alpha) = (\beta)(\delta_{\mathfrak{c}})$. Let $\mathbf{d} = (d_1, d_2, d_3, d_4)$. We have $W^2N(\mathfrak{c})\beta\delta_{\mathfrak{c}} = \sum_{k=1}^4(\mathbf{d}\diamond\mathbf{b})_k\nu_k$.

$$\beta\delta_{\mathfrak{c}} = \sum_{k=1}^4 \frac{1}{W^2N(\mathfrak{c})}\Big(\sum_{i,j=1}^4 \ell_{i,j,k}b_id_i\Big)\nu_k.$$

The coefficient of ν_i are integers if and only b_1, b_2, b_3, b_4 satisfy some congruences modulo $W^2N(\mathfrak{c})$. We also need to impose that $\mathfrak{c}|(\beta)$. This is also equivalent to some congruences conditions modulo $W^2N(\mathfrak{c})$ for b_1, b_2, b_3, b_4. Let $q_1 = [q, W^2N(\mathfrak{c})]$ and $\mathcal{V}_0' \subset \{0\ldots, q_1 - 1\}^4$ the set of r classes satisfying all these conditions and furthermore such that

$$(\mathbf{d}\diamond\mathbf{b})_4 \equiv 0 \pmod{q_1} \text{ and } \frac{(\mathbf{d}\diamond\mathbf{b})_i}{W^2N(\mathfrak{c})} \equiv (\mathbf{u}_0)_i \pmod q \text{ for } 1 \le i \le 3.$$

Thus, for $\mathfrak{d} \in \mathcal{C}$, we are interested in

$$|\Gamma_{\mathfrak{d}}| = \sum_{\mathbf{b}_0\in V_0'} \sum_{\substack{\mathbf{b}\in\mathbb{Z}^4\\ \mathbf{b}\equiv\mathbf{b}_0 \pmod{q_1}\\ \delta_{\mathfrak{c}}\beta\in\Gamma}} 1.$$

The rest of the proof follows [14]. Let $\Lambda_{\mathbf{d}}$ be the lattice introduced in Lemma 9.7. We write $\mathbf{b} = \mathbf{b}^{(1)} + q_1\mathbf{b}^{(2)}$ where $\mathbf{b}^{(1)}$ is some vector of $\Lambda_{\mathbf{d}}$ such that $\mathbf{b}^{(1)} \equiv \mathbf{b}_0 \pmod{q_1}$ (when such $\mathbf{b}^{(1)}$ exists) and $\mathbf{b}^{(2)} \in \Lambda_{\mathfrak{d}_{\mathfrak{c}}}$

$$|\Gamma_{\mathfrak{d}}| = \sum_{\mathbf{b}_0\in V_0'}'' \sum_{\substack{\mathbf{b}^{(2)}\in\Lambda_{\mathbf{d}}\\ \mathbf{b}\equiv\mathbf{b}_0 \pmod{q_1}\\ \delta_{\mathfrak{c}}\beta_1+q_1\delta_{\mathfrak{c}}\beta_2\in\Gamma}} 1,$$

where $\sum''$ indicates that the $\mathbf{b}_0$ are as above but furthermore such that there exists a vector $b^{(1)}$ in the lattice $\Lambda_{\mathfrak{d}}$ and $\beta_j = \frac{1}{W}\sum_{i=1}^4 b_i^{(j)}\nu_i$ for $j = 1, 2$. The argument now follows the proof of [14, Proposition 7.5] precisely, except that we apply Lemmas 9.8, 9.10 for the basis $\mathbf{v}$ in place of [14, Lemmas 7.3 and 7.4]. □

9.4 Initial steps in the Type II sum

We first note that Theorem 4.1 is trivial if $m > (\log X)^K$, so we may assume that

$$m < (\log x)^K. \tag{9.7}$$

If $\mathbf{a} \in \mathcal{A}_{q_1\cdots q_\ell}(\mathbf{u}_0, m, p)$ then there exists $d \in \mathbb{N}$ such that $N(a_1\nu_1 + a_2\nu_2 + a_3\nu_3) = d\prod_{i=1}^{\ell} q_i$. The conditions on q_i imply that $(m, q_1\cdots q_\ell) = 1$ but in general, it is not clear that $(d, m) = 1$. This may gives some complications in the application of Proposition 9.11. Let us write $m_0 = (d, m^\infty)$ and recall the notation $\mathcal{X} = \prod_{i=1}^3 [X_i, X_i(1+\eta_1)[$ from (4.1). In almost cases, m_0 is small. Let

$$D_0 := (\log X)^{4K}. \tag{9.8}$$

The contribution of the $\mathbf{a} \in \mathcal{X}$, such that $\mathbf{a} \equiv \mathbf{u}_0 \pmod m$ and $m_0 > D_0$, is less than

$$\begin{aligned}
\sum_{\substack{m_0 | m^\infty \\ m_0 > D_0}} \sum_{\substack{\mathbf{a}\in\mathcal{X} \\ \mathbf{a}\equiv \mathbf{u}_0 \pmod m \\ N\left(\sum_{i=1}^3 a_i\nu_i\right)\equiv 0 \pmod{m_0}}} 1 &\ll \eta_1^3 \prod_{i=1}^3 X_i \sum_{\substack{m_0 | m^\infty \\ m_0 > D_0}} \frac{4^{\omega(m_0)}}{m_0 m^2} \\
&\ll \frac{\eta_1^3 \prod_{i=1}^3 X_i}{m^2\sqrt{D_0}} \sum_{\substack{m_0 | m^\infty \\ m_0 > D_0}} \frac{4^{\omega(m_0)}}{\sqrt{m_0}} \\
&\ll \frac{\eta_1^3 \prod_{i=1}^3 X_i}{D_0^{1/3}}.
\end{aligned} \tag{9.9}$$

We now suppose that $m_0 \le D_0$. Let

$$\begin{aligned}
\mathcal{M}(m_0) := \Bigg\{ &\mathbf{v}_0 \in [1, mm_0]^3 : \mathbf{v}_0 \equiv u_0 \pmod m, \\
&N\Big(\sum_{i=1}^3 (\mathbf{v}_0)_i\nu_i\Big) \equiv 0 \pmod{m_0},\ \Big(m, \frac{N(\sum_{i=1}^3 (\mathbf{v}_0)_i\nu_i)}{m_0}\Big) = 1\Bigg\}.
\end{aligned} \tag{9.10}$$

Then for every $\mathbf{a} \in \mathcal{A}(\mathbf{u}_0, m)$ such that $m_0 = (N(a_1\nu_1 + a_2\nu_2 + a_3\nu_3), m^\infty)$, there exists exactly one $\mathbf{v}_0 \in \mathcal{M}(m_0)$ such that $\mathbf{a} \equiv \mathbf{v}_0 \pmod{mm_0}$. Putting this together with (9.9) deduce that

$$\mathcal{A}_{q_1\cdots q_\ell}(\mathbf{u}_0, m, p) = \sum_{\substack{m_0 | m^\infty \\ m_0 \le D_0}} \sum_{\mathbf{v}_0 \in \mathcal{M}(m_0)} |\mathcal{A}_{q_1\cdots q_\ell}(\mathbf{v}_0, m_0 m, p)| + O\Big(\frac{\eta_1^3 \prod_{i=1}^3 X_i}{D_0^{1/3}}\Big). \tag{9.11}$$

Any $\mathbf{a} \in \mathcal{A}(\mathbf{v}_0, mm_0)$ is such that the associated ideal $(\sum_{i=1}^3 a_i\nu_i)$ may be factored as $(\sum_{i=1}^3 a_i\nu_i) = \mathfrak{M}_0\mathfrak{J}$ with $N(\mathfrak{M}_0) = m_0$ and $(N(\mathfrak{J}), m) = 1$. This property will simplify some GCD considerations in the next sections. Let

$$m' := m_0 m \ll (\log x)^{5K} \tag{9.12}$$

denote this extended modulus (where we obtained the size bound from (9.7) and (9.8)).

9.5 Switching to ideals with norms in small boxes

We introduce the sets of principal ideals of $\mathcal{O}_K$ (recalling $\mathcal{X}$ from (4.1))

$$\widetilde{\mathcal{A}} = \Big\{ \big(\sum_{i=1}^3 a_i\nu_i\big) : \mathbf{a} \in \mathcal{X} \Big\}. \tag{9.13}$$

For any $\mathfrak{a} \in \widetilde{\mathcal{A}}$ there is exactly one $(a_1, a_2, a_3) \in \mathcal{X}$ such that $\mathfrak{a} = (a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$. We justify this in a similar way as in [14, Proof of Lemma 5.2 assuming Proposition 5.1 pp. 13-14].

If $\alpha = \sum_{i=1}^3 a_i\nu_i$ and $\beta = \sum_{i=1} b_i\nu_i$ with $\mathbf{a}, \mathbf{b} \in \mathcal{X}$ are such that $(\alpha) = (\beta)$ then $\beta\alpha^{-1}$ is a unit of $\mathcal{O}_K$. But $|\sigma(\alpha)| \ll X$ for all embedding σ and since $\alpha = N(\alpha)\prod_{\sigma \neq Id} \sigma(\alpha)^{-1}$ we have $|a_1\nu_1 + a_2\nu_2 + a_3\nu_3| \gg \eta_1^{1/10} X$ by (4.4) and then

$$\frac{\beta}{\alpha} = 1 + \frac{\beta - \alpha}{\alpha} = 1 + O(\eta_1^{9/10}).$$

If $\alpha \neq \beta$ then $\beta\alpha^{-1}$ can't be a unit because the length between two units is $\gg 1$ and we have a contradiction.

Next we consider the sets

$$\widetilde{\mathcal{A}}(\mathbf{v}_0, m', p) = \Big\{ \big(\sum_{i=1}^3 a_i\nu_i\big) \in \widetilde{\mathcal{A}} : \mathbf{a} \equiv \mathbf{v}_0 \pmod{m'} \text{ and } p | f(a_1, a_2, a_3) \Big\}$$

and for any ideal $\mathfrak{d}$,

$$\widetilde{\mathcal{A}}_{\mathfrak{d}}(\mathbf{v}_0, m', p) = \{\mathfrak{a} \in \widetilde{\mathcal{A}}(\mathbf{v}_0, m', p) : \mathfrak{d} | \mathfrak{a}\}.$$

Let $N_0^4 = \min_{(\alpha) \in \widetilde{\mathcal{A}}} N(\alpha)$. Let η_2 and η_3 defined by

$$\eta_2 = \frac{1}{(\log X)^K}, \qquad \eta_3 = \eta_2^{10000\ell^2}. \tag{9.14}$$

By the definition of $\mathcal{X}$, $N(a_1\nu_1 + a_2\nu_2 + a_3) \in [N_0^4, N_0^4(1 + O(\eta_1))]$ for all $(a_1\nu_1 + a_2\nu_2 + a_3) \in \widetilde{\mathcal{A}}$. We can choose $O(\eta_3^{-1}\eta_1)$ reals X_0 with $X_0^4 \in [N_0^4, N_0^4(1 + O(\eta_1))]$ so that the sets

$$\widetilde{\mathcal{A}}(X_0, \mathbf{v}_0, m', p) = \Big\{ \big(\sum_{i=1}^3 a_i\nu_i\big) \in \widetilde{\mathcal{A}}(\mathbf{v}_0, m', p) : N\big(\sum_{i=1}^3 a_i\nu_i\big) \in [X_0^4, X_0^4 + \eta_3 X_0^4[\Big\},$$

form a partition of $\widetilde{\mathcal{A}}(\mathbf{v}_0, m', p)$. Next we introduce the sets

$$\widetilde{\mathcal{A}}_{\mathfrak{d}}(X_0, \mathbf{v}_0, m', p) = \Big\{ \big(\sum_{i=1}^3 a_i\nu_i\big) \in \widetilde{\mathcal{A}}(X_0, \mathbf{v}_0, m', p) : \mathfrak{d} | \big(\sum_{i=1}^3 a_i\nu_i\big) \Big\}.$$

By (4.9), there exists $\varepsilon > 0$ such that $X^{\sum_{i=1}^{\ell}\theta_i+\min(\theta_0,\dots,\theta_\ell)} > X^{4+\varepsilon}$ and by (4.7) the intervals $[X^{\theta_i}, X^{\theta_i'}]$ do not overlap. Thus each $\mathfrak{a} \in \widetilde{\mathcal{A}}$ such that $N(\mathfrak{a}) \equiv 0 \pmod{q_1\cdots q_\ell}$ with $X^{\theta_i} \le q_i \le X^{\theta_i'}$, is divisible by exactly one prime ideal $\mathfrak{P}_i$ with $N(\mathfrak{P}_i) \in [X^{\theta_i}, X^{\theta_i'}]$ (for all $1 \le i \le \ell$).

We are now ready to settle the connection between the set $\mathcal{A}_q(\mathbf{v}_0, m', p)$ in Theorem 4.1 and the sets of ideals just defined above. For any primes $q_1, \dots, q_\ell$ with $q_i \in [X^{\theta_i}, X^{\theta_i'}]$, we have

$$|\mathcal{A}_{q_1\cdots q_\ell}(\mathbf{v}_0, m', p)| = \sum_{X_0} \sum_{N(\mathfrak{P}_i)=q_i} |\widetilde{\mathcal{A}}_{\mathfrak{P}_1\cdots\mathfrak{P}_\ell}(X_0, \mathbf{v}_0, m', p)|. \tag{9.15}$$

Any ideal $(a_1\nu_1 + a_2\nu_2 + a_3\nu_3)$ counted in (9.15) may be factored as

$$(a_1\nu_1 + a_2\nu_2 + a_3\nu_3) = \mathfrak{M}_0\mathfrak{I}\prod_{i=1}^{\ell}\mathfrak{P}_i, \tag{9.16}$$

where each $\mathfrak{P}_i$ is a prime ideal with norm in $[X^{\theta_i}, X^{\theta_i'}]$ and $\mathfrak{I}$ is an ideal with

$$N(\mathfrak{I}) \in \mathcal{I}_0 := \Big[\frac{X_0^4 X^{-\sum_{i=1}^{\ell}\theta_i'}}{m_0}, \frac{X_0^4(1+\eta_3)X^{-\sum_{i=1}^{\ell}\theta_i}}{m_0}\Big] = [I_1, I_2], \tag{9.17}$$

say.

We choose now $O(\eta_3^{-1}\log X)$ reals $I \in \mathcal{I}_0$ such that $\mathcal{I}_0$ is covered by the union of the intervals $[I, I(1+\eta_3)[$. Let $\hat{\mathcal{I}}_0$ denote the set of these reals I.

Since we have $(N(\sum_{i=1}^{3} a_i\nu_i)/m_0, m) = 1$ when $\mathbf{a} \equiv \mathbf{v}_0 \pmod{m'}$, we have $(m', N(\mathfrak{I})\prod_{i=1}^{\ell} N(\mathfrak{P}_i)) = 1$.

For brevity we will write $\widetilde{\mathcal{A}}(\mathbf{v}_0, m', p)$ in place of $\widetilde{\mathcal{A}}(X_0, \mathbf{v}_0, m', p)$ when the context will be clear.

To have a precise control of the size of the norms of some ideals, we cover each interval $[\theta_i, \theta_i']$ by $O(\eta_2^{-2})$ distinct intervals of size $O(\eta_2^2)$ so that,

$$\prod_{i=1}^{\ell}[\theta_i, \theta_i'] = \cup_{\mathbf{l}\in E}\mathcal{R}(\mathbf{l}), \tag{9.18}$$

where E is some subset of $\mathbb{N}^\ell$ of size $O(\eta_2^{-2\ell})$ and each $\mathcal{R}(\mathbf{l})$ is of type $\mathcal{R}(\mathbf{l}) = \prod_{i=1}^{\ell}[t_i, t_i')$ with $|t_i' - t_i| \ll \eta_2^2$ (except that in the intervals with $t_i' = \theta_i'$ we take the whole segment $[t_i, \theta_i']$), (cf [14, section 8 p.45]).

We write $\mathcal{R}(\mathbf{l}) = \mathcal{R}_1(\mathbf{l}) \times \mathcal{R}_2(\mathbf{l})$ with $\mathcal{R}_2(\mathbf{l})$ representing the first ℓ' coordinates and $\mathcal{R}_1(\mathbf{l})$ the final $\ell - \ell'$ coordinates.

For a polytope $\mathcal{R} \subset \mathbb{R}^s$ (for some s), we define

$$\mathbf{1}_{\mathcal{R}}(\mathfrak{a}) = \begin{cases} 1, & \mathfrak{a} = \mathfrak{p}_1\cdots\mathfrak{p}_s \text{ with } N(\mathfrak{p}_i) = X^{e_i} \text{ and } (e_1,\dots,e_s) \in \mathcal{R}, \\ 0, & \text{otherwise.} \end{cases}$$

Thus we need to study the quantity

$$T(\mathcal{R}(\mathbf{l})) := \sum_{X^\tau \le p \le X^{\tau'}} \sum_{\mathfrak{I}\in\mathcal{I}} \mathfrak{M}_0\mathfrak{I}\mathfrak{a}\in\mathcal{A}(\mathbf{v}_0,m',p) \sum \mathbf{1}_{\mathcal{R}(\mathbf{l})}(\mathfrak{a}), \tag{9.19}$$

with

$$\mathcal{I} := \{\mathfrak{I} : N(\mathfrak{I}) \in [I, I+\eta_3 I[, (N(\mathfrak{I}), m) = 1\} \tag{9.20}$$

for each of the $O(\eta_2^{-2\ell})$ choices of $\mathbf{l} \in E$.

9.6 Approximation weights

We recall that $\eta_3 = \eta_2^{10000\ell^2}$. A key idea of [14] is to approximate the indicator $\mathbf{1}_{\mathcal{R}_2}$ by a weight $\tilde{\mathbf{1}}_{\mathcal{R}_2}$ which will be easier to control. For $\mathcal{S} \subset \mathbb{R}^s$, with $s \in \mathbb{N}$, we consider the function

$$c_{\mathcal{S}}(t) = \iint_{\substack{(e_1,\dots,e_s)\in\mathcal{S} \\ \sum_{i=1}^s e_i \in I_t}} \frac{de_1 \cdots de_s}{\eta_3^{1/2} \prod_{i=1}^s e_i}, \tag{9.21}$$

$$\text{where } I_t := \Big[\frac{\log t}{\log X}, \frac{\log(t+\eta_3^{1/2}t)}{\log X}\Big].$$

In this previous definition we have $\sum_{i=1}^s e_i \in I_t$ if and only if $X^{\sum_{i=1}^s e_i} \in [t, t(1+\sqrt{\eta_3})]$. This function is so that $c_{\mathcal{S}}(N(\mathfrak{a}))$ corresponds to the probability for an ideal of norm close to $N(\mathfrak{a})$ to have a prime factorisation compatible with $\mathcal{S}$ (cf. [14, section 8]). We recall below some properties of this function that we will frequently use later on.

Lemma 9.12.
- *If $\mathcal{S} = \prod_{i=1}^s [u_i, u_i']$ is an hyperrectangle with $\min u_i > \varepsilon_0 > 0$ and $s > 1$, then*

$$c_{\mathcal{S}}(t+\delta) - c_{\mathcal{S}}(t) \ll \frac{\delta}{t}$$

- *If $\mathcal{S} = \prod_{i=1}^s [u_i, u_i']$ is an hyperrectangle with $\min u_i > \varepsilon_0 > 0$ then*

$$c_{\mathcal{S}}(t) \ll_{\varepsilon_0} \frac{1}{\log X}.$$

Proof. The first part is a particular case of [14, Lemma 8.3 (iii)]. The proof of the second point is a direct computation analogous to [14] :

$$c_{\mathcal{S}}(t) \le \frac{1}{\sqrt{\eta_3}} \iint_{\substack{e_i\in[u_i,u_i'] \\ 1\le i\le s-1}} \Big[\int_{e_s \in I_t - \sum_{i=1}^{s-1} e_i} \frac{\mathrm{d}\, e_s}{u_s}\Big] \prod_{i=1}^{s-1} \frac{\mathrm{d}\, e_i}{u_i}.$$

The integral over e_s is $O(\sqrt{\eta_3}(\log X)^{-1})$ and the contribution of the other integrals is $O(1)$. □

Let $\epsilon_{00} > 0$ and

$$R := X^{\epsilon_{00}}. \tag{9.22}$$

The approximate weights of $\mathbf{1}_{\mathcal{R}_2}$ are defined by

$$\tilde{\mathbf{1}}_{\mathcal{R}_2}(\mathfrak{b}) := c_{\mathcal{R}_2}(N(\mathfrak{b})) \sum_{\mathfrak{d}\mid\mathfrak{b}} \lambda_{\mathfrak{d}}, \tag{9.23}$$

where

$$\lambda_{\mathfrak{d}} := \begin{cases} \mu(\mathfrak{d}) \log \frac{R}{N(\mathfrak{d})}, & N(\mathfrak{d}) < R, \\ 0, & \text{otherwise.} \end{cases}$$

Remark. *Our weights are somewhat simpler than the one introduced in [14], because we don't need to take care of the perturbations caused by a possible exceptional character χ^*. (Ultimately we will only require estimates with moduli up to a fixed power of $\log X$, whereas in [14] larger moduli needed to be considered due to losses occurring in high dimensions.)*

We now write

$$T(\mathcal{R}) = T_{sieve}(\mathcal{R}) + T_1(\mathcal{R}),$$

where

$$T_{sieve}(\mathcal{R}) := \sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}} \sum_{\mathfrak{I}\in\mathcal{I}} \sum_{\mathfrak{m}_0\mathfrak{I}\mathfrak{a}\mathfrak{b}\in\widetilde{\mathcal{A}}(\mathbf{v}_0,m',p)} \mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})\tilde{\mathbf{1}}_{\mathcal{R}_2}(\mathfrak{b}), \tag{9.24}$$

$$T_1(\mathcal{R}) := \sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}} \sum_{\mathfrak{I}\in\mathcal{I}} \sum_{\mathfrak{m}_0\mathfrak{I}\mathfrak{a}\mathfrak{b}\in\widetilde{\mathcal{A}}(\mathbf{v}_0,m',p)} \mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})(\mathbf{1}_{\mathcal{R}_2}(\mathfrak{b}) - \tilde{\mathbf{1}}_{\mathcal{R}_2}(\mathfrak{b})), \tag{9.25}$$

and

$$P_1 := X^{\tau}, \qquad P_2 := X^{\tau'}. \tag{9.26}$$

For brevity again we will write $T_{sieve}(\mathcal{R})$ and $T_1(\mathcal{R})$ in place of $T_{sieve}(\mathcal{R},\mathbf{v}_0)$ and $T_1(\mathcal{R},\mathbf{v}_0)$ when $\mathbf{v}_0$ is clear from the context. We see that Theorem 4.1 follows immediately from the following two propositions.

Proposition 9.13 (Estimate for T_{sieve})**.** *If we have*

$$\epsilon_{00} < \sum_{j=1}^{\ell'} \theta_j - 1 - 12\tau',$$

then

$$T_{sieve}(\mathcal{R}) = M(\mathcal{R}) + E_1(\mathcal{R}),$$

where

$$M(\mathcal{R}) = (2 + O(\eta_3^{1/2}))\eta_3|\widetilde{\mathcal{A}}(X_0)|c_{\mathcal{R}}(X_0^4/mI)\frac{g(m')}{m'^3}\frac{\log(P_2/P_1)}{\varphi(D_f)},$$

$$g(m') = \prod_{\mathfrak{P}|(m')}\Big(1 - \frac{\varrho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\Big)^{-1},$$

$$\sum_{\mathcal{R}}\sum_{X_0}\sum_{I\in\hat{\mathcal{I}}_0} |E_1(\mathcal{R})| \ll \eta_3^{1/2}\eta_1^{-2\ell}(\log X)^{11}\prod_{i=1}^{3} X_i.$$

Proposition 9.14 (Bound for $T_1(\mathcal{R})$)**.** *Let $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2$ and $T_1(\mathcal{R})$ be as above. If we have*

$$\tau' < \min\Big(\frac{4 - 2\theta_1' - \ldots - 2\theta_{\ell'}'}{100}, \frac{\theta_1 + \cdots + \theta_{\ell'} - 1}{100}\Big),$$

then for any $K > 0$ we have

$$T_1(\mathcal{R}) \ll_K \frac{\prod_{i=1}^{3} X_i}{(\log X)^K}.$$

We remark that we are assuming the general setup in Propositions 9.13 and 9.14; in particular, the constants $\theta_1, \theta_1', \ldots, \theta_\ell, \theta_\ell'$ determining $\mathcal{R}$ are assumed to satisfy (4.6)-(4.10).

We will establish Proposition 9.13 in Section 10 and the harder Proposition 9.14 in Section 11. The presence of the sum over primes $p \in [P_1, P_2]$

introduces few additional complications to T_{sieve} and Proposition 9.13, but quite significant additional technical details to T_1 and Proposition 9.14. Assuming these propositions for now, we can establish Theorem 4.1 by putting all our manipulations together.

Proof of Theorem 4.1 assuming Propositions 9.13 and 9.14. We recall from (9.11) that

$$\mathcal{A}_{q_1\cdots q_\ell}(\mathbf{u}_0,m,p)=\sum_{\substack{m_0|m^\infty\\ m_0\le D_0}}\sum_{\mathbf{v}_0\in\mathcal{M}(m_0)}|\widetilde{\mathcal{A}}_{q_1\cdots q_\ell}(\mathbf{v}_0,m',p)|+O\Big(\frac{\eta_1^3\prod_{i=1}^3X_i}{D_0^{1/3}}\Big). \tag{9.27}$$

We focus on the $\widetilde{\mathcal{A}}$ terms. We use the notation $\hat{\mathcal{I}}_0$ introduced just after (9.17) and for any given real $I\in\hat{\mathcal{I}}_0$, $\mathcal{I}$ is the associated set of ideals defined just after (9.19). We recall from (9.15), (9.17) and (9.19) that

$$\begin{aligned}|\widetilde{\mathcal{A}}_{q_1\cdots q_\ell}(\mathbf{v}_0,m',p)|&=\sum_{X_0}\sum_{N(\mathfrak{P}_i)=q_i}|\widetilde{\mathcal{A}}_{\mathfrak{P}_1\cdots\mathfrak{P}_\ell}(X_0,\mathbf{v}_0,m',p)|\\ &=\sum_{X_0}\sum_{I\in\hat{\mathcal{I}}_0}\sum_{N(\mathfrak{P}_i)=q_i}\sum_{\substack{\mathfrak{J}\in\mathcal{I}\\ \mathfrak{P}_i\in\tilde{A}(\mathbf{v}_0,m',p)\\ \mathfrak{M}_0\mathfrak{J}\prod_{i=1}^\ell}}1\\ &=\sum_{X_0}\sum_{I\in\hat{\mathcal{I}}_0}\sum_{\substack{\mathcal{R}_1,\mathcal{R}_2\\ \prod_{i=1}^\ell[\theta_i,\theta_i']=\sqcup\mathcal{R}_1\times\mathcal{R}_2}}\sum_{\mathfrak{J}\in\mathcal{I}}\sum_{\mathfrak{a}}\mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})\sum_{\substack{\mathfrak{b}\\ \mathfrak{J}\mathfrak{M}_0\mathfrak{a}\mathfrak{b}\in\tilde{A}(\mathbf{v}_0,m',p)}}\mathbf{1}_{\mathcal{R}_2}(\mathfrak{b}).\end{aligned}$$

By assumption of Theorem 4.1, we have $\tau'<(\sum_{i=1}^{\ell'}\theta_i-1)/100$, and so choosing ϵ_{00} sufficiently small means that the hypothesis of Proposition 9.13 is satisfied. Thus, summing over $p\in[P_1,P_2]$ (which is $[X^\tau,X^{\tau'}]$ be (9.26)) and applying Propositions 9.13 and 9.14 (with a suitably large constant K) gives

$$\begin{aligned}\sum_{p\in[P_1,P_2]}|\widetilde{\mathcal{A}}_{q_1\cdots q_\ell}(\mathbf{v}_0,m',p)|&=\sum_{X_0}\sum_{I\in\hat{\mathcal{I}}_0}\sum_{\substack{\mathcal{R}=\mathcal{R}_1\times\mathcal{R}_2\\ \prod_{i=1}^\ell[\theta_i,\theta_i']=\sqcup\mathcal{R}_1\times\mathcal{R}_2}}\Big(T_{sieve}(\mathcal{R})+T_1(\mathcal{R})\Big)\\ &=(2+O(\eta_3^{1/2}))\eta_3\frac{\log(P_2/P_1)}{\phi(D_f)}\frac{g(m')}{m'^3}T_3+O\Big(\frac{\prod_{i=1}^3X_i}{(\log X)^{K-O(1)}}\Big),\end{aligned} \tag{9.28}$$

where

$$T_3:=\sum_{X_0}\sum_{I\in\hat{\mathcal{I}}_0}\sum_{\substack{\mathcal{R}=\mathcal{R}_1\times\mathcal{R}_2\\ \prod_{i=1}^\ell[\theta_i,\theta_i']=\sqcup\mathcal{R}_1\times\mathcal{R}_2}}|\widetilde{\mathcal{A}}(X_0)|c_{\mathcal{R}}(X_0^4/mI).$$

Here we used that there are at most $O(\eta_2^{-2\ell})$ subsets $\mathcal{R}$, $O(\eta_3^{-1}\eta_1)$ reals X_0 and $O(\eta_3^{-1}\log X)$ reals I to bound the contribution from T_1 by Proposition 9.14.

We now concentrate on T_3. Since the subsets $\mathcal{R}$ form a partition of $\mathcal{T}:=\prod_{i=1}^\ell[\theta_i,\theta_i']$, we find

$$\sum_{\substack{\mathcal{R}=\mathcal{R}_1\times\mathcal{R}_2\\ \prod_{i=1}^\ell[\theta_i,\theta_i']=\sqcup\mathcal{R}_1\times\mathcal{R}_2}}c_{\mathcal{R}}(X_0^4/mI)=c_{\mathcal{T}}(X_0^4/mI),$$

so

$$T_3 = \sum_{X_0} |\widetilde{\mathcal{A}}(X_0)| \sum_{I \in \hat{\mathcal{I}}_0} c_{\mathcal{T}}(X_0^4/mI).$$

By Lemma 9.12 applied to $c_{\mathcal{T}}$ we have for all $I \in \hat{\mathcal{I}}_0$

$$c_{\mathcal{T}}(X_0^4/mI) = \frac{1}{\eta_3} \int_I^{I(1+\eta_3)} \frac{c_{\mathcal{T}}(X_0^4/mv)}{v} dv + O(\eta_3).$$

Expanding the definition (9.21) of $c_{\mathcal{T}}$ and swapping the order of summation and integration, we find

$$\begin{aligned}
&\sum_{I \in \hat{\mathcal{I}}_0} \int_I^{I(1+\eta_3)} \frac{c_{\mathcal{T}}(X_0^4/mv)}{v} dv \\
&\qquad = \frac{1}{\eta_3^{1/2}} \iint\limits_{\substack{e_i \in [\theta_i, \theta_i'] \\ 1 \le i \le \ell}} \sum_{I \in \hat{\mathcal{I}}_0} \int\limits_{\substack{v \in [I, I(1+\eta_3)[\\ v \in \left[\frac{X_0^4}{m \prod_{i=1}^\ell X^{e_i}}, \frac{X_0^4 (1+\sqrt{\eta_3})}{m \prod_{i=1}^\ell X^{e_i}} \right]}} \frac{dv}{v} \prod_{i=1}^\ell \frac{\mathrm{d}\, e_i}{e_i} \\
&\qquad = \frac{1}{\eta_3^{1/2}} \iint\limits_{\substack{e_i \in [\theta_i, \theta_i'] \\ 1 \le i \le \ell}} \Big(\int_{X_0^4/(m \prod_{i=1}^\ell X^{e_i})}^{X_0^4 (1+\sqrt{\eta_3})/(m \prod_{i=1}^\ell X^{e_i})} \frac{dv}{v} \Big) \prod_{i=1}^\ell \frac{\mathrm{d}\, e_i}{e_i} \\
&\qquad = \frac{\log(1+\sqrt{\eta_3})}{\eta_3^{1/2}} \prod_{i=1}^\ell \log\Big(\frac{\theta_i'}{\theta_i}\Big).
\end{aligned}$$

We note that this is independent of X_0, so we find

$$\begin{aligned}
T_3 &= \frac{\log(1+\sqrt{\eta_3})}{\eta_3^{3/2}} \prod_{i=1}^\ell \log\Big(\frac{\theta_i'}{\theta_i}\Big) \sum_{X_0} |\widetilde{\mathcal{A}}(X_0)| + O\Big(\log X \sum_{X_0} |\widetilde{\mathcal{A}}(X_0)|\Big) \\
&= \frac{(1+O(\sqrt{\eta_3}))}{\eta_3} \prod_{i=1}^\ell \log\Big(\frac{\theta_i'}{\theta_i}\Big) |\widetilde{\mathcal{A}}(X)|. \qquad (9.29)
\end{aligned}$$

Putting together (9.27), (9.28) and (9.29) we find

$$\begin{aligned}
&\sum_{p \in [P_1, P_2]} \sum_{\substack{q_1, \dots q_\ell \\ q_i \in [X^{\theta_i}, X^{\theta_i'}]}} \mathcal{A}_{q_1 \cdots q_\ell}(\mathbf{u}_0, m, p) \\
&\qquad = 2 \frac{\log \frac{P_2}{P_1}}{\phi(D_f)} \prod_{i=1}^\ell \log\Big(\frac{\theta_i'}{\theta_i}\Big) |\widetilde{\mathcal{A}}(X)| \sum_{\substack{m_0 | m^\infty \\ m_0 \le D_0}} \sum_{\mathbf{v}_0 \in \mathcal{M}(m_0)} \frac{g(m')}{m'^3} \\
&\qquad\qquad + O\Big(\eta_3^{1/2} \prod_{i=1}^3 X_i\Big) + O\Big(\frac{\eta_1^3 \prod_{i=1}^3 X_i}{D_0^{1/3}}\Big). \qquad (9.30)
\end{aligned}$$

Finally it remains to estimate the inner double sum. The summand is independent of $\mathbf{v}_0$, so recalling from (9.12) that $m' = m_0 m$ we are left to estimate

$$\sum_{\substack{m_0 < D_0 \\ m_0 | m^\infty}} \frac{|\mathcal{M}(m_0)|}{(m m_0)^3} \prod_{\mathfrak{P} | (m)} \Big(\sum_{k=2}^\infty \frac{\varrho_{\mathbf{v}}(\mathfrak{P}^k)}{N(\mathfrak{P}^k)} \Big)^{-1}. \qquad (9.31)$$

By (9.10),

$$|\mathcal{M}(m_0)| \le m_0^2 m,$$

and thus for any given m the sum over m_0 converges. We may therefore extend it to all $m_0 \ge 1$ cost of an admissible error term. Next we note that the sets of the $\mathbf{a} \in [1,X]^3$ with $\mathbf{a} \equiv \mathbf{u}_0 \pmod m$ can be partitioned into sets of the $\mathbf{a} \in [1,X]^3$ such that $\mathbf{a} \equiv \mathbf{v}_0 \pmod{mm_0}$, with $m_0 \le X^2$ and $\mathbf{v}_0 \in \mathcal{M}(\mathbf{u}_0)$, and so

$$\begin{aligned}
\sum_{\substack{m_0<D_0\\ m_0|m^\infty}} \frac{|\mathcal{M}(m_0)|}{(mm_0)^3} &= (1+O(D_0^{-1/4})) \sum_{\substack{m_0<X^2\\ m_0|m^\infty}} \frac{|\mathcal{M}(m_0)|}{(mm_0)^3} \\
&= \frac{(1+O(D_0^{-1/4})}{X^3+O(X^2)} \sum_{\substack{m_0<X^2\\ m_0|m^\infty}} \sum_{\mathbf{v}_0\in\mathcal{M}(m_0)} \sum_{\substack{\mathbf{a}\in[1,X]^3\\ \mathbf{a}\equiv\mathbf{v}_0 \pmod{m_0}}} 1 \\
&= \frac{(1+O(D_0^{-1/4}))}{X^3+O(X^2)} \sum_{\substack{\mathbf{a}\in[1,X]^3\\ \mathbf{a}\equiv\mathbf{u}_0 \pmod m}} 1 \\
&= \frac{1}{m^3}(1+O(D_0^{-1/4})).
\end{aligned}$$

Substituting this into (9.30) and recalling from (9.13), (9.14) that $D_0 = (\log X)^{4K}$, $\eta_3 \ll (\log X)^{-3K}$ and $|\widetilde{\mathcal{A}}(X)| = \eta_1^3 X_1X_2X_3 + O(\eta_3 X_1X_2X_3)$ gives Theorem 4.1. □

10 Proposition 9.13: The term $T_{sieve}(\mathcal{R})$

In this part we obtain an analogue of [14, Lemma 8.6] by expanding the sieve terms and applying Proposition 9.11.

If $\mathfrak{a}$ and $\mathfrak{b}$ are some ideals satisfying $\mathbf{1}_{\mathcal{R}_1}(\mathfrak{a}) = \mathbf{1}_{\mathcal{R}_2}(\mathfrak{b}) = 1$ then $\mathfrak{a}$ and $\mathfrak{b}$ factor into prime ideals as $\mathfrak{a} = \prod_{i=\ell'+1}^{\ell} \mathfrak{P}_i$, $\mathfrak{b} = \prod_{i=1}^{\ell'} \mathfrak{P}_i$ with $N(\mathfrak{P}_i) \in [X^{t_i}, X^{t_i}(1+O(\eta_2^2 \log X))]$ for $1 \le i \le \ell$. In particular,

$$N(\mathfrak{b}) \in [B_1^4, B_1^4(1+O(\eta_2^2 \log X))] \tag{10.1}$$

where

$$B_1^4 := X^{\sum_{i=1}^{\ell'} t_i}. \tag{10.2}$$

Moreover, from the definition (9.21) of $c_{\mathcal{R}_2}$, we see that $\tilde{\mathbf{1}}_{\mathcal{R}_2}(\mathfrak{b})$ is also supported on $N(\mathfrak{b}) \in [B_1^4, B_1^4(1+O(\eta_2^2 \log X))]$.

Lemma 10.1. *Let $B_1^4 > X^{1+\epsilon}R$ and $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2$. Then we have*

$$T_{sieve}(\mathcal{R}) = M_1(\mathcal{R}) + E_1(\mathcal{R})$$

where $M_1(\mathcal{R})$ is given by

$$\begin{aligned}
M_1(\mathcal{R}) := \sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}} \sum_{\mathfrak{J}\in\mathcal{I}} \sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_1}(\mathfrak{a}) \sum_{\substack{N(\mathfrak{d})<R\\ N(\mathfrak{d}),m)=1}} \lambda_{\mathfrak{d}} \\
\times c_{\mathcal{R}_2}\Big(\frac{X_0^4}{m_0 N(\mathbf{a}\mathfrak{J})}\Big) |\widetilde{\mathcal{A}}_{\mathfrak{a}\mathfrak{d}\mathfrak{J}}(\mathbf{v}_0(\mathbf{y}), m', p)|,
\end{aligned}$$

and $E_1(\mathcal{R})$ satisfies

$$\sum_{\mathcal{R}}\sum_{X_0}\sum_{I\in\hat{\mathcal{I}}_0}|E_1(\mathcal{R})|\ll\eta_3^{1/2}\eta_1^{-2\ell}(\log X)^{11}\prod_{i=1}^{3}X_i.$$

Proof. We substitute our definition (9.23) of $\tilde{\mathbf{1}}_{\mathcal{R}_2}$ into our expression (9.24) for T_{sieve}, and write $\mathfrak{u}=\mathfrak{M}_0\mathfrak{I}\mathfrak{a}\mathfrak{b}$. This gives

$$T_{sieve}(\mathcal{R})=\sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}}\sum_{\mathfrak{I}\in\mathcal{I}}\sum_{\mathfrak{a}}\mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})\sum_{N(\mathfrak{d})<R}\lambda_{\mathfrak{d}}\sum_{\substack{\mathfrak{u}\in\widetilde{\mathcal{A}}(\mathbf{v}_0,m',p)\\ \mathfrak{M}_0\mathfrak{I}\mathfrak{a}\mathfrak{d}|\mathfrak{u}}}c_{\mathcal{R}_2}(N(\mathfrak{u}/\mathbf{a}\mathfrak{I}\mathfrak{M}_0)).\tag{10.3}$$

If $\mathfrak{u}\in\widetilde{\mathcal{A}}(\mathbf{v}_0,m',p)$ then $N(\mathfrak{u})\in[X_0^4,X_0^4(1+\eta_3)]$. By Lemma 9.12, this implies $c_{\mathcal{R}_2}(N(\mathfrak{u}/\mathbf{a}\mathfrak{I}\mathfrak{M}_0))=c_{\mathcal{R}_2}(X_0^4/m_0N(\mathbf{a}\mathfrak{I}))+O(\eta_3)$. Thus we write

$$T_{sieve}(\mathcal{R})=M_1(\mathcal{R})+O(E_1(\mathcal{R})),\tag{10.4}$$

where $M_1(\mathcal{R})$ is as given in the lemma and

$$E_1(\mathcal{R}):=\eta_3\sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}}\sum_{\mathfrak{I}\in\mathcal{I}}\sum_{\mathfrak{a}}\mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})\sum_{N(\mathfrak{d})<R}|\lambda_{\mathfrak{d}}||\widetilde{\mathcal{A}}_{\mathfrak{I}\mathfrak{a}\mathfrak{d}}(\mathbf{v}_0,m',p)|.\tag{10.5}$$

We concentrate on $E_1(\mathcal{R})$. For any $(\sum_{i=1}^3 x_i\nu_i)\in\widetilde{\mathcal{A}}$, the number of primes $p\in[P_1,P_2]$ such that $p|f(x_1,x_2,x_3)$ is finite. This allows us to remove the summation over p and replace $|\widetilde{\mathcal{A}}_{\mathfrak{I}\mathfrak{a}\mathfrak{d}}(\mathbf{v}_0,m',p)|$ with $|\widetilde{\mathcal{A}}_{\mathfrak{I}\mathfrak{a}\mathfrak{d}}(\mathbf{v}_0,m',1)|$ in $E_1(\mathcal{R})$ at the cost of a factor $O(1)$.

We then apply Proposition 9.11 to estimate $|\widetilde{\mathcal{A}}_{\mathfrak{I}\mathfrak{a}\mathfrak{d}\mathfrak{M}_0}(\mathbf{v}_0,m',1)|$, recalling that $N(\mathfrak{I}\mathfrak{a}\mathfrak{d}\mathfrak{M}_0)\ll X^4R/B_1^4$ and $m'\ll(\log X)^{O(1)}$. This gives

$$\begin{aligned}E_1(\mathcal{R})\ll\eta_3\sum_{\mathfrak{I}\in\mathcal{I}}\sum_{\mathfrak{a}}\mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})\sum_{\substack{N(\mathfrak{d})<R\\ (N(\mathfrak{d}),m')=1}}|\lambda_{\mathfrak{d}}|\frac{|\widetilde{\mathcal{A}}(X_0,\mathcal{X})|\varrho_{\mathbf{v}}(\mathfrak{a}\mathfrak{d}\mathfrak{I})}{N(\mathfrak{a}\mathfrak{I}\mathfrak{d})(m')^3}\\ +X^{o(1)}\sum_{\substack{N(\mathfrak{d})<R\\ (N(\mathfrak{d}),m)=1}}|\lambda_{\mathfrak{d}}|\Big(X^2\Big(\frac{X^4R}{B_1^4}\Big)^{1/3}+\frac{X^4R}{B_1^4}X\Big).\end{aligned}\tag{10.6}$$

Crudely, if $B_1^4>X^{1+\epsilon}R$, we see the second term in (10.6) contributes to (10.6)

$$\ll X^{3+o(1)}\Big(\frac{XR^4}{B_1^4}+\Big(\frac{XR^4}{B_1^4}\Big)^{1/3}\Big)\ll X^{3-\epsilon/4}.\tag{10.7}$$

By an Euler product upper bound and Lemma 9.6, we see that

$$\sum_{I\in\hat{\mathcal{I}}_0}\sum_{\mathfrak{I}\in\mathcal{I}}\sum_{\mathfrak{a}}\mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})\sum_{\substack{N(\mathfrak{d})<R\\ (N(\mathfrak{d}),m')=1}}|\lambda_{\mathfrak{d}}|\frac{|\widetilde{\mathcal{A}}(X_0,\mathcal{X})|\varrho_{\mathbf{v}}(\mathfrak{a}\mathfrak{d}\mathfrak{I})}{N(\mathfrak{a}\mathfrak{I}\mathfrak{d})(m')^3}\tag{10.8}$$

$$\ll(\log X)|\widetilde{\mathcal{A}}(X_0,\mathbf{v}_0,m')|\sum_{N(\mathfrak{I}),N(\mathfrak{a}),N(\mathfrak{d})<X}\frac{|\rho_{\mathbf{v}}(\mathfrak{a}\mathfrak{d}\mathfrak{I})|}{N(\mathfrak{a}\mathfrak{d}\mathfrak{I})}$$

$$\ll(\log X)^9|\widetilde{\mathcal{A}}(X_0,\mathbf{v}_0,m')|.\tag{10.9}$$

Thus, substituting (10.7) and (10.9) into (10.6) we find for $B_1^4 > X^{1+\epsilon}R$

$$\sum_{I\in\hat{\mathcal{I}}_0} E_1(\mathcal{R}) \ll \eta_3(\log X)^9|\widetilde{\mathcal{A}}(X_0,\mathbf{v}_0,m')| + X^{3-\epsilon/5}.$$

Summing this over all $O(\eta_2^{-2\ell})$ hyperrectangles $\mathcal{R}$ and all relevant X_0, and recalling (9.14) that η_3 is much smaller than η_2 we find

$$\begin{aligned}\sum_{\mathcal{R}}\sum_{X_0}\sum_{I\in\hat{\mathcal{I}}_0} E_1(\mathcal{R}) &\ll \eta_3(\log X)^9\sum_{\mathcal{R}}\sum_{X_0}|\widetilde{\mathcal{A}}(X_0,\mathbf{v}_0,m')| + X^{3-\epsilon/5}.\\ &\ll \eta_3\eta_2^{-2\ell}(\log X)^4|\widetilde{\mathcal{A}}(\mathbf{v}_0,m')| + X^{3-\epsilon/5}\\ &\ll \eta_3^{1/2}\eta_1^{-2\ell}(\log X)^{11}\prod_{i=1}^{3}X_i + X^{3-\epsilon/6}. \qquad (10.10)\end{aligned}$$

This gives the result. □

Thus we have to evaluate $M_1(\mathcal{R})$.

Lemma 10.2. *Let $B_1^4 > X^{1+\epsilon}RP_2^{12}$ and let $M_1(\mathcal{R})$ be as given by Lemma 10.1. Then we have*

$$M_1(\mathcal{R}) = (2+O(\eta_3^{1/2}))\eta_3|\widetilde{\mathcal{A}}(X_0)|c_{\mathcal{R}}(X_0^4/mI)\frac{g(m')}{m'^3}\frac{\log(P_2/P_1)}{\varphi(D_f)}.$$

Proof. First we want to apply Proposition 9.11 to estimate $|\widetilde{\mathcal{A}}_{\mathfrak{a}\mathfrak{d}\mathfrak{J}}(\mathbf{v}_0,m',p)|$. To do this we split according to residue classes $\pmod p$. For any (y_1,y_2,y_3) such that $f(y_1,y_2,y_3)\equiv 0 \pmod p$ let $\tilde{\mathbf{u}}_0(\mathbf{y})$ be a solution of the two equations $\tilde{\mathbf{u}}_0(\mathbf{y})\equiv\mathbf{y} \pmod p$ and $\tilde{\mathbf{u}}_0(\mathbf{y})\equiv\mathbf{v}_0 \pmod{m'}$. Thus

$$|\widetilde{\mathcal{A}}_{\mathfrak{a}\mathfrak{d}\mathfrak{J}}(\mathbf{v}_0,m',p)| = \sum_{\substack{y_1,y_2,y_3 \pmod p\\ f(y_1,y_2,y_3)\equiv 0 \pmod p}} |\widetilde{\mathcal{A}}_{\mathfrak{a}\mathfrak{d}\mathfrak{J}}(\tilde{\mathbf{u}}_0(\mathbf{y}),pm',1)|$$

We recall that $p\le P_2$ and $N(\mathfrak{J}\mathfrak{a}\,\mathfrak{d}) \ll XR/B_1$. Therefore, by Proposition 9.11, we can replace $|\widetilde{\mathcal{A}}_{\mathfrak{a}\mathfrak{d}\mathfrak{J}}(\tilde{\mathbf{u}}_0(\mathbf{y}),pm',1)|$ with $\rho_{\mathbf{v}}(\mathfrak{a}\mathfrak{d}\mathfrak{J})|\mathcal{A}(X_0,\chi)|/p^3m'^3N(\mathfrak{a}\mathfrak{d}\mathfrak{J})$ in $M_1(\mathcal{R})$ at the cost of a term bounded by

$$\sum_{p\le P_2}\sum_{\substack{y_1,y_2,y_3 \pmod p\\ f(y_1,y_2,y_3)\equiv 0 \pmod p}}\Big(X^{2+o(1)}\Big(\frac{XR}{B_1^4}\Big)^{1/3}P_2 + X^{o(1)}\frac{XR}{B_1^4}P_2^4\Big).$$

This is $O(X^{3-\epsilon/4})$ provided $B_1^4 > X^{1+\epsilon}RP_2^{12}$.

Since the function $\varrho_{\mathbf{v}}$ is multiplicative, $(\mathfrak{a},\mathfrak{d}\mathfrak{J})=1$, and $\mathfrak{a}$ is a product of degree one prime ideals of large enough norm, by Lemma 9.4, we have $\varrho_{\mathbf{v}}(\mathfrak{a}\mathfrak{d}\mathfrak{J})/N(\mathfrak{a}\mathfrak{d}\mathfrak{J}) = \varrho_{\mathbf{v}}(\mathfrak{d}\mathfrak{J})/(N(\mathfrak{d}\mathfrak{J})N(\mathfrak{a}))$. Thus

$$M_1(\mathcal{R}) = M_2(\mathcal{R}) + O(X^{3-\epsilon/4}), \qquad (10.11)$$

where

$$M_2(\mathcal{R}) := |\widetilde{\mathcal{A}}(X_0,\mathcal{X})|\Big(\sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}}\frac{n_p}{p}\Big)\Big(\sum_{\mathfrak{J}\in\mathcal{I}} Z_1(\mathfrak{J})Z_2(\mathfrak{J})\Big), \tag{10.12}$$

$$Z_1(\mathfrak{J}) := \sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})\frac{c_{\mathcal{R}_2}(X_0^4/(m_0N(\mathbf{a}\mathfrak{J})))}{N(\mathfrak{a})}, \tag{10.13}$$

$$Z_2(\mathfrak{J}) := \sum_{\substack{N(\mathfrak{d})<R\\ (N(\mathfrak{d}),m')=1}} \lambda_{\mathfrak{d}}\frac{\varrho_{\mathbf{v}}(\mathfrak{d}\mathfrak{J})}{N(\mathfrak{d}\mathfrak{J})(m')^3} \tag{10.14}$$

$$n_p := \frac{1}{p^2}|\{y_1,y_2,y_3 \pmod p:\ f(y_1,y_2,y_3)\equiv 0 \pmod p)\}|. \tag{10.15}$$

First we simplify $Z_1(\mathfrak{J})$. Since this is a sum of a smooth function over products of ℓ prime ideals in a bounded region, this can be estimated using the Prime Ideal Theorem. Following the arguments of [14, Section 8, proof of Lemma 8.6] we find that

$$Z_1(\mathfrak{J}) = c_{\mathcal{R}_1\times\mathcal{R}_2}(X_0^4/m_0N(\mathfrak{J})) + O(\eta_3).$$

We recall that $\mathcal{I} = \{\mathfrak{J} : (N(\mathfrak{J}),m) = 1,\ N(\mathfrak{J})\in[I,I+\eta_3 I]\}$ and $\mathcal{R} = cR_1\times\mathcal{R}_2$. Thus, by Lemma 9.12, we have

$$Z_1(\mathfrak{J}) = c_{\mathcal{R}}(X_0^4/m_0I) + O(\eta_3). \tag{10.16}$$

Now we consider $Z_2(\mathfrak{J})$. By Lemma 9.5 we find that

$$Z_2(\mathfrak{J}) = \frac{h(\mathfrak{J})g((m'))\tilde{\mathfrak{S}}}{\gamma_K m'^3} + O(16^{\omega((m)\mathfrak{J})}\exp(-c\sqrt{\log R})), \tag{10.17}$$

where

$$g((m)) := \prod_{\mathfrak{P}|(m)}\Big(1-\frac{\varrho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\Big)^{-1},$$

$$h(\mathfrak{J}) := \prod_{\mathfrak{P}|\mathfrak{J}}\Big(1-\frac{\rho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\Big)^{-1}\prod_{\mathfrak{P}_2^e||\mathfrak{J}}\Big(\frac{\rho_{\mathbf{v}}(\mathfrak{P}^e)}{N(\mathfrak{P}^e)}-\frac{\rho_{\mathbf{v}}(\mathfrak{P}^{e+1})}{N(\mathfrak{P}^{e+1})}\Big).$$

Putting together (10.16) and (10.17), we see that

$$\sum_{\mathfrak{J}\in\mathcal{I}} Z_1(\mathfrak{J})Z_2(\mathfrak{J}) = \frac{g((m'))\tilde{\mathfrak{S}}c_{\mathcal{R}}(X_0^4/m_0I)}{\gamma_K m'^3}\sum_{\mathfrak{J}\in\mathcal{I}} h(\mathfrak{J}) + O(\eta_3^2 I). \tag{10.18}$$

Since $h(\mathfrak{J})$ is multiplicative, the sum can be calculated by a contour computation

$$\begin{aligned}\sum_{\mathfrak{J}\in\mathcal{I}} h(\mathfrak{J}) &= \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{I^s((1+\eta_3)^s-1)}{s}\sum_{\mathfrak{J}}\frac{h(\mathfrak{J})}{N(\mathfrak{J})^s}ds\\ &= \mathrm{Res}_{s=0}\Big(\frac{I^s((1+\eta_3)^s-1)}{s}\sum_{\mathfrak{J}}\frac{h(\mathfrak{J})}{N(\mathfrak{J})^s}\Big) + O(\exp(-c\sqrt{\log R})).\end{aligned} \tag{10.19}$$

We see that the residue is given by

$$\begin{aligned}
&\gamma_K \log(1+\eta_3) \prod_{\mathfrak{P}} \Big(1 + h(\mathfrak{P}) + h(\mathfrak{P}^2) + ...\Big)\Big(1 - \frac{1}{N(\mathfrak{P})}\Big) \\
&= \gamma_K \log(1+\eta_3) \prod_{\mathfrak{P}} \Bigg(1 + \Big(1 - \frac{\rho(\mathfrak{P})}{N(\mathfrak{P})}\Big)^{-1} \Big(\sum_{e \geq 1} \Big(\frac{\rho(\mathfrak{P}^e)}{N(\mathfrak{P}^e)} - \frac{\rho(\mathfrak{P}^{e+1})}{N(\mathfrak{P}^{e+1})}\Big)\Big)\Bigg)\Big(1 - \frac{1}{N(\mathfrak{P})}\Big) \\
&= \gamma_K \log(1+\eta_3) \prod_{\mathfrak{P}} \Big(1 - \frac{\rho(\mathfrak{P})}{N(\mathfrak{P})}\Big)^{-1} \Big(1 - \frac{1}{N(\mathfrak{P})}\Big) \prod_{\mathfrak{P}} \Bigg(\Big(1 - \frac{\rho(\mathfrak{P})}{N(\mathfrak{P})}\Big) + \frac{\rho(\mathfrak{P})}{N(\mathfrak{P})}\Bigg) \\
&= \gamma_K \frac{\log(1+\eta_3)}{\tilde{\mathfrak{S}}}. \qquad (10.20)
\end{aligned}$$

Putting together (10.18) (10.19) and (10.20) we see that

$$\sum_{\mathfrak{I} \in \mathcal{I}} Z_1(\mathfrak{I}) Z_2(\mathfrak{I}) = \frac{g((m'))\eta_3 c_{\mathcal{R}}(X_0^4/m_0 I)}{m'^3} + O(\eta_3^2 I). \qquad (10.21)$$

Finally, we recall the definition (10.15) of n_p. Since f is the product of two linear factors when $p \equiv 1 \pmod{D_f}$, we have $n_p = 2 + O(1/p)$ for all $p \in [P_1, P_2]$. Thus

$$\sum_{\substack{p \in [P_1, P_2] \\ p \equiv 1 \pmod{D_f}}} \frac{n_p}{p} = \frac{(2 + O(\eta_3)) \log(P_2/P_1)}{\varphi(D_f)}. \qquad (10.22)$$

Putting together (10.11), (10.12), (10.21) and (10.22) now gives the result. □

We are now in a position to establish Proposition 9.13.

Proof of Proposition 9.13. We see that putting together Lemma 10.1 and 10.2 gives the desired conclusion provided $B_1^4 > X^{1+\epsilon} R P_2^{12}$. Recalling from (9.22), (9.26) and (10.2) that $R = X^{\epsilon_{00}}$, $P_2 = X^{\tau'}$, $B_1^4 = X^{\sum_{i=1}^{\ell'} t_i} \geq X^{\sum_{i=1}^{\ell'} \theta_i}$ we see that this condition is satisfied provided

$$\sum_{i=1}^{\ell'} \theta_i > 1 + \epsilon_{00} + 12\tau'$$

and ϵ is taken sufficiently small. This gives the result. □

11 Proposition 9.14: The term $T_1(\mathcal{R})$

In this section we use the dispersion method to bound $T_1(\mathcal{R})$ and establish Proposition 9.14. Let us recall the expression of $T_1(\mathcal{R})$

$$T_1(\mathcal{R}) = \sum_{\substack{p \in [P_1, P_2] \\ p \equiv 1 \pmod{D_f}}} \sum_{\mathfrak{I} \in \mathcal{I}} \mathfrak{m}_0 \sum_{\mathfrak{I}\mathfrak{a}\mathfrak{b} \in \tilde{\mathcal{A}}(\mathbf{v}_0, m', p)} \mathbf{1}_{\mathcal{R}_1}(\mathfrak{a})(\mathbf{1}_{\mathcal{R}_2}(\mathfrak{b}) - \tilde{\mathbf{1}}_{\mathcal{R}_2}(\mathfrak{b})).$$

To simplify some notation we will write

$$\tilde{g}(\mathfrak{b}) := \mathbf{1}_{\mathcal{R}_2}(\mathfrak{b}) - \tilde{\mathbf{1}}_{\mathcal{R}_2}(\mathfrak{b}). \tag{11.1}$$

We first split the sum over $\mathfrak{b}$ into ideal classes $\mathcal{C} \in Cl_K$. Let $\mathfrak{c} \in \mathcal{C}$ with $(N(\mathfrak{c}), m') = 1$ and $N(\mathfrak{c}) \ll m'^{o(1)} \ll (\log X)^{o(1)}$ and let $\mathfrak{c}' = (N(\mathfrak{c})/\mathfrak{c})$. Since the ideals in the set $\mathcal{A}$ are principal, the ideals $\mathfrak{M}_0\mathfrak{I}\mathfrak{a}\mathfrak{c}$ and $\mathfrak{b}\mathfrak{c}'$ are principal. Therefore they are respectively of the form $(\alpha), (\beta)$ with $\mathfrak{M}_0\mathfrak{I}\mathfrak{c}|(\alpha)$, $\mathfrak{c}'|(\beta)$ with $W\alpha = a_1\nu_1 + a_2\nu_2 + a_3\nu_3 + a_4\nu_4$, $W\beta = b_1\nu_1 + b_2\nu_2 + b_3\nu_3 + b_3\nu_4$, where $a_1, a_2, a_3, b_1, b_2, b_3, b_4 \in \mathbb{Z}$ and with $\mathbf{a}, \mathbf{b}$ lying in the fundamental domain $\mathcal{D}$. We will write $\mathbf{a} = (a_1, a_2, a_3, a_4)$, $\mathbf{b} = (b_1, b_2, b_3, b_4)$. In order to handle the modulo m condition between $\mathfrak{b}$ and $\mathfrak{I}\mathfrak{a}$ we split the sums according to some congruence classes on α, β modulo m'. Together this gives

$$T_1(\mathcal{R}) = \sum_{\mathcal{C}\in Cl_K} \sum_{\substack{\mathbf{a}_0,\mathbf{b}_0 \pmod{m'} \\ N(\mathfrak{c})(\mathbf{a}_0\diamond\mathbf{b}_0)_i \equiv (\mathbf{v}_0)_i \pmod{m'},\ \text{for } i=1,2,3,4}} \tilde{T}_{\mathfrak{c}}(\mathcal{R}, \mathbf{a}_0, \mathbf{b}_0), \tag{11.2}$$

with $(a_0)_4 = 0$ since $(\mathbf{a}\diamond\mathbf{b})_4 = 0$ and $\mathfrak{c} \in \mathcal{C}$ is a well chosen representative, and $\mathfrak{c}'$ as above

$$\tilde{T}_{\mathfrak{c}}(\mathcal{R}, \mathbf{a}_0, \mathbf{b}_0) = \sum_{\substack{p\in[P_1,P_2] \\ p\equiv 1 \pmod{D_f}}} \sum_{\mathfrak{I}\in\mathcal{I}} \sum_{\substack{\mathbf{a}\equiv\mathbf{a}_0 \pmod{m'} \\ \mathbf{b}\equiv\mathbf{b}_0 \pmod{m'} \\ \mathfrak{M}_0\mathfrak{I}\mathfrak{c}|(\alpha), \mathfrak{c}'|(\beta) \\ (\alpha\beta)/(N(\mathfrak{c}))\in\widetilde{\mathcal{A}}(p)}} \mathbf{1}_{\mathcal{R}_1}\Big(\frac{(\alpha)}{\mathfrak{M}_0\mathfrak{I}\mathfrak{c}}\Big)\tilde{g}\Big(\frac{(\beta)}{\mathfrak{c}'}\Big),$$

with now $\widetilde{\mathcal{A}}(p) = \widetilde{\mathcal{A}}(\mathcal{X}, \mathbf{0}, 1, p)$.

We recall that our previous conditions (10.1), (10.2) imply that $N(\beta) \in [B^4, B^4(1 + O(\eta_2^2 \log X))]$, where

$$B = B_1 N(\mathfrak{c}')^{1/4} \in [B_1, B_1(\log X)^{o(1)}]$$

The support of $\mathbf{1}_{\mathcal{R}_1}$ implies that

$$N(\alpha) \in [A^4, A^4(1 + \eta_2^2 \log X)]$$

where (recalling that $N(\mathfrak{I}) \in [I, I(1 + \eta_3)]$ from (9.20))

$$A^4 := X^{\sum_{i=\ell'+1}^{\ell} t_i} N(\mathfrak{c}) m_0 I \ll X^{\sum_{i=\ell'+1}^{\ell} t_i} I(\log X)^{5K}. \tag{11.3}$$

We note that $A^4B^4 \ll X^4(\log X)^{6K}$. We will use the notation of [14, p. 80 and 71]:

$$\mathcal{R}_{X_0} := \Big\{\mathbf{x} \in \mathbb{R}^4 : x_i \in [X_i, X_i(1+\eta_1)], i = 1, 2, 3,\ x_4 = 0, \\ N(\sum_{i=1}^{3} x_i\nu_i) \in [X_0^4, X_0^4(1+\eta_3)]\Big\}, \tag{11.4}$$

$$\mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2} := \Big\{\mathbf{a} \in \mathbb{R}^4 : \|a\| \in [A, 2A], \mathbf{a}\diamond\mathbf{b}_1 \in \mathcal{R}_{X_0},\ \mathbf{a}\diamond\mathbf{b}_2 \in \mathcal{R}_{X_0}\Big\}.$$

Let $\mathcal{F}$ be a fundamental domain such that if $\mathbf{1}_{\mathcal{R}_1}((\alpha)/\mathfrak{M}_0\mathfrak{I}\mathfrak{c}) = 1$ and $\alpha \in \mathcal{F}$ then $a_i \ll A$ for all $i = 1, 2, 3, 4$ and similarly, $b_i \ll B$ for all

$1 \le i \le 4$ whenever $\beta \in \mathcal{F}$ and $\tilde{g}((\beta)/\mathbf{c}) \neq 0$. By slight abuse of notation, we will also regard $\mathcal{F}$ as a subset of $\mathbb{R}^4$ so that $\mathbf{a} \in \mathcal{F}$ corresponds to $\alpha \in \mathcal{F}$.

We will concentrate on ideals (β) with not too many divisors. For this we introduce a slight variant of $\tilde{g}$

$$g_{\mathbf{b}} := \begin{cases} \mathbf{1}_{\mathcal{R}_2}(\mathfrak{b}/\mathfrak{c}') - \tilde{\mathbf{1}}_{\mathcal{R}_2}(\mathfrak{b}/\mathfrak{c}') & \text{if } \tau(\mathfrak{b}) \le \eta_4^{-1} \text{ and } \mathfrak{c}'|(\beta), \\ 0 & \text{otherwise,} \end{cases} \tag{11.5}$$

$$\eta_4 := (\log X)^{-K_1} \tag{11.6}$$

for a suitably large fixed constant K_1. Following [14, section 11] except that we apply Lemma 9.8, we prove that we can replace $\tilde{g}_{\mathbf{b}}$ by $g_{\mathbf{b}}$ with a error term less than $O(\eta_4 X_0^3 (\log X)^{O(1)})$. This error is sufficiently small for Proposition 9.14 when K_1 is chosen large enough in term of K.

Thus now we have to concentrate on sums

$$T_{\mathfrak{c}}(\mathcal{R}, \mathbf{a}_0, \mathbf{b}_0) = \sum_{\substack{p \in [P_1, P_2] \\ p \equiv 1 \pmod{D_f}}} \sum_{\mathfrak{I} \in \mathcal{I}} \sum_{\substack{\mathbf{a} \equiv \mathbf{a}_0 \pmod{m'} \\ \mathbf{b} \equiv \mathbf{b}_0 \pmod{m'} \\ \mathfrak{M}_0 \mathfrak{I}\mathfrak{c} | (\alpha), \mathfrak{c}' | (\beta) \\ \mathfrak{I}(\alpha\beta)/(N(\mathfrak{c})) \in \widetilde{\mathcal{A}}(p) \\ \mathbf{a} \diamond \mathbf{b} \in \mathcal{R}_{X_0}}} \mathbf{1}_{\mathcal{F}}(\mathbf{a}) \mathbf{1}_{\mathcal{R}_1}\Big(\frac{(\alpha)}{\mathfrak{M}_0 \mathfrak{I}\mathfrak{c}}\Big) g_{\mathbf{b}}. \tag{11.7}$$

11.1 Cosmetic reductions

For $T > 0$, we denote by $\mathcal{C}_T$ the subset of $\mathbb{R}^4$ defined by

$$\mathcal{C}_T = \{\mathbf{a} \in \mathcal{F} : N(\mathfrak{a}) \in [T^4, 2T^4]\},$$

so that $\mathbf{a} \in \mathcal{C}_A$ and $\mathbf{b} \in \mathcal{C}_B$. By Weber's Theorem [19], we have

$$|\mathcal{C}_T| = \lambda_K T^4 + O(T^3),$$

for some λ_K depending only on K ($\lambda_K = \gamma_K / h_K$, but we do not need this). We note that from the support of $\mathbf{1}_{\mathcal{R}_1}$ and $\mathbf{1}_{\mathcal{R}_2}$ and $\tilde{\mathbf{1}}_{\mathcal{R}_2}$ we my restrict to $\mathbf{a} \in \mathcal{C}_A$ and $\mathbf{b} \in \mathcal{C}_B$.

It will make some later technicalities simpler if we introduce the restriction $p \nmid N(\mathbf{b})$ to the terms in T_1. By Proposition 9.11 and the divisor bound, we can do this at the cost of an error term of size

$$\ll \sum_{p \in [P_1, P_2]} \sum_{\substack{\mathbf{b} \in \mathcal{C}_B \\ N(\mathfrak{b}) \equiv 0 \pmod{p}}} \sum_{\mathfrak{b}\mathfrak{u} \in \widetilde{\mathcal{A}}(0,1,p)} X^{o(1)} \ll X^{\varepsilon}(X^3 P_1^{-1} + X^2 B^{4/3} P_2^2 + B^4 P_2^5).$$

This is acceptably small provided

$$B < \frac{X^{3/4-\epsilon}}{P_2^{3/2}}. \tag{11.8}$$

We recall that $f \in \mathbb{Z}[X_1, X_2, X_3]$ is quadratic and homogeneous and D_f is the associated modulus introduced in the hypothesis of Theorem 4.1 so that when $p \equiv 1 \pmod{D_f}$, the function $f \pmod{p}$ factors as the

product of two linear factors. Thus the condition $p|f(\mathbf{a}\diamond\mathbf{b})$ is equivalent to $p|\mathbf{v}_p\cdot(\mathbf{a}\diamond\mathbf{b})$ or $p|\mathbf{w}_p\cdot(\mathbf{a}\diamond\mathbf{b})$ for two non-zero vectors $\mathbf{v}_p, \mathbf{w}_p \in \mathbb{Z}^4$. There are $O(p^5)$ choices of $\mathbf{a}_p, \mathbf{b}_p \pmod p$ such that $(\mathbf{a}_p\diamond\mathbf{b}_p)_4 = \mathbf{v}_p\cdot(\mathbf{a}_p\diamond\mathbf{b}_p) = \mathbf{w}_p\cdot(\mathbf{a}_p\diamond\mathbf{b}_p)$ whenever p is sufficiently large in terms of f. Therefore, as above, provided (11.8) holds, the contribution of the $\mathbf{a}$, $\mathbf{b}$ such that $p|\mathbf{v}_p\cdot(\mathbf{a}\diamond\mathbf{b})$ and $p|\mathbf{w}_p\cdot(\mathbf{a}\diamond\mathbf{b})$ is bounded by

$$X^{o(1)}\sum_{p\in[P_1,P_2]}\sum_{\substack{\mathbf{a}_p,\mathbf{b}_p\in\{1,\dots,p\}^4\\(\mathbf{a}_p\diamond\mathbf{b}_p)_4\equiv 0 \pmod p\\ p|\mathbf{v}_p\cdot(\mathbf{a}_p\diamond\mathbf{b}_p)\\ p|\mathbf{w}_p\cdot(\mathbf{a}_p\diamond\mathbf{b}_p)}}\sum_{\substack{\mathbf{b}\in\mathbb{Z}^4\cap C_B\\ \mathbf{b}\equiv\mathbf{b}_p \pmod p}}\sum_{\substack{\mathfrak{u}\in\widetilde{\mathcal{A}}(0,1,p)\\ \mathfrak{b}|\mathfrak{u}\\ \mathbf{u}\equiv(\mathbf{a}_p\diamond\mathbf{b}_p) \pmod p}} 1 \ll X^{3+\varepsilon}P_1^{-1}.$$

Putting this together, we see that it suffices for us to estimate for each $C\in Cl_K$ with a representative $\mathfrak{c}\in C$ and each $\mathbf{a}_0, \mathbf{b}_0 \pmod{m'}$ the sums

$$T_3(\mathcal{R}) := \sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}}\sum_{\mathfrak{I}\in\mathcal{I}}\sum_{\substack{\mathbf{b}\in\mathbb{Z}^4\cap\mathcal{C}_B\\ \mathbf{b}\equiv\mathbf{b}_0 \pmod{m'}\\ p\nmid N(\mathbf{b})}}\sum_{\substack{\mathbf{a}\in\mathbb{Z}^4\cap\mathcal{C}_A\\ (\mathbf{a}\diamond\mathbf{b})\in\mathcal{R}_{X_0}\\ p|\mathbf{v}_p\cdot(\mathbf{a}\diamond\mathbf{b})\\ \mathbf{a}\equiv\mathbf{a}_0 \pmod{m'}\\ \mathfrak{M}_0\mathfrak{I}\mathfrak{c}|\mathfrak{a}}} \mathbf{1}_{\mathcal{R}_1}\Big(\frac{\mathfrak{a}}{\mathfrak{M}_0\mathfrak{I}\mathfrak{c}}\Big)g_{\mathbf{b}}. \tag{11.9}$$

11.2 Dispersion method

We swap the order of summation, and apply Cauchy-Schwarz. The ideals $\mathfrak{I}$ and $\mathfrak{a}/\mathfrak{I}$ are coprime since $N(\mathfrak{I}) < X^{\theta_i}$ for all $1\le i\le\ell$. In the application of Cauchy-Schwarz we can group these ideals together. We recall that the set $\mathcal{R}_{X_0}$ is defined in (11.4). This gives

$$T_3^2 \ll A^4\sum_{\substack{\mathbf{a}\in\mathbb{Z}^4\cap\mathcal{C}_A\\ \mathbf{a}\equiv\mathbf{a}_0 \pmod{m'}}}\Big(\sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}}\sum_{\substack{\mathbf{b}\in\mathbb{Z}^4\cap\mathcal{C}_B\\ \mathbf{a}\diamond\mathbf{b}\in\mathcal{R}_{X_0}\\ p|\mathbf{v}_p\cdot(\mathbf{a}\diamond\mathbf{b})\\ \mathbf{b}\equiv\mathbf{b}_0 \pmod{m'}\\ p\nmid N(\mathbf{b})}} g_{\mathbf{b}}\Big)^2.$$

Thus we see that

$$T_3^2 \ll A^4T_4 \tag{11.10}$$

where, with the notation (11.4)

$$T_4 := \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}}\sum_{\substack{\mathbf{b}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_B\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod{m'}\\ p_1\nmid N(\mathbf{b}_1),\, p_2\nmid N(\mathbf{b}_2)}} g_{\mathbf{b}_1}g_{\mathbf{b}_2}\sum_{\substack{\mathbf{a}\in\mathbb{Z}^4\cap\mathcal{C}_A\\ \mathbf{a}\in\mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}\\ p_1|\mathbf{v}_{p_1}\cdot(\mathbf{a}\diamond\mathbf{b}_1)\\ p_2|\mathbf{v}_{p_2}\cdot(\mathbf{a}\diamond\mathbf{b}_2)}} 1.$$

Thus we wish to show that T_4 is small compared with A^2B^6.

11.3 Collinear $\mathbf{b}_1, \mathbf{b}_2$

We separate the situation when $\mathbf{b}_1$ and $\mathbf{b}_2$ are collinear (in which case we have $\wedge(\mathbf{b}_1,\mathbf{b}_2)=0$ where $\wedge(\mathbf{x},\mathbf{y})$ is the L^2 norm of the six 2×2

subdeterminants of the 2×4 matrix with columns $\mathbf{x}$ and $\mathbf{y}$). Thus we have

$$T_4 = T_5 + T_6, \tag{11.11}$$

where T_5 is those terms with $\wedge(\mathbf{b}_1, \mathbf{b}_2) = 0$ and T_6 is those terms with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \neq 0$.

We first concentrate on T_5.

Lemma 11.1.

$$T_5 \ll X^{o(1)} A^3 B^3.$$

Proof. Let $\mathbf{c}$ be the shortest non-zero vector with integer components which is collinear with $\mathbf{b}_1$ (this is $\mathbf{b}_1$ divided by the gcd of its components). Then we see that $\mathbf{b}_1 = \lambda_1 \mathbf{c}$ for some $\lambda \in \mathbb{Z}$, and since $\mathbf{b}_2$ is collinear with $\mathbf{b}_1$, we also have that $\mathbf{b}_2 = \lambda_2 \mathbf{c}$ for some $\lambda_2 \in \mathbb{Z}$. Thus we see that

$$T_5 \ll \eta_4^{-2} \sum_{\substack{\mathbf{c} \in \mathbb{Z}^4 \\ \|\mathbf{c}\| \ll B}} \sum_{\lambda_1, \lambda_2 \ll B/\|\mathbf{c}\|} \sum_{\substack{\mathbf{a} \in \mathbb{Z}^4 \cap \mathcal{C}_A \\ (\mathbf{a} \diamond \mathbf{c})_4 = 0}} \sum_{\substack{p_1, p_2 \in [P_1, P_2] \\ p_1 | f(\lambda_1 \mathbf{a} \diamond \mathbf{c}) \\ p_2 | f(\lambda_2 \mathbf{a} \diamond \mathbf{c})}} 1.$$

We see that the inner sum is $O(1)$ since $P_1 \gg B^{\epsilon}$ and $f(\lambda_1 \mathbf{a} \diamond \mathbf{c}) \ll B^{O(1)}$. We then split the size of $\|\mathbf{c}\|$ into dyadic ranges, giving

$$T_5 \ll \eta_4^{-2} (\log X) \sup_{C \ll B} \frac{B^2}{C^2} \sum_{\substack{\mathbf{c} \in \mathbb{Z}^4 \\ \|\mathbf{c}\| \asymp C}} \sum_{\substack{\mathbf{a} \in \mathbb{Z}^4 \cap \mathcal{C}_A \\ (\mathbf{a} \diamond \mathbf{c})_4 = 0}} 1.$$

We now let $\mathbf{z} = (\mathbf{a} \diamond \mathbf{c})$. By the divisor bound, given $\mathbf{z}$ there are $O(\tau_K(\mathfrak{z}))$ choices of $\mathbf{a}, \mathbf{c}$. Thus we see that

$$\begin{aligned} T_5 &\ll \eta_4^{-2} (\log X) \sup_{C \ll B} \frac{B^2}{C^2} \sum_{z_1, z_2, z_3 \ll AC} \tau_K(z_1 \nu_1 + z_2 \nu_2 + z_3 \nu_3) \\ &\ll \eta_4^{-3} A^3 B^3. \end{aligned}$$

□

Thus we are left to bound T_6.

11.4 Lattice counts

We now concentrate on the inner sum. Let $\Lambda_{\mathbf{b}_1, \mathbf{b}_2}$ and $\Lambda_{\mathbf{b}_1, \mathbf{b}_2, p_1, p_2}$ denote the lattices

$$\begin{aligned} \Lambda_{\mathbf{b}_1, \mathbf{b}_2} &:= \{\mathbf{x} \in \mathbb{Z}^4 : (\mathbf{x} \diamond \mathbf{b}_1)_4 = (\mathbf{x} \diamond \mathbf{b}_2)_4 = 0\}, \\ \Lambda_{\mathbf{b}_1, \mathbf{b}_2, p_1, p_2} &:= \{\mathbf{x} \in \Lambda_{\mathbf{b}_1, \mathbf{b}_2} : p_1 | \mathbf{v}_{p_1} \cdot (\mathbf{x} \diamond \mathbf{b}_1),\ p_2 | \mathbf{v}_{p_2} \cdot (\mathbf{x} \diamond \mathbf{b}_2)\}. \end{aligned}$$

Thus the inner sum in T_6 is

$$\sum_{\substack{\mathbf{a} \in \mathcal{C}_A \cap \Lambda_{\mathbf{b}_1, \mathbf{b}_2, p_1, p_2} \\ \mathbf{a} \in \mathcal{R}_{\mathbf{b}_1, \mathbf{b}_2}}} 1.$$

If $\mathbf{b}_1, \mathbf{b}_2$ are not collinear, then $\Lambda_{\mathbf{b}_1, \mathbf{b}_2}$ is a lattice of rank 2, and so it has a Minkowski-reduced basis $\{\mathbf{z}_1, \mathbf{z}_2\}$ ([14, Lemma 4.1] for example).

Without loss of generality we may assume that $\|\mathbf{z}_1\| \le \|\mathbf{z}_2\|$. Thus we have that

$$\sum_{\mathbf{a}\in\mathcal{C}_A\cap\Lambda_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}\cap\mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}} 1 = \sum_{\substack{\lambda_1,\lambda_2\in\mathbb{Z}\\ \lambda_1\mathbf{z}_1+\lambda_2\mathbf{z}_2\in\mathcal{C}_A\cap\mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}\\ \lambda_1 c_1+\lambda_2 c_2\equiv 0 \pmod{p_1}\\ \lambda_1 c_3+\lambda_2 c_4\equiv 0 \pmod{p_2}}} 1,$$

for some constants c_1, c_2, c_3, c_4 depending only on $\mathbf{b}_1, \mathbf{b}_2$, p_1 and p_2. The condition $\lambda_1\mathbf{z}_1 + \lambda_2\mathbf{z}_2 \in \mathcal{C}_A \cap \mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}$ forces (λ_1, λ_2) to lie in a region $\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2} \subseteq \mathbb{R}^2$. Since $\|\lambda_1\mathbf{z}_1 + \lambda_2\mathbf{z}_2\| \asymp |\lambda_1|\|\mathbf{z}_1\| + |\lambda_2|\|\mathbf{z}_2\|$ (by [14, Lemma 4.1]) and $\mathcal{C}_A$ only contains vectors of norm $O(A)$, we see that lying in $\mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}$ forces $\lambda_1 \ll A/\|\mathbf{z}_1\|$ and $\lambda_2 \ll A/\|\mathbf{z}_2\|$, so $\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2}$ has volume $O(A^2/\|\mathbf{z}_1\|\|\mathbf{z}_2\|)$.

By Davenport's Theorem on counting lattice points ([14, Lemma 7.1] for example), we have that

$$\sum_{\substack{(\lambda_1,\lambda_2)\in\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2}\\ \lambda_1 c_1+\lambda_2 c_2=0 \pmod{p_1}\\ \lambda_1 c_3+\lambda_2 c_4=0 \pmod{p_2}}} 1 = \frac{\operatorname{vol}(\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2})}{f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}} + O\Big(\frac{A}{\|\mathbf{z}_1\|}\Big)$$

where $f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2} = [\Lambda_{\mathbf{b}_1,\mathbf{b}_2} : \Lambda_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}]$ is the index of the lattices, given explicitly in terms of $c_1, c_2, c_3, c_4, p_1, p_2$ by

$$f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2} = \begin{cases} 1, & c_1 \equiv c_2 \equiv 0 \pmod{p_1} \text{ and } c_3 \equiv c_4 \equiv 0 \pmod{p_2},\\ p_2, & c_1 \equiv c_2 \equiv 0 \pmod{p_1} \text{ and } c_3, c_4 \text{ not both } 0 \pmod{p_2},\\ p_1, & c_3 \equiv c_4 \equiv 0 \pmod{p_2} \text{ and } c_1, c_2 \text{ not both } 0 \pmod{p_1},\\ p_1, & p_1 = p_2 \text{ and } c_1c_4 \equiv c_2c_3 \pmod{p_1} \text{ and } c_1, c_2 \text{ not all } 0 \pmod{p_1},\\ p_1p_2, & \text{otherwise.}\end{cases}$$

We split T_6 into the contribution from the main term $\operatorname{vol}(\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2})/f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}$ and the error term $O(A/\|\mathbf{z}_1\|)$. This gives

$$T_6 = T_8 + O(T_7), \tag{11.12}$$

where

$$T_7 := \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{b}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_B\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod{m'}\\ p_1\nmid N(\mathbf{b}_1),\, p_2\nmid N(\mathbf{b}_2)\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0}} \frac{\eta_4^{-2}A}{\|\mathbf{z}_1\|},$$

$$T_8 := \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{b}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_B\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod{m'}\\ p_1\nmid N(\mathbf{b}_1),\, p_2\nmid N(\mathbf{b}_2)\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0}} \frac{g_{\mathbf{b}_1}g_{\mathbf{b}_2}\operatorname{vol}(\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2})}{f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}}.$$

We first show that the contribution T_7 from the error term is small.

Lemma 11.2.

$$T_7 \ll X^{o(1)}AB^7P_2^2.$$

Proof. We note that $\mathbf{z}_1 \in \mathbb{Z}^4$ with $\|\mathbf{z}_1\|^2 \le \|\mathbf{z}_1\| \cdot \|\mathbf{z}_2\| \ll \det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2}) \ll B^2$. Thus $\|\mathbf{z}_1\| \ll B$. Thus we can rearrange the summation to give

$$T_7 \ll \eta_4^{-2} P_2^2 \sum_{\mathbf{b}_1,\mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_B} \frac{A}{\|\mathbf{z}_1\|} \ll A P_2^2 \sum_{\substack{\mathbf{z}_1 \in \mathbb{Z}^4 \\ \|\mathbf{z}_1\| \ll B}} \frac{1}{\|\mathbf{z}_1\|} \Big(\sum_{\substack{\mathbf{b} \in \mathbb{Z}^4 \cap \mathcal{C}_B \\ (\mathbf{b} \diamond \mathbf{z}_1)_4 = 0}} 1 \Big)^2$$

The condition $(\mathbf{b} \diamond \mathbf{z}_1)_4 = 0$ forces $\mathbf{b}$ to lie in a rank 3 lattice of determinant $\asymp \|\mathbf{z}_1\|$. Thus the inner sum is $O(B^3/\|z_1\| + B^2)$. Thus we obtain the bound

$$T_7 \ll \eta_4^{-2} A P_2^2 \sum_{\substack{\mathbf{z}_1 \in \mathbb{Z}^4 \\ \|\mathbf{z}_1\| \ll B}} \Big(\frac{B^6}{\|\mathbf{z}_1\|^3} + \frac{B^4}{\|\mathbf{z}_1\|} \Big) \ll A B^7 P_2^2 \eta_4^{-3}.$$

This gives the result. □

Thus we are left to show that T_8 is small compared with $A^2 B^6$.

11.5 Further lattice estimates

We recall that $\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2}$ is the region $\lambda_1, \lambda_2 \in \mathbb{R}^2$ such that $\lambda_1 \mathbf{z}_1 + \lambda_2 \mathbf{z}_2 \in \mathcal{C}_A \cap \mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}$. We see that this has volume $\operatorname{vol}(\mathcal{R}''_{\mathbf{b}_1,\mathbf{b}_2})/\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})$, where $\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})$ is the determinant of the lattice (that is, the 2-dimensional area of parallelogram generated by $\mathbf{z}_1, \mathbf{z}_2$) and $\mathcal{R}''_{\mathbf{b}_1,\mathbf{b}_2}$ is the 2-dimensional region formed by intersecting $\mathcal{C}_A$ with the $\mathbf{z}_1, \mathbf{z}_2$ plane. We thus have

$$T_8 = \sum_{\substack{p_1,p_2 \in [P_1,P_2] \\ p_1 \equiv p_2 \equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{b}_1,\mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_B \\ \mathbf{b}_1 \equiv \mathbf{b}_2 \equiv \mathbf{b}_0 \pmod{m'} \\ \wedge(\mathbf{b}_1,\mathbf{b}_2) \neq 0 \\ p_1 \nmid N(\mathbf{b}_1),\, p_2 \nmid N(\mathbf{b}_2)}} \frac{g_{\mathbf{b}_1} g_{\mathbf{b}_2} \operatorname{vol}(\mathcal{R}''_{\mathbf{b}_1,\mathbf{b}_2})}{f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2} \det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})}.$$

We first establish a few simple estimates.

Lemma 11.3.

$$\sum_{\substack{p_1,p_2 \in [P_1,P_2] \\ p_1 \equiv p_2 \equiv 1 \pmod{D_f}}} \frac{\operatorname{vol}(\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2})}{f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}} \ll \operatorname{vol}(\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2}) + O\Big(\frac{A P_2^2}{\|\mathbf{z}_1\|}\Big).$$

Proof. We have that

$$\begin{aligned} \sum_{\substack{p_1,p_2 \in [P_1,P_2] \\ p_1 \equiv p_2 \equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{a} \in \mathbb{Z}^4 \cap \mathcal{C}_A \\ \mathbf{a} \in \mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2} \\ p_1 \mid \mathbf{v}_{p_1} \cdot \mathbf{a} \diamond \mathbf{b}_1 \\ p_2 \mid \mathbf{v}_{p_2} \cdot \mathbf{a} \diamond \mathbf{b}_2}} 1 &= \sum_{\substack{\mathbf{a} \in \mathbb{Z}^4 \cap \mathcal{C}_A \\ \mathbf{a} \in \mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}}} \sum_{\substack{p_1,p_2 \in [P_1,P_2] \\ p_1 \equiv p_2 \equiv 1 \pmod{D_f} \\ p_1 \mid \mathbf{v}_{p_1} \cdot \mathbf{a} \diamond \mathbf{b}_1 \\ p_2 \mid \mathbf{v}_{p_2} \cdot \mathbf{a} \diamond \mathbf{b}_2}} 1 \\ &\ll \sum_{\substack{\mathbf{a} \in \mathbb{Z}^4 \cap \mathcal{C}_A \\ \mathbf{a} \in \mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}}} 1 \\ &\ll \operatorname{vol}(\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2}) + O\Big(\frac{A}{\|\mathbf{z}_1\|}\Big). \end{aligned}$$

On the other hand, we know that

$$\sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{a}\in\mathbb{Z}^4\cap\mathcal{C}_A\\ \mathbf{a}\in\mathcal{R}_{\mathbf{b}_1,\mathbf{b}_2}\\ p_1|\mathbf{v}_{p_1}\cdot\mathbf{a}\diamond\mathbf{b}_1\\ p_2|\mathbf{v}_{p_2}\cdot\mathbf{a}\diamond\mathbf{b}_2}} 1 = \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \Big(\frac{\mathrm{vol}\,(\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2})}{f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}}+O\Big(\frac{A}{\|\mathbf{z}_1\|}\Big)\Big).$$

Putting these together gives the result. □

Lemma 11.4. *Let*

$$\mathcal{C}_{C,d;\mathbf{c}_1,\mathbf{b}_2} := \#\Big\{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_B : \wedge(\mathbf{b}_1,\mathbf{b}_2)\sim\frac{B^2}{C},\ \mathbf{b}_1\equiv\mathbf{c}_1 \pmod d\Big\}.$$

Then we have

$$\#\mathcal{C}_{C,d;\mathbf{c}_1,\mathbf{c}_2} \ll \Big(1+\frac{B}{d}\Big)\Big(1+\frac{B}{Cd}\Big)^3.$$

Proof. The condition $\wedge(\mathbf{b}_1,\mathbf{b}_2)\sim B^2/C$ forces $\mathbf{b}_1$ to lie in a cylinder $\mathcal{C}$ with axis of length $O(B)$ proportional to $\mathbf{b}_2$, and with radius $O(B/C)$. We then see that we can cover this cylinder with

$$\ll \Big(1+\frac{B}{d}\Big)\Big(1+\frac{B}{Cd}\Big)^3$$

different hypercubes $\mathcal{B}$ of side length d. Finally, there is at most one choice of $\mathbf{b}_1$ in a hypercube $\mathcal{B}$ of side length d which satisfies $\mathbf{b}_1\equiv\mathbf{c}_1 \pmod d$, which gives the result. □

For any $\mathbf{c}_1,\mathbf{c}_2\in\mathbb{Z}^4$, the notation $\mathbf{c}_1\propto\mathbf{c}_2$ indicates that the two vectors are proportional.

Lemma 11.5. *If* $\mathbf{c}_1\not\propto\mathbf{c}_2 \pmod p$ *then*

$$\sum_{\substack{\mathbf{b}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_B\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ \text{primitive}\\ \mathbf{b}_1\equiv\mathbf{c}_1 \pmod p\\ \mathbf{b}_2\equiv\mathbf{c}_2 \pmod p}} \frac{1}{\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})} \ll \frac{B^6}{p^8}+B^{17/3}.$$

Proof. We recall that $\Lambda_{\mathbf{b}_1,\mathbf{b}_2}$ is the lattice in $\mathbb{Z}^4$ of $\mathbf{x}$ with $(\mathbf{x}\diamond\mathbf{b}_1)_4=(\mathbf{x}\diamond\mathbf{b}_2)_4=0$. By [14, Lemma 10.1], this has determinant $\wedge(\mathbf{b}_1,\mathbf{b}_2)/D_{\mathbf{b}_1,\mathbf{b}_2}$, where $\wedge(\mathbf{b}_1,\mathbf{b}_2)$ is the L^2 norm of the six 2×2 subdeterminants of the matrix with columns $\mathbf{b}_1,\mathbf{b}_2$, and $D_{\mathbf{b}_1,\mathbf{b}_2}$ is the greatest common divisor of these six subdeterminants. Note that this implies $\mathbf{b}_1\propto\mathbf{b}_2 \pmod{D_{\mathbf{b}_1,\mathbf{b}_2}}$, so since $\mathbf{b}_1,\mathbf{b}_2$ are primitive we must have $D_{\mathbf{b}_1,\mathbf{b}_2}\le B$ when $\wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0$.

We consider separately those $\mathbf{b}_1,\mathbf{b}_2$ with $\wedge(\mathbf{b}_1,\mathbf{b}_2)\ll B$, those with $B\ll\wedge(\mathbf{b}_1,\mathbf{b}_2)\ll B^{4/3}$, and those $\mathbf{b}_1,\mathbf{b}_2$ with

$$D_{\mathbf{b}_1,\mathbf{b}_2}=d,\qquad \wedge(\mathbf{b}_1,\mathbf{b}_2)\sim B^2/C$$

for each $1\le d\le B$ and $1\le C\le B^{2/3}$ with C running through powers of 2.

If $\wedge(\mathbf{b}_1, \mathbf{b}_2) \ll B$ then $\mathbf{b}_1$ lies within $O(1)$ of the line proportional to $\mathbf{b}_2$, and so there are $O(B)$ choices of $\mathbf{b}_1$. Since $\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2}) \geq 1$, these terms contribute a total (ignoring the congruence conditions $\pmod p$ for an upper bound)

$$\ll \sum_{\|\mathbf{b}_2\| \ll B} O(B) \ll B^5.$$

If $\wedge(\mathbf{b}_1, \mathbf{b}_2) \in [B, B^{4/3}]$ then we separately consider those with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \sim B^2/C$ for $C \in [B^{2/3}, B]$ running through powers of 2, and again drop the congruence constraints. By Lemma 11.4 there are

$$\ll B\Big(1 + \frac{B}{C}\Big)^3 \ll \frac{B^4}{C^3}$$

choices of $\mathbf{b}_1$ given $\mathbf{b}_2$. If $\wedge(\mathbf{b}_1, \mathbf{b}_2) \sim B^2/C$ then $\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2}) \geq B/C$ (since $D_{\mathbf{b}_1\mathbf{b}_2} \leq B$). Thus these terms contribute

$$\ll \sum_{C=2^j \in [B^{2/3}, B]} \sum_{\mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_B} \frac{C}{B}\frac{B^4}{C^3} \ll B^{17/3}.$$

Thus we are left to consider the terms with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \sim B^2/C$ for some $C \leq B^{2/3}$. The condition $D_{\mathbf{b}_1,\mathbf{b}_2} = d$ forces $\mathbf{b}_1 \propto \mathbf{b}_2 \pmod d$, and so $\mathbf{b}_1 \equiv \lambda\mathbf{b}_2 \pmod d$ for some $\lambda \in \{1, \dots, d\}$. Since $\mathbf{c}_1 \not\propto \mathbf{c}_2 \pmod p$, we see $p \nmid d$. Thus $\mathbf{b}_1 \equiv \mathbf{c}_0(\lambda) \pmod{dp}$, where $\mathbf{c}_0(\lambda) \equiv \lambda\mathbf{b}_2 \pmod d$ and $\mathbf{c}_0(\lambda) \equiv \mathbf{c}_1 \pmod p$. By Lemma 11.4, the number of choices of $\mathbf{b}_1$ is therefore

$$\ll \sum_{1 \leq \lambda \leq d} \#\mathcal{C}_{C,pd,\mathbf{c}_0(\lambda),\mathbf{b}_2} \ll d\Big(1 + \frac{B}{pd}\Big)\Big(1 + \frac{B}{pCd}\Big)^3 \ll B + \frac{B^4}{p^4C^3d^3}.$$

If $D_{\mathbf{b}_1,\mathbf{b}_2} = d$ and $\wedge(\mathbf{b}_1, \mathbf{b}_2) \sim B^2/C$ then $\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2}) \gg B^2/(Cd)$. Thus we find that the contribution from terms with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \geq B^{4/3}$ is

$$\sum_{\substack{\mathbf{b}_1,\mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_B \\ \wedge(\mathbf{b}_1,\mathbf{b}_2) \geq B \\ \mathbf{b}_1 \equiv \mathbf{c}_1 \pmod p \\ \mathbf{b}_2 \equiv \mathbf{c}_2 \pmod p \\ \text{primitive}}} \frac{1}{\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})} \ll \sum_{1 \leq d \leq B} \sum_{C=2^j \ll B^{2/3}} \frac{dC}{B^2} \sum_{\substack{\mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_B \\ \mathbf{b}_2 \equiv \mathbf{c}_2 \pmod p}} \Big(B + \frac{B^4}{C^3d^3p^4}\Big)$$

$$\ll \frac{B^6}{p^8} + B^{17/3}.$$

Thus we have a suitable bound in each case, giving the result. □

Lemma 11.6. *Let $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{Z}^4$ be non-zero $\pmod p$ with $\mathbf{c}_1 \propto \mathbf{c}_2 \pmod p$. Then we have*

$$\sum_{\substack{\mathbf{b}_1,\mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_B \\ \wedge(\mathbf{b}_1,\mathbf{b}_2) \neq 0 \\ \text{primitive} \\ \mathbf{b}_1 \equiv \mathbf{c}_1 \pmod p \\ \mathbf{b}_2 \equiv \mathbf{c}_2 \pmod p}} \frac{1}{\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})} \ll \frac{B^6}{p^7} + B^{17/3}.$$

Proof. This is similar to the proof of Lemma 11.5. Since the estimates in the proof of Lemma 11.5 when $\wedge(\mathbf{b}_1, \mathbf{b}_2) \ll B^{4/3}$ didn't depend on whether $p | D_{\mathbf{b}_1,\mathbf{b}_2}$ or not, an identical argument shows that the contribution of $\mathbf{b}_1, \mathbf{b}_2$ with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \ll B^{4/3}$ contributes $O(B^{17/3})$. Therefore we just need to consider the contribution when $\wedge(\mathbf{b}_1, \mathbf{b}_2) \gg B^{4/3}$.

We split the summation according to $\wedge(\mathbf{b}_1, \mathbf{b}_2) \sim B^2/C$ and $D_{\mathbf{b}_1,\mathbf{b}_2} = d$. Since $\mathbf{c}_1 \propto \mathbf{c}_2 \pmod p$, we have $\mathbf{c}_1 \equiv \lambda_0 \mathbf{c}_2 \pmod p$ for some λ_0. Since $\mathbf{b}_1 \equiv \mathbf{c}_1 \pmod p$ and $\mathbf{b}_2 \equiv \mathbf{c}_2 \bmod p$ we then see that $p|d$. The condition $D_{\mathbf{b}_1,\mathbf{b}_2} = d$ forces $\mathbf{b}_1 = \lambda \mathbf{b}_2 \pmod d$ for some λ, with $\lambda \equiv \lambda_0 \pmod p$. Thus, by Lemma 11.4, the number of choices of $\mathbf{b}_1, \mathbf{b}_2$ with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \sim B^2/C$ and $D_{\mathbf{b}_1,\mathbf{b}_2} = d$ is

$$\ll \sum_{\substack{\mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_B \\ \mathbf{b}_2 \equiv \mathbf{c}_2 \pmod p}} \sum_{\substack{1 \le \lambda \le d \\ \lambda \equiv \lambda_0 \pmod p}} \#\mathcal{C}_{C,d,\lambda\mathbf{b}_2,\mathbf{b}_2} \ll \Big(1 + \frac{B^4}{p^4}\Big)\frac{d}{p}\Big(1 + \frac{B}{d}\Big)\Big(1 + \frac{B}{Cd}\Big)^3$$
$$\ll \frac{B^8}{p^5 C^3 d^3} + B^5.$$

When $\wedge(\mathbf{b}_1, \mathbf{b}_2) \sim B^2/C$ and $D_{\mathbf{b}_1,\mathbf{b}_2} = d$ we have $\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2}) \gg B^2/(Cd)$. Thus the total contribution from terms with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \gg B^{4/3}$ is

$$\sum_{\substack{d \le B \\ p|d}} \sum_{C = 2^j \ll B^{2/3}} \frac{Cd}{B^2}\Big(\frac{B^8}{p^5 C^3 d^3} + B^5\Big) \ll \frac{B^6}{p^7} + B^{17/3}.$$

This gives the result. □

We are now able to make progress on our aim of bounding T_8.

Lemma 11.7. *Let T_8 be as given by* (11.12). *Then we have*

$$T_8 \ll \eta_4 A^2 B^6 + \eta_4^{-12} A^2 \sup_{\mathcal{C}_1, \mathcal{C}_2} \Big(|T_{11}| + |T_{12}|\Big),$$

where the supremum is over all hypercubes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}_B$ of side length $\eta_4^3 B$ and

$$T_{11} := \sum_{\substack{p \in [P_1, P_2] \\ p \equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{b}_1 \in \mathbb{Z}^4 \cap \mathcal{C}_1, \mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_2 \\ \mathbf{b}_1 \equiv \mathbf{b}_2 \equiv \mathbf{b}_0 \pmod{m'} \\ \wedge(\mathbf{b}_1, \mathbf{b}_2) \neq 0 \\ p \nmid N(\mathbf{b}_1) N(\mathbf{b}_2)}} \frac{g_{\mathbf{b}_1} g_{\mathbf{b}_2}}{f_{\mathbf{b}_1,\mathbf{b}_2,p,p} \det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})}, \tag{11.13}$$

$$T_{12} := \sum_{\substack{p_1, p_2 \in [P_1, P_2] \\ p_1 \equiv p_2 \equiv 1 \pmod{D_f}}} \frac{1}{p_1 p_2} \sum_{\substack{\mathbf{b}_1 \in \mathbb{Z}^4 \cap \mathcal{C}_1, \mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_2 \\ \mathbf{b}_1 \equiv \mathbf{b}_2 \equiv \mathbf{b}_0 \pmod{m'} \\ \wedge(\mathbf{b}_1, \mathbf{b}_2) \neq 0 \\ p_1 \nmid N(\mathbf{b}_1), p_2 \nmid N(\mathbf{b}_2)}} \frac{g_{\mathbf{b}_1} g_{\mathbf{b}_2} D_{\mathbf{b}_1,\mathbf{b}_2}}{\wedge(\mathbf{b}_1, \mathbf{b}_2)}. \tag{11.14}$$

Proof. Let $\eta_5 := \eta_4^3$. We wish to replace $\mathcal{R}''_{\mathbf{b}_1,\mathbf{b}_2}$ with a quantity which doesn't depend on $\mathbf{b}_1, \mathbf{b}_2$ by splitting $\mathcal{C}_B$ into $O(\eta_5^{-4}\eta_1^4)$ smaller hypercubes of side length $\eta_5 B$. We see that $\mathrm{vol}(\mathcal{R}''_{\mathbf{b}_1,\mathbf{b}_2})$ depends continuously on the components of $\mathbf{b}_1$ and $\mathbf{b}_2$, and that $\mathrm{vol}(\mathcal{R}''_{\mathbf{b}_1,\mathbf{b}_2})$ is always of size $O(A^2)$. Moreover, if we restrict $\mathbf{b}_1, \mathbf{b}_2$ to hypercubes of side length $\eta_5 B$

then $\mathrm{vol}\,(\mathcal{R}'_{\mathbf{b}_1,\mathbf{b}_2})$ varies by $O(\eta_5 A^2)$ as $\mathbf{b}_1, \mathbf{b}_2$ vary within these hypercubes. Thus we see that

$$T_8 = \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{b}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_B\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod{m'}\\ p_1\nmid N(\mathbf{b}_1),\, p_2\nmid N(\mathbf{b}_2)\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0}} \frac{g_{\mathbf{b}_1} g_{\mathbf{b}_2}\,\mathrm{vol}\,(\mathcal{R}''_{\mathbf{b}_1,\mathbf{b}_2})}{f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})}$$

$$\ll T_9 + \eta_5^{-4} A^2 \sup_{\mathcal{C}_1,\mathcal{C}_2} |T_{10}|, \tag{11.15}$$

where

$$T_9 := \eta_5\eta_4^{-2} \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{b}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_B\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod{m'}\\ p_1\nmid N(\mathbf{b}_1),\, p_2\nmid N(\mathbf{b}_2)\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0}} \frac{\mathrm{vol}\,(\mathcal{R}''_{\mathbf{b}_1,\mathbf{b}_2})}{f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})},$$

$$T_{10} = T_{10}(\mathcal{C}_1,\mathcal{C}_2) := \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod{m'}\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ p_1\nmid N(\mathbf{b}_1),\, p_2\nmid N(\mathbf{b}_2)}} \frac{g_{\mathbf{b}_1} g_{\mathbf{b}_2}}{f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2}\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})}.$$

By the above lemmas, we have that

$$T_9 \ll \eta_4^{-2}\eta_5 A^2 B^6 \ll \eta_4 A^2 B^6,$$

on recalling that $\eta_5 = \eta_4^3$. Thus we are left to bound T_{10}. We separate the terms when the two primes in the outer sum are the same. Thus

$$T_{10} = T_{11} + T_{12}, \tag{11.16}$$

where T_{11} denotes the terms with $p_1 = p_2$ and T_{12} those terms with $p_1 \neq p_2$.

T_{11} clearly is equal to the expression given in the lemma, but (recalling that $\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2}) = \wedge(\mathbf{b}_1,\mathbf{b}_2)/D_{\mathbf{b}_1,\mathbf{b}_2}$) we need to show that $f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2} = p_1p_2$ in T_{12} to obtain the desired expression. We first note that since $p_1 \nmid N(\mathbf{b}_1)$ the multiplication-by-$\mathbf{b}_1$ matrix $M_{\mathbf{b}_1}$ is invertible $\pmod{p_1}$. This means that for every $\mathbf{x} \pmod{p_1}$ there is a unique $\mathbf{a} \pmod{p_1}$ such that $\mathbf{x} = \mathbf{a}\diamond\mathbf{b}_1 \pmod{p_1}$, and so $\mathbf{v}_{p_1}\cdot(\mathbf{a}\diamond\mathbf{b}_1) = 0 \pmod{p_1}$ is therefore a non-trivial constraint on the components of $\mathbf{a} \pmod{p_1}$. Similarly since $p_2 \nmid N(\mathbf{b}_2)$, we see $p_2|\mathbf{v}_{p_2}\cdot(\mathbf{a}\diamond\mathbf{b}_2)$ is a non-trivial constraints on the components of $\mathbf{a} \pmod{p_2}$. From this it follows that we have that $f_{\mathbf{b}_1,\mathbf{b}_2,p_1,p_2} = p_1p_2$, and so T_{12} is given by the expression in the lemma. □

First we concentrate on T_{11}.

11.6 The case $p_1 = p_2$

In this section we wish to bound the sum T_{11} from (11.13). We first see by Lemma 11.6 the contribution of terms with $\mathbf{b}_1 \propto \mathbf{b}_2 \pmod{p}$ to T_{11} is

$$\ll \sum_{p\in[P_1,P_2]} \sum_{\mathbf{c}_1\propto\mathbf{c}_2 \pmod{p}} \eta_4^{-2}\Big(\frac{B^6}{p^7} + B^{17/3}\Big) \ll \frac{B^6\eta_4^{-2}}{P_1} + \eta_4^{-2}P_2^6 B^{17/3}.$$

Thus we have

$$T_{11} = T'_{11} + O\Big(\frac{B^6\eta_4^{-2}}{P_1} + \eta_4^{-2}P_2^6B^{17/3}\Big), \tag{11.17}$$

where T'_{11} counts those terms in T_{11} with $\mathbf{b}_1 \not\propto \mathbf{b}_2 \pmod p$, or equivalently with $p \nmid D_{\mathbf{b}_1,\mathbf{b}_2}$.

When $\mathbf{b}_1 \not\propto \mathbf{b}_2 \pmod p$, we see that the constraints $(\mathbf{a}\diamond\mathbf{b}_1)_4 = 0 \pmod p$ and $(\mathbf{a}\diamond\mathbf{b}_2)_4 = 0 \pmod p$ are two linearly independent linear constraints on $\mathbf{a} \pmod p$. In particular, the index $f_{\mathbf{b}_1,\mathbf{b}_2,p,p} = [\Lambda_{\mathbf{b}_1,\mathbf{b}_2} : \Lambda_{\mathbf{b}_1,\mathbf{b}_2,p,p}]$ simplifies to give

$$\frac{1}{f_{\mathbf{b}_1,\mathbf{b}_2,p,p}} = \frac{\#\{\mathbf{a} \pmod p : (\mathbf{a}\diamond\mathbf{b}_1)_4 = (\mathbf{a}\diamond\mathbf{b}_2)_4 = \mathbf{v}\cdot(\mathbf{a}\diamond\mathbf{b}_1) = \mathbf{v}\cdot(\mathbf{a}\diamond\mathbf{b}_2) = 0 \pmod p\}}{p^2}.$$

We separate the above count according to the rank of the multiplication-by-$\mathbf{a}$ matrix $M_a \pmod p$. Thus

$$\frac{1}{f_{\mathbf{b}_1,\mathbf{b}_2,p,p}} = \sum_{i=0}^{4}\frac{1}{p^2}\widetilde{S}_i(\mathbf{b}_1,\mathbf{b}_2), \tag{11.18}$$

where $\widetilde{S}_i(\mathbf{b}_1,\mathbf{b}_2)$ counts those $\mathbf{a} \pmod p$ such that $M_{\mathbf{a}}$ has rank i and satisfies $(\mathbf{a}\diamond\mathbf{b}_1)_4 = (\mathbf{a}\diamond\mathbf{b}_2)_4 = \mathbf{v}\cdot(\mathbf{a}\diamond\mathbf{b}_1) = \mathbf{v}\cdot(\mathbf{a}\diamond\mathbf{b}_2) = 0 \pmod p$.

First we consider $\widetilde{S}_4$.

Lemma 11.8.

$$\sum_{\mathbf{c}_1,\mathbf{c}_2 \pmod p}\frac{1}{p^2}\widetilde{S}_4(\mathbf{c}_1,\mathbf{c}_2) \ll p^6.$$

Proof. In this case $M_{\mathbf{a}}$ has rank 4, and so is invertible $\pmod p$. Given any choice of $\mathbf{c}_1 \pmod p$ with $p \nmid N(\mathbf{c}_1)$, we see that $\mathbf{a}\diamond\mathbf{c}_1 = M_{\mathbf{c}_1}\mathbf{a}$ where the multiplication-by-$\mathbf{c}_1$ matrix $M_{\mathbf{c}_1}$ has determinant $N(\mathbf{c}_1)$, and so is invertible $\pmod p$. Therefore, given any choice of $\mathbf{x} \pmod p$, there is a unique choice of $\mathbf{a} \pmod p$ with $p \nmid N(\mathbf{a})$ such that $\mathbf{a}\diamond\mathbf{c}_1 \equiv \mathbf{x} \pmod p$. Similarly, since we only consider $\mathbf{a}$ with $M_{\mathbf{a}}$ is invertible, given any choice of $\mathbf{y} \pmod p$ there is then a unique choice of $\mathbf{c}_2 \pmod p$ such that $\mathbf{a}\diamond\mathbf{c}_2 \equiv \mathbf{y} \pmod p$. Since there are $O(p^4)$ choices of $\mathbf{x},\mathbf{y} \pmod p$ with $\mathbf{x}_4 = \mathbf{y}_4 = 0$ and $\mathbf{v}\cdot\mathbf{x} = \mathbf{v}\cdot\mathbf{y} = 0 \pmod p$, there are therefore $O(p^4)$ choices of $\mathbf{a},\mathbf{c}_2 \pmod p$ such that $p \nmid N(\mathbf{a})$ and $(\mathbf{a}\diamond\mathbf{c}_1)_4 = (\mathbf{a}\diamond\mathbf{c}_2)_4 = \mathbf{v}\cdot(\mathbf{a}\diamond\mathbf{c}_1) = \mathbf{v}\cdot(\mathbf{a}\diamond\mathbf{c}_2) = 0 \pmod p$. Thus we have that

$$\sum_{\mathbf{c}_1,\mathbf{c}_2 \pmod p}\frac{1}{p^2}\widetilde{S}_4(\mathbf{c}_1,\mathbf{c}_2) \ll p^6,$$

as required. □

Now we consider $\widetilde{S}_2$ and $\widetilde{S}_3$.

Lemma 11.9.

$$\sum_{\mathbf{c}_1,\mathbf{c}_2 \pmod p}\frac{1}{p^2}\Big(\widetilde{S}_2(\mathbf{c}_1,\mathbf{c}_2) + \widetilde{S}_3(\mathbf{c}_1,\mathbf{c}_2)\Big) \ll p^6.$$

Proof. Since $M_{\mathbf{a}}$ is not invertible $\pmod p$ and has determinant $N(\mathbf{a})$, we see that $p|N(\mathbf{a})$ and so $p|N(\mathbf{a}\diamond\mathbf{c}_1) = N(\mathbf{a})N(\mathbf{c}_1)$. Since $f(x_1,x_2,x_3)$ is an irreducible polynomial which splits into two linear factors over a quadratic extension, and $N(x_1\nu_1+x_2\nu_2+x_3\nu_3)$ is a quartic irreducible polynomial which has no linear factors over any quadratic extension, these polynomials have no common polynomial factors over a mutual splitting field, and so define an algebraic variety of codimension 2. Thus (by Hilbert's Theorem 90 and the Lang-Weil bound) there are $O(p)$ choices of $(x_1,x_2,x_3) \pmod p$ such that $f(x_1,x_2,x_3) = N(x_1\nu_1+x_2\nu_2+x_3\nu_3) = 0 \pmod p$. Thus there are $O(p^2)$ choices of $\mathbf{x},\mathbf{y}$ with $p|N(\mathbf{x}), N(\mathbf{y})$ and $x_4 = y_4 = \mathbf{v}\cdot\mathbf{x} = \mathbf{v}\cdot\mathbf{y} = 0 \pmod p$. Given $\mathbf{c}_1$ with $p\nmid N(\mathbf{c}_1)$ and $\mathbf{x}$ and $\mathbf{y}$ as above, here is a unique $\mathbf{a} \pmod p$ such that $\mathbf{a}\diamond\mathbf{c}_1 \equiv \mathbf{x} \pmod p$, and there are $O(p^2)$ choices of $\mathbf{c}_2$ such that $\mathbf{a}\diamond\mathbf{c}_2 \equiv \mathbf{y} \pmod p$ provided $M_{\mathbf{a}}$ has rank 2 or 3. Putting this together gives the result. □

Lemma 11.10.

$$S_0(\mathbf{c}_1,\mathbf{c}_2) \ll 1.$$

Proof. The only $\mathbf{a}$ such that $M_{\mathbf{a}}$ has rank 0 is the vector $\mathbf{0} \pmod p$. □

Finally, we need to consider the situation where $M_{\mathbf{a}}$ has rank 1, which is slightly more complicated.

Lemma 11.11.

$$\sum_{\mathbf{c}_1,\mathbf{c}_2 \pmod p} \frac{1}{p^2}\widetilde{S}_1(\mathbf{c}_1,\mathbf{c}_2) \ll p^6.$$

Proof. If $M_{\mathbf{a}}$ has rank 1, then there are p^3 choices of $\mathbf{b} \pmod p$ such that $M_{\mathbf{a}}\mathbf{b} = \mathbf{0} \pmod p$. On the other hand, let $\mathfrak{a} = (a_1\nu_1+a_2\nu_2+a_3\nu_3+a_4\nu_4)$ and $\mathfrak{b} = (b_1\nu_1+b_2\nu_2+b_3\nu_3+b_4\nu_4)$. If $M_{\mathbf{a}}\mathbf{b} = \mathbf{0} \pmod p$, then the ideal $\mathfrak{a}\mathfrak{b}$ is a multiple of (p), and so $\mathfrak{b}$ is a multiple of $(p)/\gcd(\mathfrak{a},(p))$. Therefore for there to be p^3 choices of $\mathfrak{b} \pmod p$, $\mathfrak{a}$ must be a multiple of $(p)/\mathfrak{p}$ for some degree one prime ideal $\mathfrak{p}$ above p. Since there are $O(1)$ degree one prime ideals $\mathfrak{p}$ above p and there are $O(p)$ different multiples of $(p)/\mathfrak{p}$ we see that there are $O(p)$ possible vectors $\mathbf{a}$ such that $M_{\mathbf{a}}$ has rank 1.

Since the rank is unchanged by replacing $\mathbf{a}$ with $\lambda\mathbf{a}$ for any non-zero scalar λ, we see all such $\mathbf{a}$ are scalar multiples of one of $O(1)$ choices of vector $\mathbf{a}^{(0)}$.

Call such a vector $\mathbf{a}^{(0)}$ 'normal' if the constraints $(\mathbf{a}^{(0)}\diamond\mathbf{c}_2)_4 \equiv \mathbf{v}\cdot(\mathbf{a}^{(0)}\diamond\mathbf{c}_2) \equiv 0 \pmod p$ are non-trivial on $\mathbf{c}_2 \pmod p$, and call $\mathbf{a}^{(0)}$ 'exceptional' if the constraints are trivial on $\mathbf{c}_2 \pmod p$. We see that if $\mathbf{a}^{(0)}$ is normal, then there are $O(p^3)$ choices of $\mathbf{c}_2 \pmod p$ and so $O(p^4)$ choices of $(\mathbf{c}_2,\mathbf{a}) \pmod p$ with $\mathbf{a}$ a multiple of $\mathbf{a}^{(0)}$.

We now prove that when p is large enough, there are no exceptional $\mathbf{a}^{(0)}$.

If $(\mathbf{a}^{(0)}\diamond\mathbf{c})_4 \equiv 0 \pmod p\ \forall\mathbf{c}$, then this equation holds in particular for all $\mathbf{c}$ in $\{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$. Writing $\mathbf{a}^{(0)} = (a_1^{(0)},a_2^{(0)},a_3^{(0)},a_4^{(0)})$ and $\nu_i\nu_j = \sum_{k=1}^4 \lambda_{ijk}\nu_k$, we get

$$\sum_{i=1}^4 \lambda_{ij4}a_i^{(0)} \equiv 0 \pmod p \qquad j = 1,2,3,4.$$

This implies that $p|\det(\lambda_{ij4})_{1\le i,j\le 4}$ which is not possible for p large enough if this determinant is non zero.

But this determinant can't be zero, otherwise, there would be μ_1,μ_2,μ_3,μ_4 such that

$$\mu_1\begin{pmatrix}\lambda_{114}\\ \lambda_{214}\\ \lambda_{314}\\ \lambda_{414}\end{pmatrix}+\mu_2\begin{pmatrix}\lambda_{124}\\ \lambda_{224}\\ \lambda_{324}\\ \lambda_{424}\end{pmatrix}+\mu_3\begin{pmatrix}\lambda_{134}\\ \lambda_{234}\\ \lambda_{334}\\ \lambda_{434}\end{pmatrix}+\mu_4\begin{pmatrix}\lambda_{144}\\ \lambda_{244}\\ \lambda_{344}\\ \lambda_{444}\end{pmatrix}=0,$$

and then the matrix of the multiplication by $\mu_1\nu_1+\mu_2\nu_2+\mu_3\nu_3+\mu_4\nu_4$ wouldn't be invertible. Thus $c_p=0$ for all $p\in[P_1,P_2]$.

Thus, we have that

$$\frac{1}{p^2}\widetilde{S}_1(\mathbf{c}_1,\mathbf{c}_2)=\frac{1}{p}\sum_{\mathbf{a}^{(0)}\text{ normal}}\mathbf{1}_{\substack{(\mathbf{a}^{(0)}\diamond\mathbf{c}_1)_4\equiv\mathbf{v}\cdot(\mathbf{a}^{(0)}\diamond\mathbf{c}_1)\equiv 0\pmod p\\ (\mathbf{a}^{(0)}\diamond\mathbf{c}_2)_4\equiv\mathbf{v}\cdot(\mathbf{a}^{(0)}\diamond\mathbf{c}_2)\equiv 0\pmod p}}+O\Big(\frac{1}{p^2}\Big).$$

However, we have

$$\sum_{\mathbf{c}_1,\mathbf{c}_2\pmod p}\frac{1}{p}\sum_{\mathbf{a}^{(0)}\text{ normal}}\mathbf{1}_{\substack{(\mathbf{a}^{(0)}\diamond\mathbf{c}_1)_4\equiv\mathbf{v}\cdot(\mathbf{a}^{(0)}\diamond\mathbf{c}_1)\equiv 0\pmod p\\ (\mathbf{a}^{(0)}\diamond\mathbf{c}_2)_4\equiv\mathbf{v}\cdot(\mathbf{a}^{(0)}\diamond\mathbf{c}_2)\equiv 0\pmod p}}\ll p^5.$$

This gives the result. □

We're now in a position to simplify our sum.

Lemma 11.12. *Let*

$$T_{11}':=\sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1\pmod{D_f}}}\sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0\pmod m\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ p\nmid N(\mathbf{b}_1)N(\mathbf{b}_2)D_{\mathbf{b}_1,\mathbf{b}_2}}}\frac{g_{\mathbf{b}_1}g_{\mathbf{b}_2}}{f_{\mathbf{b}_1,\mathbf{b}_2,p,p}\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})}.$$

Then we have

$$T_{11}'\ll\frac{X^{o(1)}B^6}{P_1}+X^{o(1)}P_2^7B^{17/3}.$$

Proof. Firstly, by splitting $\mathbf{b}_1,\mathbf{b}_2$ into residue classes $\pmod p$, we have that

$$T_{11}'=\sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1\pmod{D_f}}}\sum_{\substack{\mathbf{c}_1,\mathbf{c}_2\pmod p\\ \mathbf{c}_1\not\equiv\mathbf{c}_2\\ N(\mathbf{c}_1)N(\mathbf{c}_2)\neq 0\pmod p}}\sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0\pmod m\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ \mathbf{b}_1\equiv\mathbf{c}_1\pmod p\\ \mathbf{b}_2\equiv\mathbf{c}_2\pmod p}}\frac{g_{\mathbf{b}_1}g_{\mathbf{b}_2}}{f_{\mathbf{b}_1,\mathbf{b}_2,p,p}\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})}.$$

Using our expression (11.18), we see that this is given by

$$\sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1\pmod{D_f}}}\sum_{\substack{\mathbf{c}_1,\mathbf{c}_2\pmod p\\ \mathbf{c}_1\not\equiv\mathbf{c}_2\\ N(\mathbf{c}_1)N(\mathbf{c}_2)\neq 0\pmod p}}\sum_{j=0}^{4}\frac{\widetilde{S}_j(\mathbf{c}_1,\mathbf{c}_2)}{p^2}\sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0\pmod m\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ \mathbf{b}_1\equiv\mathbf{c}_1\pmod p\\ \mathbf{b}_2\equiv\mathbf{c}_2\pmod p}}\frac{g_{\mathbf{b}_1}g_{\mathbf{b}_2}}{\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})}.$$

Using Lemma 11.11 we get

$$T'_{11} \ll \sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}} \sum_{\substack{\mathbf{c}_1,\mathbf{c}_2 \pmod p\\ \mathbf{c}_1\not\propto\mathbf{c}_2 \pmod p\\ N(\mathbf{c}_1)N(\mathbf{c}_2)\neq 0 \pmod p}} \frac{T(\mathbf{c}_1,\mathbf{c}_2)}{p^2} \sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod m\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ \mathbf{b}_1\equiv\mathbf{c}_1 \pmod p\\ \mathbf{b}_2\equiv\mathbf{c}_2 \pmod p}} \frac{|g_{\mathbf{b}_1}g_{\mathbf{b}_2}|}{\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})}, \tag{11.19}$$

where

$$T(\mathbf{c}_1,\mathbf{c}_2) := \widetilde{S}_0(\mathbf{c}_1,\mathbf{c}_2) + E_1(\mathbf{c}_1,\mathbf{c}_2) + \widetilde{S}_2(\mathbf{c}_1,\mathbf{c}_2) + \widetilde{S}_3(\mathbf{c}_1,\mathbf{c}_2) + \widetilde{S}_4(\mathbf{c}_1,\mathbf{c}_2).$$

By Lemma 11.5, we have that

$$\sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod m\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ \mathbf{b}_1\equiv\mathbf{c}_1 \pmod p\\ \mathbf{b}_2\equiv\mathbf{c}_2 \pmod p}} \frac{|g_{\mathbf{b}_1}g_{\mathbf{b}_2}|}{\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})} \ll \frac{\eta_4^{-2}B^6}{p^8} + \eta_4^{-2}B^{17/3}.$$

Lemmas 11.10, 11.11, 11.9, 11.8 show that

$$\sum_{\mathbf{c}_1,\mathbf{c}_2 \pmod p} \frac{T(\mathbf{c}_1,\mathbf{c}_2)}{p^2} \ll p^6.$$

Thus we see that the term T'_{11} (11.19) is

$$\ll \eta_4^{-2} \sum_{\substack{p\in[P_1,P_2]\\ p\equiv 1 \pmod{D_f}}} p^6\Big(\frac{B^6}{p^8} + B^{17/3}\Big) \ll \frac{\eta_4^{-2}B^6}{P_1} + \eta_4^{-2}B^{17/3}P_2^7.$$

This ends the proof of Lemma 11.12. □

Putting everything in this section together, we are left to show that T_{12} is small compared with B^6.

11.7 The case $p_1 \neq p_2$

In this section we bound the sum T_{12} given by (11.14).

Lemma 11.13. *We have*

$$T_{12} \ll |S_{sep}| + \frac{X^{o(1)}B^6}{P_1} + X^{o(1)}P_2^7B^{17/3},$$

where, S_{sep} is given by

$$S_{sep} := \sum_{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1} \sum_{\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2} \frac{g_{\mathbf{b}_1}g_{\mathbf{b}_2}D_{\mathbf{b}_1,\mathbf{b}_2}}{\wedge(\mathbf{b}_1,\mathbf{b}_2)}.$$

Proof. We wish to reintroduce terms with $p_1 \nmid N(\mathbf{b}_1)$ and $p_2 \nmid N(\mathbf{b}_2)$ so that the inner sum is independent of p_1, p_2. There are $O(p_1^3)$ choices of $\mathbf{c}_1 \pmod{p_1}$ such that $p_1 | N(\mathbf{c}_1)$. Thus, by Lemma 11.5, we see that the terms with $p_1 | N(\mathbf{b}_1)$ contribute a total

$$\sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \frac{1}{p_1p_2} \sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod m\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ p_1|N(\mathbf{b}_1)}} \frac{|g_{\mathbf{b}_1}g_{\mathbf{b}_2}|D_{\mathbf{b}_1,\mathbf{b}_2}}{\wedge(\mathbf{b}_1,\mathbf{b}_2)}$$

$$\ll \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \frac{1}{p_1p_2} \sum_{\substack{\mathbf{c}_1,\mathbf{c}_2 \pmod{p_1}\\ p_1|N(\mathbf{c}_1)}} \sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0\\ \mathbf{b}_1\equiv\mathbf{c}_1 \pmod{p_1}\\ \mathbf{b}_2\equiv\mathbf{c}_2 \pmod{p_2})}} \frac{|g_{\mathbf{b}_1}g_{\mathbf{b}_2}|D_{\mathbf{b}_1,\mathbf{b}_2}}{\wedge(\mathbf{b}_1,\mathbf{b}_2)}$$

$$\ll \sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \frac{\eta_4^{-2}}{p_1p_2} p_1^7\Big(\frac{B^6}{p_1^8}+B^{17/3}\Big)$$

$$\ll \frac{\eta_4^{-2}B^6}{P_1}+\eta_4^{-2}P_2^7B^{17/3}.$$

Similarly, we see that terms $p_2 | N(\mathbf{b}_2)$ contribute a total $O(B^6/P_1 + P_2^7 B^{17/3})$. Thus we find that

$$T_{12} = \Big(\sum_{\substack{p_1,p_2\in[P_1,P_2]\\ p_1\equiv p_2\equiv 1 \pmod{D_f}}} \frac{1}{p_1p_2}\Big)\Big(\sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \mathbf{b}_1\equiv\mathbf{b}_2\equiv\mathbf{b}_0 \pmod m\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)\neq 0}} \frac{g_{\mathbf{b}_1}g_{\mathbf{b}_2}D_{\mathbf{b}_1,\mathbf{b}_2}}{\wedge(\mathbf{b}_1,\mathbf{b}_2)}\Big)$$
$$+ O\Big(\frac{\eta_4^{-2}B^6}{P_1}+\eta_4^{-2}P_2^7B^{17/3}\Big).$$

Noting that the sum over p_1, p_2 is $O(1)$, this gives the result. □

Thus it remains to bound S_{sep}.

11.8 Reduction to small residue classes and small boxes

We first show that the contribution to S_{sep} from terms with $D_{\mathbf{b}_1,\mathbf{b}_2} > (\log B)^{K_2}$ or $\wedge(\mathbf{b}_1,\mathbf{b}_2) \le B^2/(\log B)^{K_2}$ is negligible if K_2 is large compared with K_1.

Lemma 11.14. *Let $K_2 > 0$ We have*

$$\sum_{\substack{\mathbf{b}_1\in\mathbb{Z}^4\cap\mathcal{C}_1,\,\mathbf{b}_2\in\mathbb{Z}^4\cap\mathcal{C}_2\\ \wedge(\mathbf{b}_1,\mathbf{b}_2)>0\\ \max(B^2/\wedge(\mathbf{b}_1,\mathbf{b}_2),D_{\mathbf{b}_1,\mathbf{b}_2})>(\log B)^{K_2}}} \frac{|g_{\mathbf{b}_1}g_{\mathbf{b}_2}|}{\det(\Lambda_{\mathbf{b}_1,\mathbf{b}_2})} \ll \frac{\eta_4^{-2}B^6}{(\log X)^{K_2}}.$$

Proof. This is similar to the proof of Lemma 11.5. Indeed, the argument in the proof of Lemma 11.5 shows that the contribution from terms with

$\wedge(\mathbf{b}_1, \mathbf{b}_2) \ll B^{4/3}$ is $O(\eta_4^{-2} B^{17/3})$, and the contribution from terms with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \sim B^2/C$ (for $C = 2^j \ll B^{2/3}$) and $D_{\mathbf{b}_1, \mathbf{b}_2} = d$ is

$$\ll \eta_4^{-2} \frac{dC}{B^2} \Big(B + \frac{B^4}{C^3 d^3} \Big) B^4.$$

Thus we see that the total contribution is

$$\ll \eta_4^{-2} B^{17/3} + \eta_4^{-2} \sum_{C = 2^j \ll B^{2/3}} \sum_{\substack{d \leq B \\ \max(d, C) > (\log B)^{K_2}}} dC \Big(B^3 + \frac{B^6}{C^3 d^3} \Big) \ll \frac{\eta_4^{-2} B^6}{(\log B)^{K_2}}.$$

□

Thus we just need to consider $D_{\mathbf{b}_1, \mathbf{b}_2} \leq (\log x)^{K_2}$ and $\wedge(\mathbf{b}_1, \mathbf{b}_2) \geq B^2/(\log x)^{K_2}$.

Lemma 11.15. *Imagine that for every cube $\mathcal{C} \subseteq [1, B]^4$, every and any $\mathbf{c} \pmod d$ we have*

$$\sum_{\substack{\mathbf{b} \in \mathbb{Z}^4 \cap \mathcal{C} \\ \mathbf{b} \equiv \mathbf{c} \pmod d}} g_{\mathbf{b}} \ll_K \eta_4^{5000} B^4.$$

Then we have

$$S_{sep} \ll_K \eta_4^{20} B^6$$

Proof. Let $\eta_6 = \eta_4^{30}$. By Lemma 11.14, the contribution to S_{sep} from terms with $\wedge(\mathbf{b}_1, \mathbf{b}_2) < \eta_6 B^2$ or from $D_{\mathbf{b}_1, \mathbf{b}_2} > \eta_6^{-1}$ is $O(\eta_4^{20} B^6)$. Thus we may focus on the remaining terms.

Since $\wedge(\mathbf{b}_1, \mathbf{b}_2)$ is continuous in $\mathbf{b}_1, \mathbf{b}_2$ we see that if a pair of cubes $\mathcal{C}_1', \mathcal{C}_2'$ of side length $\eta_6^2 B$ contains a point with $\wedge(\mathbf{b}_1, \mathbf{b}_2) \geq \eta_6 B^2$, then in fact for all $\mathbf{b}_1' \in \mathcal{C}_1'$ and $\mathbf{b}_2 \in \mathcal{C}_2'$ we have $\wedge(\mathbf{b}_1', \mathbf{b}_2') = \wedge(\mathbf{b}_1, \mathbf{b}_2)(1 + O(\eta_6))$. Thus we may replace $\wedge(\mathbf{b}_1, \mathbf{b}_2)$ with

$$\wedge(\mathcal{C}_1', \mathcal{C}_2') := \sup_{\mathbf{x} \in \mathcal{C}_1', \mathbf{y} \in \mathcal{C}_2'} \wedge(\mathbf{x}, \mathbf{y})$$

at the cost of an error term of size $\eta_6 \eta_4^{-2} B^6 \ll \eta_4^{20} B^6$. Putting this together, we have

$$S_{sep} \ll \eta_4^{20} B^6 + \frac{\eta_6^{-9}}{B^2} \sum_{d \leq \eta_6^{-1}} d \sup_{\mathcal{C}_1', \mathcal{C}_2'} \sum_{\substack{\mathbf{b}_1 \in \mathbb{Z}^4 \cap \mathcal{C}_1', \mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_2' \\ D_{\mathbf{b}_1, \mathbf{b}_2} = d}} g_{\mathbf{b}_1} g_{\mathbf{b}_2}.$$

Now we wish to simplify the condition $D_{\mathbf{b}_1, \mathbf{b}_2} = d$ to a congruence condition, which will finally allow us to separate the variables $\mathbf{b}_1, \mathbf{b}_2$. By Moebius inversion we have

$$\begin{aligned} \mathbf{1}_{D_{\mathbf{b}_1, \mathbf{b}_2} = d} &= \sum_{e | D_{\mathbf{b}_1, \mathbf{b}_2}/d} \mu(e) \\ &= \sum_{e \leq \eta_6^{-20}} \mu(e) \mathbf{1}_{\mathbf{b}_1 \propto \mathbf{b}_2 \pmod{de}} + O(\eta_6^{-20} \mathbf{1}_{D_{\mathbf{b}_1, \mathbf{b}_2} \geq \eta_6^{-20}}). \end{aligned}$$

By Lemma 11.4, the contribution of the second term to S_{sep} is $O(\eta_4^{20}B^6)$. Thus we see that

$$S_{sep} \ll \eta_4^{20}B^6 + \frac{\eta_6^{-31}}{B^2} \sup_{\substack{\mathcal{C}_1',\mathcal{C}_2' \\ de \ll \eta_6^{-21}}} |S'_{sep}| \tag{11.20}$$

where

$$S'_{sep} := \sum_{\mathbf{b},\lambda_1,\lambda_2 \pmod{de}} \Bigg(\sum_{\substack{\mathbf{b}_1 \in \mathbb{Z}^4 \cap \mathcal{C}_1', \\ \mathbf{b}_1 \equiv \lambda_1 \mathbf{b} \pmod{de} \\ \mathbf{b}_1 \equiv \mathbf{b}_0 \pmod{m}}} g_{\mathbf{b}_1} \Bigg) \Bigg(\sum_{\substack{\mathbf{b}_2 \in \mathbb{Z}^4 \cap \mathcal{C}_2', \\ \mathbf{b}_2 \equiv \lambda_2 \mathbf{b} \pmod{de} \\ \mathbf{b}_2 \equiv \mathbf{b}_0 \pmod{m}}} g_{\mathbf{b}_2} \Bigg).$$

By assumption of the lemma, we have that

$$\sum_{\substack{\mathbf{b}_1 \in \mathbb{Z}^4 \cap \mathcal{C}_1', \\ \mathbf{b}_1 \equiv \lambda_1 \mathbf{b} \pmod{de} \\ \mathbf{b}_1 \equiv \mathbf{b}_0 \pmod{m}}} g_{\mathbf{b}_1} \ll \eta_4^{5000} B^4.$$

Substituting this in then gives $|S_{sep}| \ll \eta_4^{50}B^6 + \eta_4^{5000}\eta_6^{-160}B^6 \ll \eta_4^{50}B^6$. □

Thus we see that it is sufficient to obtain a suitable bound for $g_{\mathbf{b}}$ on average over hypercubes in residue classes.

11.9 Localised bound and Proof of Proposition 9.14

To finish our proof we need to show that we have a suitable estimate for $g_{\mathbf{b}} \approx \mathbf{1}_{\mathcal{R}}(\mathbf{b}) - \widetilde{\mathbf{1}}_{\mathcal{R}}(\mathbf{b})$ over $\mathbf{b}$ restricted to small boxes and arithmetic progressions. We don't require estimates arithmetic progressions to moduli larger than $(\log X)^{O(1)}$, and there are no issues caused by a possible Siegel zero.

Proposition 11.16. *For every $K > 0$ and every polytope $\mathcal{R}$ under consideration, we have*

$$\sum_{\substack{\mathbf{b} \in \mathbb{Z}^4 \cap \mathcal{C} \\ \mathbf{b} \equiv \mathbf{c} \pmod{d}}} \Big(\mathbf{1}_{\mathcal{R}}(\mathbf{b}) - \widetilde{\mathbf{1}}_{\mathcal{R}}(\mathbf{b}) \Big) \ll_K \frac{B^4}{(\log B)^K}.$$

Proof. This is the equivalent of [14, Proposition 9.7], and the proof works in exactly the same manner for our situation. Therefore we only highlight a couple of main details.

First we estimate the contribution from $\mathbf{1}_{\mathcal{R}}(\mathbf{b})$. Since $\mathbf{b}$ is in a small cube, no two elements can generate the same ideal, and so we can write the sum as a sum of principal ideals. We can use Hecke Grossencharacters to detect the congruence conditions and the restriction of $\mathbf{b}$ to the cube $\mathcal{C}$. The Prime Number Theorem for Grossencharacters then allows one to suitably estimate the resulting sums over $\mathbf{1}_{\mathcal{R}}(\mathbf{b})$, giving an explicit main term and an error term which is $O_K(B^4/(\log B)^K)$. This is essentially the same argument as [14, Lemmas 9.1-9.4].

The contribution from $\widetilde{\mathbf{1}}_{\mathcal{R}}(\mathbf{b})$ can be estimated by swapping the order of summation in the sieve sum and using the fact that $\mathbf{b} \in \mathbb{Z} \cap \mathcal{C}$ are equidistributed in suitable aritmetic progressions as in [14, Lemmas 9.5 and 9.6]. This gives a main term and a error term $O_K(B^4/(\log B)^K)$.

The main term contributions from $\mathbf{1}_{\mathcal{R}}(\mathbf{b})$ and $\widetilde{\mathbf{1}}_{\mathcal{R}}(\mathbf{b})$ are the same apart from opposite signs and so cancel, giving the result. □

We note that the number of elements of $\mathcal{C}_B$ with $\tau(\mathfrak{d}) > \eta_4^{-1}$ is

$$\ll \eta_4^{6000} \sum_{\mathbf{b} \in \mathcal{C}_B} \tau(\mathfrak{b})^{6000} \ll \eta_4^{6000} B^4 (\log X)^{O(1)}.$$

Therefore, provided the consant K_1 defining η_4 is chosen sufficiently large, we may replace $g_{\mathfrak{b}}$ with $\mathbf{1}_{\mathcal{R}}(\mathfrak{b}/\mathfrak{c}') - \widetilde{\mathbf{1}}_{\mathcal{R}}(\mathfrak{b}/\mathfrak{c}')$ at the cost of an acceptable error term whenever $\mathfrak{c}'|\mathfrak{b}$. We note that $\mathfrak{c}'|\mathfrak{b}$ is determined by a congruence condition on $\mathbf{b} \pmod{N(\mathfrak{c}')}$, and recall than $N(\mathfrak{c}') \ll (\log X)^{o(1)}$. Therefore Proposition 11.16 implies that the hypothesis of Lemma 11.15 is satisfied. Finally, we are able to complete our proof of Proposition 9.14.

Proof of Proposition 9.14. We recall that $|\widetilde{\mathcal{A}}(X_0)| \asymp \eta_1^3 X_0^3$. Putting together the equations (11.2), (11.7) and the argument of Section 11.1, we find that provided $B < X^{3/4-\epsilon}/P_2^{3/2}$ (from (11.8)) we have

$$T_1(\mathcal{R}) = \sum_{\mathcal{C} \in Cl_K} \sum_{\substack{\mathbf{a}_0, \mathbf{b}_0 \pmod{m'} \\ N(\mathfrak{c})(\mathbf{a}_0 \diamond \mathbf{b}_0)_i \equiv (\mathbf{v}_0)_i \pmod{m'}}} T_3(\mathcal{R}) + O(X^{3+\epsilon}/P_1),$$

where T_3 is given by (11.9).

Putting together (11.10), (11.11), (11.12) and Lemmas 11.1 11.2, 11.7, 11.12, 11.13, 11.15, and Proposition 11.16 then gives

$$T_3(\mathcal{R})^2 \ll X^{o(1)} A^4 \Big(A^3 B^3 + A B^7 P_2^2 + A^2 B^{17/3} P_2^7 + \frac{A^2 B^6}{P_1} \Big) + A^4 \Big(\eta_4 A^2 B^6 + \eta_4^{-12} A^2 \cdot \eta_4^{20} B^6 \Big).$$

Since $\prod_{i=1}^3 X_i \gg\asymp A^3 B^3 (\log X)^{-K}$, this gives the result provided

$$A < B^{3-\epsilon}, \qquad B P_2^2 < A^{1-\epsilon}, \qquad P_2^{21} < B^{1-\epsilon},$$

and the constant K_1 defining η_4 is taken sufficiently large in terms of K. (Here we used that the second inequality implies (11.8).) After taking ϵ suitably small, we see that the first condition is implied by the first inequality of (4.10), whereas the final two inequalities are implied by the assumption $\tau' \leq \min(4 - 2\theta_1' - \cdots - 2\theta_{\ell'}', \theta_1 + \cdots + \theta_{\ell'} - 1)/100$. This gives Proposition 9.14. □

This completes the proof of Proposition 9.14, and hence Theorem 4.1 and Theorem 1.1.

References

[1] R. de la Bretèche. Plus grand facteur premier de valeurs de polynômes aux entiers, with an appendix : Explications des calculs du résultant dans le cas général by R. de la Bretèche and J.-F. Mestre. *Acta Arith.*, 169:221–250, 2015.

[2] R. de la Bretèche and S. Drappeau. Niveau de répartition des polynômes quadratiques et crible majorant pour les entiers friables. *J. Eur. Math. Soc.*, 22(5):1577–1624, 2020.

[3] K. Conrad. Galois groups of cubics and quartics (not in characteristic 2). *https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf*.

[4] C. Dartyge. Le problème de Tchébychev pour le douzième polynôme cyclotomique. *Proc. London Math. Soc.*, 111(1):1–62, 2015.

[5] J.-M. Deshouillers and H. Iwaniec. On the greatest prime factor of $n^2 + 1$. *Ann. Inst. Fourier (Grenoble)*, 32(4):1–11, 1982.

[6] P. Erdős. On the greatest prime factor of $\prod_{k=1}^{x} f(k)$. *J. London Math. Soc.*, 27:379–384, 1952.

[7] D. R. Heath-Brown. Diophantine approximation with square-free numbers. *Math. Z.*, 187(3):335–344, 1984.

[8] D. R. Heath-Brown. The largest prime factor of $x^3 + 2$. *Proc. London Math. Soc.*, 82(3):554–596, 2001.

[9] C. Hooley. On the greatest prime factor of a quadratic polynomial. *Acta Math.*, 281-299:21–50, 1967.

[10] A. J. Irving. The largest prime factor of x^3+2. *Acta Arith.*, 171(1):67–80, 2015.

[11] H. Iwaniec. A new form of the error term in the linear sieve. *Acta Arith.*, 37:307–320, 1980.

[12] H. Iwaniec. Rosser's sieve. *Acta Arith.*, 36:171–202, 1980.

[13] C. U. Jensen, A. Ledet, and N. Yui. *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, volume 45. Math. Sci. Res. Inst. Publ., Cambridge Univ. Press, Cambridge, 2002.

[14] J. Maynard. Primes represented by incomplete norm forms. *Forum of Mathematics, Pi*, 8(3):1–128, 2020.

[15] J. Merikoski. On the largest prime factor of $n^2 + 1$. *https://arxiv.org/abs/1908.08816v3.pdf*, 2021.

[16] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*, volume Third Edition. Springer, 712 pp., 2004.

[17] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arithmetica*, 4(3):185–208, 1958.

[18] G. Tenenbaum. Sur une question d'Erdős et Schinzel. II. *Invent. Math.*, 99:215–224, 1990.

[19] H. Weber. *Lehrbuch der Algebra*, volume 2. Vieweg and Sohn, 592 pp., 1899.

Cécile Dartyge, Institut Élie Cartan, Université de Lorraine, BP 70239, 54506 Vandœuvre-lès-Nancy Cedex, France
cecile.dartyge@univ-lorraine.fr

James Maynard, Mathematical Institute, Woodstock Road, Oxford OX2 6GG, UK
james.alexander.maynard@gmail.com