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

Cécile Dartyge, James Maynard

## - To cite this version:

Cécile Dartyge, James Maynard. On the largest prime factor of quartic polynomial values: the cyclic and dihedral cases. Journal of the European Mathematical Society, In press, 10.48550/arXiv.2212.03381 . hal-03951306v2

## HAL Id: hal-03951306 <br> https://hal.science/hal-03951306v2

Submitted on 2 Feb 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# 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 2
1.1 Outline of the proof of Theorem 1.1 ] . . . . . . . . . . . . . 4
2 Acknowledgements 6

| 3 Initial steps | 7 |
| :--- | :--- | :--- |


| 4 | Localised divisors of values of incomplete norm forms | 8 |
| :--- | :--- | :--- |

4.1 Application to Theorem 1.1 . . . . . . . . . . . . . . . . . . 11
5 Algebraic properties of auxilliary polynomials 12
5.1 Ideals . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 12
5.2 The roots of P modulo $m$. . . . . . . . . . . . . . . . . . . 13
5.3 Elimination of $a_{0}$. . . . . . . . . . . . . . . . . . . . . . . . 15
5.4 Explicit computations of $B_{13}, B_{14}, U, V$. . . . . . . . . . . . 17
5.5 Factorisation of $q$. . . . . . . . . . . . . . . . . . . . . . . . 19
5.6 The factor $q_{1}$ as a an incomplete norm form . . . . . . . . . 21
5.7 On the solutions of some congruence equations with $B_{14}$
6 The set of ideals $\mathcal{J} \quad 27$

| 7 Proof of Proposition | 3.3 | The term $S_{1}$ |
| :--- | :--- | :--- |
| 30 |  |  |

8 Proof of Proposition $|3.2|$ The sum $S_{0} \quad 34$
8.1 The variable $a_{0}$ in $S_{0}$. . . . . . . . . . . . . . . . . . . . . . 34
8.2 Splitting into small boxes . . . . . . . . . . . . . . . . . . . 37
8.3 Preparation for the application of Theorem 4.1 . . . . . . . 38
8.4 Application of Theorem 4.1 . . . . . . . . . . . . . . . . . . 45
8.5 Proof of Proposition 3.2 . . . . . . . . . . . . . . . . . . . . 47
9 Incomplete norm forms ..... 48
$9.1 \quad$ From $\mathcal{O}_{K}$ to $\mathcal{O}_{\mathbf{v}}$ and vice-versa ..... 48
9.2 Multiplication in $\mathcal{O}_{\mathbf{v}}$ ..... 52
9.3 Sums of Type I ..... 53
9.4 Initial steps in the Type II sum ..... 55
9.5 Switching to ideals with norms in small boxes ..... 56
9.6 Approximation weights ..... 58

| 10 Proposition $9.13 \mid$ | The term $T_{\text {sieve }}(\mathcal{R})$ |
| :--- | :--- | ..... 62

11 Proposition 9.14; The term $T_{1}(\mathcal{R})$ ..... 66
11.1 Cosmetic reductions ..... 68
11.2 Dispersion method ..... 69
11.3 Collinear $\mathbf{b}_{1}, \mathbf{b}_{2}$ ..... 69
11.4 Lattice counts ..... 70
11.5 Further lattice estimates ..... 72
11.6 The case $p_{1}=p_{2}$ ..... 76
11.7 The case $p_{1} \neq p_{2}$ ..... 80
11.8 Reduction to small residue classes and small boxes ..... 81
11.9 Localised bound and Proof of Proposition 9.14 ..... 83

## 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 $n \exp \left((\log n)^{\alpha}\right)$ 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 $P^{+}\left(n^{2}+1\right)$ of $n^{2}+1$ satisfies $P^{+}\left(n^{2}+1\right)>n^{11 / 10}$ 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 $P^{+}\left(n^{2}+1\right)>n^{1.279}$ infinitely often. Heath-Brown [8] showed that $P^{+}\left(n^{3}+2\right)>n^{1+10^{-303}}$ 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 $P^{+}\left(n^{4}-n^{2}+1\right)>n^{1+10^{-26531}}$. 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 $\Phi_{5}(X)=X^{4}+X^{3}+X^{2}+X+1, X^{4}-5 X^{2}+5, X^{4}+13 X+39$ are examples of polynomials with cyclic Galois group and $X^{4}+2, X^{4}+3 X+3$, $X^{4}-5 X^{2}+3$ 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

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

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 $q=q\left(a_{1}, a_{2}, a_{3}\right)$ is a ternary sextic form. If $P$ has a Galois group $V$, then $q\left(a_{1}, a_{2}, a_{3}\right)=$ $q_{1}\left(a_{1}, a_{2}, a_{3}\right) q_{2}\left(a_{1}, a_{2}, a_{3}\right) q_{3}\left(a_{1}, a_{2}, a_{3}\right)$ 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 $q\left(a_{1}, a_{2}, a_{3}\right)$ 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'.

[^0]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 $q\left(a_{1}, a_{2}, a_{3}\right)$ 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 $q\left(a_{1}, a_{2}, a_{3}\right)$ 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 $P(n), K=\mathbb{Q}\left(r_{1}\right)$ and $N_{P}=N_{K / \mathbb{Q}}$ the associated norm. Then we see that $N_{P}\left(n-r_{1}\right)=P(n)$, and so we are interested in counting integers $n$ such that the ideal $\left(n-r_{1}\right)$ has a prime ideal factor of large norm. In particular,

$$
\sum_{\substack{n \in[x, 2 x] \\ P^{+}(P(n)) \geq x^{1+\eta}}} 1=\sum_{\substack{n \in[x, 2 x] \\ \exists \mathfrak{p} \mid\left(n-r_{1}\right): N_{P}(\mathfrak{p}) \geq x^{1+\eta}}} 1 \gg \frac{1}{\log x} \sum_{n \in[x, 2 x]} \sum_{\substack{\mathfrak{p}^{\prime} \mid\left(n-r_{1}\right) \\ N_{P}(\mathfrak{p}) \geq x^{1+\eta}}} \log N_{P}(\mathfrak{p}) .
$$

By inclusion-exclusion and the fact that $\sum_{\mathfrak{p}^{e} \mid\left(n-r_{1}\right)} \log \mathfrak{p}=\log P(n)$, we have that the double sum on the right hand side is given by

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

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 $\sum_{\mathfrak{p} \mid\left(n-r_{1}\right), N_{P}(\mathfrak{p} \mid \leq 2 x} \log N_{P}(\mathfrak{p}) \geq\left(1+\delta_{0}\right) \log x$. We split the third sum according to whether $n \in \mathcal{A}$ or not. Therefore the above expression is

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

If $n \in \mathcal{A}$ then since prime ideals with $N_{P}(\mathfrak{p}) \leq 2 x$ contribute at least $\left(1+\delta_{0}\right) \log x$ to $\sum_{\mathfrak{p} \mid\left(n-r_{1}\right)} \log N_{P}(\mathfrak{p})=(4+o(1)) \log x$, the contribution
from prime ideals with $N_{P}(\mathfrak{p})>2 x$ must be $\leq\left(3-\delta_{0}-o(1)\right) \log x$. If $n \notin \mathcal{A}$ then we note from size considerations there can be at most 3 prime ideals with $N_{P}(\mathfrak{p}) \geq 2 x$ dividing $\left(n-r_{1}\right)$, and so the inner sum over $\mathfrak{p}$ is at most $3(1+\eta) \log x$. Substituting these bounds into the above, we find

$$
\sum_{\substack{n \in[x, 2 x] \\
p_{\begin{subarray}{c}{e} }}}\end{subarray}} \operatorname{ln-r_{1})} \begin{aligned}
& N_{P}(\mathfrak{p}) \geq x^{1+\eta} \\
&
\end{aligned} \log N_{P}(\mathfrak{p}) \geq \delta_{0} \# \mathcal{A} \log x-(3 \eta+o(1)) x \log x .
$$

In particular, if $\# \mathcal{A} \gg x$ then choosing $\eta=\delta_{0} \# \mathcal{A} /(4 x)$ shows that the left hand side is $\gg x \log x$. Thus it suffices to show

$$
\#\left\{n \in[x, 2 x]: \prod_{\substack{\mathfrak{p}^{e} \mid\left(n-r_{1}\right) \\ N_{P}(\mathfrak{p}) \leq x}} N_{P}(\mathfrak{p}) \geq x^{1+\delta_{0}}\right\} \gg x
$$

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

By concentrating on multiples of friable principle ideals $\mathfrak{J}=\left(a_{0}+\right.$ $a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}$ ) 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 $\mathcal{A} \subset \mathbb{Z}^{4} \cap\left[1, x^{\left(1+\delta_{0}\right) / 4}\right]$ such that

$$
\sum_{\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathcal{A}} \sum_{\substack{n \in[x, 2 x] \\\left(a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right) \mid\left(n-r_{1}\right)}} 1 \gg x .
$$

The condition $\left(a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right) \mid\left(n-r_{1}\right)$ is equivalent to a congruence condition $n \equiv k_{\mathbf{a}}\left(\bmod N_{P}\left(a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right)\right)$, 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 $\mathrm{e}(t)=\exp (2 i \pi t))$

$$
\sum_{a_{0}, a_{1}, a_{2}, a_{3} \in \mathcal{A}} \mathrm{e}\left(\frac{h k_{a_{0}, a_{1}, a_{2}, a_{3}}}{N_{P}\left(a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right)}\right) .
$$

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 $B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right), B_{13}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)$ and $q\left(a_{1}, a_{2}, a_{3}\right)$ with no common factor such that
$\mathrm{e}\left(\frac{h k_{a_{0}, a_{1}, a_{2}, a_{3}}}{N_{P}\left(a_{0}+a_{1} r_{1}+a_{2} r_{2}+a_{3} r_{3}\right)}\right) \approx \mathrm{e}\left(\frac{h B_{13}\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \overline{B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)}}{q\left(a_{1}, a_{2}, a_{3}\right)}\right)$,
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 $q\left(a_{1}, a_{2}, a_{3}\right) \asymp x^{6\left(1+\delta_{0}\right) / 4}$ is much larger than the length $x^{\left(1+\delta_{0}\right) / 4}$ 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 $q\left(a_{1}, a_{2}, a_{3}\right)$ consists only of small prime factors.

Thus our task has reduced to showing that for a positive proportion of integers $a_{1}, a_{2}, a_{3} \in\left[1, x^{\left(1+\delta_{0}\right) / 4}\right]$ we can ensure that the polynomial
$q\left(a_{1}, a_{2}, a_{3}\right)$ has a convenient prime factorisation. Specifically, we will require that

$$
\begin{equation*}
q\left(a_{1}, a_{2}, a_{3}\right)=d_{0} d_{1} \cdots d_{r} \tag{1.1}
\end{equation*}
$$

where $d_{0}<x^{2-\varepsilon}, \max \left(d_{1}, \ldots, d_{r}\right) \leq x^{1-\varepsilon}, \min \left(d_{0}, \ldots, d_{r}\right) \geq x^{\varepsilon}$ 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 $q\left(a_{1}, a_{2}, a_{3}\right)$ 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 $q\left(a_{1}, a_{2}, a_{3}\right)$ then has a suitable prime factorisation.

When the Galois group of $P$ is $C_{4}$ or $D_{4}$, it turns out that $q\left(a_{1}, a_{2}, a_{3}\right)=$ $q_{1}\left(a_{1}, a_{2}, a_{3}\right) q_{2}\left(a_{1}, a_{2}, a_{3}\right)$ 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 $q_{1}\left(a_{1}, a_{2}, a_{3}\right) \approx\left(\max _{i} a_{i}\right)^{4}$, 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 $q_{1}\left(a_{1}, a_{2}, a_{3}\right)=N_{K / \mathbb{Q}}\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right)$.

Maynard [14] gave asymptotic formulae for the number of primes represented by incomplete norm forms; that is primes $p$ such that $p=$ $N\left(a_{1}+a_{2} \omega+\cdots+a_{n-k} \omega^{n-k-1}\right)$ where $a_{1}, \ldots, a_{n-k}$ are integers, $\omega$ is a root of monic and irreducible polynomial $f \in \mathbb{Z}[X]$ of degree $n \geq 4 k$ 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

$$
\begin{equation*}
\mathcal{E}(\delta):=\left\{X<n \leq 2 X: \prod_{\substack{\mathfrak{p}^{e} \mid\left(n-r_{1}\right) \\ N_{P}(\mathfrak{p}) \leq x}} N_{P}(\mathfrak{p}) \geq X^{1+\delta}\right\} . \tag{3.1}
\end{equation*}
$$

If $\delta_{0}, \delta_{1}>0$ are such that for all $X$ large enough in terms of $\delta_{0}, \delta_{1}, P$ we have $\left|\mathcal{E}\left(\delta_{0}\right)\right|>\delta_{1} X$, then we have for sufficiently large $X$

$$
\left.\mid\{n \in] X, 2 X]: P^{+}(P(n)) \gg X^{1+\frac{\delta_{0} \delta_{1}}{3}}\right\} \mid \geq\left(\delta_{1} \delta_{0}^{2}+o(1)\right) X
$$

Proof. This is essentially [8, Lemma 2], (or [1, Lemme 4.1]) after noting that $\sum_{p \mid P(n), p \leq z} \log p \geq \sum_{\mathfrak{p} \mid\left(n-r_{1}\right), N_{P}(\mathfrak{p}) \leq z} \log N_{P}(\mathfrak{p})$.

Thus it suffices to show that $\left|\mathcal{E}\left(\delta_{0}\right)\right| \gg X$ 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

$$
\begin{equation*}
\prod_{\substack{\mathfrak{p}, N_{P}(\mathfrak{F}) \leq X}} N_{P}(\mathfrak{p}) \geq X^{1+\delta_{0}} \quad \forall \mathfrak{J} \in \mathcal{J} \tag{3.2}
\end{equation*}
$$

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

$$
\begin{aligned}
\left|\mathcal{E}\left(\delta_{0}\right)\right| & \geq \mid\left\{X<n \leq 2 X: \exists \mathfrak{J} \in \mathcal{J}_{2} \text { such that } \mathfrak{J} \mid\left(n-r_{1}\right)\right\} \mid \\
& \geq \frac{\sum_{\mathfrak{J} \in \mathcal{J}_{2}}\left|\mathcal{E}_{\mathfrak{J}}\right|}{\sup _{X \leq n \leq 2 X}\left|\left\{\mathfrak{J} \in \mathcal{J}_{2}: \mathfrak{J} \mid(n-r)\right\}\right|} \\
& \gg \sum_{\substack{\mathfrak{J} \in \mathcal{J} \\
P^{-}\left(N_{P}(\mathfrak{J})\right) \geq X^{\theta_{0}}}}\left|\mathcal{E}_{\mathfrak{J}}\right|,
\end{aligned}
$$

where $\mathcal{E}_{\mathfrak{J}}:=\left\{X<n \leq 2 X: \mathfrak{J} \mid\left(n-r_{1}\right)\right\}$. Every ideal $\mathfrak{J}$ has at most $\alpha_{0}^{-1}$ representations as $\mathfrak{J}=K L$ for $K$ a prime ideal with $N_{P}(K) \in$ [ $\left.X^{4 \alpha_{0}}, X^{5 \alpha_{0}}\right]$. Thus we see that

$$
\left|\mathcal{E}\left(\delta_{0}\right)\right| \gg \sum_{K \in \mathcal{K}_{P^{-}}} \sum_{\substack{\left.N_{P}(L)\right) \geq X^{\theta_{0}} \\ K L \in \mathcal{J}}}\left|\mathcal{E}_{K L}\right|,
$$

where

$$
\begin{equation*}
\mathcal{K}:=\left\{K \text { prime ideal, } N_{P}(K) \in\left[X^{4 \alpha_{0}}, X^{5 \alpha_{0}}\right]\right\} . \tag{3.3}
\end{equation*}
$$

We apply a linear sieve of level $X^{3 \theta_{0}}$ to bound the condition $P^{-}\left(N_{P}(L)\right) \geq$ $X^{\theta_{0}}$ from below, giving

$$
\left|\mathcal{E}\left(\delta_{0}\right)\right| \gg \sum_{K \in \mathcal{K}} \sum_{K L \in \mathcal{J}}\left(\sum_{d \mid N_{P}(L)} \lambda_{d}^{-}\right)\left|\mathcal{E}_{K L}\right|
$$

where $\lambda_{d}^{-}$are the usual Rosser-Iwaniec lower bound linear sieve weights ([12] and [11]) supported on $d<X^{3 \theta_{0}}$ with $p \mid d \Rightarrow p \leq X^{\theta_{0}}$. We see that if $X$ is large enough $\mathcal{E}_{\mathfrak{J}}$ has density $\rho_{P}\left(N_{P}(\mathfrak{J})\right) / N_{P}(\mathfrak{J})$, where

$$
\begin{equation*}
\varrho_{P}(\mathfrak{I}):=\operatorname{card}\left\{0 \leq n<N_{P}(\mathfrak{I}): n \equiv r_{1}(\bmod \mathfrak{I})\right\} . \tag{3.4}
\end{equation*}
$$

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

$$
\begin{equation*}
R_{\mathfrak{J}}:=\left|\mathcal{E}_{\mathfrak{J}}\right|-X \frac{\varrho_{P}\left(N_{P}(\mathfrak{J})\right)}{N_{P}(\mathfrak{J})} . \tag{3.5}
\end{equation*}
$$

Thus

$$
\left|\mathcal{E}_{1}\right| \gg X S_{0}+S_{1}
$$

where

$$
\begin{align*}
S_{0} & :=\sum_{K \in \mathcal{K}} \sum_{K L \in \mathcal{J}(K)}\left(\sum_{d \mid N_{P}(L)} \lambda_{d}^{-}\right) \frac{\varrho_{P}(K L)}{N_{P}(K L)} \\
S_{1} & :=\sum_{K \in \mathcal{K}} \sum_{K L \in \mathcal{J}(K)}\left(\sum_{d \mid N_{P}(L)} \lambda_{d}^{-}\right) R_{K L} . \tag{3.6}
\end{align*}
$$

To obtain Theorem 1.1 we see it suffices to prove the following two key propositions.
Proposition 3.2 (Estimate for $S_{0}$ ). Let $\theta_{0}$ 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 $\theta_{0}$ 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 $[A, 2 A]^{3}$ )
an auxiliary polynomial $q\left(a_{1}, a_{2}, a_{3}\right)=q_{1}\left(a_{1}, a_{2}, a_{3}\right) q_{2}\left(a_{1}, a_{2}, a_{3}\right)$ takes values where $P^{+}\left(q_{2}\left(a_{1}, a_{2}, a_{3}\right)\right)<A^{2-\epsilon}$ and $P^{+}\left(q_{1}\left(a_{1}, a_{2}, a_{3}\right)\right)<A^{1-\epsilon}$. The term $q_{2}$ will be a quadratic form, and so $P^{+}\left(q_{2}\left(a_{1}, a_{2}, a_{3}\right)\right)<A^{2-\epsilon}$ if $p \mid q_{2}\left(a_{1}, a_{2}, a_{3}\right)$ for some $p \in\left[A^{2 \epsilon}, A^{3 \epsilon}\right]$, which occurs if $a_{1}, a_{2}, a_{3}$ lie in suitable residue classes $(\bmod p)$. Thus it suffices to show that there are the expected number of $\left(a_{1}, a_{2}, a_{3}\right)$ such that $P^{+}\left(q_{1}\left(a_{1}, a_{2}, a_{3}\right)\right)<$ $A^{1-\epsilon}$ and $\left(a_{1}, a_{2}, a_{3}\right)$ lies in a suitable residue class modulo $p$ on average over $p \in\left[A^{2 \epsilon}, A^{3 \epsilon}\right]$. 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 $\left\{\nu_{1}, \nu_{2}, \nu_{3}, \nu_{4}\right\}$ for $\mathcal{O}_{K}$ such that $\nu_{1}=1$ and $K=\mathbb{Q}\left(\nu_{2}\right)$. Given a large value $X$, we wish to count the number of $\left(a_{1}, a_{2}, a_{3}\right)$ in a small box such that $N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)$ has only small prime factors, and such that an auxiliary quadratic form $f\left(a_{1}, a_{2}, a_{3}\right)$ is a multiple of some fairly small $p \in\left[X^{\tau}, X^{\tau^{\prime}}\right]$.

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

$$
\begin{equation*}
\mathcal{X}:=\prod_{i=1}^{3}\left[X_{i}, X_{i}\left(1+\eta_{1}\right)[\right. \tag{4.1}
\end{equation*}
$$

where $\eta_{1} \in \mathbb{R}$ and $X_{1}, X_{2}, X_{3} \in \mathbb{Z}$ are parameters satisfying

$$
\begin{align*}
\eta_{1} & :=(\log X)^{-100}  \tag{4.2}\\
X_{1}, X_{2}, X_{3} & \in\left[\eta_{1} X, X\right]  \tag{4.3}\\
N_{K / \mathbb{Q}}\left(X_{1} \nu_{1}+X_{2} \nu_{2}+X_{3} \nu_{3}\right) & \geq \eta_{1}^{1 / 10} \max _{i}\left(X_{i}^{4}\right) \tag{4.4}
\end{align*}
$$

We are then interested in the sets

$$
\begin{align*}
\mathcal{A} & :=\left\{\left(a_{1}, a_{2}, a_{3}\right) \in \mathbb{Z}^{3} \cap \mathcal{X}\right\} \\
\mathcal{A}\left(\mathbf{u}_{0}, m, p\right) & :=\left\{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{A}: \mathbf{a} \equiv \mathbf{u}_{0}(\bmod m), p \mid f\left(a_{1}, a_{2}, a_{3}\right)\right\} \\
\mathcal{A}_{d}\left(\mathbf{u}_{0}, m, p\right) & :=\left\{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{A}\left(\mathbf{u}_{0}, m, p\right): d \mid N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)\right\} \tag{4.5}
\end{align*}
$$

Since we wish to count points when $N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)$ has small prime factors, we will count how often $d \mid N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)$ 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 $\left[X^{\theta_{j}}, X^{\theta_{j}^{\prime}}\right]$ for some fixed constants $\theta_{i}, \theta_{i}^{\prime}$. We will require $\theta_{j}, \theta_{j}^{\prime}$ satisfy the following conditions.

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

$$
\begin{equation*}
\delta<\theta_{i}<\theta_{i}^{\prime}<1-\delta \quad \forall 1 \leq i \leq \ell \tag{4.6}
\end{equation*}
$$

- $\left(q_{1 j}\right.$ are distinct primes $)$

$$
\begin{equation*}
\left[\theta_{i}, \theta_{i}^{\prime}\right] \cap\left[\theta_{j}, \theta_{j}^{\prime}\right]=\emptyset \quad \forall 1 \leq i<j \leq \ell \tag{4.7}
\end{equation*}
$$

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

$$
\begin{equation*}
\sum_{i=1}^{\ell} \theta_{i}^{\prime}<4-\delta \tag{4.8}
\end{equation*}
$$

- (Impossible for $q_{1 j}^{2}$ to divide $\left.N\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)\right)$

$$
\begin{equation*}
\theta_{j}+\sum_{i=1}^{\ell} \theta_{i}>4+\delta \quad \forall 1 \leq j \leq \ell \tag{4.9}
\end{equation*}
$$

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

$$
\begin{equation*}
1+\delta<\sum_{i=1}^{\ell^{\prime}} \theta_{i}<\sum_{i=1}^{\ell^{\prime}} \theta_{i}^{\prime}<2-\delta . \tag{4.10}
\end{equation*}
$$

The conditions $\sqrt{4.6}$ - $\sqrt{4.9}$ are minor constraints to avoid some technical issues and to ensure that we expect that $d \mid N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)$ 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 $f\left(a_{1}, a_{2}, a_{3}\right)$ 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 $f\left(X_{1}, X_{2}, X_{3}\right) \in \mathbb{Z}\left[X_{1}, X_{2}, X_{3}\right]$ be a homogeneous quadratic polynomial which splits into two distinct linear factors

$$
f\left(X_{1}, X_{2}, X_{3}\right)=L_{1}\left(X_{1}, X_{2}, X_{3}\right) L_{2}\left(X_{1}, X_{2}, X_{3}\right)
$$

over a suitable extension of $\mathbb{Q}$. Let $D_{f} \in \mathbb{N}$ such that if $p \equiv 1\left(\bmod D_{f}\right)$ then the $\mathbb{F}_{p}$-reduction of the two linear forms $L_{1}\left(X_{1}, X_{2}, X_{3}\right), L_{2}\left(X_{1}, X_{2}, X_{3}\right)$ are in $\mathbb{F}_{p}\left[X_{1}, X_{2}, X_{3}\right]$.

Let $K$ be a quartic extension of $\mathbb{Q}$ with $\left\{\nu_{1}, \nu_{2}, \nu_{3}, \nu_{4}\right\}$ being a $\mathbb{Z}$-basis for $\mathcal{O}_{K}$ such that $\nu_{1}=1$ and $K=\mathbb{Q}\left(\nu_{2}\right)$. Let $X_{1}, X_{2}, X_{3}$ satisfy 4.3) and (4.4). Let $\ell, \ell^{\prime} \in \mathbb{N}$ such that $1 \leq \ell^{\prime}<\ell$ and $\theta_{1}, \theta_{1}^{\prime}, \ldots, \theta_{\ell}, \theta_{\ell}^{\prime}$ be reals satisfying 4.6)-4.10. Let $0<\tau<\tau^{\prime}$ satisfy

$$
\begin{equation*}
\tau^{\prime}<\min \left(\frac{4-2 \theta_{1}^{\prime}-\ldots-2 \theta_{\ell^{\prime}}^{\prime}}{100}, \frac{\theta_{1}+\cdots+\theta_{\ell^{\prime}}-1}{100}\right) \tag{4.11}
\end{equation*}
$$

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

Then for any choice of $\mathbf{u}_{0}(\bmod m)$ and $K>0$, we have

$$
\begin{aligned}
& \sum_{\substack{p \in\left[X^{\tau}, X^{\tau^{\prime}}\right] \\
p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{q_{1}, \ldots, q_{\ell} \text { prime } \\
q_{j} \in\left[X^{\theta_{j}}, X^{\theta_{j}^{\prime}}\right] \forall 1 \leq j \leq \ell}}\left|\mathcal{A}_{q_{1} \cdots q_{\ell}}\left(\mathbf{u}_{0}, m, p\right)\right| \\
&= \eta_{1}^{3} X_{1} X_{2} X_{3} \frac{2 \log \left(\frac{\tau^{\prime}}{\tau}\right)}{m^{3} \varphi\left(D_{f}\right)} \prod_{i=1}^{\ell} \log \left(\frac{\theta_{i}^{\prime}}{\theta_{i}}\right)+O\left(\frac{X_{1} X_{2} X_{3}}{(\log X)^{K}}\right) .
\end{aligned}
$$

The implied constant depends on $f, K, A, \delta$ and the $\nu_{i}, \theta_{i}, \theta_{i}^{\prime}$ 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 $N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)$ is a multiple of $q_{1} \ldots q_{\ell}$. 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 $N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+\right.$ $\left.a_{2} \nu_{2}+a_{3} \nu_{3}\right)=m_{1} m_{2}$ where $m_{1}=q_{1} \cdots q_{\ell^{\prime}}$ is a product of $\ell^{\prime}$ primes of constrained size and $m_{2}=q_{\ell^{\prime}+1} \cdots q_{\ell} r$ is the product of $\ell-\ell^{\prime}$ 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 $q\left(a_{1}, a_{2}, a_{3}\right)$ 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 $r_{1} r_{2}+r_{3} r_{4} \in \mathbb{Z}$ (c.f. Lemma 5.9), and that $q$ factorises as $q_{1} q_{2}$ 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 $K:=\mathbb{Q}\left(r_{1}+r_{3}\right)$ of $\mathbb{Q}$, the form $q_{1}$ satisfies

$$
q_{1}\left(a_{1}, a_{2}, a_{3}\right)= \pm N_{K / \mathbb{Q}}\left(a_{1}+a_{2}\left(r_{1}+r_{3}\right)+a_{3}\left(r_{1}^{2}+r_{1} r_{3}+r_{3}^{2}\right)\right),
$$

and so takes the shape of an incomplete norm form (c.f. Proposition 5.11).
The quadratic $q_{2}$ takes the form

$$
\begin{align*}
q_{2}\left(a_{1}, a_{2}, a_{3}\right) & =\left[a_{1}+\left(r_{1}+r_{2}\right) a_{2}+\left(r_{1}^{2}+r_{1} r_{2}+r_{2}^{2}\right) a_{3}\right]  \tag{4.12}\\
& \times\left[a_{1}+\left(r_{3}+r_{4}\right) a_{2}+\left(r_{3}^{2}+r_{3} r_{4}+r_{4}^{2}\right) a_{3}\right] .
\end{align*}
$$

Since the two polynomials $P_{1}(X):=\left(X-\left(r_{1}+r_{2}\right)\right)\left(X-\left(r_{3}+r_{4}\right)\right)$ and $P_{2}(X):=\left(X-\left(r_{1}^{2}+r_{1} r_{2}+r_{2}^{2}\right)\right)\left(X-\left(r_{3}^{2}+r_{3} r_{4}+r_{4}^{2}\right)\right)$ are in $\left.\mathbb{Z}[X]^{2}\right] r_{1}+r_{2}$ and $r_{1}^{2}+r_{1} r_{2}+r_{2}^{2}$ are of degree at most 2 over $\mathbb{Q}$. Let $\Delta_{1}$ and $\Delta_{2}$ be the discriminant of these two polynomials and

$$
D_{q_{2}}:= \begin{cases}{\left[8, \Delta_{1}, \Delta_{2}\right]} & \text { if } \Delta_{1} \Delta_{2} \neq 0  \tag{4.13}\\ {\left[8, \Delta_{1}+\Delta_{2}\right]} & \text { otherwise }\end{cases}
$$

[^1]Since $P$ is irreducible of degree 4, we don't have $\Delta_{1}=\Delta_{2}=00^{3}$ If $p \equiv 1\left(\bmod D_{q_{2}}\right)$ and $\Delta_{1} \Delta_{2} \neq 0$, then $\left(\Delta_{1} / p\right)=\left(\Delta_{2} / p\right)=1$ 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 $p \equiv 1\left(\bmod D_{q_{2}}\right)$ and $\Delta_{1} \Delta_{2}=0$.

Then $N_{K / \mathbb{Q}}\left(\sum_{i=1}^{4} a_{i} \nu_{i}\right)$ is a quartic form in the integer variables $a_{1}, a_{2}, a_{3}, a_{4}$, and we have for all $a_{1}, a_{2}, a_{3}, a_{4} \in \mathbb{Z}$

$$
N_{K / \mathbb{Q}}\left(\sum_{i=1}^{4} a_{i} \nu_{i}\right)=\prod_{i=1}^{4}\left(\sum_{j=1}^{4} a_{j} \sigma_{i}\left(\nu_{j}\right)\right),
$$

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 $r_{1} r_{2}+r_{3} r_{4} \in \mathbb{Q}$. We are interested in the auxiliary polynomial $q_{2}$ (see 5.25), given by

To ensure that $q_{1}\left(a_{1}, a_{2}, a_{3}\right)=N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)$ is composed only of suitably small prime factors, we will look for $a_{1}, a_{2}, a_{3}$ such that

$$
q_{11} q_{12} q_{13} q_{14} \ldots q_{1 \ell} \mid N_{K / \mathbb{Q}}\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)
$$

for some suitable primes $q_{11}, q_{12}, q_{13}, q_{14}, \ldots, q_{1 \ell}<X^{1-\delta}$ with $\prod_{j=1}^{\ell} q_{1 j}>$ $X^{3+\delta}$. 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 $\mathbb{Z}\left[r_{1}\right]$ the function

$$
\varrho_{P}(\mathfrak{I})=\operatorname{card}\left\{0 \leq n<N_{P}(\mathfrak{I}): n \equiv r_{1}(\bmod \mathfrak{I})\right\},
$$

where $N_{P}=N_{\mathbb{Q}\left(r_{1}\right) / \mathbb{Q}}$ is the norm on $\mathbb{Q}\left(r_{1}\right)$. 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 $\mathcal{O}_{\mathbb{Q}\left(r_{1}\right)}$ such that $\left(N_{P}(\mathfrak{I}), \operatorname{Disc}(P)\right)=1$. If the equation $n \equiv r_{1}(\bmod \mathfrak{I})$ 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 $m \in \mathbb{Z}, \mathfrak{I}\left|m \Leftrightarrow N_{P}(\mathfrak{I})\right| m$.

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

[^2]
### 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 $\alpha \in \mathbb{Z}\left[r_{1}\right]$, 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 $m_{\alpha}: \mathbb{Q}\left(r_{1}\right) \rightarrow \mathbb{Q}\left(r_{1}\right)$ be the multiplication-by- $\alpha$ map: $m_{\alpha}(x)=\alpha x$. Let $M_{\alpha}$ be the matrix of $m_{\alpha}$ with respect to the basis $\left\{1, r_{1}, r_{1}^{2}, r_{1}^{3}, \ldots, r_{1}^{n-1}\right\}$ and $N_{P}(\alpha)=N_{\mathbb{Q}\left(r_{1}\right) / \mathbb{Q}}(\alpha)$ its determinant. For $P(X)=X^{4}+2$ the corresponding matrix is

$$
\left(\begin{array}{cccc}
a_{0} & -2 a_{3} & -2 a_{2} & -2 a_{1} \\
a_{1} & a_{0} & -2 a_{3} & -2 a_{2} \\
a_{2} & a_{1} & a_{0} & -2 a_{3} \\
a_{3} & a_{2} & a_{1} & a_{0}
\end{array}\right) .
$$

More generally since $r_{1}^{n}=-c_{0}-c_{1} r_{1}-\cdots-c_{n-1} r_{1}^{n-1}$, we have

$$
M_{\alpha}=\left(\begin{array}{ccccc}
a_{0} & -c_{0} a_{n-1} & * & \cdots & *  \tag{5.1}\\
a_{1} & a_{0}-c_{1} a_{n-1} & * & \cdots & * \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
a_{n-1} & a_{n-2}-c_{n-1} a_{n-1} & * & \cdots & *
\end{array}\right) .
$$

In this section we prove results analogous to [4, Lemma 4.1] or [1, Lemma 3.2]. As in these two papers, we let $B_{i j}=B_{i j}(\alpha)$ 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 $M_{\alpha}$ and multiply it by $(-1)^{i+j}$. If $\alpha=a_{0}+a_{1} r_{1}+\cdots+a_{n-1} r_{1}^{n-1}$ then $B_{i j}$ is a polynomial in the $a_{i}$. By an abuse of notation we will sometimes use $B_{i j}$ to refer to this polynomial, and sometimes the value attained at a particular point $\left(a_{0}, a_{1}, \ldots, a_{n-1}\right)$. 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 $\left(N_{P}(\alpha), B_{1 n} \operatorname{Disc}(P)\right)=1$. Then there exists an integer $k_{\alpha}$, with $0 \leq k_{\alpha}<N_{P}(\alpha)$ such that we have

$$
n-r_{1} \equiv 0(\bmod (\alpha)) \Leftrightarrow n \equiv k_{\alpha}\left(\bmod N_{P}(\alpha)\right) .
$$

This integer $k_{\alpha}$ satisfies the congruence

$$
k_{\alpha} \equiv B_{2 n} \overline{B_{1 n}}\left(\bmod N_{P}(\alpha)\right) .
$$

Furthermore, if $\mathfrak{J}$ is an ideal of $\mathbb{Z}\left[r_{1}\right]$ containing a principal ideal $(\alpha)$ with $\alpha$ as above then there exists a unique $k_{\mathfrak{J}}$ with $0 \leq k_{\mathfrak{J}}<N_{P}(\mathfrak{J})$ and

$$
n-r_{1} \in \mathfrak{J} \Leftrightarrow n \equiv k_{\mathfrak{J}}\left(\bmod N_{P}(\mathfrak{J})\right)
$$

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 $\left(m_{i, j}\right)_{1 \leq i, j \leq n}$ be the coefficients of $M_{\alpha}$. We obtain the equations

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

This system can be represented as

$$
\left(\begin{array}{cccc}
m_{2,1} & m_{3,1} & \ldots & m_{n, 1}  \tag{5.2}\\
m_{2,2} & m_{3,2} & \ldots & m_{n, 2} \\
\vdots & \vdots & \ldots & \vdots \\
m_{2, n} & m_{3, n} & \ldots & m_{n, n}
\end{array}\right)\left(\begin{array}{c}
r_{1} \\
r_{1}^{2} \\
\vdots \\
r_{1}^{n-1}
\end{array}\right)=\left(\begin{array}{c}
-m_{1,1} \\
-m_{1,2} \\
\vdots \\
-m_{1, n}
\end{array}\right)(\bmod (\alpha))
$$

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

$$
r_{1} \operatorname{det}\left(\begin{array}{cccc}
m_{2,1} & m_{3,1} & \ldots & m_{n, 1}  \tag{5.3}\\
\vdots & \vdots & \ldots & \vdots \\
m_{2, i-1} & m_{3, i-1} & \ldots & m_{n, i-1} \\
m_{2, i+1} & m_{3, i+1} & \ldots & m_{n, i+1} \\
\vdots & \vdots & \ldots & \vdots \\
m_{2, n-1} & m_{3, n-1} & \ldots & m_{n, n-1} \\
m_{2, n} & m_{3, n} & \ldots & m_{n, n}
\end{array}\right)=\operatorname{det}\left(\begin{array}{cccc}
-m_{1,1} & m_{3,1} & \ldots & m_{n, 1} \\
\vdots & \vdots & \ldots & \vdots \\
-m_{1, i-1} & m_{3, i-1} & \ldots & m_{n, i-1} \\
-m_{1, i+1} & m_{3, i+1} & \ldots & m_{n, i+1} \\
\vdots & \vdots & \ldots & \vdots \\
-m_{1, n-1} & m_{3, n-1} & \ldots & m_{n, n-1} \\
-m_{1, n} & m_{3, n} & \ldots & m_{n, n}
\end{array}\right)(\bmod (\alpha)) .
$$

The transpose of the matrix on the left is the submatrix of $M_{\alpha}$ obtained by removing the first line and the $i^{t h}$ column. The matrix on the right is the submatrix of $M_{\alpha}$ obtained by removing the second line and the $i^{t h}$ column and by multiplying all elements of the first column by -1 .

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

$$
M_{\alpha}^{-1}=\frac{1}{N_{P}(\alpha)}\left(\begin{array}{cccc}
B_{11} & B_{21} & \ldots & B_{n 1}  \tag{5.4}\\
B_{12} & B_{22} & \ldots & B_{n 2} \\
\vdots & \vdots & \ldots & \vdots \\
B_{1 n} & B_{2 n} & \ldots & B_{n n}
\end{array}\right) .
$$

With this notation, 5.3 becomes

$$
(-1)^{i+1} B_{1 i} r_{1} \equiv-(-1)^{i+2} B_{2 i}(\bmod (\alpha))
$$

In particular, this gives

$$
\begin{equation*}
B_{1 i} r_{1} \equiv B_{2 i}(\bmod (\alpha)) \tag{5.5}
\end{equation*}
$$

By Lemma 5.1 (and the assumption $(N(\alpha), \operatorname{Disc}(P))=1$ ), if an integer is congruent to $0(\bmod (\alpha))$ 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 $J \mid(\alpha)$, thus it suffices to take $k_{J} \in\left[0, N_{P}(J)\right]$ such that $k_{J} \equiv k_{\alpha}\left(\bmod N_{P}(J)\right)$. The claim now follows from 5.5 .

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

$$
\alpha^{-1}=\frac{1}{N_{P}(\alpha)}\left(B_{11}+B_{12} r_{1}+\cdots+B_{1 n} r_{1}^{n-1}\right)
$$

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

$$
\left(\begin{array}{c}
B_{21}  \tag{5.6}\\
B_{22} \\
\vdots \\
B_{2(n-1)} \\
B_{2 n}
\end{array}\right)=\left(\begin{array}{c}
-c_{0} B_{1 n} \\
B_{11}-c_{1} B_{1 n} \\
\vdots \\
B_{1(n-2)}-c_{n-2} B_{1 n} \\
B_{1(n-1)}-c_{n-1} B_{1 n}
\end{array}\right)
$$

In particular the last line implies that

$$
\begin{equation*}
B_{2 n}=B_{1(n-1)}-c_{n-1} B_{1 n} \tag{5.7}
\end{equation*}
$$

For $n=4$, and $c_{3}=0$, we recover the formula $B_{14} r_{1} \equiv B_{24}=B_{13}(\bmod (\alpha))$, 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 $q_{3}=q_{3}\left(a_{1}, a_{2}, a_{3}\right)$ in $a_{1}, a_{2}, a_{3}$ such that

$$
\begin{equation*}
B_{24} B_{13}-B_{14} B_{23}=q_{3} N_{P}(\alpha) \tag{5.8}
\end{equation*}
$$

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

$$
r_{1} B_{13} B_{24} \equiv r_{1} B_{14} B_{23}\left(\bmod N_{P}(\alpha)\right) .
$$

Since this holds for all $a_{0}, a_{1}, a_{2}, a_{3}$, we deduce that there exists a form $q_{3}=q_{3}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)$ such that whenever $\left(N_{P}(\alpha), \operatorname{Disc}(P)\right)=1$ we have ${ }^{4}$

$$
\begin{equation*}
B_{24} B_{13}-B_{14} B_{23}=q_{3} N_{P}(\alpha) \tag{5.9}
\end{equation*}
$$

Since both sides are polynomials, this must actually hold for all $\alpha$ (including $\left(N_{P}(\alpha), \operatorname{Disc}(P)\right) \neq 1$.) 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 $B_{i j}, i \neq j$ 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

$$
\begin{equation*}
q_{3}\left(a_{1}, a_{2}, a_{3}\right)=a_{2}^{2}-a_{1} a_{3}-c_{3} a_{2} a_{3}+c_{2} a_{3}^{2} \tag{5.10}
\end{equation*}
$$

When $c_{3}=0$ this coincides with the form $-q_{4}$ given in [1, equation (2.7)].

[^3]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 $\operatorname{Resultant}\left(P_{1}, P_{2} ; x\right)$ 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

$$
\begin{align*}
R & :=R\left(a_{1}, a_{2}, a_{3}\right)=\operatorname{Resultant}\left(B_{14}, N_{P}(\alpha) ; a_{0}\right) \\
R_{0} & :=R_{0}\left(a_{1}, a_{2}, a_{3}\right)=\operatorname{Resultant}\left(B_{13}, B_{14} ; a_{0}\right) \tag{5.11}
\end{align*}
$$

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
$q_{3}^{2} R=\operatorname{Resultant}\left(B_{14}, q_{3} N_{P}(\alpha) ; a_{0}\right)=\operatorname{Resultant}\left(B_{14}, B_{24} B_{13}-B_{14} B_{23} ; a_{0}\right)$.
But $B_{24}=B_{13}-c_{3} B_{14}$ and $B_{13}$ is also of degree 2 in $a_{0}$. We deduce that

$$
q_{3}^{2} R=\operatorname{Resultant}\left(B_{14}, B_{13}^{2} ; a_{0}\right)=R_{0}^{2}
$$

This ends the proof of Lemma 5.4
We see that the polynomial $q_{3}$ divides $R_{0}$, and so we can write

$$
\begin{equation*}
R_{0}=q q_{3} \tag{5.12}
\end{equation*}
$$

for some homogeneous polynomial $q=q\left(a_{1}, a_{2}, a_{3}\right)$. Moreover, since $R_{0}$ is the resultant of $B_{13}$ and $B_{14}$, there are two polynomials $U$ and $V \in$ $\mathbb{Z}\left[a_{0}, a_{1}, a_{2}, a_{3}\right]$ such that

$$
\begin{equation*}
U B_{13}+V B_{14}=q q_{3} \tag{5.13}
\end{equation*}
$$

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 $\left(B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right), q\left(a_{1}, a_{2}, a_{3}\right)\right)=$ 1. Then $\left(N_{P}(\alpha), B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right)=1$ and for $h \in \mathbb{Z}$ we have
$\mathrm{e}\left(\frac{-h k_{\alpha}}{N_{P}(\alpha)}\right)=\mathrm{e}\left(\frac{-h U\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \overline{B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)}}{q\left(a_{1}, a_{2}, a_{3}\right)}+h R\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right)$,
where $U=U\left(a_{0}, a_{1}, a_{2}, a_{3}\right)$ is defined by 5.13 and $R$ is given by

$$
R\left(a_{0}, a_{1}, a_{2}, a_{3}\right)=\frac{U}{q B_{14}}-\frac{B_{24}}{N_{P}(\alpha) B_{14}}
$$

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 $\left(N_{P}(\alpha), B_{14}\right)=1$. By Lemma 5.2

$$
\mathrm{e}\left(\frac{k_{\alpha}}{N_{P}(\alpha)}\right)=\mathrm{e}\left(\frac{B_{24} \overline{B_{14}}}{N_{P}(\alpha)}\right)
$$

We use the Bézout relation

$$
\begin{equation*}
\frac{\bar{u}}{v}+\frac{\bar{v}}{u} \equiv \frac{1}{u v}(\bmod 1) \quad \text { for }(u, v)=1, \tag{5.14}
\end{equation*}
$$

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

$$
\begin{equation*}
\mathrm{e}\left(\frac{k_{\alpha}}{N_{P}(\alpha)}\right)=\mathrm{e}\left(-\frac{B_{24} \overline{N_{P}(\alpha)}}{B_{14}}+\frac{B_{24}}{B_{14} N_{P}(\alpha)}\right) . \tag{5.15}
\end{equation*}
$$

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

$$
\begin{aligned}
U N_{P}(\alpha) q_{3} & =U\left[B_{13}\left(B_{13}-c_{3} B_{14}\right)-B_{14} B_{23}\right] \\
& =U\left(B_{13}^{2}-B_{14}\left(B_{23}+c_{3} B_{13}\right)\right) \\
& \left.=B_{13}\left(q_{3} q-V B_{14}\right)-U B_{14}\left(B_{23}+c_{3} B_{13}\right)\right) .
\end{aligned}
$$

This rearranges to give

$$
\left(U N_{P}(\alpha)-q B_{13}\right) q_{3}=B_{14}\left(-V B_{13}-U\left(B_{23}+c_{3} B_{13}\right)\right)
$$

Since $q_{3}$ and $B_{14}$ are coprime, we deduce that

$$
\begin{equation*}
U N_{P}(\alpha)-q B_{13} \equiv 0\left(\bmod B_{14}\right) . \tag{5.16}
\end{equation*}
$$

Since $B_{24} \equiv B_{13}\left(\bmod B_{14}\right)$, we obtain

$$
B_{24} \overline{N_{P}(\alpha)} \equiv B_{13} \overline{N_{P}(\alpha)}\left(\bmod B_{14}\right) \equiv U \bar{q}\left(\bmod B_{14}\right) .
$$

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 $a_{0}$

$$
\begin{align*}
B_{13}= & -a_{2} a_{0}^{2}+\left(a_{1}^{2}+c_{3} a_{1} a_{2}+\left(-c_{3}^{2}+c_{2}\right) a_{2}^{2}+\left(-2 c_{2}\right) a_{1} a_{3}\right. \\
& \left.+\left(c_{3}^{3}-c_{2} c_{3}+c_{1}\right) a_{2} a_{3}+\left(-c_{2} c_{3}^{2}+c_{2}^{2}+c_{1} c_{3}-c_{0}\right) a_{3}^{2}\right) a_{0} \\
& +\left(-c_{3}\right) a_{1}^{3}+c_{3}^{2} a_{1}^{2} a_{2}+\left(-c_{2} c_{3}\right) a_{1} a_{2}^{2}+\left(c_{1} c_{3}-c_{0}\right) a_{2}^{3} \\
& +\left(-c_{3}^{3}+2 c_{2} c_{3}\right) a_{1}^{2} a_{3}+\left(c_{2} c_{3}^{2}-3 c_{1} c_{3}+2 c_{0}\right) a_{1} a_{2} a_{3} \\
& +\left(-c_{1} c_{3}^{2}+2 c_{0} c_{3}\right) a_{2}^{2} a_{3}+\left(-c_{2}^{2} c_{3}+2 c_{1} c_{3}^{2}-2 c_{0} c_{3}\right) a_{1} a_{3}^{2} \\
& +\left(c_{1} c_{2} c_{3}-c_{0} c_{3}^{2}-c_{0} c_{2}\right) a_{2} a_{3}^{2}+\left(-c_{1}^{2} c_{3}+c_{0} c_{2} c_{3}+c_{0} c_{1}\right) a_{3}^{3},  \tag{5.17}\\
B_{14}= & -a_{3} a_{0}^{2}+\left(2 a_{1} a_{2}-c_{3} a_{2}^{2}-c_{3} a_{1} a_{3}+c_{3}^{2} a_{2} a_{3}+\left(-c_{2} c_{3}+2 c_{1}\right) a_{3}^{2}\right) a_{0} \\
& -a_{1}^{3}+c_{3} a_{1}^{2} a_{2}-c_{2} a_{1} a_{2}^{2}+c_{1} a_{2}^{3}+\left(-c_{3}^{2}+2 c_{2}\right) a_{1}^{2} a_{3}+\left(c_{2} c_{3}-3 c_{1}\right) a_{1} a_{2} a_{3} \\
& +\left(-c_{1} c_{3}+c_{0}\right) a_{2}^{2} a_{3}+\left(-c_{2}^{2}+2 c_{1} c_{3}-c_{0}\right) a_{1} a_{3}^{2} \\
& +\left(c_{1} c_{2}-c_{0} c_{3}\right) a_{2} a_{3}^{2}+\left(-c_{1}^{2}+c_{0} c_{2}\right) a_{3}^{3} . \tag{5.18}
\end{align*}
$$

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 $V$

$$
\begin{aligned}
U= & a_{0}\left(-a_{1}^{2} a_{3}^{2}+2 a_{1} a_{2}^{2} a_{3}-2 c_{3} a_{1} a_{2} a_{3}^{2}+2 c_{2} a_{1} a_{3}^{3}-c_{3} a_{2}^{3} a_{3}+\right. \\
& \left.\quad\left(2 c_{3}^{2}-c_{2}\right) a_{2}^{2} a_{3}^{2}+\left(-c_{3}^{3}+c_{1}\right) a_{2} a_{3}^{3}+\left(c_{2} c_{3}^{2}-c_{2}^{2}-c_{1} c_{3}+c_{0}\right) a_{3}^{4}\right) \\
& +3 a_{1}^{3} a_{2} a_{3}-2 c_{3} a_{1}^{3} a_{3}^{2}-4 a_{1}^{2} a_{2}^{3}+4 c_{3} a_{1}^{2} a_{2}^{2} a_{3} \\
& +\left(c_{3}^{2}-6 c_{2}\right) a_{1}^{2} a_{2} a_{3}^{2}+\left(-c_{3}^{3}+3 c_{2} c_{3}+2 c_{1}\right) a_{1}^{2} a_{3}^{3} \\
& +4 c_{3} a_{1} a_{2}^{4}+\left(-9 c_{3}^{2}+3 c_{2}\right) a_{1} a_{2}^{3} a_{3}+\left(6 c_{3}^{3}+c_{2} c_{3}-3 c_{1}\right) a_{1} a_{2}^{2} a_{3}^{2} \\
& +\left(-c_{3}^{4}-5 c_{2} c_{3}^{2}+3 c_{2}^{2}+2 c_{1} c_{3}+c_{0}\right) a_{1} a_{2} a_{3}^{3}+\left(c_{2} c_{3}^{3}+c_{1} c_{3}^{2}-4 c_{1} c_{2}-c_{0} c_{3}\right) a_{1} a_{3}^{4}-c_{3}^{2} a_{2}^{5} \\
& +\left(3 c_{3}^{3}-c_{2} c_{3}-c_{1}\right) a_{2}^{4} a_{3}+\left(-3 c_{3}^{4}+5 c_{1} c_{3}-2 c_{0}\right) a_{2}^{3} a_{3}^{2} \\
& +\left(c_{3}^{5}+3 c_{2} c_{3}^{3}-2 c_{2}^{2} c_{3}-7 c_{1} c_{3}^{2}+c_{1} c_{2}+4 c_{0} c_{3}\right) a_{2}^{2} a_{3}^{3} \\
& +\left(-2 c_{2} c_{3}^{4}+c_{2}^{2} c_{3}^{2}+3 c_{1} c_{3}^{3}+2 c_{1} c_{2} c_{3}-2 c_{0} c_{3}^{2}-c_{1}^{2}-2 c_{0} c_{2}\right) a_{2} a_{3}^{4} \\
& +\left(c_{2}^{2} c_{3}^{3}-c_{2}^{3} c_{3}-3 c_{1} c_{2} c_{3}^{2}+2 c_{1} c_{2}^{2}+c_{1}^{2} c_{3}+2 c_{0} c_{2} c_{3}-c_{0} c_{1}\right) a_{3}^{5}
\end{aligned}
$$

$$
V=a_{0}\left(a_{1}^{2} a_{2} a_{3}-2 a_{1} a_{2}^{3}+2 c_{3} a_{1} a_{2}^{2} a_{3}-2 c_{2} a_{1} a_{2} a_{3}^{2}+c_{3} a_{2}^{4}\right.
$$

$$
\left.+\left(-2 c_{3}^{2}+c_{2}\right) a_{2}^{3} a_{3}+\left(c_{3}^{3}-c_{1}\right) a_{2}^{2} a_{3}^{2}+\left(-c_{2} c_{3}^{2}+c_{2}^{2}+c_{1} c_{3}-c_{0}\right) a_{2} a_{3}^{3}\right)
$$

$$
-a_{1}^{4} a_{3}+a_{1}^{3} a_{2}^{2}-2 c_{3} a_{1}^{3} a_{2} a_{3}+4 c_{2} a_{1}^{3} a_{3}^{2}+2 c_{3} a_{1}^{2} a_{2}^{3}+\left(-c_{3}^{2}-4 c_{2}\right) a_{1}^{2} a_{2}^{2} a_{3}
$$

$$
+\left(-c_{3}^{3}+5 c_{2} c_{3}\right) a_{1}^{2} a_{2} a_{3}^{2}+\left(2 c_{2} c_{3}^{2}-6 c_{2}^{2}-2 c_{1} c_{3}+2 c_{0}\right) a_{1}^{2} a_{3}^{3}+\left(-3 c_{3}^{2}+c_{2}\right) a_{1} a_{2}^{4}
$$

$$
+\left(6 c_{3}^{3}-c_{2} c_{3}-c_{1}\right) a_{1} a_{2}^{3} a_{3}+\left(-3 c_{3}^{4}-7 c_{2} c_{3}^{2}+5 c_{2}^{2}+6 c_{1} c_{3}-5 c_{0}\right) a_{1} a_{2}^{2} a_{3}^{2}
$$

$$
+\left(7 c_{2} c_{3}^{3}-4 c_{2}^{2} c_{3}-5 c_{1} c_{3}^{2}+5 c_{0} c_{3}\right) a_{1} a_{2} a_{3}^{3}+\left(-4 c_{2}^{2} c_{3}^{2}+4 c_{2}^{3}+4 c_{1} c_{2} c_{3}-4 c_{0} c_{2}\right) a_{1} a_{3}^{4}
$$

$$
+\left(c_{3}^{3}-c_{2} c_{3}+c_{1}\right) a_{2}^{5}+\left(-3 c 3^{4}+4 c_{2} c_{3}^{2}-c_{2}^{2}-3 c_{1} c_{3}+2 c_{0}\right) a_{2}^{4} a_{3}
$$

$$
+\left(3 c_{3}^{5}-3 c_{2} c_{3}^{3}+c_{1} c_{3}^{2}+c_{1} c_{2}-2 c_{0} c_{3}\right) a_{2}^{3} a_{3}^{2}
$$

$$
+\left(-c_{3}^{6}-2 c_{2} c_{3}^{4}+5 c_{2}^{2} c_{3}^{2}+3 c_{1} c_{3}^{3}-2 c_{2}^{3}-4 c_{1} c_{2} c_{3}-2 c_{0} c_{3}^{2}+4 c_{0} c_{2}\right) a_{2}^{2} a_{3}^{3}
$$

$$
+\left(2 c_{2} c_{3}^{5}-3 c_{2}^{2} c_{3}^{3}-2 c_{1} c_{3}^{4}+c_{2}^{3} c_{3}+c_{1} c_{2} c_{3}^{2}+2 c_{0} c_{3}^{3}+c_{1}^{2} c_{3}-2 c_{0} c_{2} c_{3}-c_{0} c_{1}\right) a_{2} a_{3}^{4}
$$

$$
\begin{equation*}
+\left(-c_{2}^{2} c_{3}^{4}+2 c_{2}^{3} c_{3}^{2}+2 c_{1} c_{2} c_{3}^{3}-c_{2}^{4}-2 c_{1} c_{2}^{2} c_{3}-c_{1}^{2} c_{3}^{2}-2 c_{0} c_{2} c_{3}^{2}+2 c_{0} c_{2}^{2}+2 c_{0} c_{1} c_{3}-c_{0}^{2}\right) a_{3}^{5} \tag{5.20}
\end{equation*}
$$

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 $U=a_{0} U_{1}+U_{0}, V=a_{0} V_{1}+V_{0}$. Then $U_{1}$ satisfies:

$$
\begin{align*}
U_{1}= & -a_{1}^{2} a_{3}^{2}+2 a_{1} a_{2}^{2} a_{3}-2 c_{3} a_{1} a_{2} a_{3}^{2}+2 c_{2} a_{1} a_{3}^{3}-c_{3} a_{2}^{3} a_{3}+ \\
& \left(2 c_{3}^{2}-c_{2}\right) a_{2}^{2} a_{3}^{2}+\left(-c_{3}^{3}+c_{1}\right) a_{2} a_{3}^{3}+\left(c_{2} c_{3}^{2}-c_{2}^{2}-c_{1} c_{3}+c_{0}\right) a_{3}^{4} \\
= & a_{3}\left(-a_{1}^{2} a_{3}+2 a_{1} a_{2}^{2}-2 c_{3} a_{1} a_{2} a_{3}+2 c_{2} a_{1} a_{3}^{2}-c_{3} a_{2}^{3}+\right. \\
& \left.\left(2 c_{3}^{2}-c_{2}\right) a_{2}^{2} a_{3}+\left(-c_{3}^{3}+c_{1}\right) a_{2} a_{3}^{2}+\left(c_{2} c_{3}^{2}-c_{2}^{2}-c_{1} c_{3}+c_{0}\right) a_{3}^{3}\right) . \tag{5.21}
\end{align*}
$$

We observe that

$$
\begin{equation*}
a_{2} U_{1}+a_{3} V_{1}=0 \tag{5.22}
\end{equation*}
$$

### 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

$$
R\left(a_{1}, a_{2}, a_{3}\right)=t_{P} \prod_{1 \leq i<j \leq 4}\left(a\left(r_{i}\right)-a\left(r_{j}\right)\right)^{2} .
$$

Furthermore, the resultant $R_{0}$ is divisible by

$$
\prod_{1 \leq i<j \leq 4}\left(a\left(r_{i}\right)-a\left(r_{j}\right)\right) .
$$

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

$$
t_{P}=\prod_{1 \leq i<j \leq 4} \frac{1}{\left(r_{i}-r_{j}\right)^{2}}
$$

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 $g_{a}: \overline{\mathbb{Q}}[X] / P(X) \rightarrow$ $\overline{\mathbb{Q}}[X] / P(X)$ 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 $L_{1}(X), \ldots, L_{4}(X)$ be the Lagrange interpolation polynomials for the roots $r_{1}, \ldots, r_{4}$ of $P$. Thus $L_{i}(x)=\prod_{j \neq i}\left(x-r_{j}\right) /\left(r_{i}-r_{j}\right)$ and in particular $L_{i}\left(r_{j}\right)=1$ if $i=j, 0$ if $i \neq j$. Then for all $i=1,2,3,4$,

$$
g_{a}\left(L_{i}(X)\right)=a(X) L_{i}(X)=\sum_{j=1}^{4} a\left(r_{j}\right) L_{j}(X) L_{i}(X)=a\left(r_{i}\right) L_{i}(X),
$$

in $\overline{\mathbb{Q}}[X] /(P)$, since $P(X) \mid L_{i}(X) L_{j}(X)$ if $i \neq j$ and $P(X) \mid\left(L_{i}^{2}(X)-L_{i}(X)\right)$. Thus the matrix of $g_{a}$ with respect to the basis $\left\{L_{1}(X), L_{2}(X), L_{3}(X), L_{4}(X)\right\}$ is diagonal with coefficients $a\left(r_{1}\right), a\left(r_{2}\right), a\left(r_{3}\right), a\left(r_{4}\right)$ 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 $\left\{1, X, X^{2}, X^{3}\right\}$. Then the matrix of $N_{P}(\alpha) g_{a}^{-1}$ with respect to the standard basis is $N_{P}(\alpha) M_{\alpha}^{-1}$ with $M_{\alpha}^{-1}$ given by 5.4. Thus have

$$
\left(\begin{array}{llll}
B_{11} & B_{21} & B_{31} & B_{41}  \tag{5.23}\\
B_{12} & B_{22} & B_{32} & B_{42} \\
B_{13} & B_{23} & B_{33} & B_{34} \\
B_{14} & B_{24} & B_{34} & B_{44}
\end{array}\right)=T\left(\begin{array}{cccc}
\prod_{j \neq 1} a\left(r_{j}\right) & 0 & 0 & 0 \\
0 & \prod_{j \neq 2} a\left(r_{j}\right) & 0 & 0 \\
0 & 0 & \prod_{j \neq 3} a\left(r_{j}\right) & 0 \\
0 & 0 & 0 & \prod_{j \neq 4} a\left(r_{j}\right)
\end{array}\right) T^{-1}
$$

The form $N_{P}(\alpha)=\prod_{i=1}^{4} a\left(r_{i}\right)$ is quartic and monic in $a_{0}$. If we write $B_{14}=B_{14}\left(a_{0}\right)$ as an element of $\mathbb{Z}\left[a_{1}, a_{2}, a_{3}\right]\left[a_{0}\right]$, the resultant $R$ satisfies

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

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 $y \mapsto$ $N_{P}\left(y+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right)$. 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

$$
\left(\begin{array}{llll}
B_{11}\left(d_{1}\right) & B_{21}\left(d_{1}\right) & B_{31}\left(d_{1}\right) & B_{41}\left(d_{1}\right) \\
B_{12}\left(d_{1}\right) & B_{22}\left(d_{1}\right) & B_{32}\left(d_{1}\right) & B_{42}\left(d_{1}\right) \\
B_{13}\left(d_{1}\right) & B_{23}\left(d_{1}\right) & B_{33}\left(d_{1}\right) & B_{34}\left(d_{1}\right) \\
B_{14}\left(d_{1}\right) & B_{24}\left(d_{1}\right) & B_{34}\left(d_{1}\right) & B_{44}\left(d_{1}\right)
\end{array}\right)=T\left(\begin{array}{cccc}
\prod_{\ell \neq 1} P_{1}\left(r_{\ell}\right) & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{array}\right) T^{-1} .
$$

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

$$
\left(\begin{array}{l}
B_{11}\left(d_{1}\right) \\
B_{12}\left(d_{1}\right) \\
B_{13}\left(d_{1}\right) \\
B_{14}\left(d_{1}\right)
\end{array}\right)=T\left(\begin{array}{cccc}
\prod_{\ell \neq 1} P_{1}\left(r_{\ell}\right) & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{array}\right)\left(\begin{array}{l}
1 \\
1 \\
1 \\
1
\end{array}\right)=T\left(\begin{array}{c}
\prod_{j=2}^{4} P_{1}\left(r_{j}\right) \\
0 \\
0 \\
0
\end{array}\right) .
$$

In particular we deduce that $B_{14}\left(d_{1}\right)$ is the coefficient of $X^{3}$ in the polynomial $\prod_{j=2}^{4} P_{1}\left(r_{j}\right) L_{1}(X)$. Since $L_{1}(X)=\prod_{j=2}^{4}\left(X-r_{j}\right) /\left(r_{1}-r_{j}\right)$, we get

$$
B_{14}\left(d_{1}\right)=\frac{\prod_{j=2}^{4} P_{1}\left(r_{j}\right)}{\prod_{j=2}^{4}\left(r_{1}-r_{j}\right)}=-\prod_{i=2}^{4} \frac{a\left(r_{j}\right)-a\left(r_{1}\right)}{r_{j}-r_{1}}
$$

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

$$
B_{14}\left(d_{i}\right)=\frac{\prod_{j \neq i} P_{i}\left(r_{j}\right)}{\prod_{j \neq i}^{4}\left(r_{i}-r_{j}\right)}=-\prod_{j \neq i} \frac{a\left(r_{j}\right)-a\left(r_{i}\right)}{r_{j}-r_{i}}
$$

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 $B_{1 n}$, then $t_{P}^{-1}=(-1)^{n} \prod_{1 \leq i<j \leq n}\left(r_{i}-r_{j}\right)^{2}$. 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 $X^{\ell}$ in the Lagrange interpolation polynomials associated with the roots $r_{1}, \ldots, r_{n}$ of $P(X)$.
Lemma 5.8. The polynomial $q\left(a_{1}, a_{2}, a_{3}\right) \in \mathbb{Q}\left[a_{1}, a_{2}, a_{3}\right]$ satisfies

$$
q= \pm \prod_{1 \leq i<j \leq 4} \frac{a\left(r_{i}\right)-a\left(r_{j}\right)}{r_{i}-r_{j}}
$$

where $a(r):=a_{0}+a_{1} r+a_{2} r^{2}+a_{3} r^{3}$.
Proof. This follows immediately from putting together Lemmas 5.65 .5 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

$$
\begin{aligned}
R_{3}(X) & =\left(X-\left(r_{1} r_{2}+r_{3} r_{4}\right)\right)\left(X-\left(r_{1} r_{3}+r_{2} r_{4}\right)\right)\left(X-\left(r_{1} r_{4}+r_{2} r_{3}\right)\right) \\
& =X^{3}-c_{2} X^{2}+\left(c_{3} c_{1}-4 c_{0}\right) X-\left(c_{3}^{2} c_{0}+c_{1}^{2}-4 c_{2} c_{0}\right),
\end{aligned}
$$

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 $q \in \mathbb{Q}\left[a_{1}, a_{2}, a_{3}\right]$ has the factorisation

$$
q= \pm q_{1} q_{2}
$$

where $q_{1} \in \mathbb{Q}\left[a_{1}, a_{2}, a_{3}\right]$ has degree 4 and $q_{2} \in \mathbb{Q}\left[a_{1}, a_{2}, a_{3}\right]$ has degree 2. These are explicitly given by

$$
\begin{equation*}
q_{1}=\frac{\left(a\left(r_{1}\right)-a\left(r_{3}\right)\right)\left(a\left(r_{1}\right)-a\left(r_{4}\right)\right)\left(a\left(r_{2}\right)-a\left(r_{3}\right)\right)\left(a\left(r_{2}\right)-a\left(r_{4}\right)\right)}{\left(r_{1}-r_{3}\right)\left(r_{1}-r_{4}\right)\left(r_{2}-r_{3}\right)\left(r_{2}-r_{4}\right)}, \tag{5.24}
\end{equation*}
$$

and

$$
\begin{equation*}
q_{2}=\frac{\left(a\left(r_{1}\right)-a\left(r_{2}\right)\right)\left(a\left(r_{3}\right)-a\left(r_{4}\right)\right)}{\left(r_{1}-r_{2}\right)\left(r_{3}-r_{4}\right)}, \tag{5.25}
\end{equation*}
$$

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 $q_{1}, q_{2} \in \mathbb{Q}\left[a_{1}, a_{2}, a_{3}\right]$, so that this is also a factorisation over $\mathbb{Q}$. A direct computation gives for all $1 \leq i<j \leq 4$ :

$$
\begin{equation*}
\frac{a\left(r_{i}\right)-a\left(r_{j}\right)}{r_{i}-r_{j}}=a_{1}+a_{2}\left(r_{i}+r_{j}\right)+a_{3}\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}\right) . \tag{5.26}
\end{equation*}
$$

If $G=C_{4}$ then $G=\langle\sigma\rangle$ for some 4-cycle $\sigma$. Then we can label the roots such that $\sigma$ is the permutation $\sigma=\left(r_{1} r_{3} r_{2} r_{4}\right)$. With this choice of root ordering, we have $\sigma\left(r_{1} r_{2}+r_{3} r_{4}\right)=r_{1} r_{2}+r_{3} r_{4}$. Since $\sigma\left(q_{1}\right)=q_{1}$ and $\sigma\left(q_{2}\right)=q_{2}$, we have that $r_{1} r_{2}+r_{3} r_{4}, q_{1}$ and $q_{2}$ are fixed by all of $G=\left\{I d, \sigma, \sigma^{2}, \sigma^{3}\right\}$, and so $r_{1} r_{2}+r_{3} r_{4} \in \mathbb{Q}$ and $q_{1}, q_{2} \in \mathbb{Q}\left[a_{1}, a_{2}, a_{3}\right]$, giving the result in this case.

If $G=D_{4}$, then $G=\langle\sigma, \tau\rangle$ where $\tau$ is a transposition and $\sigma$ a 4cycle. We can label the roots such that $\tau=\left(r_{3} r_{4}\right)$. This implies that $\sigma\left(r_{3}\right) \neq r_{4}$, since otherwise we could suppose that $\sigma=\left(r_{3} r_{4} r_{1} r_{2}\right)$ and $G$ would contains the following subset of 9 permutations :

$$
\begin{gathered}
\left\{I d, \tau, \sigma, \sigma^{2}, \sigma^{3}, \sigma \tau,(\sigma \tau)^{2}, \tau \sigma,(\tau \sigma)^{2}\right\}=\left\{I d,\left(r_{3} r_{4}\right),\left(r_{1} r_{2} r_{3} r_{4}\right),\left(r_{1} r_{3}\right)\left(r_{2} r_{4}\right),\right. \\
\left.\left(r_{1} r_{4} r_{3} r_{2}\right),\left(r_{1} r_{2} r_{3}\right),\left(r_{1} r_{3} r_{2}\right),\left(r_{1} r_{2} r_{4}\right),\left(r_{1} r_{4} r_{2}\right)\right\},
\end{gathered}
$$

which is not possible since $|G|=8$. We prove in the same way that $\sigma\left(r_{4}\right) \neq r_{3}$. We can thus label the roots of $P$ so that $\sigma\left(r_{3}\right)=r_{2}$. This implies that $\sigma\left(r_{4}\right)=r_{1}, \sigma\left(r_{2}\right)=r_{4}$ and $\sigma\left(r_{1}\right)=r_{3}$, that is $\sigma=\left(r_{1} r_{3} r_{2} r_{4}\right)$. Again we observe that $r_{1} r_{2}+r_{3} r_{4} \in \mathbb{Q}$ since it is fixed by $\sigma$ and $\tau$.

Since $\tau\left(q_{1}\right)=q_{1}=\sigma\left(q_{1}\right)$ and $\tau\left(q_{2}\right)=q_{2}=\sigma\left(q_{2}\right)$ we also observe that $q_{1}, q_{2} \in \mathbb{Q}\left[a_{1}, a_{2}, a_{3}\right]$ 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 $K:=\mathbb{Q}\left(r_{1}+r_{3}\right)$. Then the form $q_{1}$ defined in (5.24) satisfies

$$
q_{1}\left(a_{1}, a_{2}, a_{3}\right)= \pm N_{K / \mathbb{Q}}\left(a_{1}+a_{2}\left(r_{1}+r_{3}\right)+a_{3}\left(r_{1}^{2}+r_{1} r_{3}+r_{3}^{2}\right)\right) .
$$

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 $\sigma=\left(r_{1} r_{3} r_{2} r_{4}\right)$ and $r_{1} r_{2}+r_{3} r_{4} \in \mathbb{Q}$. We see that
$q_{1}=\prod_{i=0}^{3} \sigma^{i}\left(\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}}\right)=N_{\mathbb{Q}\left(r_{1}\right) / \mathbb{Q}}\left(a_{1}+a_{2}\left(r_{1}+r_{3}\right)+a_{3}\left(r_{1}^{2}+r_{1} r_{3}+r_{3}^{2}\right)\right)$.
To finish the proof, it remains to prove that $\mathbb{Q}\left(r_{1}+r_{3}\right)=\mathbb{Q}\left(r_{1}\right)$ 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 $\sigma^{2}$. But $c_{3}=-\left(r_{1}+r_{2}+\right.$ $\left.r_{3}+r_{4}\right)=-\left(r_{1}+r_{3}\right)-\sigma^{2}\left(r_{1}+r_{3}\right)$ so if $\mathbb{Q}\left(r_{1}+r_{3}\right)$ is fixed by $\sigma^{2}$ then $\mathbb{Q}\left(r_{1}+r_{3}\right)=\mathbb{Q}$. But in this case $r_{1}+r_{3}=\sigma\left(r_{1}+r_{3}\right)=r_{3}+r_{2}$, so the roots would not be distinct, which contradicts our assumption. Thus $\mathbb{Q}\left(r_{1}+r_{3}\right)=\mathbb{Q}\left(r_{1}\right)$ as desired.

Case 2: $G=D_{4}$. Let $G=\langle\sigma, \tau\rangle$ with $\sigma$ as above and $\tau=\left(r_{3} r_{4}\right)$. We work with the permutation $\sigma \tau=\left(r_{1} r_{3}\right)\left(r_{2} r_{4}\right)$. 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 $\left[K_{0}: \mathbb{Q}\right]=4$. We observe that $r_{1}+r_{3}, \frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}} \in K_{0}$.

Now, by looking the orbit of $\{1,3\}$ under the subgroup of $S_{4}^{3}$ generated by $\{(1324),(34)\}$, we see that

$$
N_{L / \mathbb{Q}}\left(\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}}\right)=q_{1}^{2}
$$

and

$$
N_{L / K_{0}}\left(\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}}\right)=\left(\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}}\right)^{2},
$$

since $\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}} \in K_{0}$. By the transitive property of the norms,
$N_{L / \mathbb{Q}}\left(\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}}\right)=N_{K_{0} / \mathbb{Q}}\left(N_{L / K_{0}}\left(\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}}\right)\right)=N_{K_{0} / \mathbb{Q}}\left(\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}}\right)^{2}$.
We deduce that $q_{1}= \pm N_{K_{0} / \mathbb{Q}}\left(\frac{a\left(r_{1}\right)-a\left(r_{3}\right)}{r_{1}-r_{3}}\right)$.
As in the case (i), to finish the proof it remains to check that $\mathbb{Q}\left(r_{1}+\right.$ $\left.r_{3}\right)=K_{0}$. We have already seen that $\mathbb{Q}\left(r_{1}+r_{3}\right) \subset K_{0}$, and so it suffices to show $\left[\mathbb{Q}\left(r_{1}+r_{3}\right): \mathbb{Q}\right]=4$. 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 $\sigma^{2}=\left(r_{1} r_{2}\right)\left(r_{3} r_{4}\right)$.

We will apply Theorem 4.1 with $K=\mathbb{Q}\left(r_{1}+r_{3}\right)$ and $\nu_{1}=1, \nu_{2}=$ $r_{1}+r_{3}, \nu_{3}=r_{1}^{2}+r_{3}^{2}+r_{1} r_{3}$. In the next lemma, we verify that these 3 vectors $\nu_{1}, \nu_{2}, \nu_{3}$ 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, $1, r_{1}+r_{3}, r_{1}^{2}+r_{3}^{2}+r_{1} r_{3}$ 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 $r_{1}^{2}+r_{3}^{2}+r_{1} r_{3}=u+v\left(r_{1}+r_{3}\right)$. If we apply $\sigma^{2}=\left(r_{1} r_{2}\right)\left(r_{3} r_{3}\right)$ to this expression, we find $r_{2}^{2}+r_{4}^{2}+r_{2} r_{4}=u+v\left(r_{2}+r_{4}\right)$. Summing this two equations gives

$$
\sum_{i=1}^{4} r_{i}^{2}+r_{1} r_{3}+r_{2} r_{4}=2 u+v\left(r_{1}+r_{2}+r_{3}+r_{4}\right)
$$

This contradicts the fact that $r_{1} r_{3}+r_{2} r_{4} \notin \mathbb{Q}\left(\right.$ since $\left.\sum_{i} r_{i}, \sum_{i} r_{i}^{2} \in \mathbb{Q}\right)$.

### 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 44 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 $\delta_{P}$ be the discriminant of the splitting field of $P$.

Lemma 5.13. Suppose that $\left(p, a_{3} \delta_{P} \operatorname{Disc} P\right)=1$ and $a_{2} \in \mathbb{Z}$. Let $Q_{p}\left(a_{2}, a_{3}\right)$ denote the number of integers $a_{1}$ with $0 \leq a_{1}<p$ such that

$$
\begin{equation*}
q_{1}\left(a_{1}, a_{2}, a_{3}\right) \equiv q_{2}\left(a_{1}, a_{2}, a_{3}\right) \equiv 0(\bmod p) . \tag{5.27}
\end{equation*}
$$

Then

$$
Q_{p}\left(a_{2}, a_{3}\right)= \begin{cases}1, & \text { if } P\left(\left(a_{2}-c_{3} a_{3}\right) \overline{a_{3}}\right) \equiv 0(\bmod p) \\ 0, & \text { otherwise }\end{cases}
$$

Proof. Let $L$ be the splitting field of $P$ and $\mathcal{O}_{L}$ its ring of integers. Since $\left(p, \delta_{P}\right)=1, p$ 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 $N_{L}\left(\mathfrak{P}_{i}\right)=p^{t}$ for some integers $s, t$ with $s t=[L: \mathbb{Q}]$. Formulas $5.24,55$, 5.25 give us the factorisation of the polynomials $q_{1}$ and $q_{2}$ over $\mathcal{O}_{L}$. The condition $q_{1}\left(a_{1}, a_{2}, a_{3}\right) \equiv$ $q_{2}\left(a_{1}, a_{2}, a_{3}\right) \equiv 0(\bmod p)$ is equivalent to one of the factors of $q_{1}$ and one of the factors of $q_{2}$ vanishing $\left(\bmod \mathfrak{P}_{m}\right)$ for each $1 \leq m \leq s$.

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

$$
\left\{\begin{aligned}
a_{1}+a_{2}\left(r_{i}+r_{j}\right)+a_{3}\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}\right) & \equiv 0\left(\bmod \mathfrak{P}_{m}\right), \\
a_{1}+a_{2}\left(r_{k}+r_{\ell}\right)+a_{3}\left(r_{k}^{2}+r_{k} r_{\ell}+r_{\ell}^{2}\right) & \equiv 0\left(\bmod \mathfrak{P}_{m}\right) .
\end{aligned}\right.
$$

Eliminating $a_{1}$, we find

$$
a_{2}\left(r_{i}+r_{j}-r_{k}-r_{\ell}\right) \equiv a_{3}\left(r_{k}^{2}+r_{k} r_{\ell}+r_{\ell}^{2}-r_{i}^{2}-r_{i} r_{j}-r_{j}^{2}\right)\left(\bmod \mathfrak{P}_{m}\right)
$$

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

$$
\left(r_{3}-r_{2}\right) a_{2} \equiv a_{3}\left(r_{2}-r_{3}\right)\left(r_{1}+r_{2}+r_{3}\right)\left(\bmod \mathfrak{P}_{m}\right)
$$

Since $p \nmid \operatorname{Disc}(P)$ and $\left(r_{3}-r_{2}\right) \mid \operatorname{Disc}(P)$, we see that $r_{3}-r_{2} \not \equiv 0\left(\bmod \mathfrak{P}_{m}\right)$, and so (recalling $c_{3}=-r_{1}-r_{2}-r_{3}-r_{4} \in \mathbb{Z}$ ) we have $a_{2} \equiv a_{3}\left(c_{3}+\right.$ $\left.r_{4}\right)\left(\bmod \mathfrak{P}_{m}\right)$. This implies that $r_{4} \equiv\left(a_{2}-a_{3} c_{3}\right) \overline{a_{3}}\left(\bmod \mathfrak{P}_{m}\right)$ and so

$$
P\left(\left(a_{2}-a_{3} c_{3}\right) \overline{a_{3}}\right) \equiv 0\left(\bmod \mathfrak{P}_{m}\right)
$$

Since this argument is valid for all $m$, we find that $P\left(\left(a_{2}-a_{3} c_{3}\right) \overline{a_{3}}\right) \equiv$ $0(\bmod p)$. Thus if $P\left(\left(a_{2}-c_{3} a_{3}\right) \overline{a_{3}}\right) \not \equiv 0(\bmod p)$ then $Q_{p}\left(a_{2}, a_{3}\right)=0$.

Now we suppose that $P\left(\left(a_{2}-c_{3} a_{3}\right) \overline{a_{3}}\right) \equiv 0(\bmod p)$. Then there exists $j \in\{1,2,3,4\}$ such that $r_{j} \equiv\left(a_{2}-a_{3} c_{3}\right) \overline{a_{3}}(\bmod p)$. We may suppose that $j=4$; the other cases are analogous. We see that this implies that $a_{2} \equiv a_{3}\left(-r_{1}-r_{2}-r_{3}\right)(\bmod p)$ and that $r_{4} \in \mathbb{Z}+p \mathcal{O}_{L}$. Moreover, we check that
$a_{2}\left(r_{1}+r_{3}\right)+a_{3}\left(r_{1}^{2}+r_{1} r_{3}+r_{3}^{2}\right)=a_{3}\left(-c_{2}-c_{3} r_{4}-r_{4}^{2}\right)(\bmod p)$,
$a_{2}\left(r_{1}+r_{2}\right)+a_{3}\left(r_{1}^{2}+r_{1} r_{2}+r_{2}^{2}\right)=a_{2}\left(r_{1}+r_{3}\right)+a_{3}\left(r_{1}^{2}+r_{1} r_{3}+r_{3}^{2}\right)(\bmod p)$.
Thus the system (5.27) admits the solution $a_{1}=-\left(a_{2}\left(r_{1}+r_{3}\right)+a_{3}\left(r_{1}^{2}+\right.\right.$ $\left.\left.r_{1} r_{3}+r_{3}^{2}\right)\right)(\bmod p)$, noting this is in $\mathbb{Z}+p \mathcal{O}_{L}$. Thus $Q_{p}\left(a_{2}, a_{3}\right) \geq 1$.

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

$$
\left\{\begin{array}{l}
a_{1}+a_{2}\left(r_{i}+r_{j}\right)+a_{3}\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}\right)=0\left(\bmod \mathfrak{P}_{m}\right), \\
a_{1}+a_{2}\left(r_{i}+r_{k}\right)+a_{3}\left(r_{i}^{2}+r_{i} r_{k}+r_{k}^{2}\right)=0\left(\bmod \mathfrak{P}_{m}\right),
\end{array}\right.
$$

then we must have $\left(a_{2}-c_{3} a_{3}\right) \overline{a_{3}}=r_{\ell}\left(\bmod \mathfrak{P}_{m}\right)$. 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 $a_{1} \equiv-a_{2}\left(r_{i}+r_{j}\right)-a_{3}\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}\right)(\bmod p)$ (noting that these are the same for all choices of $\{i, j, k\}=\{1,2,3\}$ ). Thus $Q_{p}\left(a_{2}, a_{3}\right)=1$ when $P\left(\left(a_{2}-c_{3} a_{3}\right) \overline{a_{3}}\right) \equiv 0(\bmod p)$.

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 $B_{14} \equiv 0(\bmod p)$ or $B_{13} \equiv 0(\bmod p)$. 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 $\Delta_{14} \in \mathbb{Z}\left[a_{1}, a_{2}, a_{3}\right]$ be the discriminant of $B_{14}$ viewed as a polynomial in $a_{0}$. Then

$$
\begin{equation*}
\Delta_{14}=-q_{3} h, \tag{5.28}
\end{equation*}
$$

where $h$ is given by

$$
\begin{aligned}
h\left(a_{1}, a_{2}, a_{3}\right)= & -4 a_{1}^{2}+4 c_{3} a_{1} a_{2}+\left(-3 c_{3}^{2}+4 c_{2}\right) a_{1} a_{3}-c_{3} a_{2}^{2}+\left(c_{3}^{3}-4 c_{1}\right) a_{2} a_{3} \\
& \quad+\left(-c_{2} c_{3}^{2}+4 c_{1} c_{3}-4 c_{0}\right) a_{3}^{2} \\
= & \left(r_{1}+r_{2}-r_{3}-r_{4}\right)^{2} q_{3}\left(a_{1}, a_{2}, a_{3}\right)-q_{2}\left(a_{1}, a_{2}, a_{3}\right)
\end{aligned}
$$

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 $t_{2}:=\left(r_{1}+r_{2}\right)\left(r_{3}+r_{4}\right)$. 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 $\left(r_{3} r_{4}\right)$, so $t_{2} \in \mathbb{Q}$. Let $R(X)$ be a cubic resolvent associated to $P$, given by (see 3])

$$
\begin{aligned}
R(X):= & \left(X-\left(r_{1}+r_{2}\right)\left(r_{3}+r_{4}\right)\right)\left(X-\left(r_{1}+r_{3}\right)\left(r_{2}+r_{4}\right)\right)\left(X-\left(r_{1}+r_{4}\right)\left(r_{2}+r_{3}\right)\right) \\
& =X^{3}-2 c_{2} X^{2}+\left(c_{2}^{2}+c_{3} c_{1}-4 c_{0}\right) X+\left(c_{3}^{2} c_{0}+c_{1}^{2}-c_{3} c_{2} c_{1}\right) .
\end{aligned}
$$

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 $\left(r_{1}+r_{2}\right)\left(r_{3}+r_{4}\right)=0$, then we have in fact $r_{1}+r_{2}=r_{3}+r_{4}=0$ since $\sigma\left(r_{1}+r_{2}\right)=r_{3}+r_{4}$. 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 $r_{1}-r_{2}= \pm\left(r_{3}-r_{4}\right)$. If we compose with the embedding $\tau=\left(r_{3} r_{4}\right)$, 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 $\left(q\left(a_{1}, a_{2}, a_{3}\right), q_{3}\left(a_{1}, a_{2}, a_{3}\right)\right)=$ 1 and $q\left(a_{1}, a_{2}, a_{3}\right)$ is squarefree. Let $t_{2}=\left(r_{1}+r_{2}\right)\left(r_{3}+r_{4}\right) \in \mathbb{Z}$. Let $p$ be a prime with $p \mid q\left(a_{1}, a_{2}, a_{3}\right)$ and $p \nmid a_{2} a_{3} \delta_{P} \operatorname{Disc} P$.
(i). If $p \mid q_{1}\left(a_{1}, a_{2}, a_{3}\right)$ or $p \nmid c_{3}^{2}-4 t_{2}$, then

$$
\left|\left\{0 \leq a_{0}<p: B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \equiv 0(\bmod p)\right\}\right|=2 .
$$

(ii). If $p \mid q_{2}\left(a_{1}, a_{2}, a_{3}\right)$ and $p \mid c_{3}^{2}-4 t_{2}$ then

$$
\left|\left\{0 \leq a_{0}<p: B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \equiv 0(\bmod p)\right\}\right|=1 .
$$

(iii). We have

$$
\left.\mid\left\{0 \leq a_{0}<p: B_{13}\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \equiv B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \equiv 0(\bmod p)\right)\right\} \mid=1
$$

Proof. We recall from 5.11) and 5.12 that $q \mid R_{0}$, the resultant of $B_{13}$ and $B_{14}$ viewed as polynomials in $a_{0}$. Therefore since $p \mid q\left(a_{1}, a_{2}, a_{3}\right)$, we have that $p \mid R_{0}\left(a_{1}, a_{2}, a_{3}\right)$, 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 $R_{0}\left(a_{1}, a_{2}, a_{3}\right)=q\left(a_{1}, a_{2}, a_{3}\right) q_{3}\left(a_{1}, a_{2}, a_{3}\right) \equiv$ $0\left(\bmod p^{2}\right)$. But this is impossible since we assume that $q\left(a_{1}, a_{2}, a_{3}\right)$ is squarefree and coprime to $q_{3}\left(a_{1}, a_{2}, a_{3}\right)$ with $p \mid q\left(a_{1}, a_{2}, a_{3}\right)$. 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 $B_{14} \equiv 0(\bmod p)$ is 1 when $p \mid \Delta_{14}$ and 2 otherwise.

If $p \mid q_{2}$, by Lemma $5.14 p \mid \Delta_{14}$ if and only if $p \mid\left(r_{1}+r_{2}-r_{3}-r_{4}\right)^{2}$. This gives the assertion (i) and (ii) in the case $p \mid q_{2}$ because $\left(r_{1}+r_{2}-r_{3}-r_{4}\right)^{2}=$ $c_{3}^{2}-4 t_{2}$.

We now consider the case $p \mid q_{1}$. 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 $a_{1} \equiv-a_{2}\left(r_{i}+r_{j}\right)-a_{3}\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}\right)\left(\bmod \mathfrak{P}_{m}\right)$. We may suppose that $i=1$ and $j=3$, the other cases being similar. Substituting $-a_{2}\left(r_{1}+\right.$ $\left.r_{3}\right)-a_{3}\left(r_{1}^{2}+r_{1} r_{3}+r_{3}^{2}\right)$ for $a_{1}$ in the expression for $h$ in Lemma 5.14 gives

$$
\begin{gather*}
h\left(a_{1}, a_{2}, a_{3}\right) \equiv-\left(a_{3}\left(r_{1}+r_{2}+r_{3}\right)+a_{2}\right)\left(a_{3}\left(r_{1}+r_{3}+r_{4}\right)+a_{2}\right) \\
\times\left(r_{1}-r_{2}+r_{3}-r_{4}\right)^{2}\left(\bmod \mathfrak{P}_{m}\right) . \tag{5.29}
\end{gather*}
$$

We have that $a_{3}\left(r_{1}+r_{2}+r_{3}\right)+a_{2} \not \equiv 0\left(\bmod \mathfrak{P}_{m}\right)$. If this were not the case we would have $a_{3}\left(-c_{3}-r_{4}\right)+a_{2} \equiv 0\left(\bmod \mathfrak{P}_{m}\right)$, and then
$P\left(\left(a_{2}-a_{3} c_{3}\right) \overline{a_{3}}\right)=0(\bmod p)$. By Lemma 5.13 we would have $p \mid\left(q_{1}, q_{2}\right)$ which is not possible when $q$ is squarefree. Similarly $a_{3}\left(r_{1}+r_{3}+r_{4}\right)+a_{2} \not \equiv$ $0\left(\bmod \mathfrak{P}_{m}\right)$.

Thus $\Delta_{14} \equiv 0\left(\bmod \mathfrak{P}_{m}\right)$ if and only if $r_{1}-r_{2}+r_{3}-r_{4} \equiv 0\left(\bmod \mathfrak{P}_{m}\right)$ for all $m$. But this is equivalent to $r_{1}-r_{2}+r_{3}-r_{4} \equiv 0(\bmod p)$, and so $\gamma\left(r_{1}-r_{2}+r_{3}-r_{3}\right) \equiv 0(\bmod p)$ for all embeddings $\gamma$. Applying this with $\gamma=\iota, \tau$ we see that $p \mid \Delta_{14}$ if and only if $r_{1} \equiv r_{2}(\bmod p)$, which is impossible since $p \nmid \operatorname{Disc}(P)$. Thus when $p \mid q_{1}$ we have $p \nmid \Delta_{14}$, and so $B_{14}$ has two roots $(\bmod p)$.

Lemma 5.17. Let $a_{0}, a_{1}, a_{2}, a_{3}, p \in \mathbb{Z}$ be such that $\left(q\left(a_{1}, a_{2}, a_{3}\right), q_{3}\left(a_{1}, a_{2}, a_{3}\right)\right)=$ $1, q\left(a_{1}, a_{2}, a_{3}\right)$ is squarefree and $p \mid\left(q\left(a_{1}, a_{2}, a_{3}\right), B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right)$. Then we have

$$
p\left|N_{P}(\alpha) \Leftrightarrow p\right| B_{13}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)
$$

where $\alpha=a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}$.
Proof. This is a variant of [4, Lemma 13.3] (or [1, Section 6.1]). By (5.6) and 5.8, we have

$$
\left(B_{13}-c_{3} B_{14}\right) B_{13}-B_{14}\left(B_{12}-c_{2} B_{14}\right)=q_{3} N_{P}(\alpha) .
$$

The Lemma follows from this formula since $\left(p, q_{3}\left(a_{1}, a_{2}, a_{3}\right)\right)=1$.

## 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 $\alpha=a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3} \in \mathcal{D}_{P}$, then $\max \left(\left|a_{0}\right|,\left|a_{1}\right|,\left|a_{2}\right|,\left|a_{3}\right|\right) \ll N_{P}(\alpha)^{1 / 4}$ and so $|\sigma(\alpha)| \ll N_{P}(\alpha)^{1 / 4}$ for all embeddings $\sigma$. We recall that the forms $q_{1}\left(a_{1}, a_{2}, a_{3}\right)$ and $q_{2}\left(a_{1}, a_{2}, a_{3}\right)$ are defined by (5.24) and (5.25), the polynomials $P_{1}(X):=\left(X-\left(r_{1}+\right.\right.$ $\left.\left.r_{2}\right)\right)\left(X-\left(r_{3}+r_{4}\right)\right)$ and $P_{2}(X):=\left(X-\left(r_{1}^{2}+r_{1} r_{2}+r_{2}^{2}\right)\right)\left(X-\left(r_{3}^{2}+r_{3} r_{4}+r_{4}^{2}\right)\right)$ with discriminants $\Delta_{1}$ and $\Delta_{2}$ respectively, $D_{q_{2}}$ from 4.13, and $\delta_{P}$ is the discriminant of the splitting field of $P$. With this notation we introduce a constant $q_{0}$ depending only on the polynomial $P$

$$
\begin{equation*}
q_{0}=512\left(1+c_{3}^{2}+\left|c_{2}\right|+\left|t_{1}\right|+\left|t_{2}\right|\right) \delta_{P} \text { Disc } P \tag{6.1}
\end{equation*}
$$

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

$$
\alpha_{0}, \theta_{11}, \ldots, \theta_{16}, \theta_{21}, \tau_{11}, \ldots, \tau_{16}, \tau_{21} \in(0,1)
$$

These constants will be required to satisfy various inequalities, specifically

$$
\begin{gather*}
{\left[\theta_{i j}, \theta_{i j}+\tau_{i j}\right] \cap\left[\theta_{i^{\prime} j^{\prime}}, \theta_{i^{\prime} j^{\prime}}+\tau_{i^{\prime} j^{\prime}}\right]=\emptyset \quad \text { for }(i, j) \neq\left(i^{\prime}, j^{\prime}\right),}  \tag{6.2}\\
0<\theta_{1 j}<\theta_{1 j}+\tau_{1 j}<7 / 32 \text { for all } 1 \leq j \leq 6,  \tag{6.3}\\
\alpha_{0}<\frac{1}{2^{15}},  \tag{6.4}\\
\sum_{j=1}^{6}\left(\theta_{1 j}+\tau_{1 j}\right)<1+\alpha_{0} / 2,  \tag{6.5}\\
\theta_{11}, \theta_{12}, \theta_{13}, \theta_{14}, \theta_{15}, \theta_{16}, \theta_{21}>1+\alpha_{0}-\sum_{j=1}^{6} \theta_{1 j},  \tag{6.6}\\
\frac{1+\alpha_{0}}{4}<\theta_{11}+\theta_{12}+\theta_{13}<\frac{2+\alpha_{0}}{4}-\tau_{11}-\tau_{12}-\tau_{13},  \tag{6.7}\\
\theta_{21}+\tau_{21}<\frac{2+\alpha_{0}}{200}-\frac{\sum_{i=1}^{3}\left(\theta_{1 i}+\tau_{1 i}\right)}{50},  \tag{6.8}\\
\theta_{21}+\tau_{21}<\left(\frac{4\left(\theta_{11}+\theta_{12}+\theta_{13}\right)}{1+\alpha_{0}}-1\right) \frac{2+\alpha_{0}}{800} . \tag{6.9}
\end{gather*}
$$

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:
$\alpha_{0}=0.00001, \quad \theta_{11}=0.1398, \quad \theta_{12}=0.1401, \quad \theta_{13}=0.1402$,
$\theta_{14}=0.21, \quad \theta_{15}=0.19, \quad \theta_{16}=0.1799, \quad \theta_{21}=0.001$, $\tau_{i j}=0.0000001$ 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 $(\alpha)$ of $\mathcal{O}_{\mathbb{Q}\left(r_{1}\right)}$ with generator $\alpha=a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}$ where $\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathbb{Z}^{4} \cap \mathcal{D}_{P}$, satisfying the conditions (C1), (C2), (C3), (C4) and (C5) below.
(C1) $q\left(a_{1}, a_{2}, a_{3}\right)$ is squarefree.
(C2) Size conditions: We have

$$
\begin{aligned}
q\left(a_{1}, a_{2}, a_{3}\right) & \geq X^{3 / 2} \\
\left|B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right| & \geq X^{3 / 4} \\
N_{P}(\alpha) & \in\left[X^{1+\alpha_{0} / 2}, X^{1+\alpha_{0}}\right] .
\end{aligned}
$$

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

$$
\begin{equation*}
X^{4 \alpha_{0}}<N_{P}(K) \leq X^{5 \alpha_{0}} \tag{6.10}
\end{equation*}
$$

(C4) Factorisations conditions of auxiliary polynomials: The values of the forms $q_{1}\left(a_{1}, a_{2}, a_{3}\right)$ and $q_{2}\left(a_{1}, a_{2}, a_{3}\right)$ evaluated at $a_{1}, a_{2}, a_{3}$ can be factored as:

$$
\begin{align*}
& q_{1}\left(a_{1}, a_{2}, a_{3}\right)=\prod_{j=1}^{7} q_{1 j}  \tag{6.11}\\
& q_{2}\left(a_{1}, a_{2}, a_{3}\right)=q_{21} q_{22} \text { with } q_{21} \equiv 1\left(\bmod D_{q_{2}}\right)
\end{align*}
$$

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

$$
q_{i j} \in\left[X^{\theta_{i j}}, X^{\theta_{i j}+\tau_{i j}}\right]
$$

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

$$
P^{-}\left(q_{22}\right), P^{-}\left(q_{17}\right)>q_{0}
$$

where $q_{0}$ is given by 6.1.
(C5) Coprimality conditions:
(a) $\left(a_{2}, a_{3}\right)=30$ and $a_{2}, a_{3} \equiv 30(\bmod 900), a_{1} \equiv 1(\bmod 30)$.
(b) $\left(N_{P}(\alpha), q_{0}\right)=1$.
(c) $\left(q\left(a_{1}, a_{2}, a_{3}\right), q_{3}\left(a_{1}, a_{2}, a_{3}\right)\right)=1$.
(d) $\left(q\left(a_{1}, a_{2}, a_{3}\right), B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right)=1$.
(e) $\left(q\left(a_{1}, a_{2}, a_{3}\right), a_{2} a_{3}\right)=1$.

With this definition of $\mathcal{J}$, we can verify the property 3.2 if $\delta_{0}$ is chosen small enough.
Lemma 6.1. We have that for all $\mathfrak{J} \in \mathcal{J}$

$$
\prod_{\substack{\mathfrak{p} \boldsymbol{e} \| \mathcal{I} \\ N_{P}(\mathfrak{p}) \leq X}} N_{P}(\mathfrak{p}) \geq X^{1+\alpha_{0} / 2}
$$

Proof. This is a consequence of (C2) which forces $N_{P}(\alpha) \geq X^{1+\alpha_{0} / 2}$ and (C3), which forces all ideal factors of $(\alpha)$ to have norm at most $\max \left(X^{5 \alpha_{0}}, X^{1-3 \alpha_{0}}\right)<X$. (We note that 6.4 implies that $19 \alpha_{0}<1$ ).

The next Lemma says that the congruence $n \equiv r_{1}(\bmod \mathfrak{J})$ can be solved when $\mathfrak{J} \in \mathcal{J}$. We recall that $\varrho_{P}$ 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 $\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathbb{Z}^{4} \cap \mathcal{D}_{P}$ satisfying (C1),(C2),(C3),(C4),(C5) and such that $\mathfrak{J}=(\alpha)$. By Lemma 5.5 and $(\mathrm{C} 5)(\mathrm{d}),\left(N_{P}(\mathfrak{J}), B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right)=1$. 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 $P^{-}\left(N_{P}(\mathfrak{J})\right)>X^{\theta_{0}}$. This condition implies (C5)(b).

We see from condition $(C 2)$ that if $\mathfrak{a} \in \mathcal{J}$ then $\mathfrak{a}=\left(a_{0}+a_{1} \nu_{1}+a_{2} \nu_{2}+\right.$ $\left.a_{3} \nu_{3}\right)$ for some $\mathbf{a} \in \mathbb{Z}^{4}$ which lies in the region

$$
\begin{array}{r}
\mathcal{R}:=\left\{\mathbf{a} \in \mathbb{R}^{4} \cap \mathcal{D}_{P}: 7 X^{1+\alpha_{0} / 2}<\tilde{N}\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \leq X^{1+\alpha_{0}}\right. \\
\left.\left|B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right| \geq X^{3 / 4},\left|q\left(a_{1}, a_{2}, a_{3}\right)\right| \geq X^{3 / 2}\right\} . \tag{6.12}
\end{array}
$$

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

$$
\begin{equation*}
\widetilde{N}\left(a_{1}, a_{2}, a_{3}, a_{4}\right):=\prod_{i=1}^{4}\left(\sum_{j=1}^{4} a_{j} \sigma_{i}\left(\nu_{j}\right)\right) . \tag{6.13}
\end{equation*}
$$

By our choice of $\mathcal{D}_{P}$ we see that if $\mathbf{a} \in \mathcal{R}$ then $\left|a_{i}\right| \ll X^{\left(1+\alpha_{0}\right) / 4}$ for all $i \in\{1,2,3,4\}$. For notational convenience we set $I_{\mathcal{C}}$ to be the set

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

so that condition $(C 4)$ forces $q_{i j} \in\left[X^{\theta_{i j}}, X^{\theta_{i j}+\tau_{i j}}\right]$ 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

$$
\alpha_{0}<\eta_{0}<1-\frac{9}{4} \alpha_{0}, \quad 12 \theta_{0}+19 \alpha_{0}<1 .
$$

Then for $X \geq 2, H=X^{\eta_{0}}$ we have

$$
\begin{equation*}
S_{1} \ll(\log H) \sum_{K \in \mathcal{K}} \sum_{\substack{A \\ N_{P}(A) \mid \mathcal{P}\left(X^{\theta_{0}}\right) \\ N_{P}(A) \leq X^{3 \theta_{0}}}} \sum_{h \leq H^{2}} \frac{\left|E_{1}(X, h ; K A)\right|+\left|E_{2}(X, h ; K A)\right|}{h+h^{2} / H}+o(X), \tag{7.1}
\end{equation*}
$$

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

$$
E_{\ell}(X, h ; K A):=\sum_{\substack{(\alpha) \in \mathcal{J} \\ K A \mid(\alpha)}} \mathrm{e}\left(\frac{h \ell X}{N_{P}(\alpha)}-\frac{h U \overline{B_{14}}}{q}\right) .
$$

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 $E_{\ell}$. 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 $P^{-}(r)>2^{k} D$. Suppose that for every $p \mid r$ there is no polynomial $w \in$ $\mathbb{Z}[X]$ of degree $\leq k+1$ such that $f(X) \equiv w(X) g(X)(\bmod p)$. Moreover,
suppose that $v(X)$ is not the zero polynomial $(\bmod p)$ for any $p \mid r$. Then for $A, B, h \geq 1$ we have

$$
\begin{aligned}
& \sum_{\substack{A<n \leq A+B \\
(v(n) g(n), r)=1}} \mathrm{e}\left(\frac{h f(n) \overline{g(n)}}{r}\right) \lll k, D, \varepsilon \\
& r^{\varepsilon} B\left[\left(\frac{\Delta}{r_{0}}\right)^{1 / 2^{k+1}}+\left(\frac{r_{0}}{\Delta B^{2}}\right)^{1 / 2^{k+1}}\right. \\
&\left.+\sum_{j=1}^{k}\left(\frac{r_{k+1-j}}{B}\right)^{1 / 2^{j}}\right]
\end{aligned}
$$

where $\Delta:=\left(r_{0}, h\right)$.
Proof. This is [1] Lemme 3.10] (a small variation of [8, Theorem 2]).
To apply this lemma, the denominator $q\left(a_{1}, a_{2}, a_{3}\right)$ in our exponential phase must have a good factorisation. We will apply Theorem 4.1 to show that for a positive proportion of $\left(a_{1}, a_{2}, a_{3}\right)$ the denominator $q=$ $q\left(a_{1}, a_{2}, a_{3}\right)$ has such a factorisation. We want the $\mathrm{e}\left(h U \overline{B_{14}} / q\right)$ 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 $U=a_{0} U_{1}+U_{0}, V=a_{0} V_{1}+V_{0}$ as in 5.21) and in 5.22). If $a_{0}, a_{1}, a_{2}, a_{3} \in \mathbb{Z}$ are such that $\left(a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right) \in \mathcal{J}$, then

$$
\left(U_{0}\left(a_{1}, a_{2}, a_{3}\right), U_{1}\left(a_{1}, a_{2}, a_{3}\right), q\left(a_{1}, a_{2}, a_{3}\right)\right)=1
$$

Proof. Imagine for a contradiction that $p \mid q\left(a_{1}, a_{2}, a_{3}\right), U_{0}\left(a_{1}, a_{2}, a_{3}\right), U_{1}\left(a_{1}, a_{2}, a_{3}\right)$. Condition (C4) implies that $q\left(a_{1}, a_{2}, a_{3}\right)$ has no prime factors smaller that $q_{0}$, so certainly $p>2$. Then $U\left(a_{0}^{\prime}, a_{1}, a_{2}, a_{3}\right)=0(\bmod p)$ for all $a_{0}^{\prime}$, and so the equation $U B_{13}+V B_{14}=q q_{3}$ s.13) simplifies to give

$$
V\left(a_{0}^{\prime}, a_{1}, a_{2}, a_{3}\right) B_{14}\left(a_{0}^{\prime}, a_{1}, a_{2}, a_{3}\right) \equiv 0(\bmod p)
$$

for all $a_{0}^{\prime}$. Condition (C5)(d) then implies that $B_{14}\left(a_{0}^{\prime}, a_{1}, a_{2}, a_{3}\right)$ does not identically vanish $(\bmod p)$, so $V_{1}\left(a_{1}, a_{2}, a_{3}\right)=V_{0}\left(a_{1}, a_{2}, a_{3}\right)=0(\bmod p)$.

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 $a_{0}^{\prime}$ such that $B_{14}\left(a_{0}^{\prime}, a_{1}, a_{2}, a_{3}\right)=B_{13}\left(a_{0}^{\prime}, a_{1}, a_{2}, a_{3}\right)=0(\bmod p)$. Evaluating (5.13) at $a_{0}^{\prime}, a_{1}, a_{2}, a_{3}$ then implies that

$$
q\left(a_{1}, a_{2}, a_{3}\right) q_{3}\left(a_{1}, a_{2}, a_{3}\right) \equiv 0\left(\bmod p^{2}\right) .
$$

This is impossible since $\left(q\left(a_{1}, a_{2}, a_{3}\right), q_{3}\left(a_{1}, a_{2}, a_{3}\right)\right)=1$ and $q\left(a_{1}, a_{2}, a_{3}\right)$ 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 $q\left(a_{1}, a_{2}, a_{3}\right)$ being not too small.
Lemma 7.4 (Bounding terms with $q_{2}\left(a_{1}, a_{2}, a_{3}\right)$ small). Let $\tau_{20}>0$ and for $\ell=1,2, E_{\ell}^{\prime}(X, h ; K A)$ be the contribution in $E_{\ell}(X, h ; K A)$ given by the $(\alpha) \in \mathcal{J}$ such that $\left|q_{2}\left(a_{1}, a_{2}, a_{3}\right)\right| \leq X^{\left(1+\alpha_{0}\right) / 2-\tau_{20}}$. Then

$$
E_{\ell}^{\prime}(X, h ; K A) \ll \frac{X^{1+\alpha_{0}-\tau_{20} / 2}}{N_{P}(K A)} .
$$

Proof. If $E_{\ell}^{\prime}(X, h ; K A)=0$ then the result is trivial. If $E_{\ell}^{\prime}(X, h ; K A) \neq 0$ then there exists at least an ideal $(\tilde{\alpha}) \in \mathcal{J}$ such that $N_{P}(A K) \mid(\tilde{\alpha})$. By the last assertion of Lemma 5.2, this implies that there exists an integer $j$ such that $r_{1} \equiv j(\bmod K A)$. The condition $K A \mid(\alpha)$ is therefore equivalent to

$$
a_{0} \equiv-a_{1} j-a_{2} j^{2}-a_{3} j^{3}\left(\bmod N_{P}(A K)\right)
$$

Thus, for any given $a_{1}, a_{2}, a_{3}$ there are $O\left(X^{\left(1+\alpha_{0}\right) / 4} / N_{P}(K A)\right)$ terms $a_{0}$ in $E_{\ell}^{\prime}(X, h ; K A)$.

We recall that $q_{2}\left(a_{1}, a_{2}, a_{3}\right)=\prod_{i=0}^{1} L_{i}\left(a_{1}, a_{2}, a_{3}\right)$ with for $i=0,1$ :

$$
L_{i}\left(a_{1}, a_{2}, a_{3}\right)=a_{1}+\left(r_{1+2 i}+r_{2+2 i}\right) a_{2}+\left(r_{1+2 i}^{2}+r_{1+2 i} r_{2+2 i}+r_{2+2 i}^{2}\right) a_{3} .
$$

If $\left|q_{2}\left(a_{1}, a_{2}, a_{3}\right)\right| \leq X^{\left(1+\alpha_{0}\right) / 2-\tau_{20}}$ then

$$
\begin{equation*}
\min _{i=0,1}\left|L_{2 i}\left(a_{1}, a_{2}, a_{3}\right)\right| \ll X^{\left(1+\alpha_{0}\right) / 4-\tau_{20} / 2} \tag{7.2}
\end{equation*}
$$

For any given $a_{2}, a_{3}$, the number of $a_{1}$ satisfying $\sqrt{7.2}$ is $O\left(X^{\left(1+\alpha_{0}\right) / 4-\tau_{20} / 2}\right)$. Since there are $O\left(X^{\left(1+\alpha_{0}\right) / 2}\right)$ choices of $a_{2}, a_{3}$, the total number of terms in $E^{\prime}(X, h ; K A)$ is $O\left(X^{1+\alpha_{0}-\tau_{20} / 2}\right)$.

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 $\eta_{0}$ is slightly larger than $\alpha_{0}$ and $\theta_{0}$ is sufficiently small. This gives

$$
S_{1} \ll(\log H) \sum_{K \in \mathcal{K}} \sum_{\substack{A \\ N_{P}(A) \mid \mathcal{P}\left(X^{\theta_{0}}\right) \\ N_{P}(A) \leq X^{3 \theta_{0}}}} \sum_{h \leq H^{2}} \frac{\left|E_{1}(X, h ; K A)\right|+\left|E_{2}(X, h ; K A)\right|}{h+h^{2} / H}+o(X),
$$

where

$$
E_{\ell}(X, h ; K A):=\sum_{\substack{(\alpha) \in \mathcal{J} \\ K A \mid(\alpha)}} \mathrm{e}\left(\frac{h \ell X}{N_{P}(\alpha)}-\frac{h U \overline{B_{14}}}{q}\right) .
$$

We write $E_{\ell}=E_{\ell}^{\prime}+E_{\ell}$ where $E_{\ell}^{\prime}$ is the contribution from terms in $E_{\ell}$ with $\left|q_{2}\left(a_{1}, a_{2}, a_{3}\right)\right| \leq Y$, and $E_{\ell}^{\prime \prime}$ is the contribution from terms with $\left|q_{2}\left(a_{1}, a_{2}, a_{3}\right)\right|>Y$. By Lemma 7.4, the contribution to $S_{1}$ from $E_{\ell}^{\prime}$ is $O\left(X^{1-\epsilon+o(1)}\right)$ provided

$$
\begin{equation*}
Y<X^{\left(1+\alpha_{0}\right) / 2-4 \eta_{0}-\epsilon} \tag{7.3}
\end{equation*}
$$

Therefore we concentrate on the contribution from $E_{\ell}^{\prime \prime}$. As in the proof of Lemma 7.4 there exists an integer $j$ such that the condition $K A \mid(\alpha)$ is equivalent to

$$
\begin{equation*}
a_{0} \equiv-a_{1} j-a_{2} j^{2}-a_{3} j^{3}\left(\bmod N_{P}(A K)\right) \tag{7.4}
\end{equation*}
$$

Let $\tilde{a}_{0}=\tilde{a}_{0}\left(a_{1}, a_{2}, a_{3} ; K A\right)$ be a solution of the congruence (7.4). We may write $a_{0}=\tilde{a}_{0}+m N_{P}(K A)$ with $m \in \mathcal{R}^{\prime}\left(a_{1}, a_{2}, a_{3}\right)$ where

$$
\mathcal{R}^{\prime}\left(a_{1}, a_{2}, a_{3}\right):=\left\{m:\left(\tilde{a}_{0}+m N_{P}(K A), a_{1}, a_{2}, a_{3}\right) \in \mathcal{R}\right\}
$$

(We recall that $\mathcal{R}$ is the domain defined in 6.12).) This set $\mathcal{R}^{\prime}\left(a_{1}, a_{2}, a_{3}\right)$ can be written as a finite union of intervals $I^{\prime}\left(a_{1}, a_{2}, a_{3}\right)$.

Any $a_{0}$ of the above form ensures that conditions ( $C 2$ ) and ( $C 3$ ) are satisfied. Conditions (C1), (C4) and (C5) parts (a),(c),(e) don't depend on $a_{0}$. Thus we find

$$
E_{\ell}^{\prime \prime}(X, h ; K A) \ll \sum_{\substack{a_{1}, a_{2}, a_{3} \ll X^{\left(1+\alpha_{0}\right) / 4} \\ q_{2}\left(a_{1} a_{2}, a_{3}\right)>Y}}\left|\sum_{\substack{m \in I^{\prime}\left(a_{1}, a_{2}, a_{3}\right) \\ 6.11}} \mathrm{e}\left(\frac{h \ell X}{N_{P}(\alpha)}-\frac{h U \overline{B_{14}}}{q}\right)\right| .
$$

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

We now need to control the gcd between $N_{P}(K A)$ and $q$. We define $t=\left(N_{P}(K A), q\right)$ and $t^{\prime}=q / t$. Since $q$ is squarefree, $\left(t, t^{\prime}\right)=1$. We apply Bezout formula (5.14) to separate the congruence in $t$ and in $t^{\prime}$ and use partial summation to remove the factor $e\left(h \ell X / N_{P}(\alpha)\right)$. This gives for $\ell=1,2,($ as in [1] p. 239])

$$
\begin{equation*}
\left.E_{\ell}^{\prime \prime}(X, h ; K A) \ll X^{2 \eta_{0}+\alpha_{0} / 4} \sum_{\substack{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{C} \\ q_{2}\left(a_{1}, a_{2}, a_{3}\right)>Y}} \max _{\substack{6.11}} \sum_{\substack{\frac{1+\alpha_{0}}{4}}} \sum_{\substack{m \leq B \\ N_{P}(K A)}} \mathrm{e}\left(\frac{h \bar{t} f(m) \overline{g(m)}}{t^{\prime}}\right) \right\rvert\, \tag{7.5}
\end{equation*}
$$

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

$$
f(m):=U\left(\tilde{a}_{0}+m N_{P}(K A)\right), \quad g(m):=B_{14}\left(\tilde{a}_{0}+m N_{P}(K A)\right) .
$$

We recall from 6.11) that for all $a_{1}, a_{2}, a_{3}$ under consideration $q\left(a_{1}, a_{2}, a_{3}\right)$ factors as $\prod_{i=1}^{7} q_{1 i} \prod_{j=1}^{2} q_{2 j}$ for some integers $q_{i j}$ 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 $p \mid q\left(a_{1}, a_{2}, a_{3}\right)$, there is no polynomial $w(X) \in \mathbb{Z}[X]$ of degree less than 10 such that $f(X) \equiv w(X) g(X)(\bmod p)$.

Let $p \mid q\left(a_{1}, a_{2}, a_{3}\right)$. By (C5)(e), $a_{3}$ is coprime with $p$, and so by (5.18), $B_{14}(\bmod p)$ is a polynomial of degree exactly two in $a_{0}$ since its lead coefficient is $-a_{3}$. By Lemma 7.3, $\left(p, U_{0}\left(a_{1}, a_{2}, a_{3}\right), U_{1}\left(a_{1}, a_{2}, a_{3}\right)\right)=1$, and so $U\left(a_{0}, a_{1}, a_{2}, a_{3}\right)(\bmod p)$ is not identically zero and has degree at most 1 in $a_{0}$. This implies that for all $p \mid q$, there is no polynomial $w \in \mathbb{Z}[X]$ such that $U\left(X, a_{1}, a_{2}, a_{3}\right) \equiv w(X) B_{14}\left(X, a_{1}, a_{2}, a_{3}\right)(\bmod p)$ and we can apply Lemma 7.2 with $k=8$. We take $r_{0}=q_{22} /\left(q_{22}, t\right), r_{1}=q_{21} /\left(q_{21}, t\right)$, $r_{2}=q_{17} /\left(q_{17}, t\right), r_{3}=q_{16} /\left(q_{16}, t\right), \ldots, r_{8}=q_{11} /\left(q_{11}, t\right)$. By 6.11) and (6.6), we observe that $q_{17}<q_{1 j}$ for all $1 \leq j \leq 6$. Let

$$
\begin{equation*}
\theta_{\max }+\tau_{\max }=\sup _{(i, j) \in I_{\mathcal{C}}}\left(\theta_{i j}+\tau_{i j}\right) \tag{7.6}
\end{equation*}
$$

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

$$
\begin{aligned}
& \left|\sum_{\substack{m \leq B \\
\left(g(m), t^{\prime}\right)=1}} \mathrm{e}\left(\frac{h \bar{t} f(m) \overline{g(m)}}{t^{\prime}}\right)\right| \\
& \\
& \\
&
\end{aligned} \ll q^{\varepsilon} B\left(\left(\frac{(h, q)\left(q_{22}, t\right)}{q_{22}}\right)^{1 / 2^{9}}+\left(\frac{q_{22}}{B^{2}}\right)^{1 / 2^{9}}+\sup _{(i, j) \in I_{\mathcal{C}}}\left(\frac{q_{i j}}{B}\right)^{1 / 2^{8}}\right) . .
$$

We insert this bound into $E_{\ell}^{\prime \prime}(X, h ; K A)$, and then subsitute this into $S_{1}$. Writing $q_{22}=X^{\theta_{22}}$, this gives

$$
\begin{aligned}
S_{1} & \ll X^{2 \eta_{0}+1+\frac{5 \alpha_{0}}{4}+\varepsilon}\left(X^{-\theta_{22} 2^{-9}}+X^{\left(\theta_{22}-\frac{1+\alpha_{0}}{2}+6 \theta_{0}+10 \alpha_{0}\right) 2^{-9}}\right. \\
& \left.+X^{\left(\theta_{\text {max }}+\tau_{\text {max }}-\frac{1+\alpha_{0}}{4}+3 \theta_{0}+5 \alpha_{0}\right) 2^{-8}}\right)+X^{1-\epsilon+o(1)} .
\end{aligned}
$$

Thus we see that $S_{1}=o(X)$ provided

$$
\begin{aligned}
2 \eta_{0}+\frac{5 \alpha_{0}}{4} & <\frac{\theta_{22}}{2^{9}} \\
\frac{\theta_{22}}{2^{9}} & <\frac{1}{2^{9}}\left(\frac{1+\alpha_{0}}{2}-6 \theta_{0}-10 \alpha_{0}\right)-2 \eta_{0}-\frac{5 \alpha_{0}}{4} \\
\frac{\theta_{\max }+\tau_{\max }}{2^{8}} & <\frac{1}{2^{8}}\left(\frac{1+\alpha_{0}}{4}-3 \theta_{0}-5 \alpha_{0}\right)-2 \eta_{0}-\frac{5 \alpha_{0}}{4} .
\end{aligned}
$$

We recall that $q_{22}=q_{2}\left(a_{1}, a_{2}, a_{3}\right) / q_{21}$, that $q_{2}\left(a_{1}, a_{2}, a_{3}\right) \in\left[Y, X^{\left(1+\alpha_{0}\right) / 2}\right]$ and $q_{21} \in\left[X^{\theta_{21}}, X^{\theta_{21}+\tau_{21}}\right]$. Thus on choosing $Y=X^{\left(1+\alpha_{0}\right) / 4-4 \eta_{0}-\epsilon}$ so (7.3) is satisfied, we see that the bound $S_{1}=o(X)$ holds provided

$$
\begin{aligned}
2 \eta_{0}+\frac{5 \alpha_{0}}{4} & <\left(\frac{1+\alpha_{0}}{4}-\theta_{21}-\tau_{21}-4 \eta_{0}\right) \frac{1}{2^{9}} \\
\frac{1}{2^{9}}\left(\frac{1+\alpha_{0}}{4}-\theta_{21}\right) & <\frac{1}{2^{9}}\left(\frac{1+\alpha_{0}}{2}-6 \theta_{0}-10 \alpha_{0}\right)-2 \eta_{0}-\frac{5 \alpha_{0}}{4} \\
\frac{\theta_{\max }+\tau_{\max }}{2^{8}} & <\frac{1}{2^{8}}\left(\frac{1+\alpha_{0}}{4}-3 \theta_{0}-5 \alpha_{0}\right)-2 \eta_{0}-\frac{5 \alpha_{0}}{4} .
\end{aligned}
$$

These follow from (6.3), 6.4) and 6.8 on taking $\theta_{0}$ sufficiently small and $\eta_{0}$ sufficiently close to $\alpha_{0}$.

## 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 $\alpha=a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}$, 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 $O\left(X^{\varepsilon}\right)$ is not always sufficient.

Lemma 8.1 (Removing the variable $a_{0}$ ). Let $12 \theta_{0}+22 \alpha_{0}<1$. We have

$$
S_{0}=\left(\frac{4 \mathrm{e}^{\gamma}}{3} \log (5 / 4) \log 2+o(1)\right) \prod_{p<X_{0}^{\theta}}\left(1-\frac{g(p)}{p}\right) S_{01}+O\left(X^{-\alpha_{0} / 5}\right),
$$

where

$$
\begin{align*}
S_{01} & :=\sum_{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{C} \cap \mathcal{G}} I\left(a_{1}, a_{2}, a_{3}\right) h\left(q\left(a_{1}, a_{2}, a_{3}\right)\right),  \tag{8.1}\\
g(p) & :=\left|\left\{\mathfrak{P}: N_{P}(\mathfrak{P})=p\right\}\right|,  \tag{8.2}\\
\mathcal{C} & :=\left\{\left(a_{1}, a_{2}, a_{3}\right) \in \mathbb{R}^{3}: \exists a_{0} \in \mathbb{R} \text { s.t. }\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathcal{R}\right\}  \tag{8.3}\\
\mathcal{G} & :=\left\{\left(a_{1}, a_{2}, a_{3}\right) \in \mathbb{Z}^{3}: \exists a_{0} \in \mathbb{Z} \text { s.t. }(\alpha) \in \mathcal{J}\right\}  \tag{8.4}\\
h(q) & :=\mu^{2}(q) \prod_{p \mid q} \frac{(1-2 / p)}{1-g(p) / p} \mathbf{1}_{P^{-}(q)>q_{0}},  \tag{8.5}\\
I\left(a_{1}, a_{2}, a_{3}\right) & :=\int_{a_{0} \in \mathcal{D}\left(a_{1}, a_{2}, a_{3}\right)} \frac{\mathrm{d} a_{0}}{\widetilde{N}_{P}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)},  \tag{8.6}\\
\mathcal{D}\left(a_{1}, a_{2}, a_{3}\right) & :=\left\{a_{0} \in \mathbb{R}:\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathcal{R}\right\} . \tag{8.7}
\end{align*}
$$

Here $\widetilde{N}_{P}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)$ is the quartic form coinciding with $N_{P}\left(a_{0}+a_{1} r_{1}+\right.$ $\left.a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right)$ on integers.

Proof. We want to isolate the variable $a_{0}$. We note that the condition $(\alpha) \in \mathcal{J}$ implies that $\left(q\left(a_{1}, a_{2}, a_{3}\right), B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right)=1$ and that $\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathcal{R}$ 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 $\left(q, B_{14}\right)=1$ when evaluated at $a_{0}, a_{1}, a_{2}, a_{3}$. This give rise to a squarefree $r \mid\left(q, B_{14}\right)$ which we decompose as $r=r_{1}^{\prime} r_{2}^{\prime}$ with $r_{1}^{\prime} \mid N_{P}(K A)$ and $\left(r_{2}^{\prime}, N_{P}(K A)\right)=1$. This yields

$$
\begin{align*}
S_{0} & =\sum_{K \in \mathcal{K}} \sum_{A} \lambda_{N_{P}(A)}^{-} \sum_{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{C} \cap \mathcal{G}} \sum_{\substack{r_{1}^{\prime}\left|N_{P}(K A) \\
r_{1}^{\prime}\right| q\left(a_{1}, a_{2}, a_{3}\right)}} \mu\left(r_{1}^{\prime}\right) \\
& \times \sum_{\substack{r_{2}^{\prime} \mid q\left(a_{1}, a_{2}, a_{3}\right) \\
\left(r_{2}^{\prime}, N_{P}(K A)\right)=1}} \mu\left(r_{2}^{\prime}\right) \sum_{\tilde{a}_{0} \in S\left(r_{1}^{\prime}, r_{2}^{\prime}\right)} \sum_{\substack{a_{0} \in \mathcal{D}\left(a_{1}, a_{2}, a_{3}\right) \\
a_{0} \equiv \tilde{a}_{0}\left(\bmod r_{2}^{\prime} N_{P}(K A)\right)}} \frac{1}{N_{P}(\alpha)}, \tag{8.8}
\end{align*}
$$

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

$$
\begin{equation*}
S\left(r_{1}^{\prime}, r_{2}^{\prime}\right):=\left\{0 \leq a_{0} \leq r_{2}^{\prime} N_{P}(K A): r_{1}^{\prime} r_{2}^{\prime}\left|B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right), K A\right|(\alpha)\right\} . \tag{8.9}
\end{equation*}
$$

(We have suppressed the dependence of $S\left(r_{1}^{\prime}, r_{2}^{\prime}\right)$ 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

$$
\begin{equation*}
\sum_{a_{0} \in \mathcal{D}\left(a_{1}, a_{2}, a_{3}\right)} \frac{1}{N_{P}(\alpha)}=\frac{I\left(a_{1}, a_{2}, a_{3}\right)}{r_{2}^{\prime} N_{P}(A K)}+O\left(\frac{1}{X^{1+\alpha_{0} / 2}}\right) . \tag{8.10}
\end{equation*}
$$

The $O\left(X^{-\left(1+\alpha_{0} / 2\right)}\right)$ error term in 8.10) contributes to $S_{0}$ a total

$$
\ll \frac{1}{X^{1+\alpha_{0} / 2-o(1)}} \sum_{N_{P}(K) \ll X^{5 \alpha_{0}}} \sum_{N_{P}(A) \leq X^{3 \theta_{0}}} \sum_{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{C}} 1 \ll X^{-1 / 4+3 \theta_{0}+21 \alpha_{0} / 4+o(1)} .
$$

(Recall that if $\mathbf{a} \in \mathcal{R}$ then $\|\mathbf{a}\|_{\infty} \ll X^{\left(1+\alpha_{0}\right) / 4}$ by our choice of fundamental domain $)$. This is $O\left(X^{-\alpha_{0} / 4+o(1)}\right)$ 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

$$
\sum_{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{C}} \sum_{K \in \mathcal{K}} \sum_{A} \lambda_{N_{P}(A)} \sum_{\substack{r_{1}^{\prime} r_{2}^{\prime}\left|q\left(a_{1}, a_{2}, a_{3}\right) \\ r_{1}^{\prime}\right| N_{P}(K A) \\\left(r_{2}^{\prime}, N_{P}(K A)\right)=1}} \mu\left(r_{1}^{\prime}\right) \mu\left(r_{2}^{\prime}\right) \frac{\left|S\left(r_{1}^{\prime}, r_{2}^{\prime}\right)\right| I\left(a_{1}, a_{2}, a_{3}\right)}{r_{2}^{\prime} N_{P}(A K)}
$$

By the Chinese Remainder Theorem, we have

$$
\begin{equation*}
\left|S\left(r_{1}^{\prime}, r_{2}^{\prime}\right)\right|=\prod_{p \mid r_{2}^{\prime} N_{P}(K A)}\left|S\left(r_{1}^{\prime}, r_{2}^{\prime}, p\right)\right|, \tag{8.12}
\end{equation*}
$$

where

$$
\left|S\left(r_{1}^{\prime}, r_{2}^{\prime}, p\right)\right|:= \begin{cases}\left|\left\{0 \leq a_{0}<p: p \mid\left(B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right), N_{P}(\alpha)\right)\right\}\right|, & \text { if } p \mid r_{1}^{\prime}, \\ \left|\left\{0 \leq a_{0}<p: p \mid B_{14}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)\right\}\right|, & \text { if } p \mid r_{2}^{\prime}, \\ \left|\left\{0 \leq a_{0}<p: p \mid N_{P}(\alpha)\right\}\right|, & \text { if } p \mid N_{P}(K A) / r_{1}^{\prime} .\end{cases}
$$

We compute $\left|S\left(r_{1}^{\prime}, r_{2}^{\prime}, p\right)\right|$ using Lemmas 5.16 and 5.17 Under the condition $P^{-}(q)>q_{0}$ we find

$$
\left|S\left(r_{1}^{\prime}, r_{2}^{\prime}, p\right)\right|= \begin{cases}2 & \text { if } p \mid r_{2}^{\prime} \\ 1 & \text { if } p \mid N_{P}(K A)\end{cases}
$$

Using this bound in 8.12 gives

$$
\left|S\left(r_{1}^{\prime}, r_{2}^{\prime}\right)\right|=2^{\omega\left(r_{2}^{\prime}\right)}
$$

Inserting this in the previous expression 8.11 for the main term of $S_{0}$, we see that the sum over $r_{1}^{\prime}$ is 1 if $\left(q\left(a_{1}, a_{2}, a_{3}\right), N_{P}(K A)\right)=1$, and 0 otherwise. Thus the expression 8.11 simplifies to

$$
\sum_{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{C}} I\left(a_{1}, a_{2}, a_{3}\right)\left(\sum_{r_{2}^{\prime} \mid q\left(a_{1}, a_{2}, a_{3}\right)} \frac{\mu\left(r_{2}^{\prime}\right) 2^{\omega\left(r_{2}^{\prime}\right)}}{r_{2}^{\prime}}\right) h_{1}\left(q\left(a_{1}, a_{2}, a_{3}\right)\right),
$$

where

$$
h_{1}(q):=\left(\sum_{\substack{K \in \mathcal{K} \\\left(N_{P}(K), q\right)=1}} \frac{1}{N_{P}(K)}\right)\left(\sum_{\left(N_{P}(A), q\right)=1} \frac{\lambda_{N_{P}(A)}^{-}}{N_{P}(A)}\right) .
$$

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 $q \ll X^{O(1)}$

$$
\begin{aligned}
\sum_{\substack{K \in \mathcal{K} \\
\left(N_{P}(K), q\right)=1}} \frac{1}{N_{P}(K)} & =\log (5 / 4)+o(1), \\
\sum_{\left(N_{P}(A), q\right)=1} \frac{\lambda_{N_{P}(A)}^{-}}{N_{P}(A)} & =\sum_{\substack{d \leq X^{3 \theta_{0}} \\
(\bar{d}, q)=1}} \frac{\lambda_{d}^{-} g(d)}{d} \\
& =\left(\frac{2 e^{\gamma} \log 2}{3}+o(1)\right) \prod_{p<X^{\theta_{0}}}\left(1-\frac{g(p)}{p}\right) \prod_{\substack{p \mid q \\
p \leq X^{\theta_{0}}}}\left(1-\frac{g(p)}{p}\right)^{-1} .
\end{aligned}
$$

Here we used the fact that the linear sieve lower bound function evaluated at 3 is $2 e^{\gamma} \log 2 / 3$. 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 $\mathfrak{a}=\left(a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right)$ 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
$\left.\left.\left.\left.\left.\left.\left.\mathcal{H}=] A_{0}, A_{0}+\eta_{1} A_{0}\right] \times\right] A_{1}, A_{1}\left(1+\eta_{1}\right)\right] \times\right] A_{2}, A_{2}\left(1+\eta_{1}\right)\right] \times\right] A_{3}, A_{3}\left(1+\eta_{1}\right)\right]$.
The number of such hyper-rectangles is $O\left(\eta_{1}^{-4}\right)(\log X)^{4}=O\left(\eta_{1}^{-5}\right)$.
Furthermore the contribution to $S_{01}$ from hyper-rectangles such that $\min \left(\left|A_{i}\right|\right) \leq X^{1 / 4-7 \alpha_{0} / 8}$ is $O\left(X^{1-\alpha_{0} / 8+\varepsilon}\right)$ which is sufficiently small.

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

$$
\begin{align*}
\min \left(\left|A_{0}\right|,\left|A_{1}\right|,\left|A_{2}\right|,\left|A_{3}\right|\right) & \geq X^{1 / 4-7 \alpha_{0} / 8}, \\
\min \left(\left|A_{0}\right|,\left|A_{1}\right|,\left|A_{2}\right|,\left|A_{3}\right|\right) & \geq \eta_{1} \max \left(\left|A_{0}\right|,\left|A_{1}\right|,\left|A_{2}\right|,\left|A_{3}\right|\right),  \tag{8.14}\\
q_{1}\left(A_{1}, A_{2}, A_{3}\right) & \geq \eta_{1}^{1 / 10} \max \left(\left|A_{1}\right|,\left|A_{2}\right|,\left|A_{3}\right|\right)^{4} .
\end{align*}
$$

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 hyperrectangle $\mathcal{H}$ we associate its projection to $\mathbb{R}^{3}$ by ignoring $a_{0}$ :

$$
\begin{equation*}
\left.\left.\left.\left.\left.\left.\mathcal{H}^{\prime}=\right] A_{1}, A_{1}\left(1+\eta_{1}\right)\right] \times\right] A_{2}, A_{2}\left(1+\eta_{1}\right)\right] \times\right] A_{3}, A_{3}\left(1+\eta_{1}\right)\right] . \tag{8.15}
\end{equation*}
$$

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

$$
S_{01} \gg \sum_{\mathcal{H} \in \mathscr{H}_{\mathcal{R}}} \frac{A_{0} \eta_{1}}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)} S_{02}(\mathcal{H}),
$$

where

$$
S_{02}(\mathcal{H}):=\sum_{\substack{q_{i j} \in\left[X^{\theta_{i j}, X^{\theta_{i j}+\tau_{i j}}} \begin{array}{c}
(i, j) \in I_{\mathcal{C}} \\
q_{21} \equiv 1\left(\bmod D_{q_{2}}\right)
\end{array}\right.}} \sum_{\substack{\left.\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\
\prod_{j=1}^{6} q_{1 j}\left|q_{1}\left(a_{1}, a_{2}, a_{3}\right) \\
q_{21}\right| q_{2}\left(a_{1}, a_{2}, a_{3}\right) \\
\left(q_{1}, a_{2}, a_{3}\right), q_{3}\left(a_{1}, a_{2}, a_{3}\right)\right)=1 \\
\left(q_{2}, a_{2} a_{3}\right)=1 \\
\left(a_{2}, a_{3}\right)=30, a_{1} \equiv 1(\bmod 30) \\
a_{2}, a_{3} \equiv 30(\bmod 900)}} h\left(q\left(a_{1}, a_{2}, a_{3}\right)\right) .
$$

We recall from $\sqrt[6.13]{ }$ that $\tilde{N}_{P}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)$ is the quartic form coinciding with $N_{P}\left(a_{0}+a_{1} r_{1}+a_{2} r_{1}^{2}+a_{3} r_{1}^{3}\right)$ 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

$$
S_{01} \geq \sum_{\mathcal{H} \in \mathscr{H}_{\mathcal{R}}} S_{01}^{\prime}(\mathcal{H})
$$

where

$$
\begin{aligned}
S_{01}^{\prime}(\mathcal{H}) & :=\sum_{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{C} \cap \mathcal{H}^{\prime} \cap \mathcal{G}} h\left(q\left(a_{1}, a_{2}, a_{3}\right)\right) I_{\mathcal{H}}\left(a_{1}, a_{2}, a_{3}\right), \\
I_{\mathcal{H}}\left(a_{1}, a_{2}, a_{3}\right) & : \int_{A_{0}}^{A_{0}\left(1+\eta_{1}\right)} \frac{\mathrm{d} a_{0}}{\widetilde{N}_{P}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)}=\frac{A_{0} \eta_{1}(1+o(1))}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)} .
\end{aligned}
$$

We recall from 6.11) that if $\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{G}$ then $q_{1}\left(a_{1}, a_{2}, a_{3}\right)$ and $q_{2}\left(a_{1}, a_{2}, a_{3}\right)$ factor as $\prod_{i=1}^{6} q_{1 i}$ and $q_{21} q_{22}$ respectively with $q_{21}, q_{11}, q_{12}, q_{13}, q_{14}, q_{15}$ primes satisfying $q_{i j} \geq X^{\theta_{i j}}$. In particular, we see that for any choice of $a_{1}, a_{2}, a_{3}$ there are $O(1)$ choices of $q_{i j}$ such that $q_{i}\left(a_{1}, a_{2}, a_{2}\right)=\prod_{j} q_{i j}$. Thus, summing over these representations, we find

$$
S_{01}(\mathcal{H}) \gg \frac{A_{0} \eta_{1}}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)} S_{02}(\mathcal{H})
$$

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 $\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}$, the $a_{i}$ are in small intervals. Let

$$
\begin{equation*}
Z:=(\log X)^{\lambda_{0}}, \quad Z^{\prime}:=X^{\alpha_{0} / 10000} \tag{8.16}
\end{equation*}
$$

where $\alpha_{0}$ is the constant used to define the set $\mathcal{K}$ (which will be chosen sufficiently small later on) and $\lambda_{0}$ 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

$$
\begin{equation*}
Z^{1000}<Z^{\prime 100}<\min \left(A_{0}, A_{1}, A_{2}, A_{3}\right) \tag{8.17}
\end{equation*}
$$

For brevity we will write

$$
\begin{equation*}
N_{\mathcal{H}}=\tilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right) \tag{8.18}
\end{equation*}
$$

Lemma 8.3 (Removing the condition $\left.\left(q, q_{3}\right)=1\right)$. Let $S_{02}(\mathcal{H})$ be as in Lemma 8.2. Then we have

$$
S_{02}(\mathcal{H})=S_{03}(\mathcal{H})+O\left(\frac{\eta_{1}^{3} A_{1} A_{2} A_{3}}{Z^{3 / 4}}\right)
$$

where

$$
\begin{aligned}
& S_{03}(\mathcal{H}):=\sum_{d \leq Z} \mu(d) \sum_{\substack{q_{i j} \in\left[X^{\left.\theta_{i j}, X^{\theta_{i j}}+\tau_{i j}\right]} \\
(i, j) \in I_{\mathcal{C}}\right.}} \sum_{\substack{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\
\prod_{j=1}^{6} q_{1 j} \mid q_{1}\left(a_{1}, a_{2}, a_{3}\right)}} h\left(q\left(a_{1}, a_{2}, a_{3}\right)\right) . \\
& \xrightarrow{(i, j) \in I_{\mathcal{C}}}{ }_{q_{21}} \equiv 1\left(\bmod D_{q_{2}}\right) \quad \prod_{j=1}^{6} q_{1 j} \mid q_{1}\left(a_{1}, a_{2}, a_{3}\right) \\
& q_{21} \mid q_{2}\left(a_{1}, a_{2}, a_{3}\right) \\
& { }_{d \mid q\left(a_{1}, a_{2}, a_{3}\right)}^{d \mid q(a)} \\
& d \mid q_{3}\left(a_{1}, a_{2}, a_{3}\right) \\
& \left(q\left(a_{1}, a_{2}, a_{3}\right), q_{3}\left(a_{1}, a_{2}, a_{3}\right)\right)=1 \\
& \left(a_{2}, a_{3}\right)=30, a_{1} \equiv 1(\bmod 30) \\
& a_{2}, a_{3} \equiv 30(\bmod 900)
\end{aligned}
$$

Proof. First, we detect the condition $\left(q, q_{3}\right)=1$ via Möbius inversion

$$
S_{02}(\mathcal{H})=\sum_{\substack{ \\
q_{i j} \in\left[X^{\theta_{i j}, X^{\theta_{i j}+\tau_{i j}}\left(\begin{array}{c}
(i, j) \in I_{\mathcal{C}} \\
q_{21} \equiv 1\left(\bmod D_{q_{2}}\right)
\end{array}\right.} \begin{array}{c}
\begin{subarray}{c}{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\
\prod_{j=1}^{6} q_{1 j}\left|q_{1}\left(a_{1}, a_{2}, a_{3}\right) \\
q_{21}\right| q_{2}\left(a_{1}, a_{2}, a_{3}\right) \\
\left(q\left(a_{1}, a_{2}, a_{3}\right), q_{3}\left(a_{1}, a_{2}, a_{3}\right)\right)=1 \\
\left(q, a_{2} a_{3}\right)=1 \\
\left(a_{2}, a_{3}\right)=30, a_{1} \equiv 1(\bmod 30) \\
a_{2}, a_{3} \equiv 30(\bmod 900)} }
\end{array}\right.}\end{subarray}} h\left(q\left(a_{1}, a_{2}, a_{3}\right)\right) .
$$

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 $d \leq Z$, $U_{21}(\mathcal{H})$ is the contribution from $Z<d \leq Z^{\prime}$ and $U_{22}(\mathcal{H})$ is the contribution from $d>Z^{\prime}$. 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 $q_{3}\left(a_{1}, a_{2}, a_{3}\right)=-a_{1} a_{3}+a_{2}^{2}-c_{3} a_{2} a_{3}-$ $c_{2} a_{3}^{2}$, so the condition $q_{3} \equiv 0(\bmod d)$ implies that $a_{1} \equiv \overline{a_{3}}\left(a_{2}^{2}-c_{3} a_{2} a_{3}-\right.$ $\left.c_{2} a_{3}^{2}\right)(\bmod d)$. (We restrict ourselves to $\left(a_{3}, q\left(a_{1}, a_{2}, a_{3}\right)\right)=1$ so $\left(a_{3}, d\right)=$ 1.) Inserting this into the condition $q\left(a_{1}, a_{2}, a_{3}\right) \equiv 0(\bmod d)$ and multiplying by $a_{3}^{6}$ gives $Q\left(a_{2}, a_{3}\right):=q\left(a_{2}^{2}-c_{3} a_{2} a_{3}-c_{2} a_{3}^{2}, a_{2} a_{3}, a_{3}^{2}\right) \equiv 0(\bmod d)$, for a polynomial $Q\left(a_{2}, a_{3}\right)$ which is of degree 12 in $a_{2}$ (and non-zero). For any given $a_{3}$ the number of roots of $Q\left(a_{2}, a_{3}\right)(\bmod d)$ is $O\left(12^{\omega(d)}\right)$. For any choice of $a_{1}, a_{2}, a_{3}$ under consideration, there are $O(1)$ choices of primes $q_{i j} \in\left[X^{\theta_{i j}}, X^{\theta_{i j}+\tau_{i j}}\right]$ with $q_{i j} \mid q_{1}\left(a_{1}, a_{2}, a_{3}\right) q_{2}\left(a_{1}, a_{2}, a_{3}\right)$. Thus,
letting $b\left(a_{2}, a_{3}\right)=\overline{a_{3}}\left(a_{2}^{2}-c_{3} a_{2} a_{3}-c_{2} a_{3}^{2}\right.$ ), and noting $Z^{\prime}<A_{i}^{0.99}$ (recall (8.17), we deduce

$$
\begin{aligned}
U_{21}(\mathcal{H}) & \ll \sum_{Z<d \leq Z^{\prime}} \sum_{\substack{a_{3} \in\left[A_{3}, A_{3}\left(1+\eta_{1}\right)\right]}} \sum_{\substack{a_{2} \in\left[A_{2}, A_{2}\left(1+\eta_{1}\right)\right] \\
Q\left(a_{2}, a_{3}\right) \equiv 0(\bmod d)}} \sum_{\substack{a_{1} \in\left[A_{1}, A_{1}\left(1+\eta_{1}\right)\right] \\
a_{1} \equiv b\left(a_{2}, a_{3}\right)(\bmod d)}} 1 \\
& \ll A_{1} A_{2} A_{3} \eta_{1}^{3} \sum_{Z<d<Z^{\prime}} \frac{12^{\omega(d)}}{d^{2}} \ll A_{1} A_{2} A_{3} \eta_{1}^{3} Z^{-3 / 4} .
\end{aligned}
$$

We now consider $U_{22}$. Since $Q\left(a_{2}, a_{3}\right) \equiv 0(\bmod d)$, if $Q\left(a_{2}, a_{3}\right) \neq 0$ there are $O\left(X^{\epsilon}\right)$ choices of $d$ given $a_{2}, a_{3}$. We have $Q\left(a_{2}, a_{3}\right)=0$ if and only if $\exists(i, j)$ such that

$$
\left(a_{2}^{2}-c_{3} a_{2} a_{3}-c_{2} a_{3}^{2}\right)+\left(r_{i}+r_{j}\right) a_{2} a_{3}+a_{3}^{2}\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}\right)=0,
$$

which rearranges to

$$
a_{2}^{2}+a_{2} a_{3}\left(r_{i}+r_{j}-c_{3}\right)+a_{3}^{2}\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}-c_{2}\right)=0
$$

Since $a_{3} \neq 0, a_{2} / a_{3}$ is a root of $X^{2}+\left(r_{i}+r_{j}-c_{3}\right) X+r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}-c_{2}$ 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 $Q\left(a_{2}, a_{3}\right)=0$. Moreover, in this case we still have $d \mid q_{3}\left(a_{1}, a_{2}, a_{3}\right) \neq 0$, so there are $O\left(X^{\epsilon}\right)$ choices of $d$ given $a_{1}, a_{2}, a_{3}$. We deduce that (using $Z^{\prime} \ll A_{1}, A_{3}$ )

$$
\begin{aligned}
& U_{22}(\mathcal{H}) \ll \sum_{d>Z^{\prime}} \mu^{2}(d) \sum_{\substack{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\
Q\left(a_{2}, a_{3}\right) \neq 0 \\
a_{1} \equiv b\left(a_{2}, a_{3}\right)(\bmod d)}} 1+\sum_{\substack{d>Z^{\prime}}} \sum_{\begin{array}{c}
\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\
Q\left(a_{2}, a_{3}\right)=0 \\
d \mid a_{3}\left(a_{1}, a_{2}, a_{3}\right)
\end{array}} \mu^{2}(d) \\
& \ll \sum_{a_{2} \in\left[A_{2}, A_{2}\left(1+\eta_{1}\right)\right]} \sum_{\substack{a_{3} \in\left[A_{3}, A_{3}\left(1+\eta_{1}\right)\right] \\
Q\left(a_{2}, a_{3}\right) \neq 0}} \sum_{\substack{d>Z^{\prime} \\
d \left\lvert\, \begin{array}{c}
d \\
\alpha_{2}\left(a_{3}\right) \\
\mu^{2}(d)=1
\end{array}\right.}} \sum_{\begin{array}{c}
a_{1} \in\left[A_{1}, A_{1}\left(1+\eta_{1}\right)\right] \\
a_{1} \equiv b\left(a_{2}, a_{3}\right)(\bmod d)
\end{array}} 1 \\
& +\sum_{a_{1} \ll A_{1}, a_{2} \ll A_{2}} \sum_{\substack{0<a_{3} \ll A_{3} \\
Q\left(a_{2}, a_{3}\right)=0}} \sum_{d \mid q_{3}\left(a_{1}, a_{2}, a_{3}\right)} 1 \\
& \ll \frac{A_{1}}{Z^{\prime}} \sum_{\substack{a_{2} \in\left[A_{2}, A_{2}\left(1+\eta_{1}\right)\right] \\
a_{3} \in\left[A_{3}, A_{3}\left(1+\eta_{1}\right)\right] \\
Q\left(a_{2}, a_{3}\right) \neq 0}} \tau\left(Q\left(a_{2}, a_{3}\right)\right)+A_{1} A_{2} X^{\varepsilon} \ll \frac{A_{1} A_{2} A_{3} X^{\varepsilon}}{Z^{\prime}} .
\end{aligned}
$$

This gives the result.
Lemma 8.4 (Removing the condition $\left(q, a_{2} a_{3}\right)=1$ ). Let $S_{03}(\mathcal{H})$ be as given in Lemma 8.3. Then we have

$$
S_{03}(\mathcal{H})=S_{04}(\mathcal{H})+O\left(\frac{\eta_{1}^{3} A_{1} A_{2} A_{3}}{Z^{1 / 2}}\right)
$$

where
$S_{04}(\mathcal{H}):=\sum_{\substack{d \leq Z \\ s_{2} s_{3} \leq Z}} \mu(d) \mu\left(s_{2} s_{3}\right) \sum_{\substack{q_{i j} \in\left[X^{\left.\theta_{i j}, X^{\theta_{i j}}+\tau_{i j}\right]} \begin{array}{c}\forall(i, j) \in I_{\mathcal{C}} \\ q_{21} \equiv 1\left(\bmod D_{q_{2}}\right)\end{array}\right.}} \sum_{\substack{\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \in \mathcal{H}^{\prime} \\ \prod_{j=1}^{6} q_{1 j}\left|q_{1}\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \\ q_{2}\right| q_{2}\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \\\left[d, s_{2} s_{3}\right]\left|q\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \\ d\right| q_{3}\left(a_{1}, a_{2}, a_{3}\right)}} h\left(q\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right)\right)$.

Proof. We remove the condition $\left(a_{2} a_{3}, q\left(a_{1}, a_{2}, a_{3}\right)\right)=1$ via Mobius inversion, giving

We write $s$ as $s=s_{2} s_{3}$ with $s_{2} \mid a_{2}$ and $s_{3} \mid a_{3}$, and write $a_{2}=s_{2} a_{2}^{\prime}, a_{3}=$ $s_{3} a_{3}^{\prime}$. Let $U_{3}(\mathcal{H})$ denote the contribution given by the $s>Z$ and $S_{04}(\mathcal{H})$ the remaining contribution with $s \leq Z$. Thus we are left to bound $U_{3}(\mathcal{H})$.

Since each $q_{i}\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right)$ has a finite number of prime factors in [ $\left.X^{\theta_{i j}}, X^{\theta_{i j}+\tau_{i j}}\right]$, there are $O(1)$ choices of the $q_{i j}$, so

$$
U_{3}(\mathcal{H}) \ll \sum_{d \leq Z} \mu^{2}(d) \sum_{Z<s_{2} s_{3} \ll N_{\mathcal{H}}^{1 / 4}} \mu^{2}\left(s_{2} s_{3}\right) \sum_{\substack{\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \in \mathcal{H}^{\prime} \\[d, s]\left|q\left(a_{1}, a_{2}^{\prime} s_{2}, a_{3}^{\prime} s_{3}\right) \\ d\right| q_{3}\left(a_{1}, a_{2}^{\prime} s_{2}, a_{3}^{\prime} s_{3}\right)}} 1
$$

The form $q$ is monic of degree 6 in $a_{1}$ (by 5.24, 5.25) and [ $d, s_{2} s_{3}$ ] is squarefree, so given $s_{2}, s_{3}, a_{2}^{\prime}, a_{3}^{\prime}$ there are $O\left(6^{\omega\left(\left[a, s_{2} s_{3}\right]\right)}\right)$ choices of $a_{1}\left(\bmod \left[d, s_{2} s_{3}\right]\right)$ such that $q\left(a_{1}, a_{2}^{\prime} s_{2}, a_{3}^{\prime} s_{3}\right)=0\left(\bmod \left[d, s_{2} s_{3}\right]\right)$. Since $\left(a_{1}, a_{2}^{\prime} s_{2}, a_{3}^{\prime} s_{3}\right) \in \mathcal{H}^{\prime}$ we obtain

$$
\begin{aligned}
U_{3}(\mathcal{H}) & \ll \sum_{d<Z} \mu^{2}(d) \sum_{Z<s_{2} s_{3} \ll N_{\mathcal{H}}^{1 / 4}} \mu^{2}\left(s_{2} s_{3}\right) 6^{\omega\left(\left[s_{2} s_{3}, d\right]\right)}\left(\frac{\eta_{1} A_{2}}{s_{2}}+1\right)\left(\frac{\eta_{1} A_{3}}{s_{3}}+1\right)\left(\frac{\eta_{1} A_{1}}{\left[s_{2} s_{3}, d\right]}+1\right) \\
& \ll Z N_{\mathcal{H}}^{1 / 4+\varepsilon}+Z N_{\mathcal{H}}^{1 / 4+\varepsilon}\left(\left|A_{1}\right|+\left|A_{2}\right|+\left|A_{3}\right|\right)+\frac{A_{1} A_{2} A_{3} \eta_{1}^{2}}{\min \left(A_{1}, A_{2}, A_{3}\right)} Z X^{\varepsilon} \\
& +\eta_{1}^{3} A_{1} A_{2} A_{3} \sum_{d<Z} \sum_{s>Z} \frac{6^{\omega([d, s])}}{s[s, d]} .
\end{aligned}
$$

This final term is seen to be $O\left(\eta_{1}^{3} A_{1} A_{2} A_{3}(\log Z)^{O(1)} / Z\right)$. Since $\max \left(A_{1}, A_{2}, A_{3}\right) \ll$ $N_{\mathcal{H}}^{1 / 4}$ and $Z=(\log X)^{O(1)}$, this gives

$$
U_{3}(\mathcal{H}) \ll \frac{\eta_{1}^{3} A_{1} A_{2} A_{3}}{Z^{1 / 2}}+N_{\mathcal{H}}^{1 / 2+\epsilon}
$$

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

$$
S_{04}(\mathcal{H})=S_{05}(\mathcal{H})+O\left(\frac{\eta_{1}^{3} A_{1} A_{2} A_{3}}{Z}\right)
$$

where
$S_{05}(\mathcal{H}):=\sum_{\substack{u \leq Z^{20} \\ d \leq Z \\ s_{2} s_{3} \leq Z}} \mu(d) \mu\left(s_{2} s_{3}\right) \ell(u) \sum_{\substack{q_{i j} \in\left[X^{\theta_{i j}, X^{\theta_{i j}+\tau_{i j}}} \begin{array}{c}\forall(i, j) \in I_{C} \\ q_{21} \equiv 1\left(\bmod D_{q_{2}}\right)\end{array}\right.}} \sum_{\substack{\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \in \mathcal{H}^{\prime} \\ \prod_{j=1}^{6} q_{1 j}\left|q_{1}\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \\ q_{21}\right| q_{2}\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \\\left[\begin{array}{c}\left.d, s_{2} s_{3}, u\right]\left|q\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right) \\ d\right| q_{3}\left(a_{1}, a_{2}, a_{3}\right) \\\left(s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right)=30, a_{1} \equiv 1(\bmod 30) \\ s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime} \equiv 30(\bmod 900)\end{array}\right.}} 1$,
and $\ell$ is the multiplicative function defined by

$$
\ell\left(p^{\nu}\right):= \begin{cases}\frac{g(p)-2}{p-g(p)}, & \text { if } p>q_{0} \text { and } \nu=1, \\ -1, & \text { if } 7 \leq p \leq q_{0} \text { and } \nu=1, \\ -h(p), & \text { if } \nu=2, \\ 0, & \text { if } \nu \geq 3,\end{cases}
$$

with $q_{0}$ given by 6.1.
Proof. Recalling 8.5 , we see that $h=1 * \ell$ where $\ell$ is as given by the lemma. In particular,

$$
h\left(q\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right)\right)=\sum_{u \mid q\left(a_{1}, s_{2} a_{2}^{\prime}, s_{3} a_{3}^{\prime}\right)} \ell(u) .
$$

Since $a_{1} \equiv 1(\bmod 30)$ and $30 \mid\left(a_{2}, a_{3}\right),(u, 30)=1$. 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 $u=v^{2} w$ with $\mu^{2}(v w)=1$. 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 $v^{2}>Z^{10} \geq w$.

First we bound $U_{41}(\mathcal{H})$ with $w>Z^{10}$. Since $q_{0}>10$, we see that $|\ell(u)| \leq 10^{\omega(v w)} / w$. Following an entirely analogous argument to our bound for $U_{2}(\mathcal{H})$ in Lemma 8.3 we can find that

$$
\begin{aligned}
U_{41}(\mathcal{H}) & \ll Z \sum_{\substack{s_{2} s_{3}<Z \\
\mu^{2}\left(s_{2} s_{3}\right)=1}} \sum_{\substack{w \geq Z^{10} \\
w v^{2} \mid q}} \mu^{2}(v w) \frac{(60)^{\omega(v w)}}{w}\left(\frac{\eta_{1} A_{1}}{w v^{2}}+1\right) \frac{\eta_{1}^{2} A_{2} A_{3}}{s_{2} s_{3}} \\
& \ll A_{2} A_{3} X^{\varepsilon}+\eta_{1}^{3} A_{1} A_{2} A_{3}(\log X) Z^{-3} \ll \frac{A_{1} A_{2} A_{3}}{Z} .
\end{aligned}
$$

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

$$
U_{42}(\mathcal{H}) \leq V^{\prime}(\mathcal{H})+\sum_{(i, j) \in I_{\mathcal{C}}} V_{i j}(\mathcal{H}),
$$

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

First we consider $V_{21}(\mathcal{H})$. By (6.6), we have $\sum_{i=1}^{6} \theta_{1 i}+\theta_{21}>1+$ $\alpha_{0}$. We recall $q_{1}\left(a_{1}, a_{2} a_{3}\right) \ll X^{1+\alpha_{0}}$ for all $\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}$ and that $\prod_{j=1}^{6} q_{1 j} \mid q_{1}\left(a_{1}, a_{2}, a_{3}\right)$ with $\prod_{j=1}^{6} q_{1 j} \gg X^{\sum_{j=1}^{6} \theta_{1 j}}$. Therefore we must have that $\left(q_{21}, q_{1}\left(a_{1}, a_{2}, a_{3}\right)\right)=1$. Since $\alpha_{0}<1 / 19$ by (6.4) and $q_{21}^{2} \leq$ $X^{2 \theta_{21}+2 \tau_{21}} \leq X^{1 / 4-7 \alpha_{0} / 8} \leq \min \left(A_{1}, A_{2}, A_{3}\right)$ by (6.8) and (8.14), we deduce that

$$
\begin{aligned}
V_{21}(\mathcal{H}) & \ll X^{\varepsilon} \sum_{\substack{q_{21} \in\left[X^{\theta_{21}, X^{\left.\theta_{21}+\tau_{21}\right]}}\right.}} \sum_{\substack{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\
q_{21}^{2} \mid q_{2}\left(a_{1}, a_{2}, a_{3}\right)}} 1 \\
& \ll X^{-\theta_{21}+\varepsilon} A_{1} A_{2} A_{3} .
\end{aligned}
$$

We now consider $V_{1 j}(\mathcal{H})$. As with $V_{21}(\mathcal{H})$, we can't have $q_{1 j}^{2} \mid q_{1}\left(a_{1}, a_{2}, a_{3}\right)$ by size considerations and 6.6). Therefore if $q_{1 i}^{2} \mid q\left(a_{1}, a_{2}, a_{3}\right)$ then $q_{1 i} \mid\left(q_{1}\left(a_{1}, a_{2}, a_{3}\right), q_{2}\left(a_{1}, a_{2}, a_{3}\right)\right)$, and so Lemma 5.13 shows that $P\left(\left(a_{2}-c_{3} a_{3}\right) \overline{a_{3}}\right) \equiv 0\left(\bmod q_{1 i}\right)$. Again, we have that $q_{1 j} \leq \min \left(A_{1}, A_{2}, A_{3}\right)$. Thus we have

$$
\begin{aligned}
V_{1 i}(\mathcal{H}) & \ll X^{\varepsilon} \sum_{\substack{q_{1 i} \in\left[X^{\theta_{1 i}, X^{\left.\theta_{1 i}+\tau_{1 i}\right]}}\right.}} \sum_{\substack{\left(a_{2}, a_{3}\right) \in\left[A_{2}, A_{2}\left(1+\eta_{1}\right)\right] \times\left[A_{3}, A_{3}\left(1+\eta_{1}\right)\right] \\
P\left(\left(a_{2}-c_{3} a_{3}\right) \overline{a_{3}}\right) \equiv 0\left(\bmod q_{1 i}\right)}} \sum_{\substack{a_{1} \in\left[A_{1}, A_{1}\left(1+\eta_{1}\right)\right] \\
q_{1 i} \mid q_{1}\left(a_{1}, a_{2}, a_{3}\right)}} 1 \\
& \ll X^{-\theta_{1 i}+\varepsilon} A_{1} A_{2} A_{3} .
\end{aligned}
$$

Finally, we are left to bound $V^{\prime}(\mathcal{H})$. Each $v$ counted in $V^{\prime}(\mathcal{H})$ may factored as $v=v_{1} v_{2} v_{3}$, with

$$
v_{1}:=\prod_{\substack{p\left|v \\ p^{2}\right| q_{1}\left(a_{1}, a_{2}, a_{3}\right)}} p, \quad v_{2}:=\prod_{\substack{p\left|v / v_{1} \\ p^{2}\right| q_{2}\left(a_{1}, a_{2}, a_{3}\right)}} p, \quad v_{3}:=\frac{v}{v_{1} v_{2}} .
$$

Since $v$ was squarefree, we see that $v_{1}, v_{2}, v_{3}$ are pairwise coprime and squarefree.

By Lemma 5.13 again, $P\left(\left(a_{2}-c_{3} a_{3}\right) \overline{a_{3}}\right) \equiv 0\left(\bmod v_{3}\right)$. In $V^{\prime}(\mathcal{H}), v$ is coprime with all the $q_{i j}$, and so for any $a_{1}, a_{2}, a_{3} \in \mathcal{H}$

$$
\begin{align*}
& v_{1}^{2} v_{3} \ll \frac{q_{1}\left(a_{1}, a_{2}, a_{3}\right)}{\prod_{j=1}^{5} q_{1 j}} \ll X^{1+\alpha_{0}-\sum_{j=1}^{5} \theta_{1 j}}<\eta_{1} A_{2},  \tag{8.19}\\
& v_{2}^{2} v_{3} \ll \frac{q_{2}\left(a_{1}, a_{2}, a_{3}\right)}{q_{21}} \ll X^{\left(1+\alpha_{0}\right) / 2-\theta_{21}} . \tag{8.20}
\end{align*}
$$

Thus we have
$V^{\prime}(\mathcal{H}) \ll \sum_{\substack{s, d<Z \\ \mu^{2}(d) \mu^{2}(s)=1}} \sum_{w<Z^{10}} \frac{10^{\omega(w)}}{w} \sum_{\substack{v_{1} v_{2} v_{3}>Z^{5} \\ \mu^{2}\left(w v_{1} v_{2} v_{3}\right)=1}} \sum_{\substack{a_{2} \in\left[A_{2}, A_{2}\left(1+\eta_{1}\right)\right] \\ a_{3} \in\left[A_{3}, A_{3}\left(1+\eta_{1}\right)\right] \\ P\left(\left(a_{2}-c_{3} a_{3}\right) \bar{a}_{3}\right) \equiv 0\left(\bmod v_{3}\right)}} \sum_{\substack{a_{1} \in\left[A_{1}, A_{1}\left(1+\eta_{1}\right)\right] \\ v_{1}^{2} v_{3}\left|q_{1}\left(a_{1}, a_{2}, a_{3}\right) \\ v_{2}^{2} v_{3}\right| q_{2}\left(a_{1}, a_{2}, a_{3}\right)}} 1$.
Let $d_{1} \in \mathbb{Z}\left[a_{2}, a_{3}\right]$ denote the discriminant of $q_{1}$ (viewing $q_{1}$ as a polynomial in $a_{1}$ ), and $d_{2} \in \mathbb{Z}\left[a_{2}, a_{3}\right]$ denote the discriminant of $q_{2}$. By Lemma 5.13 we see that the inner sum restricts $a_{1}$ to one of $O\left(6^{\omega\left(v_{1} v_{2} v_{3}\right)}\right)$ residue classes modulo $v_{1}^{2} v_{2}^{2} v_{3} /\left(v_{1}, d_{1}\left(a_{2}, a_{3}\right)\right)\left(v_{2}, d_{2}\left(a_{2}, a_{3}\right)\right)$. Thus

$$
\begin{equation*}
\sum_{\substack{a_{1} \in\left[A_{1}, A_{1}\left(1+\eta_{1}\right)\right] \\ v_{1}^{2} v_{3}\left|q_{1}\left(a_{1}, a_{2}, a_{3}\right) \\ v_{2}^{2} v_{3}\right| q_{2}\left(a_{1}, a_{2}, a_{3}\right)}} 1 \ll 6^{\omega\left(v_{1} v_{2} v_{3}\right)}\left(\frac{\eta_{1} A_{1}\left(v_{1}, d_{1}\left(a_{2}, a_{3}\right)\right)\left(v_{2}, d_{2}\left(a_{2}, a_{3}\right)\right)}{v_{1}^{2} v_{2}^{2} v_{3}}+1\right) . \tag{8.21}
\end{equation*}
$$

Let $I_{1}=\{(1,3),(1,4),(2,3),(2,4)\}$ be the set of the indexes $(i, j)$ such that $\left(r_{i}, r_{j}\right)$ is involved in the factorisation of $q_{1}$. We note that

$$
\begin{aligned}
& d_{1}\left(a_{2}, a_{3}\right)=\prod_{\substack{(i, j),(k, l) \in I_{1} \\
(i, j) \neq(k, l)}}\left(a_{2}\left(r_{i}+r_{j}-r_{k}-r_{\ell}\right)+a_{3}\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}-r_{k}^{2}-r_{\ell}^{2}-r_{k} r_{\ell}\right)\right) \\
& d_{2}\left(a_{2}, a_{3}\right)=-\left(a_{2}\left(r_{1}+r_{2}-r_{3}-r_{4}\right)+a_{3}\left(r_{1}^{2}+r_{1} r_{2}+r_{2}^{2}-r_{3}^{2}-r_{3} r_{4}-r_{4}^{2}\right)\right)^{2} .
\end{aligned}
$$

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 $d_{1}\left(a_{2}, a_{3}\right), d_{2}\left(a_{2}, a_{3}\right)$ in 8.21, we write $w_{i}=\left(v_{i}, d_{i}\left(a_{2}, a_{3}\right)\right)$ for $i=1,2$ and next forget the coprimality between $v_{i} / w_{i}$ and $d_{i}\left(a_{2}, a_{3}\right) / w_{i}$. This sum is thus bounded by

$$
\sum_{\substack{v_{1} v_{2} v_{3} \geq Z^{5} \\
v_{1}^{2} v_{3} \leq X^{1+\alpha_{0}-\sum_{j=1}^{6} \theta_{1 j}}}} \frac{6^{\omega\left(v_{1} v_{2} v_{3}\right)}}{v_{1}^{2} v_{2}^{2} v_{3}} \sum_{\substack{w_{1}\left|v_{1} \\
w_{2}\right| v_{2}}} w_{1} w_{2} \sum_{\begin{array}{c}
a_{2} \in\left[A_{2}, A_{2}\left(1+\eta_{1}\right)\right] \\
a_{3} \in\left[A_{3}, A_{3}\left(1+\eta_{1}\right)\right. \\
v_{1}^{2}\left(a_{2}, a_{3}\right) \equiv 0\left(\bmod w_{1}\right) \\
d_{2}\left(a_{2}, X_{3}\right) \equiv 0 \\
\mu^{2}\left(v_{1} v_{2} v_{0} v_{3}\right)=1
\end{array}} 1 .
$$

If the coefficient in $a_{2}^{2}$ in $d_{2}\left(a_{2}, a_{3}\right)$ is non zero, then the inner sum over $a_{2}, a_{3}$ is

$$
\ll \eta_{1} A_{3}\left(1+\frac{\eta_{1} A_{2}}{w_{1} w_{2} v_{3}}\right) 12^{\omega\left(w_{1} w_{2} v_{3}\right)},
$$

otherwise the condition $w_{2} \mid d_{2}\left(a_{2}, a_{3}\right)$ is equivalent to $w_{2} \mid d_{P} a_{3}$ 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

$$
\ll\left(1+\frac{\eta_{1} A_{3}}{w_{2}}\right)\left(1+\frac{\eta_{1} A_{2}}{w_{1} v_{3}}\right) 12^{\omega\left(v_{1} v_{2} v_{3}\right)} \ll 12^{\omega\left(w_{1} w_{2} v_{3}\right)}\left(1+\frac{\eta_{1} A_{3}}{w_{2}}+\frac{\eta_{1} A_{2}}{w_{1} v_{3}}+\frac{\eta_{1}^{2} A_{2} A_{3}}{w_{1} w_{2} v_{3}}\right) .
$$

Finally we obtain that

$$
\begin{aligned}
V^{\prime}(\mathcal{H}) & \ll Z^{2}(\log Z)^{10} \sum_{\substack{v_{1} v_{2} v_{3} \geq Z^{5} \\
v_{1}^{2} v_{3} \leq X^{1+\alpha_{0}-\sum_{j=1}^{6} \theta_{1 j}} \\
v_{2}^{2} v_{3} \leq X^{\left(1+\alpha_{0}\right) / 2-\theta_{21}} \\
\mu^{2}\left(v_{1} v_{2} v_{3}\right)=1}} 6^{\omega\left(v_{1} v_{2} v_{3}\right)}\left[\eta_{1}^{2} A_{2} A_{3}\right. \\
& \left.+\sum_{\substack{w_{1}\left|v_{1} \\
w_{2}\right| v_{2}}} \frac{12^{\omega\left(w_{1} w_{2} v_{3}\right)} \eta_{1} A_{1} w_{1} w_{2}}{v_{1}^{2} v_{2}^{2} v_{3}^{2}}\left(\eta_{1} A_{3}+\frac{\eta_{1} A_{2}}{w_{1} v_{3}}+\frac{\eta_{1}^{2} A_{2} A_{3}}{w_{1} w_{2} v_{3}}\right)\right] \\
& \ll Z^{-3}(\log Z)^{10} \eta_{1}^{3} A_{1} A_{2} A_{3}+Z^{3} \frac{A_{1} A_{2} A_{3}}{\min \left(A_{1}, A_{2}, A_{3}\right)} X^{3\left(1+\alpha_{0}\right) / 4-\sum_{(i, j) \in I_{\mathcal{C}}} \theta_{i j} / 2}
\end{aligned}
$$

By (8.14) and (6.6) we see that $X^{3\left(1+\alpha_{0}\right) / 4-\sum_{i j \in I_{\mathcal{C}}} \theta_{i j} / 2} \leq \min \left(A_{1}, A_{2}, A_{3}\right) X^{-\epsilon}$. Putting everything together then gives the result.

Lemma 8.6 (Removing $\left.\left(a_{2}, a_{3}\right) / 30=1\right)$. Let $S_{05}(\mathcal{H})$ be as given in Lemma 8.5. Then we have

$$
S_{05}(\mathcal{H})=S_{06}(\mathcal{H})+O\left(\frac{\eta_{1}^{3} A_{1} A_{2} A_{3}}{Z}\right)
$$

where
$S_{06}(\mathcal{H}):=\sum_{\substack{t \leq Z^{50} \\ u \leq Z^{20} \\ d \leq Z \\ s_{2} s_{3} \leq Z \\(t, 30)=1}} \mu(d) \mu\left(s_{2} s_{3}\right) \ell(u) \mu(t) \sum_{\substack{q_{i j} \in\left[X^{\left.\theta_{i j}, X^{\theta_{i j}}+\tau_{i j}\right]} \begin{array}{c}\forall(i, j) \in I_{\mathcal{C}} \\ q_{21} \equiv 1\left(\bmod D_{q_{2}}\right)\end{array}\right.}} \sum_{\substack{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\ \prod_{j=1}^{6} q_{1 j}\left|q_{1}\left(a_{1}, a_{2}, a_{3}\right) \\ q_{21}\right| q_{2}\left(a_{1}, a_{2}, a_{3}\right) \\\left[d, s_{2} s_{3}, u\right]\left|q\left(a_{1}, a_{2}, a_{3}\right) \\ d\right| q_{3}\left(a_{1}, a_{2}, a_{3}\right) \\\left[t, s_{2}\right]\left|a_{2} \\\left[t, s_{3}\right]\right| a_{3}\\}}^{\substack{a_{2}, a_{3} \equiv 30(\bmod 900) \\ a_{1} \equiv 1(\bmod 30)}} 1$.
Proof. Since we have $a_{2}, a_{3} \equiv 30(\bmod 900)$, we can detect $\left(a_{2}, a_{3}\right) \mid 30$ using Möbius inversion $\mathbf{1}_{\left(a_{2}, a_{3}\right) \mid 30}=\sum_{\substack{t \mid\left(a_{2}, a_{3}\right) \\(t, 30)=1}} \mu(t)$ and separately consider $(t, 30)=1$
the contribution $S_{06}(\mathcal{H})$ from terms with $t \leq Z^{50}$ and the contribution $U_{5}(\mathcal{H})$ from terms with $t>Z^{50}$. Since there are $O(1)$ choices of the $q_{i j}$ given a choice of $a_{1}, a_{2}, a_{3}$, we see that

$$
\begin{aligned}
U_{5}(\mathcal{H}) & \ll \sum_{t>Z^{50}} \sum_{\substack{u \leq Z^{20} \\
d, s_{2} s_{3} \leq Z}} \sum_{\substack{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\
t \mid\left(a_{2}, a_{3}\right)}} O(1) \\
& \ll Z^{30} \sum_{Z^{50}<t<\min \left(A_{2}, A_{3}\right)} \eta_{1} A_{1}\left(\frac{\eta_{1} A_{2}}{t}+1\right)\left(\frac{\eta_{1} A_{3}}{t}+1\right) \ll \frac{\eta_{1}^{3} A_{1} A_{2} A_{3}}{Z} .
\end{aligned}
$$

This gives the result.

### 8.4 Application of Theorem 4.1

Lemma 8.7 (Application of Theorem4.1). Let $S_{06}(\mathcal{H})$ be as in Lemma 8.6. Then we have

$$
S_{06}(\mathcal{H}) \gg \eta_{1}^{3} A_{1} A_{2} A_{3}
$$

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 $\left(q\left(a_{1}, a_{2}, a_{3}\right), 30\right)=1$ and thus we may impose that $\left(d s_{2} s_{3} t u, 30\right)=1$. Splitting $\left(a_{1}, a_{2}, a_{3}\right)$ into residue classes $\left(\bmod \left[t, u, d, s_{2}, s_{3}\right]\right)$, we see that

$$
\begin{equation*}
S_{06}(\mathcal{H})=\sum_{\substack{t \leq Z^{50} \\ u \leq Z^{20} \\ d \leq Z \\ s_{2} s_{3} \leq Z \\\left(d s_{2} s_{3} t u, 30\right)=1}} \mu(d) \mu\left(s_{2} s_{3}\right) \ell(u) \mu(t) \sum_{\mathbf{u}_{0} \in \mathcal{S}\left(d, s_{2}, s_{3}, t, u\right)} S_{07}\left(\mathbf{u}_{0},\left[d, s_{2}, s_{3}, t, u\right]\right) \tag{8.22}
\end{equation*}
$$

where

$$
\begin{aligned}
& S_{07}\left(\mathbf{u}_{0}, m\right):=\sum_{\substack{q_{i j} \in\left[X^{\theta}{ }_{i j}, X^{\theta_{i j}+\tau_{i j}} \begin{array}{c}
\forall(i, j) \in I_{\mathcal{C}} \\
q_{21} \equiv 1\left(\bmod D_{q_{2}}\right)
\end{array}\right.}} \sum_{\substack{\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{H}^{\prime} \\
\prod_{j=1}^{6} q_{1 j}\left|q_{1}\left(a_{1}, a_{2}, a_{3}\right) \\
q_{21}\right| q_{2}\left(a_{1}, a_{2}, a_{3}\right) \\
\left(a_{1}, a_{2}, a_{3}\right) \equiv \mathbf{u}_{0}(\bmod \bmod ) \\
a_{2}, a_{3} \equiv 30(\bmod 900), a_{1} \equiv 1 \text { (mod 30) }}} 1, \\
& \mathcal{S}\left(d, s_{2}, s_{3}, t, u\right):=\left\{\left(u_{1}, u_{2}, u_{3}\right)\left(\bmod \left[d, s_{2} s_{3}, t, u\right]\right):\left[d, s_{2} s_{3}, u\right] \mid q\left(u_{1}, u_{2}, u_{3}\right),\right. \\
& \left.d\left|q_{3}\left(u_{1}, u_{2}, u_{3}\right),\left[s_{2}, t\right]\right| u_{2},\left[s_{3}, t\right] \mid u_{3}\right\} .
\end{aligned}
$$

We now apply Theorem 4.1 on incomplete norms with $K=\mathbb{Q}\left(r_{1}+r_{3}\right)$, $\nu_{1}=1, \nu_{2}=r_{1}+r_{3}, \nu_{3}=r_{1}^{2}+r_{3}^{2}+r_{1} r_{3}$ and $\nu_{4}$ such that $\nu_{4}$ is in the ring of integers of $K$ and $\left(\nu_{1}, \nu_{2}, \nu_{3}, \nu_{4}\right)$ is a $\mathbb{Q}$-basis of $K$. By Theorem 4.1 (taking $X_{i}=A_{i}, \ell=5, \ell^{\prime}=3, \theta_{i}=\theta_{1 i} \frac{\log X}{\log A_{1}}, \theta_{i}^{\prime}=\left(\theta_{1 i}+\tau_{1 i}\right) \frac{\log X}{\log A_{1}}$, $\left.\tau=\theta_{21} \frac{\log X}{\log A_{1}}, \tau^{\prime}=\left(\theta_{21}+\tau_{21}\right) \frac{\log X}{\log A_{1}}\right)$, we have that

$$
S_{07}\left(\mathbf{u}_{0}, m\right)=(1+o(1)) \frac{\eta_{1}^{3} A_{1} A_{2} A_{3}}{30^{5} m^{3} \varphi\left(D_{q_{2}}\right)} \prod_{(i, j) \in I_{\mathcal{C}}} \log \left(1+\tau_{i j} / \theta_{i j}\right) .
$$

Here we have used the fact that $\sqrt{4.3)}$ and $(4.4)$ hold by $\sqrt{8.14)}$. 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 $\frac{4}{1+\alpha_{0}} \leq \frac{\log X}{\log A_{1}} \leq \frac{4}{1+\alpha_{0} / 2}$. Substituting this into our expression 8.22 for $S_{06}$, we find that

$$
\begin{equation*}
S_{06}(\mathcal{H})=(1+o(1)) \frac{\eta_{1}^{3}}{30^{5}} \frac{A_{1} A_{2} A_{3}}{\varphi\left(D_{q_{2}}\right)} \prod_{(i, j) \in I_{\mathcal{C}}} \log \left(1+\tau_{i j} / \theta_{i j}\right) \sum_{m \leq Z^{72}} \frac{L(m)}{m^{3}} \tag{8.23}
\end{equation*}
$$

where

$$
L(m):=\sum_{\substack{d \leq Z \\ s_{2} s_{3} \leq Z \\ u \leq Z^{2} \\\left(d s_{2} s_{3} t u, 30 \\ t<Z^{0} \\\left[d, s_{2} \leq s_{3}, t, u\right]=m\right.}} \mu(d) \mu\left(s_{2} s_{3}\right) \mu(t) \ell(u)\left|\mathcal{S}\left(d, s_{2}, s_{3}, t, u\right)\right| .
$$

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

$$
\begin{aligned}
L^{*}(m) & :=\sum_{\substack{[d, s, t, u]=m \\
\left(d s_{2} s_{3} t u, 30\right)=1}}|\mu(d) \mu(s) \mu(t) \ell(u)| \sum_{s_{2} s_{3}=s}\left|\mathcal{S}\left(d, s_{2}, s_{3}, t, u\right)\right|, \\
\tilde{L}(m) & :=\sum_{\substack{[d, s, t, u]=m \\
\left(d s_{2} s_{3} t u, 30\right)=1}} \mu(d) \mu(s) \mu(t) \ell(u) \sum_{s_{2} s_{3}=s}\left|\mathcal{S}\left(d, s_{2}, s_{3}, t, u\right)\right|,
\end{aligned}
$$

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

$$
\begin{aligned}
\sum_{m \leq Z^{72}} \frac{L(m)}{m^{3}} & =\sum_{m \leq Z} \frac{\tilde{L}(m)}{m^{3}}+O\left(\sum_{m>Z} \frac{L^{*}(m)}{m^{3}}\right) \\
& =\sum_{m} \frac{\tilde{L}(m)}{m^{3}}+O\left(\sum_{m>Z} \frac{\tau(m)^{5}}{m^{2}}\right) \\
& =\prod_{7 \leq p \leq q_{0}}\left(1+\frac{\tilde{L}(p)}{p^{3}}\right) \prod_{p>q_{0}}\left(1+\frac{\tilde{L}(p)}{p^{3}}\right)+O\left(\frac{1}{Z^{1 / 2}}\right) .
\end{aligned}
$$

From our bounds on $L^{*}$ we see that $\prod_{p>q_{0}}\left(1+\tilde{L}(p) / p^{3}\right) \gg 1$ and the product over $p \leq q_{0}$ 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 $7 \leq p \leq q_{0}$. If $p \mid\left[d, s_{2}, s_{3}\right]$ then for $u=1$ or $p$, we have

$$
\left|\mathcal{S}\left(d, s_{2}, s_{3}, u, 1\right)\right|=\left|\mathcal{S}\left(d, s_{2}, s_{3}, u, p\right)\right|
$$

Since $\ell(p)+\ell(1)=0$ when $7 \leq p \leq q_{0}$, we deduce

$$
\sum_{\left[d, s_{2}, s_{3}\right]=p} \sum_{\left[d, s_{2}, s_{3}, t, u\right]=p} \mu(d) \mu\left(s_{2} s_{3}\right) \mu(t) \ell(u)\left|\mathcal{S}\left(d, s_{1}, s_{2}, t, u\right)\right|=0 .
$$

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

$$
\tilde{L}(p)=1-p-\left|\left\{\left(u_{1}, u_{2}, u_{3}\right)(\bmod p): p \mid q\left(u_{1}, u_{2}, u_{3}\right)\right\}\right| .
$$

Then

$$
1+\tilde{L}(p) / p^{3} \geq\left(p^{3}-6 p^{2}-p+1\right) / p^{3}>0
$$

when $p \geq 7$. Thus $\sum_{m \leq Z^{72}} L(m) / m^{3} \gg 1$, and so substituting this into 8.23 and using the fact $\tau_{i j} / \theta_{i j} \gg 1$ 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

$$
S_{0} \gg \frac{1}{\log X} \sum_{\mathcal{H} \in \mathscr{H}_{\mathcal{R}}} \frac{A_{0} A_{1} A_{2} A_{3} \eta_{1}^{4}}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)}+O\left(\frac{1}{Z^{1 / 2}}\right)
$$

(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 $\theta_{0}$ sufficiently small and assuming that $\alpha_{0}$ satisfies (6.4).) We note that

$$
\sum_{\mathcal{H} \in \mathscr{H}_{\mathcal{R}}} \frac{A_{0} A_{1} A_{2} A_{3} \eta_{1}^{4}}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)}=\sum_{\mathcal{H} \subset \mathcal{R}} \frac{A_{0} A_{1} A_{2} A_{3} \eta_{1}^{4}}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)}-\sum_{\substack{\mathcal{H} \subset \mathcal{R} \\ \mathcal{H} \text { bad }}} \frac{A_{0} A_{1} A_{2} A_{3} \eta_{1}^{4}}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)}
$$

If $\mathcal{H}$ is bad, then $\max \left(A_{1}, A_{2}, A_{3}\right)^{4} \eta_{1}^{1 / 10} \geq q_{1}\left(A_{1}, A_{2}, A_{3}\right)$ or there exists $i \in\{0,1,2,3\}$ such that $\left|A_{i}\right|<\eta_{1} \max \left(\left|A_{0}\right|,\left|A_{1}\right|,\left|A_{2}\right|,\left|A_{3}\right|\right)$. The first inequality implies that there exists $(i, j) \in I_{\mathcal{C}}$ such that
$L_{i, j}\left(A_{1}, A_{2}, A_{3}\right):=\left|A_{1}+\left(r_{i}+r_{j}\right) A_{2}+\left(r_{i}^{2}+r_{i} r_{j}+r_{j}^{2}\right) A_{3}\right| \ll \eta_{1}^{1 / 40} \max \left(A_{1}, A_{2}, A_{3}\right)$.
Thus, by partial summation

$$
\begin{aligned}
& \sum_{\substack{\mathcal{H} \subset \mathcal{R} \\
\mathcal{H} \text { bad }}} \frac{A_{0} A_{1} A_{2} A_{3} \eta_{1}^{4}}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)} \ll \sum_{\substack{(i, j) \in I_{\mathcal{C}}}} \sum_{\substack{\text { ( } \\
X^{1-\frac{7 \alpha_{0}}{8}} \ll 2^{\ell}}} \sum_{\substack{\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathcal{R} \\
\ll X^{2} \frac{1+\alpha_{0}}{4}}} \frac{1}{A^{4}} \\
& +\sum_{i=0}^{3} \sum_{\substack{ \\
X^{1-\frac{7 \alpha_{0}}{8}}}} \sum_{\substack{ \\
<A \ll X^{\frac{1+\alpha_{0}}{4}}}} \frac{1}{\substack{\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathcal{R} \\
a_{j}=\eta_{1} A \\
\max \left(a_{0}, a_{1}, a_{2}, a_{3}\right) \ll A}} \\
& \ll \eta_{1}^{1 / 40} \log X \text {. }
\end{aligned}
$$

Similarly, we find by partial summation

$$
\begin{aligned}
\sum_{\mathcal{H} \subset \mathcal{R}} \frac{A_{0} A_{1} A_{2} A_{3} \eta_{1}^{4}}{\widetilde{N}_{P}\left(A_{0}, A_{1}, A_{2}, A_{3}\right)} & =(1+o(1)) \sum_{\left(a_{0}, a_{1}, a_{2}, a_{3}\right) \in \mathcal{R}} \frac{1}{\widetilde{N}_{P}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)} \\
& \gg \log X .
\end{aligned}
$$

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, $C l_{K}$ its class group. Let $\nu_{1}, \nu_{2}, \nu_{3}, \nu_{4} \in \mathcal{O}_{K}$ such that $\mathbf{v}=\left(\nu_{1}, \nu_{2}, \nu_{3}, \nu_{4}\right)$ is a $\mathbb{Q}$-basis of $K$. We suppose for convenience that $\nu_{1}=1$ and $K=\mathbb{Q}\left(\nu_{2}\right)$. We then define $\mathcal{O}_{\mathbf{v}}=\mathbb{Z}\left[\nu_{1}, \nu_{2}, \nu_{3}, \nu_{4}\right]$ 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 $\mathbb{Q}\left(r_{1}\right)$ encountered earlier.

There exists an integral basis of $\mathcal{O}_{K}, \mathbf{w}=\left(\omega_{1}, \omega_{2}, \omega_{3}, \omega_{4}\right)$ and some integers $w_{i j}, 1 \leq i \leq j \leq 4$, such that

$$
\begin{equation*}
\nu_{j}=\sum_{i=1}^{j} w_{i j} \omega_{i} \quad(j=1,2,3,4) \tag{9.1}
\end{equation*}
$$

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

### 9.1 From $\mathcal{O}_{K}$ to $\mathcal{O}_{\mathrm{v}}$ and vice-versa

We denote by $L_{\mathbf{w v}}=\left(w_{i j}\right)_{1 \leq i, j \leq 4}$ the matrix of $\mathbf{v}$ in $\mathbf{w}$ so that for all $1 \leq j \leq 4, \nu_{j}=\sum_{i=1}^{4} w_{i j} \omega_{i}$.

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

$$
\begin{equation*}
W=\left|w_{11} w_{22} w_{33} w_{44}\right| \in \mathbb{Z}^{*} \tag{9.2}
\end{equation*}
$$

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 $\mathcal{V}_{0} \subset\{0, \ldots, W-1\}^{4}$ such that for all $\mathbf{a} \in \mathbb{Z}^{4}$ we have

$$
\frac{1}{W} \sum_{i=1}^{4} a_{i} \nu_{i} \in \mathcal{O}_{K} \Leftrightarrow \exists \mathbf{u} \in \mathcal{V}_{0}: \mathbf{a} \equiv \mathbf{u}(\bmod W)
$$

Proof. Let $\alpha \in \mathcal{O}_{K}$. There exist $\left(a_{1}, a_{2}, a_{3}, a_{4}\right) \in \mathbb{Z}^{4}$ and $\left(a_{1}^{\prime}, a_{2}^{\prime}, a_{3}^{\prime}, a_{4}^{\prime}\right) \in$ $\mathbb{Q}^{4}$ such that $\alpha=\sum_{i=1}^{4} a_{i} \omega_{i}=\sum_{i=1}^{4} a_{i}^{\prime} \nu_{i}$. With our previous notation,

$$
\left(\begin{array}{l}
a_{1}^{\prime} \\
a_{2}^{\prime} \\
a_{3}^{\prime} \\
a_{4}^{\prime}
\end{array}\right)=\left(L_{\mathbf{w v}}\right)^{-1}\left(\begin{array}{l}
a_{1} \\
a_{2} \\
a_{3} \\
a_{4}
\end{array}\right) .
$$

The matrix $\left(L_{\mathbf{w v}}\right)^{-1}$ is of type $\frac{1}{W}\left(w_{i j}^{\prime}\right)_{1 \leq i, j \leq 4}$ where the coefficients $w_{i j}^{\prime}$ 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

$$
\sum_{j=1}^{4} a_{j} \nu_{j}=\sum_{i=1}^{4}\left(\sum_{j=1}^{4} w_{i j} a_{j}\right) \omega_{i} .
$$

Then for any $\mathbf{a}=\left(a_{1}, a_{2}, a_{3}, a_{4}\right) \in \mathbb{Z}^{4}, \frac{1}{W} \sum_{i=1}^{4} a_{i} \nu_{i} \in \mathcal{O}_{K}$ if and only if for all $1 \leq i \leq 4$, we have

$$
\sum_{j=1}^{4} w_{i j} a_{j} \equiv 0(\bmod W)
$$

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

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

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

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 $\left\|\mathbf{b}_{0}\right\| \ll B$. We suppose that $\mathfrak{b}_{0}=\left(W^{-1} \sum_{i=1}^{4}\left(\mathbf{b}_{0}\right)_{i} \nu_{i}\right)$ is an integral ideal whose norm satisfies $N\left(\mathfrak{b}_{0}\right)=B_{0}^{4} \gg B^{4}$. Let $q$ such that $W \mid q$ and $10 q W \leq \delta_{0} B$.

Then there exists a set $\mathcal{W}\left(\mathbf{b}_{0}\right)$ of $W^{4}$ elements $\beta_{0}^{\prime} \in \mathcal{O}_{K}$ with $\beta_{0}^{\prime}=$ $W^{-1} \sum_{i=1}^{4}\left(\mathbf{b}_{0}^{\prime}\right)_{i} \nu_{i}$ and with $\mathbf{b}_{0}^{\prime} \in \mathcal{C}$, such that for all $\mathbf{b} \in \mathcal{C}, \mathbf{b} \equiv \mathbf{b}_{0}(\bmod q)$ if and only if $\beta=\frac{1}{W} \sum_{i=1}^{4} b_{i} \nu_{i} \in \mathcal{O}_{K}$ and there exists $\beta_{0}^{\prime} \in \mathcal{W}\left(\mathbf{b}_{0}\right)$ with $\beta \equiv \beta_{0}^{\prime}(\bmod q)$.

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

Let $\beta_{0}:=\frac{1}{W} \sum_{i=1}^{4}\left(\mathbf{b}_{0}\right)_{i} \nu_{i}$. For all $\mathbf{v}=\left(v_{1}, \ldots, v_{4}\right) \in\{0, \ldots, W-1\}^{4}$, there exists $\mathbf{u}=\mathbf{u}\left(\mathbf{b}_{0}, \mathbf{v}\right) \in \mathbb{Z}^{4}$ such that $\mathbf{b}_{0}+q(\mathbf{v}+W \mathbf{u}) \in \mathcal{C}$ since $q W \leq \delta_{0} B$, the side length of $\mathcal{C}$. We will prove that the set
$\mathcal{W}:=\left\{\beta_{0}^{\prime}=\frac{1}{W} \sum_{i=1}^{4} b_{i}^{\prime} \nu_{i}\right.$ with $\left.\mathbf{b}^{\prime}=\mathbf{b}_{0}+q\left(\mathbf{v}+W \mathbf{u}\left(\mathbf{b}_{0}, \mathbf{v}\right)\right), \mathbf{v} \in\{0, \ldots, W-1\}^{4}\right\}$
satisfies the conclusion of the lemma.
First we suppose that $\mathbf{b} \equiv \mathbf{b}_{0}(\bmod q)$. This implies that there exist four integers $m_{1}, m_{2}, m_{3}, m_{4}$ such that $b_{i}=\left(\mathbf{b}_{0}\right)_{i}+q m_{i}$. We get

$$
\beta:=\frac{1}{W} \sum_{i=1}^{4} \mathbf{b}_{i} \nu_{i}=\frac{1}{W} \sum_{i=1}^{4}\left(\left(\mathbf{b}_{0}\right)_{i}+m_{i} q\right) \nu_{i}=\beta_{0}+\frac{q}{W} \sum_{i=1}^{4} m_{i} \nu_{i} .
$$

Since $W \mid q$, this implies that $\beta \in \mathcal{O}_{K}$. If we choose $\beta_{0}^{\prime}=\beta_{0}+\frac{q}{W} \sum_{i=1}^{4} v_{i} \nu_{i}+$ with $0 \leq v_{1}, \ldots, v_{4}<W$ such that $v_{i} \equiv m_{i}(\bmod W)$ then we would have $\beta=\beta_{0}^{\prime}+\frac{q}{W} \sum_{i=1}^{4}\left(m_{i}-v_{i}+W u_{i}\right) \nu_{i}$, and thus $\beta \equiv \beta_{0}^{\prime}(\bmod q)$.

Now we prove the reciprocal assertion. We suppose that there exists $\beta_{0}^{\prime} \in \mathcal{W}$ such that $\beta \equiv \beta_{0}^{\prime}(\bmod q)$. Then $\beta=\beta_{0}^{\prime}+q \gamma$ 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 $\frac{b_{i}}{W}=\frac{\left(\mathbf{b}_{0}\right)_{i}+q\left(v_{i}+W u_{i}+g_{i}\right)}{W}$. This implies that $\mathbf{b} \equiv \mathbf{b}_{0}(\bmod q)$.

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

$$
\begin{equation*}
\varrho_{\mathbf{v}}(\mathfrak{d}):=\frac{\left|\left\{\mathbf{a} \in[1, N(\mathfrak{d})]^{3}: \mathfrak{d} \mid\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)\right\}\right|}{N(\mathfrak{d})^{2}} . \tag{9.3}
\end{equation*}
$$

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

$$
\left|\left\{\mathbf{x} \in\left[1, p^{2}\right]^{3}: p^{2} \mid N\left(\sum_{i=1}^{3} x_{i} \nu_{i}\right)\right\}\right| \ll p^{4}
$$

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 $\mathfrak{a}, \mathfrak{b}, \varrho_{\mathbf{v}}(\mathfrak{a b})=\varrho_{\mathbf{v}}(\mathfrak{a}) \varrho_{\mathbf{v}}(\mathfrak{b})$ if $(N(\mathfrak{a}), N(\mathfrak{b}))=1$.
5. For $k \geq 3$, we have

$$
\left|\left\{\mathbf{x} \in\left[1, p^{k}\right]^{3}: p^{k} \mid N\left(\sum_{i=1}^{3} x_{i} \nu_{i}\right)\right\}\right| \ll k p^{11 k / 4} .
$$

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 $\nu_{1}, \nu_{2}, \nu_{3}$ 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

$$
\varrho_{\mathbf{v}}(\mathfrak{d})=\frac{\left|\left\{\mathbf{a} \in[1, N(\mathfrak{d})]^{3}: \mathfrak{d} \mid\left(a_{1} \omega_{1}+a_{2} \omega_{2}+a_{3} \omega_{3}\right)\right\}\right|}{N(\mathfrak{d})^{2}},
$$

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 $N\left(\nu_{1}\right) \neq 0$, for any choice of $x_{2}, x_{3}, g_{x_{2}, x_{3}}\left(x_{1}\right):=N\left(x_{1} \nu_{1}+x_{2} \nu_{2}+x_{3} \nu_{3}\right)$ is a non-zero polynomial of degree 4 in $x_{1}$. Thus, given $x_{2}, x_{3}$, if $N\left(x_{1} \nu_{1}+x_{2} \nu_{2}+x_{3} \nu_{3}\right) \equiv 0\left(\bmod p^{k}\right)$, we see that $\left\|x_{1}-\alpha\right\|_{p} \ll p^{-k / 4}$ for one of the 4 roots $\alpha$ of $g_{x_{2}, x_{3}}$ over $\overline{\mathbb{Q}_{p}}$. Thus there are $O\left(p^{3 k / 4}\right)$ choices of $x_{1} \in\left[1, p^{k}\right]$ for each choice of $x_{2}, x_{3}$. This gives the result.

Let $\gamma_{K}$ be the residue in $s=1$ of $\zeta_{K}$ and we define $\tilde{\mathfrak{S}}$ to be the Euler product $5^{5}$

$$
\begin{equation*}
\tilde{\mathfrak{S}}:=\prod_{\mathfrak{P}}\left(1-\frac{\varrho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\right)\left(1-\frac{1}{N(\mathfrak{P})}\right)^{-1} \tag{9.4}
\end{equation*}
$$

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

$$
\sum_{\substack{N(\mathfrak{d})<R \\(\mathfrak{d}, \mathfrak{J})=1 \\(N(\mathfrak{d}), m)=1}} \frac{\mu(\mathfrak{d}) \varrho_{\mathbf{V}}(\mathfrak{d})}{N(\mathfrak{d})} \log \frac{R}{N(\mathfrak{d})}=\frac{\tilde{\mathfrak{S}}}{\gamma_{K}} \prod_{\mathfrak{P} \mid(m) \mathfrak{I}}\left(1-\frac{\varrho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\right)^{-1}+O\left(2^{4 \omega((m) \mathfrak{I})} \exp (-c \sqrt{\log R})\right) .
$$

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 $\exp (-c \sqrt{\log R}) \prod_{\mathfrak{P} \mid J}(1-$ $\left.\frac{1}{N(\mathfrak{F})^{3 / 4}}\right)^{-1}$, which is clearly sufficient for our slightly stronger bound.

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

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

Proof. By Rankin's trick, we have

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

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

[^4]
### 9.2 Multiplication in $\mathcal{O}_{\mathrm{v}}$

Definition. For any vectors $\mathbf{d}, \mathbf{e} \in \mathbb{Z}^{4} \backslash\{\mathbf{0}\}$, 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 $\mathbf{d} \in \mathbb{Z}^{4} \backslash\{\mathbf{0}\}$ let $\Lambda_{\mathbf{d}}$ be the subset of $\mathbb{Z}^{4}$ defined by

$$
\Lambda_{\mathbf{d}}=\left\{\mathbf{e} \in \mathbb{Z}^{4}:(\mathbf{d} \diamond \mathbf{e})_{4}=0\right\}
$$

Then $\Lambda_{\mathbf{d}}$ is a lattice of rank 3 and $\operatorname{det}\left(\Lambda_{\mathbf{d}}\right) \ll\|\mathbf{d}\| / D$, where $D$ is the $G C D$ 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

$$
\nu_{i} \nu_{j}=\sum_{k=1}^{4} \lambda_{i j k} \nu_{k} .
$$

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

$$
\sum_{i=1}^{4}(\mathbf{d} \diamond \mathbf{e})_{i} \nu_{i}=\sum_{k=1}^{4}\left(\sum_{i, j=1}^{4} \lambda_{i j k} d_{i} e_{j}\right) \nu_{k}
$$

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

$$
\Lambda_{\mathbf{d}}=\left\{\mathbf{e} \in \mathbb{Z}^{4}: \sum_{j=1}^{4}\left(\sum_{i=1}^{4} \lambda_{i j 4} d_{i}\right) e_{j}=0\right\} .
$$

The terms $\sum_{i=1}^{4} \lambda_{i j 4} d_{i}$, 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 $\Lambda_{\mathrm{d}}$ has rank 3. By [7], the determinant of $\Lambda_{\mathrm{d}}$ is equal to the determinant of the dual lattice that is for us the lattice spanned by the vector

$$
T(\mathbf{d}):=\left(\begin{array}{c}
\sum_{i=1}^{4} \lambda_{i 14} d_{i}  \tag{9.5}\\
\sum_{i=1}^{4} \lambda_{i 24} d_{i} \\
\sum_{i=1}^{4} \lambda_{i 34} d_{i} \\
\sum_{i=1}^{4} \lambda_{i 44} d_{i}
\end{array}\right) .
$$

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

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

$$
\sum_{\max \left(\left|x_{1}\right|,\left|x_{2}\right|,\left|x_{3}\right|\right) \ll X} \tau\left(\sum_{i=1}^{3} x_{i} \nu_{i}\right)^{m} \ll X^{3}(\log X)^{O_{m}(1)} .
$$

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 $N(\mathfrak{d}) \ll$ $X^{1 / n}$

$$
\sum_{\substack{\max \left(\left|x_{1}\right|,\left|x_{2}\right|,\left|x_{3}\right|\right) \ll X \\ \mathfrak{d} \mid\left(\sum_{i=1}^{3} x_{i} \nu_{i}\right)}} 1 .
$$

Since the $\nu_{i}$ are linear combinations of some $\theta^{j}, j=0,1,2,3$ for $\theta$ such that $K=\mathbb{Q}(\theta)$, the condition $\mathfrak{d} \mid\left(\sum_{i=1}^{3} x_{i} \nu_{i}\right)$ can be split in the $x_{i}$ into arithmetic progression $(\bmod N(\mathfrak{d}))$, and thus the argument of [14 combined with Lemma 9.4 apply also in our case.

Lemma 9.9. Let $\mathbf{d} \in \mathbb{Z}^{4} \backslash\{\mathbf{0}\} \cap[-D, D]^{4}$ 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 $\left\|\mathbf{z}_{1}(\mathbf{d})\right\| \ll$ $D^{1 / 3}$ and

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

Furthermore we have

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

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
$\left|\left\{\mathbf{a} \in \mathbb{Z}^{3} \cap \mathcal{R}: \mathfrak{d} \mid\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right), \mathbf{a} \equiv \mathbf{a}_{0}(\bmod q)\right\}\right|=\frac{\varrho_{\mathbf{v}}(\mathfrak{d}) \operatorname{vol}(\mathcal{R})}{N(\mathfrak{d}) q^{3}}+O\left(N(\mathfrak{d})^{4} X^{2}\right)$.
Proof. The proof is identical as the proof of [14] Lemma 7.4] with $\mathbf{v}$ in place of $\left(1, \ldots, \theta^{n-1}\right)$. In fact, the arguments of [14] give a slightly stronger error term of $O\left(X^{2} \varrho_{\mathbf{v}}(N(\delta))(q N(\delta))^{-2}+\varrho_{\mathbf{v}}(N(\delta))\right)$.

### 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

$$
\Gamma=\left\{\sum_{i=1}^{3} a_{i} \nu_{i}: \mathbf{a} \in \mathbb{Z}^{3} \cap \mathcal{R}, \mathbf{a} \equiv \mathbf{u}_{0}(\bmod q)\right\} .
$$

$$
\begin{align*}
& \text { Let } \Gamma_{\mathfrak{d}}=\{\kappa \in \Gamma: \mathfrak{d} \mid(\kappa)\} \text {. Then we have } \\
& \sum_{\substack{N(\mathfrak{d}) \in[D, 2 D] \\
(N(\mathfrak{d}), q)=1}}| | \Gamma_{\mathfrak{d}}\left|-\frac{\varrho_{\mathbf{v}}(\mathfrak{d}) \operatorname{vol}(\mathcal{R})}{q^{3} N(\mathfrak{d})}\right| \ll X^{2} q^{1+o(1)} D^{1 / 3+o(1)}+D q^{4+o(1)} . \tag{9.6}
\end{align*}
$$

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 $C l_{K}$. 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 $\left|d_{i}\right| \ll D^{1 / n} q^{o(1)}$. Then $\delta_{\mathfrak{c}}:=\frac{1}{W N(c)} \sum_{i=1}^{4} d_{i} \nu_{i}$ is a generator of the principal fractional ideal $\mathfrak{d} \mathfrak{c}^{-1}$. In [14] it is proved that $\left|\sigma_{0}\left(\delta_{\mathrm{c}}\right)\right| \gg D^{1 / 4} q^{o(1)}$ for all embeddings $\sigma_{0}$.

Let $\alpha \in \Gamma_{\mathfrak{d}}$, so $(\alpha)=\mathfrak{a}^{\prime} \mathfrak{d}$ for some integral ideal $\mathfrak{a}^{\prime}$. Since $(\alpha)=\mathfrak{a}^{\prime} \mathfrak{c d c}{ }^{-1}$ and $(\alpha)$ and $\mathfrak{d}^{-1}=\left(\delta_{\mathfrak{c}}\right)$ are principal, $\mathfrak{a}^{\prime} \mathfrak{c}$ is principal too, so $\mathfrak{a}^{\prime} \mathfrak{c}=(\beta)$ 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 $\mathbf{b}=\left(b_{1}, b_{2}, b_{3}, b_{4}\right) \in \mathbb{Z}^{4}$ satisfies $(\mathbf{b}(\bmod W)) \in \mathcal{V}_{0}$. Then $(\alpha)=$ $(\beta)\left(\delta_{\mathfrak{c}}\right)$. Let $\mathbf{d}=\left(d_{1}, d_{2}, d_{3}, d_{4}\right)$. We have $W^{2} N(\mathfrak{c}) \beta \delta_{\mathfrak{c}}=\sum_{k=1}^{4}(\mathbf{d} \diamond \mathbf{b})_{k} \nu_{k}$.

$$
\beta \delta_{\mathfrak{c}}=\sum_{k=1}^{4} \frac{1}{W^{2} N(\mathfrak{c})}\left(\sum_{i, j=1}^{4} \ell_{i, j, k} b_{i} d_{i}\right) \nu_{k}
$$

The coefficient of $\nu_{i}$ are integers if and only $b_{1}, b_{2}, b_{3}, b_{4}$ satisfy some congruences modulo $W^{2} N(\mathfrak{c})$. We also need to impose that $\mathfrak{c} \mid(\beta)$. This is also equivalent to some congruences conditions modulo $W^{2} N(\mathfrak{c})$ for $b_{1}, b_{2}, b_{3}, b_{4}$. Let $q_{1}=\left[q, W^{2} N(\mathfrak{c})\right]$ and $\mathcal{V}_{0}^{\prime} \subset\left\{0 \ldots, q_{1}-1\right\}^{4}$ the set of r classes satisfying all these conditions and furthermore such that

$$
(\mathrm{d} \diamond \mathbf{b})_{4} \equiv 0\left(\bmod q_{1}\right) \text { and } \frac{(\mathrm{d} \diamond \mathbf{b})_{i}}{W^{2} N(\mathfrak{c})} \equiv\left(\mathbf{u}_{0}\right)_{i}(\bmod q) \text { for } 1 \leq i \leq 3
$$

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

$$
\left|\Gamma_{\mathfrak{J}}\right|=\sum_{\mathbf{b}_{0} \in V_{0}^{\prime}} \sum_{\substack{\mathbf{b} \in \mathbb{Z}^{4} \\ \mathbf{b} \equiv \mathbf{b}_{0}\left(\bmod \\ \delta_{\mathbf{c}} \beta \in \Gamma\right.}} 1 .
$$

The rest of the proof follows [14]. Let $\Lambda_{\mathrm{d}}$ 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 $\Lambda_{\mathrm{d}}$ such that $\mathbf{b}^{(1)} \equiv \mathbf{b}_{0}\left(\bmod q_{1}\right)\left(\right.$ when such $\mathbf{b}^{(1)}$ exists) and $\mathbf{b}^{(2)} \in \Lambda_{\mathfrak{o}_{\mathfrak{c}}}$
where $\sum^{\prime \prime}$ 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

$$
\begin{equation*}
m<(\log x)^{K} \tag{9.7}
\end{equation*}
$$

If $\mathbf{a} \in \mathcal{A}_{q_{1} \cdots q_{\ell}}\left(\mathbf{u}_{0}, m, p\right)$ then there exists $d \in \mathbb{N}$ such that $N\left(a_{1} \nu_{1}+a_{2} \nu_{2}+\right.$ $\left.a_{3} \nu_{3}\right)=d \prod_{i=1}^{\ell} q_{i}$. The conditions on $q_{i}$ imply that $\left(m, q_{1} \cdots q_{\ell}\right)=1$ 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 $m_{0}=\left(d, m^{\infty}\right)$ and recall the notation $\mathcal{X}=\prod_{i=1}^{3}\left[X_{i}, X_{i}\left(1+\eta_{1}\right)[\right.$ from 4.1). In almost cases, $m_{0}$ is small. Let

$$
\begin{equation*}
D_{0}:=(\log X)^{4 K} \tag{9.8}
\end{equation*}
$$

The contribution of the $\mathbf{a} \in \mathcal{X}$, such that $\mathbf{a} \equiv \mathbf{u}_{0}(\bmod m)$ and $m_{0}>D_{0}$, is less than

$$
\begin{align*}
\sum_{\substack{m_{0} \mid m^{\infty} \\
m_{0}>D_{0}}} \sum_{\substack{\mathbf{a} \in \mathcal{X} \\
\mathbf{a} \equiv \mathbf{u}_{0}(\bmod m) \\
N\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right) \equiv 0\left(\bmod m_{0}\right)}} 1 & \ll \eta_{1}^{3} \prod_{i=1}^{3} X_{i} \sum_{\substack{m_{0} \mid m^{\infty} \\
m_{0}>D_{0}}} \frac{4^{\omega\left(m_{0}\right)}}{m_{0} m^{2}} \\
& \ll \frac{\eta_{1}^{3} \prod_{i=1}^{3} X_{i}}{m^{2} \sqrt{D_{0}}} \sum_{\substack{m_{0} \mid m^{\infty} \\
m_{0}>D_{0}}} \frac{4^{\omega\left(m_{0}\right)}}{\sqrt{m_{0}}} \\
& \ll \frac{\eta_{1}^{3} \prod_{i=1}^{3} X_{i}}{D_{0}^{1 / 3}}
\end{align*}
$$

We now suppose that $m_{0} \leq D_{0}$. Let

$$
\begin{align*}
\mathcal{M}\left(m_{0}\right) & :=\left\{\mathbf{v}_{0} \in\left[1, m m_{0}\right]^{3}: \mathbf{v}_{0} \equiv u_{0}(\bmod m)\right. \\
& \left.N\left(\sum_{i=1}^{3}\left(\mathbf{v}_{0}\right)_{i} \nu_{i}\right) \equiv 0\left(\bmod m_{0}\right),\left(m, \frac{N\left(\sum_{i=1}^{3}\left(\mathbf{v}_{0}\right)_{i} \nu_{i}\right)}{m_{0}}\right)=1\right\} \tag{9.10}
\end{align*}
$$

Then for every $\mathbf{a} \in \mathcal{A}\left(\mathbf{u}_{0}, m\right)$ such that $m_{0}=\left(N\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right), m^{\infty}\right)$, there exists exactly one $\mathbf{v}_{0} \in \mathcal{M}\left(m_{0}\right)$ such that $\mathbf{a} \equiv \mathbf{v}_{0}\left(\bmod m m_{0}\right)$. Putting this together with 9.9) deduce that

$$
\begin{equation*}
\mathcal{A}_{q_{1} \cdots q_{\ell}}\left(\mathbf{u}_{0}, m, p\right)=\sum_{\substack{m_{0} \mid m^{\infty} \infty \\ m_{0} \leq D_{0}}} \sum_{\mathbf{v}_{0} \in \mathcal{M}\left(m_{0}\right)}\left|\mathcal{A}_{q_{1} \cdots q_{\ell}}\left(\mathbf{v}_{0}, m_{0} m, p\right)\right|+O\left(\frac{\eta_{1}^{3} \prod_{i=1}^{3} X_{i}}{D_{0}^{1 / 3}}\right) \tag{9.11}
\end{equation*}
$$

Any $\mathbf{a} \in \mathcal{A}\left(\mathbf{v}_{0}, m m_{0}\right)$ is such that the associated ideal $\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right)$ may be factored as $\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right)=\mathfrak{M}_{0} \mathfrak{J}$ with $N\left(\mathfrak{M}_{0}\right)=m_{0}$ and $(N(\mathfrak{J}), m)=1$. This property will simplify some GCD considerations in the next sections. Let

$$
\begin{equation*}
m^{\prime}:=m_{0} m \ll(\log x)^{5 K} \tag{9.12}
\end{equation*}
$$

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)

$$
\begin{equation*}
\widetilde{\mathcal{A}}=\left\{\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right): \mathbf{a} \in \mathcal{X}\right\} \tag{9.13}
\end{equation*}
$$

For any $\mathfrak{a} \in \widetilde{\mathcal{A}}$ there is exactly one $\left(a_{1}, a_{2}, a_{3}\right) \in \mathcal{X}$ such that $\mathfrak{a}=\left(a_{1} \nu_{1}+\right.$ $a_{2} \nu_{2}+a_{3} \nu_{3}$ ). We justify this in a similar way as in [14] Proof of Lemma 5.2 assuming Proposition $5.1 \mathrm{pp} .13-14$ ].

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 $\sigma$ and since $\alpha=N(\alpha) \prod_{\sigma \neq I d} \sigma(\alpha)^{-1}$ we have $\left|a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right| \gg \eta_{1}^{1 / 10} X$ by 4.4 and then

$$
\frac{\beta}{\alpha}=1+\frac{\beta-\alpha}{\alpha}=1+O\left(\eta_{1}^{9 / 10}\right)
$$

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

$$
\widetilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)=\left\{\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right) \in \widetilde{\mathcal{A}}: \mathbf{a} \equiv \mathbf{v}_{0}\left(\bmod m^{\prime}\right) \text { and } p \mid f\left(a_{1}, a_{2}, a_{3}\right)\right\}
$$

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

$$
\widetilde{\mathcal{A}}_{\mathfrak{d}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)=\left\{\mathfrak{a} \in \widetilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right): \mathfrak{d} \mid \mathfrak{a}\right\}
$$

Let $N_{0}^{4}=\min _{(\alpha) \in \tilde{\mathcal{A}}} N(\alpha)$. Let $\eta_{2}$ and $\eta_{3}$ defined by

$$
\begin{equation*}
\eta_{2}=\frac{1}{(\log X)^{K}}, \quad \eta_{3}=\eta_{2}^{10000 \ell^{2}} \tag{9.14}
\end{equation*}
$$

By the definition of $\mathcal{X}, N\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3}\right) \in\left[N_{0}^{4}, N_{0}^{4}\left(1+O\left(\eta_{1}\right)\right)\right]$ for all $\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3}\right) \in \widetilde{\mathcal{A}}$. We can choose $O\left(\eta_{3}^{-1} \eta_{1}\right)$ reals $X_{0}$ with $X_{0}^{4} \in\left[N_{0}^{4}, N_{0}^{4}\left(1+O\left(\eta_{1}\right)\right)\right]$ so that the sets

$$
\widetilde{\mathcal{A}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}, p\right)=\left\{\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right) \in \widetilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right): N\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right) \in\left[X_{0}^{4}, X_{0}^{4}+\eta_{3} X_{0}^{4}[ \},\right.\right.
$$

form a partition of $\widetilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)$. Next we introduce the sets

$$
\widetilde{\mathcal{A}}_{\mathfrak{d}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}, p\right)=\left\{\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right) \in \widetilde{\mathcal{A}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}, p\right): \mathfrak{d} \mid\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right)\right\}
$$

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

We are now ready to settle the connection between the set $\mathcal{A}_{q}\left(\mathbf{v}_{0}, m^{\prime}, p\right)$ in Theorem 4.1 and the sets of ideals just defined above. For any primes $q_{1}, \ldots, q_{\ell}$ with $q_{i} \in\left[X^{\theta_{i}}, X^{\theta_{i}^{\prime}}\right]$, we have

$$
\begin{equation*}
\left|\mathcal{A}_{q_{1} \cdots q_{\ell}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)\right|=\sum_{X_{0}} \sum_{N\left(\mathfrak{P}_{i}\right)=q_{i}}\left|\widetilde{\mathcal{A}}_{\mathfrak{P}_{1} \cdots \mathfrak{F}_{\ell}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}, p\right)\right| . \tag{9.15}
\end{equation*}
$$

Any ideal $\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)$ counted in 9.15 may be factored as

$$
\begin{equation*}
\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}\right)=\mathfrak{M}_{0} \mathfrak{I} \prod_{i=1}^{\ell} \mathfrak{P}_{i} \tag{9.16}
\end{equation*}
$$

where each $\mathfrak{P}_{i}$ is a prime ideal with norm in $\left[X^{\theta_{i}}, X^{\theta_{i}^{\prime}}\right]$ and $\mathfrak{I}$ is an ideal with

$$
\begin{equation*}
N(\mathfrak{I}) \in \mathcal{I}_{0}:=\left[\frac{X_{0}^{4} X^{-\sum_{i=1}^{\ell} \theta_{i}^{\prime}}}{m_{0}}, \frac{X_{0}^{4}\left(1+\eta_{3}\right) X^{-\sum_{i=1}^{\ell} \theta_{i}}}{m_{0}}\right]=\left[I_{1}, I_{2}\right] \tag{9.17}
\end{equation*}
$$

say.
We choose now $O\left(\eta_{3}^{-1} \log X\right)$ reals $I \in \mathcal{I}_{0}$ such that $\mathcal{I}_{0}$ is covered by the union of the intervals $\left[I, I\left(1+\eta_{3}\right)\left[\right.\right.$. Let $\hat{\mathcal{I}}_{0}$ denote the set of these reals $I$.

Since we have $\left(N\left(\sum_{i=1}^{3} a_{i} \nu_{i}\right) / m_{0}, m\right)=1$ when $\mathbf{a} \equiv \mathbf{v}_{0}\left(\bmod m^{\prime}\right)$, we have $\left(m^{\prime}, N(\mathfrak{I}) \prod_{i=1}^{\ell} N\left(\mathfrak{P}_{i}\right)\right)=1$.

For brevity we will write $\widetilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)$ in place of $\widetilde{\mathcal{A}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}, p\right)$ when the context will be clear.

To have a precise control of the size of the norms of some ideals, we cover each interval $\left[\theta_{i}, \theta_{i}^{\prime}\right]$ by $O\left(\eta_{2}^{-2}\right)$ distinct intervals of size $O\left(\eta_{2}^{2}\right)$ so that,

$$
\begin{equation*}
\prod_{i=1}^{\ell}\left[\theta_{i}, \theta_{i}^{\prime}\right]=\cup_{\mathbf{l} \in E} \mathcal{R}(\mathbf{l}) \tag{9.18}
\end{equation*}
$$

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

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 $\ell^{\prime}$ coordinates and $\mathcal{R}_{1}(\mathbf{l})$ the final $\ell-\ell^{\prime}$ coordinates.

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

$$
\mathbf{1}_{\mathcal{R}}(\mathfrak{a})= \begin{cases}1, & \mathfrak{a}=\mathfrak{p}_{1} \cdots \mathfrak{p}_{s} \text { with } N\left(\mathfrak{p}_{i}\right)=X^{e_{i}} \text { and }\left(e_{1}, \ldots, e_{s}\right) \in \mathcal{R} \\ 0, & \text { otherwise }\end{cases}
$$

Thus we need to study the quantity

$$
\begin{equation*}
T(\mathcal{R}(\mathbf{l})):=\sum_{X^{\tau} \leq p \leq X^{\tau^{\prime}}} \sum_{\mathfrak{J} \in \mathcal{I} \mathfrak{M}_{0} \mathfrak{J} \mathfrak{a} \in \mathcal{A}\left(\mathbf{v}_{0}, m^{\prime}, p\right)} \mathbf{1}_{\mathcal{R}(\mathbf{l})}(\mathfrak{a}), \tag{9.19}
\end{equation*}
$$

with

$$
\begin{equation*}
\mathcal{I}:=\left\{\mathfrak{I}: N(\mathfrak{I}) \in\left[I, I+\eta_{3} I[,(N(\mathfrak{I}), m)=1\}\right.\right. \tag{9.20}
\end{equation*}
$$

for each of the $O\left(\eta_{2}^{-2 \ell}\right)$ 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

$$
\begin{align*}
& c_{\mathcal{S}}(t)=\iint_{\substack{\left(e_{1}, \ldots, e_{s}\right) \in \mathcal{S} \\
\sum_{i=1}^{s} e_{i} \in I_{t}}} \frac{d e_{1} \cdots d e_{s}}{\eta_{3}^{1 / 2} \prod_{i=1}^{s} e_{i}},  \tag{9.21}\\
& \text { where } I_{t}:=\left[\frac{\log t}{\log X}, \frac{\log \left(t+\eta_{3}^{1 / 2} t\right)}{\log X}\right] .
\end{align*}
$$

In this previous definition we have $\sum_{i=1}^{s} e_{i} \in I_{t}$ if and only if $X^{\sum_{i=1}^{s} e_{i}} \in$ $\left[t, t\left(1+\sqrt{\eta_{3}}\right)\right]$. 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 $\mathcal{S}=\prod_{i=1}^{s}\left[u_{i}, u_{i}^{\prime}\right]$ 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 $\mathcal{S}=\prod_{i=1}^{s}\left[u_{i}, u_{i}^{\prime}\right]$ 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]:

$$
c_{\mathcal{S}}(t) \leq \frac{1}{\sqrt{\eta_{3}}} \iint_{\substack{e_{i} \in\left[u_{i}, u_{i}^{\prime}\right] \\ 1 \leq i \leq s-1}}\left[\int_{e_{s} \in I_{t}-\sum_{i=1}^{s-1} e_{i}} \frac{\mathrm{~d} e_{s}}{u_{s}}\right] \prod_{i=1}^{s-1} \frac{\mathrm{~d} e_{i}}{u_{i}} .
$$

The integral over $e_{s}$ is $O\left(\sqrt{\eta_{3}}(\log X)^{-1}\right)$ and the contribution of the other integrals is $O(1)$.

Let $\epsilon_{00}>0$ and

$$
\begin{equation*}
R:=X^{\epsilon_{00}} \tag{9.22}
\end{equation*}
$$

The approximate weights of $\mathbf{1}_{\mathcal{R}_{2}}$ are defined by

$$
\begin{equation*}
\tilde{\mathbf{1}}_{\mathcal{R}_{2}}(\mathfrak{b}):=c_{\mathcal{R}_{2}}(N(\mathfrak{b})) \sum_{\mathfrak{d} \mid \mathfrak{b}} \lambda_{\mathfrak{l}} \tag{9.23}
\end{equation*}
$$

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 $\chi^{*}$. (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

$$
T(\mathcal{R})=T_{\text {sieve }}(\mathcal{R})+T_{1}(\mathcal{R})
$$

where

$$
\begin{align*}
T_{\text {sieve }}(\mathcal{R}) & :=\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\
p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\mathfrak{T} \in \mathcal{I}_{\mathfrak{M}_{0} \mathcal{J}_{\mathfrak{a b}} \in \tilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)}} \mathbf{1}_{\mathcal{R}_{1}}(\mathfrak{a}) \tilde{\mathbf{1}}_{\mathcal{R}_{2}}(\mathfrak{b}),  \tag{9.24}\\
T_{1}(\mathcal{R}) & :=\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\
p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\mathfrak{J} \in \mathcal{I}_{\mathfrak{M}_{0} \mathcal{J}_{\mathfrak{a b}} \in \tilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)}} \sum_{\mathcal{R}_{1}(\mathfrak{a})\left(\mathbf{1}_{\mathcal{R}_{2}}(\mathfrak{b})-\tilde{\mathbf{1}}_{\mathcal{R}_{2}}(\mathfrak{b})\right),} \tag{9.25}
\end{align*}
$$

and

$$
\begin{equation*}
P_{1}:=X^{\tau}, \quad P_{2}:=X^{\tau^{\prime}} \tag{9.26}
\end{equation*}
$$

For brevity again we will write $T_{\text {sieve }}(\mathcal{R})$ and $T_{1}(\mathcal{R})$ in place of $T_{\text {sieve }}\left(\mathcal{R}, \mathbf{v}_{0}\right)$ and $T_{1}\left(\mathcal{R}, \mathbf{v}_{0}\right)$ 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 $T_{\text {sieve }}$ ). If we have

$$
\epsilon_{00}<\sum_{j=1}^{\ell^{\prime}} \theta_{j}-1-12 \tau^{\prime}
$$

then

$$
T_{\text {sieve }}(\mathcal{R})=M(\mathcal{R})+E_{1}(\mathcal{R})
$$

where

$$
\begin{aligned}
& M(\mathcal{R})=\left(2+O\left(\eta_{3}^{1 / 2}\right)\right) \eta_{3}\left|\widetilde{\mathcal{A}}\left(X_{0}\right)\right| c_{\mathcal{R}}\left(X_{0}^{4} / m I\right) \frac{g\left(m^{\prime}\right)}{m^{\prime 3}} \frac{\log \left(P_{2} / P_{1}\right)}{\varphi\left(D_{f}\right)}, \\
& g\left(m^{\prime}\right)=\prod_{\mathfrak{P} \mid\left(m^{\prime}\right)}\left(1-\frac{\varrho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\right)^{-1}, \\
& \sum_{\mathcal{R}} \sum_{X_{0}} \sum_{I \in \hat{\mathcal{I}}_{0}}\left|E_{1}(\mathcal{R})\right| \ll \eta_{3}^{1 / 2} \eta_{1}^{-2 \ell}(\log X)^{11} \prod_{i=1}^{3} X_{i} .
\end{aligned}
$$

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

$$
\tau^{\prime}<\min \left(\frac{4-2 \theta_{1}^{\prime}-\ldots-2 \theta_{\ell^{\prime}}^{\prime}}{100}, \frac{\theta_{1}+\cdots+\theta_{\ell^{\prime}}-1}{100}\right)
$$

then for any $K>0$ we have

$$
T_{1}(\mathcal{R}) \ll K_{K} \frac{\prod_{i=1}^{3} X_{i}}{(\log X)^{K}} .
$$

We remark that we are assuming the general setup in Propositions 9.13 and 9.14 in particular, the constants $\theta_{1}, \theta_{1}^{\prime}, \ldots, \theta_{\ell}, \theta_{\ell}^{\prime}$ 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 $p \in\left[P_{1}, P_{2}\right]$
introduces few additional complications to $T_{\text {sieve }}$ 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

$$
\begin{equation*}
\mathcal{A}_{q_{1} \cdots q_{\ell}}\left(\mathbf{u}_{0}, m, p\right)=\sum_{\substack{m_{0} \mid m^{\infty} \\ m_{0} \leq D_{0}}} \sum_{\mathbf{v}_{0} \in \mathcal{M}\left(m_{0}\right)}\left|\widetilde{\mathcal{A}}_{q_{1} \cdots q_{\ell}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)\right|+O\left(\frac{\eta_{1}^{3} \prod_{i=1}^{3} X_{i}}{D_{0}^{1 / 3}}\right) . \tag{9.27}
\end{equation*}
$$

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

$$
\begin{aligned}
& \left|\widetilde{\mathcal{A}}_{q_{1} \cdots q_{\ell}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)\right|=\sum_{X_{0}} \sum_{N\left(\mathfrak{F}_{i}\right)=q_{i}}\left|\widetilde{\mathcal{A}}_{\mathfrak{P}_{1} \cdots \mathfrak{P}_{\ell}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}, p\right)\right| \\
& =\sum_{X_{0}} \sum_{I \in \hat{\mathcal{I}}_{0}} \sum_{N\left(\mathfrak{P}_{i}\right)=q_{i}} \sum_{\substack{\mathfrak{J} \in \mathcal{I} \\
\mathfrak{M}_{0} \mathfrak{J} \\
\prod_{i=1}^{\ell} \mathfrak{P}_{i} \in \tilde{A}\left(\mathbf{v}_{0}, m^{\prime}, p\right)}} 1 \\
& =\sum_{X_{0}} \sum_{I \in \hat{\mathcal{I}}_{0}} \sum_{\substack{\mathcal{R}_{1}, \mathcal{R}_{2} \\
\prod_{i=1}^{\ell}\left[\theta_{i}, \theta_{i}^{\prime}\right]=\sqcup \mathcal{R}_{1} \times \mathcal{R}_{2}}} \sum_{\mathfrak{J} \in \mathcal{I}} \sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_{1}}(\mathfrak{a}) \sum_{\substack{\mathfrak{b} \\
\mathfrak{J} \mathfrak{M}_{0} \mathfrak{a b} \in \hat{A}\left(\mathbf{v}_{0}, m^{\prime}, p\right)}} \mathbf{1}_{\mathcal{R}_{2}}(\mathfrak{b}) .
\end{aligned}
$$

By assumption of Theorem 4.1. we have $\tau^{\prime}<\left(\sum_{i=1}^{\ell^{\prime}} \theta_{i}-1\right) / 100$, and so choosing $\epsilon_{00}$ sufficiently small means that the hypothesis of Proposition 9.13 is satisfied. Thus, summing over $p \in\left[P_{1}, P_{2}\right]$ (which is $\left[X^{\tau}, X^{\tau^{\prime}}\right]$ be (9.26) ) and applying Propositions 9.13 and 9.14 (with a suitably large constant $K$ ) gives

$$
\begin{align*}
& \sum_{p \in\left[P_{1}, P_{2}\right]}\left|\widetilde{\mathcal{A}}_{q_{1} \cdots q_{\ell}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)\right|=\sum_{X_{0}} \sum_{\substack{I \in \hat{\mathcal{I}}_{0}}} \sum_{\substack{\mathcal{R}=\mathcal{R}_{1} \times \mathcal{R}_{2} \\
\prod_{i=1}^{\ell}\left[\theta_{i}, \theta_{i}^{\prime}\right]=\sqcup \mathcal{R}_{1} \times \mathcal{R}_{2}}}\left(T_{\text {sieve }}(\mathcal{R})+T_{1}(\mathcal{R})\right) \\
& =\left(2+O\left(\eta_{3}^{1 / 2}\right)\right) \eta_{3} \frac{\log \left(P_{2} / P_{1}\right)}{\phi\left(D_{f}\right)} \frac{g\left(m^{\prime}\right)}{m^{\prime 3}} T_{3}+O\left(\frac{\prod_{i=1}^{3} X_{i}}{(\log X)^{K-O(1)}}\right), \tag{9.28}
\end{align*}
$$

where

$$
T_{3}:=\sum_{X_{0}} \sum_{\substack{I \in \hat{\mathcal{I}}_{0}}} \sum_{\substack{\mathcal{R}=\mathcal{R}_{1} \times \mathcal{R}_{2} \\ \prod_{i=1}^{\ell}\left[\theta_{i}, \theta_{i}^{\prime}\right]=\sqcup \mathcal{R}_{1} \times \mathcal{R}_{2}}}\left|\widetilde{\mathcal{A}}\left(X_{0}\right)\right| c_{\mathcal{R}}\left(X_{0}^{4} / m I\right) .
$$

Here we used that there are at most $O\left(\eta_{2}^{-2 \ell}\right)$ subsets $\mathcal{R}, O\left(\eta_{3}^{-1} \eta_{1}\right)$ reals $X_{0}$ and $O\left(\eta_{3}^{-1} \log X\right)$ 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 $\mathcal{T}:=\prod_{i=1}^{\ell}\left[\theta_{i}, \theta_{i}^{\prime}\right]$, we find

$$
\sum_{\substack{\mathcal{R}=\mathcal{R}_{1} \times \mathcal{R}_{2} \\=1\left[\theta_{i}, \theta_{i}^{\prime}\right]=\cup \mathcal{R}_{1} \times \mathcal{R}_{2}}} c_{\mathcal{R}}\left(X_{0}^{4} / m I\right)=c_{\mathcal{T}}\left(X_{0}^{4} / m I\right),
$$

So

$$
T_{3}=\sum_{X_{0}}\left|\widetilde{\mathcal{A}}\left(X_{0}\right)\right| \sum_{I \in \hat{\mathcal{I}}_{0}} c_{\mathcal{T}}\left(X_{0}^{4} / m I\right) .
$$

By Lemma 9.12 applied to $c_{\mathcal{T}}$ we have for all $I \in \hat{\mathcal{I}}_{0}$

$$
c_{\mathcal{T}}\left(X_{0}^{4} / m I\right)=\frac{1}{\eta_{3}} \int_{I}^{I\left(1+\eta_{3}\right)} \frac{c_{\mathcal{T}}\left(X_{0}^{4} / m v\right)}{v} d v+O\left(\eta_{3}\right) .
$$

Expanding the definition 9.21 of $c_{\mathcal{T}}$ and swapping the order of summation and integration, we find

$$
\begin{aligned}
& \sum_{I \in \hat{\mathcal{I}}_{0}} \int_{I}^{I\left(1+\eta_{3}\right)} \frac{c_{\mathcal{T}}\left(X_{0}^{4} / m v\right)}{v} d v \\
& =\frac{1}{\eta_{3}^{1 / 2}} \iint_{\substack{e_{i} \in\left[i_{i}, \theta_{i}^{\prime}\right]^{\prime} \\
1 \leq i \leq \ell}} \sum_{\substack{I \in \hat{\mathcal{I}}_{0}}} \int_{\substack{v \in\left[I, I\left(1+\eta_{3}\right)\left[ \\
v \in\left[\begin{array}{c}
x_{0}^{4} \\
m \Pi_{i=1}^{l} X^{e}
\end{array}, \frac{x_{0}^{4}(1+\sqrt{n 3})}{m \prod_{i=1}^{\ell} X^{e_{i}}}\right]\right.\right.}} \frac{d v}{v} \prod_{i=1}^{\ell} \frac{\mathrm{d} e_{i}}{e_{i}} \\
& =\frac{1}{\eta_{3}^{1 / 2}} \iint_{\substack{e_{i} \in\left[\theta_{i}, \theta_{i}^{\prime}\right] \\
1 \leq i \leq \ell}}\left(\int_{X_{0}^{4} /\left(m \prod_{i=1}^{\ell} X^{e_{i}}\right)}^{X_{0}^{4}\left(1+\sqrt{\eta_{3}}\right) /\left(m \prod_{i=1}^{\ell} X^{e_{i}}\right)} \frac{d v}{v}\right) \prod_{i=1}^{\ell} \frac{\mathrm{d} e_{i}}{e_{i}} \\
& =\frac{\log \left(1+\sqrt{\eta_{3}}\right)}{\eta_{3}^{1 / 2}} \prod_{i=1}^{\ell} \log \left(\frac{\theta_{i}^{\prime}}{\theta_{i}}\right) .
\end{aligned}
$$

We note that this is independent of $X_{0}$, so we find

$$
\begin{align*}
T_{3} & =\frac{\log \left(1+\sqrt{\eta_{3}}\right)}{\eta_{3}^{3 / 2}} \prod_{i=1}^{\ell} \log \left(\frac{\theta_{i}^{\prime}}{\theta_{i}}\right) \sum_{X_{0}}\left|\widetilde{\mathcal{A}}\left(X_{0}\right)\right|+O\left(\log X \sum_{X_{0}}\left|\widetilde{\mathcal{A}}\left(X_{0}\right)\right|\right) \\
& =\frac{\left(1+O\left(\sqrt{\eta_{3}}\right)\right)}{\eta_{3}} \prod_{i=1}^{\ell} \log \left(\frac{\theta_{i}^{\prime}}{\theta_{i}}\right)|\widetilde{\mathcal{A}}(X)| . \tag{9.29}
\end{align*}
$$

Putting together 9.27, 9.28 and 9.29 we find

$$
\begin{align*}
\sum_{p \in\left[P_{1}, P_{2}\right]} & \sum_{\substack{q_{1}, \ldots q_{\ell} \\
q_{i} \in\left[X^{\theta_{i}, X^{\theta_{i}^{\prime}}}\right.}} \mathcal{A}_{q_{1} \cdots q_{\ell}}\left(\mathbf{u}_{0}, m, p\right) \\
= & 2 \frac{\log \frac{P_{2}}{P_{1}}}{\phi\left(D_{f}\right)} \prod_{i=1}^{\ell} \log \left(\frac{\theta_{i}^{\prime}}{\theta_{i}}\right)|\widetilde{\mathcal{A}}(X)| \sum_{\substack{m_{0} \mid m_{\infty}^{\infty} \\
m_{0} \leq D_{0}}} \sum_{\mathbf{v}_{0} \in \mathcal{M}\left(m_{0}\right)} \frac{g\left(m^{\prime}\right)}{m^{\prime 3}} \\
& \quad+O\left(\eta_{3}^{1 / 2} \prod_{i=1}^{3} X_{i}\right)+O\left(\frac{\eta_{1}^{3} \prod_{i=1}^{3} X_{i}}{D_{0}^{1 / 3}}\right) . \tag{9.30}
\end{align*}
$$

Finally it remains to estimate the inner double sum. The summand is independent of $\mathbf{v}_{0}$, so recalling from 9.12 that $m^{\prime}=m_{0} m$ we are left to estimate

$$
\begin{equation*}
\sum_{\substack{m_{0}<D_{0} \\ m_{0} \mid m^{\infty}}} \frac{\left|\mathcal{M}\left(m_{0}\right)\right|}{\left(m m_{0}\right)^{3}} \prod_{\mathfrak{P} \mid(m)}\left(\sum_{k=2}^{\infty} \frac{\varrho_{\mathbf{v}}\left(\mathfrak{P}^{k}\right)}{N\left(\mathfrak{P}^{k}\right)}\right)^{-1} . \tag{9.31}
\end{equation*}
$$

By (9.10),

$$
\left|\mathcal{M}\left(m_{0}\right)\right| \leq m_{0}^{2} m
$$

and thus for any given $m$ the sum over $m_{0}$ converges. We may therefore extend it to all $m_{0} \geq 1$ cost of an admissible error term. Next we note that the sets of the $\mathbf{a} \in[1, X]^{3}$ with $\mathbf{a} \equiv \mathbf{u}_{0}(\bmod m)$ can be partitioned into sets of the $\mathbf{a} \in[1, X]^{3}$ such that $\mathbf{a} \equiv \mathbf{v}_{0}\left(\bmod m m_{0}\right)$, with $m_{0} \leq X^{2}$ and $\mathbf{v}_{0} \in \mathcal{M}\left(\mathbf{u}_{0}\right)$, and so

$$
\begin{aligned}
\sum_{\substack{m_{0}<D_{0} \\
m_{0} \mid m^{\infty}}} \frac{\left|\mathcal{M}\left(m_{0}\right)\right|}{\left(m m_{0}\right)^{3}} & =\left(1+O\left(D_{0}^{-1 / 4}\right)\right) \sum_{\substack{m_{0}<X^{2} \\
m_{0} \mid m^{\infty}}} \frac{\left|\mathcal{M}\left(m_{0}\right)\right|}{\left(m m_{0}\right)^{3}} \\
& =\frac{\left(1+O\left(D_{0}^{-1 / 4}\right)\right.}{X^{3}+O\left(X^{2}\right)} \sum_{\substack{m_{0}<X^{2} \\
m_{0} \mid m^{\infty}}} \sum_{\mathbf{v} 0 \in \mathcal{M}\left(m_{0}\right)} \sum_{\substack{\mathbf{a} \in[1, X]^{3} \\
\mathbf{a} \equiv \mathbf{v}_{0}\left(\bmod m_{0}\right)}} 1 \\
& =\frac{\left(1+O\left(D_{0}^{-1 / 4}\right)\right)}{X^{3}+O\left(X^{2}\right)} \sum_{\substack{\mathbf{a} \in[1, X]^{3} \\
\mathbf{a} \equiv \mathbf{u}_{0}(\bmod m)}} 1 \\
& =\frac{1}{m^{3}}\left(1+O\left(D_{0}^{-1 / 4}\right)\right) .
\end{aligned}
$$

Substituting this into (9.30 and recalling from 9.13, 9.14) that $D_{0}=$ $(\log X)^{4 K}, \eta_{3} \ll(\log X)^{-3 K}$ and $|\widetilde{\mathcal{A}}(X)|=\eta_{1}^{3} X_{1} X_{2} X_{3}+O\left(\eta_{3} X_{1} X_{2} X_{3}\right)$ gives Theorem 4.1

## 10 Proposition 9.13: The term $T_{\text {sieve }}(\mathcal{R})$

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 $\mathfrak{a}=\prod_{i=\ell^{\prime}+1}^{\ell} \mathfrak{P}_{i}, \mathfrak{b}=\prod_{i=1}^{\ell^{\prime}} \mathfrak{P}_{i}$ with $N\left(\mathfrak{P}_{i}\right) \in\left[X^{t_{i}}, X^{t_{i}}\left(1+O\left(\eta_{2}^{2} \log X\right)\right)\right]$ for $1 \leq i \leq \ell$. In particular,

$$
\begin{equation*}
N(\mathfrak{b}) \in\left[B_{1}^{4}, B_{1}^{4}\left(1+O\left(\eta_{2}^{2} \log X\right)\right)\right] \tag{10.1}
\end{equation*}
$$

where

$$
\begin{equation*}
B_{1}^{4}:=X^{\sum_{i=1}^{\ell^{\prime}} t_{i}} . \tag{10.2}
\end{equation*}
$$

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 $N(\mathfrak{b}) \in\left[B_{1}^{4}, B_{1}^{4}\left(1+O\left(\eta_{2}^{2} \log X\right)\right)\right]$.
Lemma 10.1. Let $B_{1}^{4}>X^{1+\epsilon} R$ and $\mathcal{R}=\mathcal{R}_{1} \times \mathcal{R}_{2}$. Then we have

$$
T_{\text {sieve }}(\mathcal{R})=M_{1}(\mathcal{R})+E_{1}(\mathcal{R})
$$

where $M_{1}(\mathcal{R})$ is given by

$$
\begin{aligned}
M_{1}(\mathcal{R}):= & \sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\
p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\mathfrak{J} \in \mathcal{I}} \sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_{1}}(\mathfrak{a}) \sum_{\substack{N(\mathfrak{d})<R \\
N(\mathfrak{d}), m)=1}} \lambda_{\mathfrak{J}} \\
& \times c_{\mathcal{R}_{2}}\left(\frac{X_{0}^{4}}{m_{0} N(\mathbf{a} \mathfrak{I})}\right)\left|\widetilde{\mathcal{A}}_{\mathfrak{a j} \mathfrak{J}}\left(\mathbf{v}_{0}(\mathbf{y}), m^{\prime}, p\right)\right|,
\end{aligned}
$$

and $E_{1}(\mathcal{R})$ satisfies

$$
\sum_{\mathcal{R}} \sum_{X_{0}} \sum_{I \in \hat{\mathcal{I}}_{0}}\left|E_{1}(\mathcal{R})\right| \ll \eta_{3}^{1 / 2} \eta_{1}^{-2 \ell}(\log X)^{11} \prod_{i=1}^{3} X_{i}
$$

Proof. We substitute our definition (9.23) of $\tilde{\mathbf{1}}_{\mathcal{R}_{2}}$ into our expression (9.24) for $T_{\text {sieve }}$, and write $\mathfrak{u}=\mathfrak{M}_{0} \mathfrak{I a b}$. This gives

$$
\begin{equation*}
T_{\text {sieve }}(\mathcal{R})=\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\ p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\mathfrak{J} \in \mathcal{I}} \sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_{1}}(\mathfrak{a}) \sum_{N(\mathfrak{d})<R} \lambda_{\mathfrak{d}} \sum_{\substack{\mathfrak{u} \in \tilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right) \\ \mathfrak{M} 0 \\ \mathfrak{J} \mathfrak{a} \mathfrak{o} \mid \mathfrak{u}}} c_{\mathcal{R}_{2}}\left(N\left(\mathfrak{u} / \mathbf{a} \mathfrak{J} \mathfrak{M}_{0}\right)\right) . \tag{10.3}
\end{equation*}
$$

If $\mathfrak{u} \in \widetilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)$ then $N(\mathfrak{u}) \in\left[X_{0}^{4}, X_{0}^{4}\left(1+\eta_{3}\right)\right]$. By Lemma 9.12 , this implies $c_{\mathcal{R}_{2}}\left(N\left(\mathfrak{u} / \mathbf{a} \mathfrak{I} M_{0}\right)\right)=c_{\mathcal{R}_{2}}\left(X_{0}^{4} / m_{0} N(\mathbf{a} \mathfrak{I})\right)+O\left(\eta_{3}\right)$. Thus we write

$$
\begin{equation*}
T_{\text {sieve }}(\mathcal{R})=M_{1}(\mathcal{R})+O\left(E_{1}(\mathcal{R})\right) \tag{10.4}
\end{equation*}
$$

where $M_{1}(\mathcal{R})$ is as given in the lemma and

$$
\begin{equation*}
E_{1}(\mathcal{R}):=\eta_{3} \sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\ p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\mathfrak{J} \in \mathcal{I}} \sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_{1}}(\mathfrak{a}) \sum_{N(\mathfrak{d})<R}\left|\lambda_{\mathfrak{d}} \| \widetilde{\mathcal{A}}_{\mathfrak{J a d}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)\right| . \tag{10.5}
\end{equation*}
$$

We concentrate on $E_{1}(\mathcal{R})$. For any $\left(\sum_{i=1}^{3} x_{i} \nu_{i}\right) \in \widetilde{\mathcal{A}}$, the number of primes $p \in\left[P_{1}, P_{2}\right]$ such that $p \mid f\left(x_{1}, x_{2}, x_{3}\right)$ is finite. This allows us to remove the summation over $p$ and replace $\left|\widetilde{\mathcal{A}}_{\mathfrak{J a d}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)\right|$ with $\left|\widetilde{\mathcal{A}}_{\mathfrak{J a d}}\left(\mathbf{v}_{0}, m^{\prime}, 1\right)\right|$ in $E_{1}(\mathcal{R})$ at the cost of a factor $O(1)$.

We then apply Proposition 9.11 to estimate $\left|\widetilde{\mathcal{A}}_{\mathfrak{I a d M}_{0}}\left(\mathbf{v}_{0}, m^{\prime}, 1\right)\right|$, recalling that $N\left(\mathfrak{I a d}_{0}\right) \ll X^{4} R / B_{1}^{4}$ and $m^{\prime} \ll(\log X)^{O(1)}$. This gives

$$
\begin{align*}
E_{1}(\mathcal{R}) & \ll \eta_{3} \sum_{\mathfrak{J} \in \mathcal{I}} \sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_{1}}(\mathfrak{a}) \sum_{\substack{N(\mathfrak{d})<R \\
\left(N(\mathfrak{d}), m^{\prime}\right)=1}}\left|\lambda_{\mathfrak{d}}\right| \frac{\left|\widetilde{\mathcal{A}}\left(X_{0}, \mathcal{X}\right)\right| \varrho_{\mathbf{v}}(\mathfrak{a d} \mathfrak{I})}{N(\mathfrak{a} \mathfrak{I d})\left(m^{\prime}\right)^{3}}  \tag{10.6}\\
& +X^{o(1)} \sum_{\substack{N(\mathfrak{d})<R \\
(N(\mathfrak{d}), m)=1}}\left|\lambda_{\mathfrak{d}}\right|\left(X^{2}\left(\frac{X^{4} R}{B_{1}^{4}}\right)^{1 / 3}+\frac{X^{4} R}{B_{1}^{4}} X\right) .
\end{align*}
$$

Crudely, if $B_{1}^{4}>X^{1+\epsilon} R$, we see the second term in 10.6 contributes to (10.6)

$$
\begin{equation*}
\ll X^{3+o(1)}\left(\frac{X R^{4}}{B_{1}^{4}}+\left(\frac{X R^{4}}{B_{1}^{4}}\right)^{1 / 3}\right) \ll X^{3-\epsilon / 4} \tag{10.7}
\end{equation*}
$$

By an Euler product upper bound and Lemma 9.6, we see that

$$
\begin{align*}
& \sum_{I \in \hat{\mathcal{I}}_{0}} \sum_{\mathfrak{J} \in \mathcal{I}} \sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_{1}}(\mathfrak{a}) \sum_{\substack{N(\mathfrak{o})<R \\
\left(N(\mathfrak{d}), m^{\prime}\right)=1}}\left|\lambda_{\mathfrak{O}}\right| \frac{\left|\widetilde{\mathcal{A}}\left(X_{0}, \mathcal{X}\right)\right| \varrho_{\mathbf{v}}(\mathfrak{a d} \mathfrak{I})}{N(\mathfrak{a} \mathfrak{I d})\left(m^{\prime}\right)^{3}}  \tag{10.8}\\
& \ll(\log X)\left|\widetilde{\mathcal{A}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}\right)\right| \sum_{N(\mathfrak{I}), N(\mathfrak{a}), N(\mathfrak{d})<X} \frac{\left|\rho_{\mathbf{v}}(\mathfrak{a d I})\right|}{N(\mathfrak{a d I})} \\
& \ll(\log X)^{9}\left|\widetilde{\mathcal{A}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}\right)\right| . \tag{10.9}
\end{align*}
$$

Thus, substituting 10.7 and 10.9 into 10.6 we find for $B_{1}^{4}>X^{1+\epsilon} R$

$$
\sum_{I \in \hat{\mathcal{I}}_{0}} E_{1}(\mathcal{R}) \ll \eta_{3}(\log X)^{9}\left|\widetilde{\mathcal{A}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}\right)\right|+X^{3-\epsilon / 5}
$$

Summing this over all $O\left(\eta_{2}^{-2 \ell}\right)$ hyperrectangles $\mathcal{R}$ and all relevant $X_{0}$, and recalling (9.14) that $\eta_{3}$ is much smaller than $\eta_{2}$ we find

$$
\begin{align*}
\sum_{\mathcal{R}} \sum_{X_{0}} \sum_{I \in \hat{\mathcal{I}}_{0}} E_{1}(\mathcal{R}) & \ll \eta_{3}(\log X)^{9} \sum_{\mathcal{R}} \sum_{X_{0}}\left|\widetilde{\mathcal{A}}\left(X_{0}, \mathbf{v}_{0}, m^{\prime}\right)\right|+X^{3-\epsilon / 5} . \\
& \ll \eta_{3} \eta_{2}^{-2 \ell}(\log X)^{4}\left|\widetilde{\mathcal{A}}\left(\mathbf{v}_{0}, m^{\prime}\right)\right|+X^{3-\epsilon / 5} \\
& \ll \eta_{3}^{1 / 2} \eta_{1}^{-2 \ell}(\log X)^{11} \prod_{i=1}^{3} X_{i}+X^{3-\epsilon / 6} . \tag{10.10}
\end{align*}
$$

This gives the result.
Thus we have to evaluate $M_{1}(\mathcal{R})$.
Lemma 10.2. Let $B_{1}^{4}>X^{1+\epsilon} R P_{2}^{12}$ and let $M_{1}(\mathcal{R})$ be as given by Lemma 10.1. Then we have

$$
M_{1}(\mathcal{R})=\left(2+O\left(\eta_{3}^{1 / 2}\right)\right) \eta_{3}\left|\widetilde{\mathcal{A}}\left(X_{0}\right)\right| c_{\mathcal{R}}\left(X_{0}^{4} / m I\right) \frac{g\left(m^{\prime}\right)}{m^{\prime 3}} \frac{\log \left(P_{2} / P_{1}\right)}{\varphi\left(D_{f}\right)}
$$

Proof. First we want to apply Proposition 9.11 to estimate $\left|\widetilde{\mathcal{A}}_{\mathfrak{a} \mathfrak{J}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)\right|$. To do this we split according to residue classes $(\bmod p)$. For any $\left(y_{1}, y_{2}, y_{3}\right)$ such that $f\left(y_{1}, y_{2}, y_{3}\right) \equiv 0(\bmod p)$ let $\tilde{\mathbf{u}}_{0}(\mathbf{y})$ be a solution of the two equations $\tilde{\mathbf{u}}_{0}(\mathbf{y}) \equiv \mathbf{y}(\bmod p)$ and $\tilde{\mathbf{u}}_{0}(\mathbf{y}) \equiv \mathbf{v}_{0}\left(\bmod m^{\prime}\right)$. Thus

$$
\left|\widetilde{\mathcal{A}}_{\mathfrak{a} \mathfrak{I}}\left(\mathbf{v}_{0}, m^{\prime}, p\right)\right|=\sum_{\substack{y_{1}, y_{2}, y_{3}(\bmod p) \\ f\left(y_{1}, y_{2}, y_{3}\right) \equiv 0(\bmod p)}}\left|\widetilde{\mathcal{A}}_{\mathfrak{a d} \mathcal{I}}\left(\tilde{\mathbf{u}}_{0}(\mathbf{y}), p m^{\prime}, 1\right)\right|
$$

We recall that $p \leq P_{2}$ and $N(\Im \mathfrak{I a d}) \ll X R / B_{1}$. Therefore, by Proposition 9.11. we can replace $\left|\widetilde{\mathcal{A}}_{\mathfrak{a d} \mathfrak{I}}\left(\tilde{\mathbf{u}}_{0}(\mathbf{y}), p m^{\prime}, 1\right)\right|$ with $\rho_{\mathbf{v}}(\mathfrak{a d} \mathfrak{I})\left|\mathcal{A}\left(X_{0}, \chi\right)\right| / p^{3} m^{\prime 3} N(\mathfrak{a d I})$ in $M_{1}(\mathcal{R})$ at the cost of a term bounded by

$$
\sum_{p \leq P_{2}} \sum_{\substack{y_{1}, y_{2}, y_{3}(\bmod p) \\ f\left(y_{1}, y_{2}, y_{3}\right) \equiv 0(\bmod p)}}\left(X^{2+o(1)}\left(\frac{X R}{B_{1}^{4}}\right)^{1 / 3} P_{2}+X^{o(1)} \frac{X R}{B_{1}^{4}} P_{2}^{4}\right) .
$$

This is $O\left(X^{3-\epsilon / 4}\right)$ provided $B_{1}^{4}>X^{1+\epsilon} R P_{2}^{12}$.
Since the function $\varrho_{\mathbf{v}}$ is multiplicative, $(\mathfrak{a}, \mathfrak{d} \mathfrak{I})=1$, and $\mathfrak{a}$ is a product of degree one prime ideals of large enough norm, by Lemma 9.4 we have $\varrho_{\mathbf{v}}(\mathfrak{a d} \mathfrak{I}) / N(\mathfrak{a d I})=\varrho_{\mathbf{v}}(\mathfrak{d} \mathfrak{I}) /(N(\mathfrak{d} \mathfrak{I}) N(\mathfrak{a}))$. Thus

$$
\begin{equation*}
M_{1}(\mathcal{R})=M_{2}(\mathcal{R})+O\left(X^{3-\epsilon / 4}\right), \tag{10.11}
\end{equation*}
$$

where

$$
\begin{align*}
M_{2}(\mathcal{R}) & :=\left|\widetilde{\mathcal{A}}\left(X_{0}, \mathcal{X}\right)\right|\left(\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\
p \equiv 1\left(\bmod D_{f}\right)}} \frac{n_{p}}{p}\right)\left(\sum_{\mathfrak{T} \in \mathcal{I}} Z_{1}(\mathfrak{I}) Z_{2}(\mathfrak{I})\right)  \tag{10.12}\\
Z_{1}(\mathfrak{I}) & :=\sum_{\mathfrak{a}} \mathbf{1}_{\mathcal{R}_{1}}(\mathfrak{a}) \frac{c_{\mathcal{R}_{2}}\left(X_{0}^{4} /\left(m_{0} N(\mathbf{a} \mathfrak{I})\right)\right)}{N(\mathfrak{a})},  \tag{10.13}\\
Z_{2}(\mathfrak{I}) & :=\sum_{\substack{N(\mathfrak{d})<R \\
\left(N(\mathfrak{d}), m^{\prime}\right)=1}} \lambda_{\mathfrak{o}} \frac{\varrho_{\mathbf{v}}(\mathfrak{d} \mathfrak{I})}{N(\mathfrak{d} \mathfrak{I})\left(m^{\prime}\right)^{3}}  \tag{10.14}\\
n_{p} & :=\frac{1}{p^{2}}\left|\left\{y_{1}, y_{2}, y_{3}(\bmod p): f\left(y_{1}, y_{2}, y_{3}\right) \equiv 0(\bmod p)\right\}\right| . \tag{10.15}
\end{align*}
$$

First we simplify $Z_{1}(\mathfrak{I})$. Since this is a sum of a smooth function over products of $\ell$ 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

$$
Z_{1}(\mathfrak{I})=c_{\mathcal{R}_{1} \times \mathcal{R}_{2}}\left(X_{0}^{4} / m_{0} N(\mathfrak{I})\right)+O\left(\eta_{3}\right)
$$

We recall that $\mathcal{I}=\left\{\mathfrak{I}:(N(\mathfrak{I}), m)=1, N(\mathfrak{I}) \in\left[I, I+\eta_{3} I\right]\right\}$ and $\mathcal{R}=$ $c R_{1} \times \mathcal{R}_{2}$. Thus, by Lemma 9.12 , we have

$$
\begin{equation*}
Z_{1}(\mathfrak{I})=c_{\mathcal{R}}\left(X_{0}^{4} / m_{0} I\right)+O\left(\eta_{3}\right) . \tag{10.16}
\end{equation*}
$$

Now we consider $Z_{2}(\mathfrak{I})$. By Lemma 9.5 we find that

$$
\begin{equation*}
Z_{2}(\mathfrak{I})=\frac{h(\mathfrak{I}) g\left(\left(m^{\prime}\right)\right) \tilde{\mathfrak{S}}}{\gamma_{K} m^{\prime 3}}+O\left(16^{\omega((m) \mathfrak{I})} \exp (-c \sqrt{\log R})\right) \tag{10.17}
\end{equation*}
$$

where

$$
\begin{aligned}
g((m)) & :=\prod_{\mathfrak{P} \mid(m)}\left(1-\frac{\varrho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\right)^{-1}, \\
h(\mathfrak{J}) & :=\prod_{\mathfrak{P} \mid \mathfrak{J}}\left(1-\frac{\rho_{\mathbf{v}}(\mathfrak{P})}{N(\mathfrak{P})}\right)^{-1} \prod_{\mathfrak{P}_{2}^{e}| | \mathfrak{J}}\left(\frac{\rho_{\mathbf{v}}\left(\mathfrak{P}^{e}\right)}{N\left(\mathfrak{P}^{e}\right)}-\frac{\rho_{\mathbf{v}}\left(\mathfrak{P}^{e+1}\right)}{N\left(\mathfrak{P}^{e+1}\right)}\right) .
\end{aligned}
$$

Putting together (10.16) and 10.17 , we see that

$$
\begin{equation*}
\sum_{\mathfrak{J} \in \mathcal{I}} Z_{1}(\mathfrak{I}) Z_{2}(\mathfrak{I})=\frac{g\left(\left(m^{\prime}\right)\right) \tilde{\mathfrak{S}} c_{\mathcal{R}}\left(X_{0}^{4} / m_{0} I\right)}{\gamma_{K} m^{\prime 3}} \sum_{\mathfrak{J} \in \mathcal{I}} h(\mathfrak{J})+O\left(\eta_{3}^{2} I\right) . \tag{10.18}
\end{equation*}
$$

Since $h(\mathfrak{I})$ is multiplicative, the sum can be calculated by a contour computation

$$
\begin{align*}
\sum_{\mathfrak{J} \in \mathcal{I}} h(\mathfrak{J}) & =\frac{1}{2 \pi i} \int_{2-i \infty}^{2+i \infty} \frac{I^{s}\left(\left(1+\eta_{3}\right)^{s}-1\right)}{s} \sum_{\mathfrak{I}} \frac{h(\mathfrak{I})}{N(\mathfrak{I})^{s}} d s \\
& =\operatorname{Res}_{s=0}\left(\frac{I^{s}\left(\left(1+\eta_{3}\right)^{s}-1\right)}{s} \sum_{\mathfrak{J}} \frac{h(\mathfrak{I})}{N(\mathfrak{I})^{s}}\right)+O(\exp (-c \sqrt{\log R})) . \tag{10.19}
\end{align*}
$$

We see that the residue is given by

$$
\begin{align*}
& \gamma_{K} \log \left(1+\eta_{3}\right) \prod_{\mathfrak{P}}\left(1+h(\mathfrak{P})+h\left(\mathfrak{P}^{2}\right)+\ldots\right)\left(1-\frac{1}{N(\mathfrak{P})}\right) \\
& =\gamma_{K} \log \left(1+\eta_{3}\right) \prod_{\mathfrak{P}}\left(1+\left(1-\frac{\rho(\mathfrak{P})}{N(\mathfrak{P})}\right)^{-1}\left(\sum_{e \geq 1}\left(\frac{\rho\left(\mathfrak{P}^{e}\right)}{N\left(\mathfrak{P}^{e}\right)}-\frac{\rho\left(\mathfrak{P}^{e+1}\right)}{N\left(\mathfrak{P}^{e+1}\right)}\right)\right)\right)\left(1-\frac{1}{N(\mathfrak{P})}\right) \\
& =\gamma_{K} \log \left(1+\eta_{3}\right) \prod_{\mathfrak{P}}\left(1-\frac{\rho(\mathfrak{P})}{N(\mathfrak{P})}\right)^{-1}\left(1-\frac{1}{N(\mathfrak{P})}\right) \prod_{\mathfrak{P}}\left(\left(1-\frac{\rho(\mathfrak{P})}{N(\mathfrak{P})}\right)+\frac{\rho(\mathfrak{P})}{N(\mathfrak{P})}\right) \\
& =\gamma_{K} \frac{\log \left(1+\eta_{3}\right)}{\tilde{\mathfrak{S}}} . \tag{10.20}
\end{align*}
$$

Putting together 10.18 10.19 and 10.20 we see that

$$
\begin{equation*}
\sum_{\mathfrak{\Im} \in \mathcal{I}} Z_{1}(\mathfrak{I}) Z_{2}(\mathfrak{I})=\frac{g\left(\left(m^{\prime}\right)\right) \eta_{3} c_{\mathcal{R}}\left(X_{0}^{4} / m_{0} I\right)}{m^{\prime 3}}+O\left(\eta_{3}^{2} I\right) \tag{10.21}
\end{equation*}
$$

Finally, we recall the definition 10.15 of $n_{p}$. Since $f$ is the product of two linear factors when $p \equiv 1\left(\bmod D_{f}\right)$, we have $n_{p}=2+O(1 / p)$ for all $p \in\left[P_{1}, P_{2}\right]$. Thus

$$
\begin{equation*}
\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\ p \equiv 1\left(\bmod D_{f}\right)}} \frac{n_{p}}{p}=\frac{\left(2+O\left(\eta_{3}\right)\right) \log \left(P_{2} / P_{1}\right)}{\varphi\left(D_{f}\right)} . \tag{10.22}
\end{equation*}
$$

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 $R=X^{\epsilon_{00}}, P_{2}=X^{\tau^{\prime}}, B_{1}^{4}=X^{\sum_{i=1}^{\ell^{\prime}} t_{i}} \geq$ $X^{\sum_{i=1}^{\ell^{\prime}} \theta_{i}}$ we see that this condition is satisfied provided

$$
\sum_{i=1}^{\ell^{\prime}} \theta_{i}>1+\epsilon_{00}+12 \tau^{\prime}
$$

and $\epsilon$ 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 $T_{1}(\mathcal{R})$

To simplify some notation we will write

$$
\begin{equation*}
\tilde{g}(\mathfrak{b}):=\mathbf{1}_{\mathcal{R}_{2}}(\mathfrak{b})-\tilde{\mathbf{1}}_{\mathcal{R}_{2}}(\mathfrak{b}) . \tag{11.1}
\end{equation*}
$$

We first split the sum over $\mathfrak{b}$ into ideal classes $\mathcal{C} \in C l_{K}$. Let $\mathfrak{c} \in \mathcal{C}$ with $\left(N(\mathbf{c}), m^{\prime}\right)=1$ and $N(\mathbf{c}) \ll m^{\prime o(1)} \ll(\log X)^{o(1)}$ and let $\mathfrak{c}^{\prime}=$ $(N(\mathfrak{c}) / \mathfrak{c})$. Since the ideals in the set $\mathcal{A}$ are principal, the ideals $\mathfrak{M}_{0} \mathfrak{I a c}$ and $\mathfrak{b c}$ ' are principal. Therefore they are respectively of the form $(\alpha),(\beta)$ with $\mathfrak{M}_{0} \mathfrak{I c}\left|(\alpha), \mathfrak{c}^{\prime}\right|(\beta)$ 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 $\mathbf{a}=\left(a_{1}, a_{2}, a_{3}, a_{4}\right)$, $\mathbf{b}=\left(b_{1}, b_{2}, b_{3}, b_{4}\right)$. In order to handle the modulo $m$ condition between $\mathfrak{b}$ and $\mathfrak{I a}$ we split the sums according to some congruence classes on $\alpha, \beta$ modulo $m^{\prime}$. Together this gives

$$
\begin{equation*}
T_{1}(\mathcal{R})=\sum_{\mathcal{C} \in C l_{K}} \sum_{\substack{\mathbf{a}_{0}, \mathbf{b}_{0}\left(\bmod m^{\prime}\right) \\ N(\mathfrak{c})\left(\mathbf{a}_{0} \triangleleft \mathbf{b}_{0}\right)_{i} \equiv\left(\mathbf{v}_{0}\right)_{i}\left(\bmod m^{\prime}\right), \text { for } i=1,2,3,4}} \tilde{T}_{\mathfrak{c}}\left(\mathcal{R}, \mathbf{a}_{0}, \mathbf{b}_{0}\right), \tag{11.2}
\end{equation*}
$$

with $\left(a_{0}\right)_{4}=0$ since $(\mathbf{a} \diamond \mathbf{b})_{4}=0$ and $\mathfrak{c} \in \mathcal{C}$ is a well chosen representative, and $\mathfrak{c}^{\prime}$ as above
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 $N(\beta) \in$ $\left[B^{4}, B^{4}\left(1+O\left(\eta_{2}^{2} \log X\right)\right)\right]$, where

$$
B=B_{1} N\left(\mathfrak{c}^{\prime}\right)^{1 / 4} \in\left[B_{1}, B_{1}(\log X)^{o(1)}\right]
$$

The support of $\mathbf{1}_{\mathcal{R}_{1}}$ implies that

$$
N(\alpha) \in\left[A^{4}, A^{4}\left(1+\eta_{2}^{2} \log X\right)\right]
$$

where (recalling that $N(\mathfrak{I}) \in\left[I, I\left(1+\eta_{3}\right)\right]$ from 9.20 )

$$
\begin{equation*}
A^{4}:=X^{\sum_{i=\ell^{\prime}+1}^{\ell} t_{i}} N(\mathfrak{c}) m_{0} I \ll X^{\sum_{i=\ell^{\prime}+1}^{\ell} t_{i}} I(\log X)^{5 K} . \tag{11.3}
\end{equation*}
$$

We note that $A^{4} B^{4} \ll X^{4}(\log X)^{6 K}$. We will use the notation of [14, p . 80 and 71]:

$$
\begin{gather*}
\mathcal{R}_{X_{0}}:=\left\{\mathbf{x} \in \mathbb{R}^{4}: x_{i} \in\left[X_{i}, X_{i}\left(1+\eta_{1}\right)\right], i=1,2,3, x_{4}=0,\right. \\
 \tag{11.4}\\
\left.N\left(\sum_{i=1}^{3} x_{i} \nu_{i}\right) \in\left[X_{0}^{4}, X_{0}^{4}\left(1+\eta_{3}\right)\right]\right\}, \\
\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}:=\left\{\mathbf{a} \in \mathbb{R}^{4}:\|a\| \in[A, 2 A], \mathbf{a} \diamond \mathbf{b}_{1} \in \mathcal{R}_{X_{0}}, \mathbf{a} \diamond \mathbf{b}_{2} \in \mathcal{R}_{X_{0}}\right\} .
\end{gather*}
$$

Let $\mathcal{F}$ be a fundamental domain such that if $\mathbf{1}_{\mathcal{R}_{1}}\left((\alpha) / \mathfrak{M}_{0} \mathfrak{I} \mathfrak{c}\right)=1$ 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
$1 \leq i \leq 4$ 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 $(\beta)$ with not too many divisors. For this we introduce a slight variant of $\tilde{g}$

$$
\begin{align*}
& g_{\mathrm{b}}:= \begin{cases}\mathbf{1}_{\mathcal{R}_{2}}\left(\mathfrak{b} / \mathfrak{c}^{\prime}\right)-\tilde{\mathbf{1}}_{\mathcal{R}_{2}}\left(\mathfrak{b} / \mathfrak{c}^{\prime}\right) & \text { if } \tau(\mathfrak{b}) \leq \eta_{4}^{-1} \text { and } \mathfrak{c}^{\prime} \mid(\beta), \\
0 & \text { otherwise, }\end{cases}  \tag{11.5}\\
& \eta_{4}:=(\log X)^{-K_{1}} \tag{11.6}
\end{align*}
$$

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 $O\left(\eta_{4} X_{0}^{3}(\log X)^{O(1)}\right)$. 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

### 11.1 Cosmetic reductions

For $T>0$, we denote by $\mathcal{C}_{T}$ the subset of $\mathbb{R}^{4}$ defined by

$$
\mathcal{C}_{T}=\left\{\mathbf{a} \in \mathcal{F}: N(\mathfrak{a}) \in\left[T^{4}, 2 T^{4}\right]\right\}
$$

so that $\mathbf{a} \in \mathcal{C}_{A}$ and $\mathbf{b} \in \mathcal{C}_{B}$. By Weber's Theorem [19], we have

$$
\left|\mathcal{C}_{T}\right|=\lambda_{K} T^{4}+O\left(T^{3}\right),
$$

for some $\lambda_{K}$ depending only on $K\left(\lambda_{K}=\gamma_{K} / h_{K}\right.$, 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

$$
\ll \sum_{p \in\left[P_{1}, P_{2}\right]} \sum_{\substack{\mathbf{b} \in \mathcal{C}_{B} \\ N(\mathfrak{b}) \equiv 0 \\(\bmod p)}} \sum_{\substack{\mathfrak{b} u \in \mathcal{A}(0,1, p)}} X^{o(1)} \ll X^{\varepsilon}\left(X^{3} P_{1}^{-1}+X^{2} B^{4 / 3} P_{2}^{2}+B^{4} P_{2}^{5}\right) .
$$

This is acceptably small provided

$$
\begin{equation*}
B<\frac{X^{3 / 4-\epsilon}}{P_{2}^{3 / 2}} \tag{11.8}
\end{equation*}
$$

We recall that $f \in \mathbb{Z}\left[X_{1}, X_{2}, X_{3}\right]$ is quadratic and homogeneous and $D_{f}$ is the associated modulus introduced in the hypothesis of Theorem 4.1 so that when $p \equiv 1\left(\bmod D_{f}\right)$, the function $f(\bmod p)$ factors as the
product of two linear factors. Thus the condition $p \mid f(\mathbf{a} \diamond \mathbf{b})$ is equivalent to $p \mid \mathbf{v}_{p} \cdot(\mathbf{a} \diamond \mathbf{b})$ or $p \mid \mathbf{w}_{p} \cdot(\mathbf{a} \diamond \mathbf{b})$ for two non-zero vectors $\mathbf{v}_{p}, \mathbf{w}_{p} \in \mathbb{Z}^{4}$. There are $O\left(p^{5}\right)$ choices of $\mathbf{a}_{p}, \mathbf{b}_{p}(\bmod p)$ such that $\left(\mathbf{a}_{p} \diamond \mathbf{b}_{p}\right)_{4}=\mathbf{v}_{p} \cdot\left(\mathbf{a}_{p} \diamond \mathbf{b}_{p}\right)=$ $\mathbf{w}_{p} \cdot\left(\mathbf{a}_{p} \diamond \mathbf{b}_{p}\right)$ whenever $p$ is sufficiently large in terms of $f$. Therefore, as above, provided $\sqrt{11.8}$ holds, the contribution of the $\mathbf{a}, \mathbf{b}$ such that $p \mid \mathbf{v}_{p} \cdot(\mathbf{a} \diamond \mathbf{b})$ and $p \mid \mathbf{w}_{p} \cdot(\mathbf{a} \diamond \mathbf{b})$ is bounded by

$$
X^{o(1)} \sum_{p \in\left[P_{1}, P_{2}\right]} \sum_{\substack{\mathbf{a}_{p}, \mathbf{b}_{p} \in\{1, \ldots, p\}^{4} \\\left(\mathbf{a}_{p} \diamond \mathbf{b}_{p}\right)_{4} \equiv 0(\bmod p) \\ p \mid \mathbf{v}_{p} \cdot\left(\mathbf{a}_{p} \diamond \mathbf{b}_{p}\right)}} \sum_{\substack{\mathbf{b} \in \mathbb{Z}^{4} \cap C_{B} \\ p \mid \mathbf{w}_{p} \cdot\left(\mathbf{a}_{p} \diamond \mathbf{b}_{p}\right)}} 1 \ll X^{\substack{u}} \sum_{\substack{\mathcal{A}(0,1, p) \\ \mathfrak{b} \mid \mathfrak{u}}} 1<P_{1}^{-1}
$$

Putting this together, we see that it suffices for us to estimate for each $C \in C l_{K}$ with a representative $\mathfrak{c} \in C$ and each $\mathbf{a}_{0}, \mathbf{b}_{0}\left(\bmod m^{\prime}\right)$ the sums

### 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 $1 \leq i \leq \ell$. 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

$$
\left.T_{3}^{2} \ll A^{4} \sum_{\substack{\mathbf{a} \in \mathbb{Z}^{4} \cap \mathcal{C}_{A}}} \sum_{\substack{p \in\left[P_{1}, P_{2}\right]}} \sum_{\substack{\mathbf{b} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B} \\ \mathbf{a} \equiv \mathbf{a}_{0}\left(\bmod m^{\prime}\right)}} g_{\mathbf{b}}\right)^{2}
$$

Thus we see that

$$
\begin{equation*}
T_{3}^{2} \ll A^{4} T_{4} \tag{11.10}
\end{equation*}
$$

where, with the notation 11.4

$$
T_{4}:=\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\ p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{b}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B} \\ \mathbf{b}_{1}=\mathbf{b}_{2}=\mathbf{b}_{0}\left(\text { mod } m^{\prime}\right) \\ p_{1} \uparrow N\left(\mathbf{b}_{1}\right), p_{2} \uparrow N\left(\mathbf{b}_{2}\right)}} g_{\mathbf{b}_{1} g_{\mathbf{b}_{2}}} \sum_{\substack{\mathbf{a} \in \mathbb{Z}^{4} \cap \mathcal{C}_{A} \\ \mathbf{a} \in \mathcal{R}_{1} \\ p_{1}\left|\mathbf{b}_{1}, \mathbf{b}_{2} \\ p_{2}\right| \mathbf{v}_{p_{2}} \cdot\left(\mathbf{a}<\mathbf{b}_{1}\right)}} 1 .
$$

Thus we wish to show that $T_{4}$ is small compared with $A^{2} B^{6}$.

### 11.3 Collinear $b_{1}, b_{2}$

We separate the situation when $\mathbf{b}_{1}$ and $\mathbf{b}_{2}$ are collinear (in which case we have $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)=0$ where $\wedge(\mathbf{x}, \mathbf{y})$ is the $L^{2}$ norm of the six $2 \times 2$
subdeterminants of the $2 \times 4$ matrix with columns $\mathbf{x}$ and $\mathbf{y}$ ). Thus we have

$$
\begin{equation*}
T_{4}=T_{5}+T_{6} \tag{11.11}
\end{equation*}
$$

where $T_{5}$ is those terms with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)=0$ and $T_{6}$ is those terms with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0$.

We first concentrate on $T_{5}$.

## Lemma 11.1.

$$
T_{5} \ll X^{o(1)} A^{3} B^{3} .
$$

Proof. Let 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

$$
T_{5} \ll \eta_{4}^{-2} \sum_{\substack{\mathbf{c} \in \mathbb{Z}^{4} \\\|\mathbf{c}\| \ll B}} \sum_{\lambda_{1}, \lambda_{2} \ll B /\|\mathbf{c}\| \mathbf{a} \in \mathbb{Z}^{4} \cap \mathcal{C}_{A}} \sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\(\mathbf{a}<\mathbf{c})_{4}=0 \\ p_{1} \mid f\left(\lambda_{1} \mathbf{a} c \\ p_{2} \mid f\left(\lambda_{2} \mathbf{a}<\mathbf{c}\right)\right.}} 1 .
$$

We see that the inner sum is $O(1)$ since $P_{1} \gg B^{\epsilon}$ and $f\left(\lambda_{1} \mathbf{a} \diamond \mathbf{c}\right) \ll B^{O(1)}$. We then split the size of $\|\mathbf{c}\|$ into dyadic ranges, giving

$$
T_{5} \ll \eta_{4}^{-2}(\log X) \sup _{C \ll B} \frac{B^{2}}{C^{2}} \sum_{\substack{\mathbf{c} \in \mathbb{Z}^{4} \\\|\mathbf{c}\| \simeq C}} \sum_{\substack{\mathbf{a} \in \mathbb{Z}^{4} \cap \mathcal{C}_{A} \\(\mathbf{a}<\mathbf{c})_{4}=0}} 1 .
$$

We now let $\mathbf{z}=(\mathbf{a} \diamond \mathbf{c})$. By the divisor bound, given $\mathbf{z}$ there are $O\left(\tau_{K}(\mathfrak{z})\right)$ choices of $\mathbf{a}, \mathbf{c}$. Thus we see that

$$
\begin{aligned}
T_{5} & \ll \eta_{4}^{-2}(\log X) \sup _{C \ll B} \frac{B^{2}}{C^{2}} \sum_{z_{1}, z_{2}, z_{3} \ll A C} \tau_{K}\left(z_{1} \nu_{1}+z_{2} \nu_{2}+z_{3} \nu_{3}\right) \\
& \ll \eta_{4}^{-3} A^{3} B^{3} .
\end{aligned}
$$

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

$$
\begin{aligned}
\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}} & :=\left\{\mathbf{x} \in \mathbb{Z}^{4}:\left(\mathbf{x} \diamond \mathbf{b}_{1}\right)_{4}=\left(\mathbf{x} \diamond \mathbf{b}_{2}\right)_{4}=0\right\} \\
\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}} & :=\left\{\mathbf{x} \in \Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}: p_{1}\left|\mathbf{v}_{p_{1}} \cdot\left(\mathbf{x} \diamond \mathbf{b}_{1}\right), p_{2}\right| \mathbf{v}_{p_{2}} \cdot\left(\mathbf{x} \diamond \mathbf{b}_{2}\right)\right\} .
\end{aligned}
$$

Thus the inner sum in $T_{6}$ is

$$
\sum_{\substack{\mathbf{a} \in \mathcal{C}_{A} \cap \Lambda_{\mathbf{l}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}^{\mathbf{a} \in \mathcal{R}_{\mathbf{b}}, \mathbf{b}_{2}}}} 1 .
$$

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 $\left\{\mathbf{z}_{1}, \mathbf{z}_{2}\right\}$ ([14, Lemma 4.1] for example).

Without loss of generality we may assume that $\left\|\mathbf{z}_{1}\right\| \leq\left\|\mathbf{z}_{2}\right\|$. Thus we have that

$$
\sum_{\mathbf{a} \in \mathcal{C}_{A} \cap \Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}} \cap \mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}} 1=\sum_{\substack{\lambda_{1}, \lambda_{2} \in \mathbb{Z} \\ \lambda_{1} \mathbf{z}_{1}+\lambda_{2} \mathbf{z}_{2} \in \mathcal{R}_{A} \cap \mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}} \\ \lambda_{1} c_{1}+\lambda_{2} c_{2} \equiv 0\left(\bmod p_{1}\right) \\ \lambda_{1} c_{3}+\lambda_{2} c_{4} \equiv 0\left(\bmod p_{2}\right)}} 1,
$$

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 $\left(\lambda_{1}, \lambda_{2}\right)$ to lie in a region $\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime} \subseteq \mathbb{R}^{2}$. Since $\left\|\lambda_{1} \mathbf{z}_{1}+\lambda_{2} \mathbf{z}_{2}\right\| \asymp\left|\lambda_{1}\right|\left\|\mathbf{z}_{1}\right\|+\left|\lambda_{2}\right|\left\|\mathbf{z}_{2}\right\|$ (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 $\lambda_{1} \ll A /\left\|\mathbf{z}_{1}\right\|$ and $\lambda_{2} \ll A /\left\|\mathbf{z}_{2}\right\|$, so $\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime}$ has volume $O\left(A^{2} /\left\|\mathbf{z}_{1}\right\|\left\|\mathbf{z}_{2}\right\|\right)$.

By Davenport's Theorem on counting lattice points (14 Lemma 7.1] for example), we have that

$$
\sum_{\begin{array}{c}
\left(\lambda_{1}, \lambda_{2}\right) \in \mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime} \\
\lambda_{1} c_{1}+\lambda_{2} c_{2}=0\left(\bmod p_{1}\right) \\
\lambda_{1} c_{3}+\lambda_{2} c_{4}=0\left(\bmod p_{2}\right)
\end{array}} 1=\frac{\operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime}\right)}{f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}}+O\left(\frac{A}{\left\|\mathbf{z}_{1}\right\|}\right)
$$

where $f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}=\left[\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}: \Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}\right]$ is the index of the lattices, given explicitly in terms of $c_{1}, c_{2}, c_{3}, c_{4}, p_{1}, p_{2}$ by

$$
f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}= \begin{cases}1, & c_{1} \equiv c_{2} \equiv 0\left(\bmod p_{1}\right) \text { and } c_{3} \equiv c_{4} \equiv 0\left(\bmod p_{2}\right), \\ p_{2}, & c_{1} \equiv c_{2} \equiv 0\left(\bmod p_{1}\right) \text { and } c_{3}, c_{4} \text { not both } 0\left(\bmod p_{2}\right), \\ p_{1}, & c_{3} \equiv c_{4} \equiv 0\left(\bmod p_{2}\right) \text { and } c_{1}, c_{2} \text { not both } 0\left(\bmod p_{1}\right), \\ p_{1}, & p_{1}=p_{2} \text { and } c_{1} c_{4} \equiv c_{2} c_{3}\left(\bmod p_{1}\right) \text { and } c_{1}, c_{2} \operatorname{not} \text { all } 0\left(\bmod p_{1}\right), \\ p_{1} p_{2}, & \text { otherwise. }\end{cases}
$$

We split $T_{6}$ into the contribution from the main term $\operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime}\right) / f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}$ and the error term $O\left(A /\left\|\mathbf{z}_{1}\right\|\right)$. This gives

$$
\begin{equation*}
T_{6}=T_{8}+O\left(T_{7}\right), \tag{11.12}
\end{equation*}
$$

where

$$
\begin{aligned}
& T_{7}:=\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\
p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{b}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B} \\
\mathbf{b}_{1} \equiv \mathbf{b}_{2}=\mathbf{b}_{0}\left(\bmod m^{\prime}\right) \\
p_{1} \nmid N\left(\mathbf{b}_{1}\right), p_{2} \nmid N\left(\mathbf{b}_{2}\right) \\
\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0}} \frac{\eta_{4}^{-2} A}{\left\|\mathbf{z}_{1}\right\|},
\end{aligned}
$$

We first show that the contribution $T_{7}$ from the error term is small.

## Lemma 11.2.

$$
T_{7} \ll X^{o(1)} A B^{7} P_{2}^{2} .
$$

Proof. We note that $\mathbf{z}_{1} \in \mathbb{Z}^{4}$ with $\left\|\mathbf{z}_{1}\right\|^{2} \leq\left\|\mathbf{z}_{1}\right\| \cdot\left\|\mathbf{z}_{2}\right\| \ll \operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right) \ll$ $B^{2}$. Thus $\left\|\mathbf{z}_{1}\right\| \ll B$. Thus we can rearrange the summation to give

$$
T_{7} \ll \eta_{4}^{-2} P_{2}^{2} \sum_{\mathbf{b}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B}} \frac{A}{\left\|\mathbf{z}_{1}\right\|} \ll A P_{2}^{2} \sum_{\substack{\mathbf{z}_{1} \in \mathbb{Z}^{4} \\\left\|\mathbf{z}_{1}\right\| \ll B}} \frac{1}{\left\|\mathbf{z}_{1}\right\|}\left(\sum_{\substack{\mathbf{b} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B} \\\left(\mathbf{b}<\mathbf{z}_{1}\right)_{4}=0}} 1\right)^{2}
$$

The condition $\left(\mathbf{b} \diamond \mathbf{z}_{1}\right)_{4}=0$ forces $\mathbf{b}$ to lie in a rank 3 lattice of determinant $\asymp\left\|\mathbf{z}_{1}\right\|$. Thus the inner sum is $O\left(B^{3} /\left\|z_{1}\right\|+B^{2}\right)$. Thus we obtain the bound

$$
T_{7} \ll \eta_{4}^{-2} A P_{2}^{2} \sum_{\substack{\mathbf{z}_{1} \in \mathbb{Z}^{4} \\\left\|\mathbf{z}_{1}\right\| \ll B}}\left(\frac{B^{6}}{\left\|\mathbf{z}_{1}\right\|^{3}}+\frac{B^{4}}{\left\|\mathbf{z}_{1}\right\|}\right) \ll A B^{7} P_{2}^{2} \eta_{4}^{-3} .
$$

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 $\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime}$ 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 $\operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime \prime}\right) / \operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)$, where $\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)$ is the determinant of the lattice (that is, the 2-dimensional area of parallelogram generated by $\mathbf{z}_{1}, \mathbf{z}_{2}$ ) and $\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime \prime}$ is the 2-dimensional region formed by intersecting $\mathcal{C}_{A}$ with the $\mathbf{z}_{1}, \mathbf{z}_{2}$ plane. We thus have

We first establish a few simple estimates.

## Lemma 11.3.

$$
\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\ p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \frac{\operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime}\right)}{f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}} \ll \operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime}\right)+O\left(\frac{A P_{2}^{2}}{\left\|\mathbf{z}_{1}\right\|}\right) .
$$

Proof. We have that

$$
\begin{aligned}
& \ll \sum_{\substack{\mathbf{a} \in \mathbb{Z}^{4} \cap \mathcal{C}_{A} \\
\mathbf{a} \in \mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}}} 1 \\
& \ll \operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime}\right)+O\left(\frac{A}{\left\|\mathbf{z}_{1}\right\|}\right) \text {. }
\end{aligned}
$$

On the other hand, we know that

$$
\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\ p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{a} \in \mathbb{Z}^{4} \cap \mathcal{C}_{A} \\ \mathbf{a} \in \mathcal{R}_{\mathbf{b}_{1}}, \mathbf{b}_{2} \\ p_{1} \mid \mathbf{v}_{p_{1}} \cdot \mathbf{a} \diamond \mathbf{b}_{1}}} 1=\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\ p_{2} \mid \mathbf{v}_{p_{2}} \cdot \mathbf{a} \diamond \mathbf{b}_{2}}}\left(\frac{\operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}}^{\prime} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)\right.}{\left.f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}\right)}+O\left(\frac{A}{\left\|\mathbf{z}_{1}\right\|}\right)\right)
$$

Putting these together gives the result.
Lemma 11.4. Let

$$
\mathcal{C}_{C, d ; \mathbf{c}_{1}, \mathbf{b}_{2}}:=\#\left\{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B}: \wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim \frac{B^{2}}{C}, \mathbf{b}_{1} \equiv \mathbf{c}_{1}(\bmod d)\right\} .
$$

Then we have

$$
\# \mathcal{C}_{C, d ; \mathbf{c}_{1}, \mathbf{c}_{2}} \ll\left(1+\frac{B}{d}\right)\left(1+\frac{B}{C d}\right)^{3} .
$$

Proof. The condition $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim B^{2} / C$ 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

$$
\ll\left(1+\frac{B}{d}\right)\left(1+\frac{B}{C d}\right)^{3}
$$

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 $\mathbf{b}_{1} \equiv \mathbf{c}_{1}(\bmod d)$, 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 $\mathbf{c}_{1} \not \propto \mathbf{c}_{2}(\bmod p)$ then

Proof. We recall that $\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}$ is the lattice in $\mathbb{Z}^{4}$ of $\mathbf{x}$ with $\left(\mathbf{x} \diamond \mathbf{b}_{1}\right)_{4}=(\mathbf{x} \diamond$ $\left.\mathbf{b}_{2}\right)_{4}=0$. By [14] Lemma 10.1], this has determinant $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) / D_{\mathbf{b}_{1}, \mathbf{b}_{2}}$, where $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)$ is the $L^{2}$ norm of the six $2 \times 2$ 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 $\mathbf{b}_{1} \propto \mathbf{b}_{2}\left(\bmod D_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)$, so since $\mathbf{b}_{1}, \mathbf{b}_{2}$ are primitive we must have $D_{\mathbf{b}_{1}, \mathbf{b}_{2}} \leq B$ when $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq$ 0 .

We consider separately those $\mathbf{b}_{1}, \mathbf{b}_{2}$ with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \ll B$, those with $B \ll \wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \ll B^{4 / 3}$, and those $\mathbf{b}_{1}, \mathbf{b}_{2}$ with

$$
D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d, \quad \wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim B^{2} / C
$$

for each $1 \leq d \leq B$ and $1 \leq C \leq B^{2 / 3}$ with $C$ running through powers of 2.

If $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \ll B$ 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 $\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right) \geq 1$, these terms contribute a total (ignoring the congruence conditions $(\bmod p)$ for an upper bound)

$$
\ll \sum_{\left\|\mathbf{b}_{2}\right\| \ll B} O(B) \ll B^{5} .
$$

If $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \in\left[B, B^{4 / 3}\right]$ then we separately consider those with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim$ $B^{2} / C$ for $C \in\left[B^{2 / 3}, B\right]$ running through powers of 2 , and again drop the congruence constraints. By Lemma 11.4 there are

$$
\ll B\left(1+\frac{B}{C}\right)^{3} \ll \frac{B^{4}}{C^{3}}
$$

choices of $\mathbf{b}_{1}$ given $\mathbf{b}_{2}$. If $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim B^{2} / C$ then $\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right) \geq B / C$ (since $D_{\mathbf{b}_{1} \mathbf{b}_{2}} \leq B$ ). Thus these terms contribute

$$
\ll \sum_{C=2^{j} \in\left[B^{2 / 3}, B\right]} \sum_{\mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B}} \frac{C}{B} \frac{B^{4}}{C^{3}} \ll B^{17 / 3} .
$$

Thus we are left to consider the terms with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim B^{2} / C$ for some $C \leq B^{2 / 3}$. The condition $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d$ forces $\mathbf{b}_{1} \propto \mathbf{b}_{2}(\bmod d)$, and so $\mathbf{b}_{1} \equiv \lambda \mathbf{b}_{2}(\bmod d)$ for some $\lambda \in\{1, \ldots, d\}$. Since $\mathbf{c}_{1} \not \propto \mathbf{c}_{2}(\bmod p)$, we see $p \nmid d$. Thus $\mathbf{b}_{1} \equiv \mathbf{c}_{0}(\lambda)(\bmod d p)$, where $\mathbf{c}_{0}(\lambda) \equiv \lambda \mathbf{b}_{2}(\bmod d)$ and $\mathbf{c}_{0}(\lambda) \equiv \mathbf{c}_{1}(\bmod p)$. By Lemma 11.4 , the number of choices of $\mathbf{b}_{1}$ is therefore

$$
\ll \sum_{1 \leq \lambda \leq d} \# \mathcal{C}_{C, p d, \mathbf{c}_{0}(\lambda), \mathbf{b}_{2}} \ll d\left(1+\frac{B}{p d}\right)\left(1+\frac{B}{p C d}\right)^{3} \ll B+\frac{B^{4}}{p^{4} C^{3} d^{3}}
$$

If $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d$ and $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim B^{2} / C$ then $\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right) \gg B^{2} /(C d)$. Thus we find that the contribution from terms with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \geq B^{4 / 3}$ is

$$
\begin{array}{ll}
\sum_{\substack{\left.\mathbf{b}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B} \\
\wedge_{1}\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \geq B \\
\mathbf{b}_{2} \equiv \mathbf{c}_{1}(\text { mod } p) \\
\mathbf{c o c}_{2} \text { (mod } p\right) \\
\text { primitive }}} \frac{1}{\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)} & \ll \sum_{1 \leq d \leq B} \sum_{C=2^{j} \ll B^{2 / 3}} \frac{d C}{B^{2}} \sum_{\substack{\mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B} \\
\mathbf{b}_{2} \equiv \mathbf{c}_{2}(\bmod p)}}\left(B+\frac{B^{4}}{C^{3} d^{3} p^{4}}\right) \\
& \ll \frac{B^{6}}{p^{8}}+B^{17 / 3} .
\end{array}
$$

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 $(\bmod p)$ with $\mathbf{c}_{1} \propto \mathbf{c}_{2}(\bmod p)$.
Then we have

$$
\begin{aligned}
& \sum_{\substack{\mathbf{b}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B} \\
\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0}} \frac{1}{\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)} \ll \frac{B^{6}}{p^{7}}+B^{17 / 3} . \\
& \mathbf{p r i m i t i v e}_{\mathbf{b}_{1} \equiv \mathbf{c}_{1}(\bmod p)}^{\mathbf{b}_{2} \equiv \mathbf{c}_{2}(\bmod p)}
\end{aligned}
$$

Proof. This is similar to the proof of Lemma 11.5 Since the estimates in the proof of Lemma 11.5 when $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \ll B^{4 / 3}$ didn't depend on whether $p \mid D_{\mathbf{b}_{1}, \mathbf{b}_{2}}$ or not, an identical argument shows that the contribution of $\mathbf{b}_{1}, \mathbf{b}_{2}$ with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \ll B^{4 / 3}$ contributes $O\left(B^{17 / 3}\right)$. Therefore we just need to consider the contribution when $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \gg B^{4 / 3}$.

We split the summation according to $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim B^{2} / C$ and $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=$ $d$. Since $\mathbf{c}_{1} \propto \mathbf{c}_{2}(\bmod p)$, we have $\mathbf{c}_{1} \equiv \lambda_{0} \mathbf{c}_{2}(\bmod p)$ for some $\lambda_{0}$. Since $\mathbf{b}_{1} \equiv \mathbf{c}_{1}(\bmod p)$ and $\mathbf{b}_{2} \equiv \mathbf{c}_{2} \bmod p$ we then see that $p \mid d$. The condition $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d$ forces $\mathbf{b}_{1}=\lambda \mathbf{b}_{2}(\bmod d)$ for some $\lambda$, with $\lambda \equiv \lambda_{0}(\bmod p)$. Thus, by Lemma 11.4 the number of choices of $\mathbf{b}_{1}, \mathbf{b}_{2}$ with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim$ $B^{2} / C$ and $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d$ is

$$
\begin{aligned}
\ll \sum_{\substack{\mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B} \\
\mathbf{b}_{2}=\mathbf{c}_{2}(\bmod p)}} \sum_{\substack{1 \leq \lambda \leq d \\
\lambda \equiv \lambda_{0}(\bmod p)}} \# \mathcal{C}_{C, d, \lambda \mathbf{b}_{2}, \mathbf{b}_{2}} & \ll\left(1+\frac{B^{4}}{p^{4}}\right) \frac{d}{p}\left(1+\frac{B}{d}\right)\left(1+\frac{B}{C d}\right)^{3} \\
& \ll \frac{B^{8}}{p^{5} C^{3} d^{3}}+B^{5} .
\end{aligned}
$$

When $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim B^{2} / C$ and $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d$ we have $\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right) \gg B^{2} /(C d)$. Thus the total contribution from terms with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \gg B^{4 / 3}$ is

$$
\sum_{\substack{d \leq B \\ p \mid d}} \sum_{C=2^{j} \ll B^{2 / 3}} \frac{C d}{B^{2}}\left(\frac{B^{8}}{p^{5} C^{3} d^{3}}+B^{5}\right) \ll \frac{B^{6}}{p^{7}}+B^{17 / 3}
$$

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

$$
T_{8} \ll \eta_{4} A^{2} B^{6}+\eta_{4}^{-12} A^{2} \sup _{\mathcal{C}_{1}, \mathcal{C}_{2}}\left(\left|T_{11}\right|+\left|T_{12}\right|\right),
$$

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

$$
\begin{align*}
& T_{11}:=\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\
p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\
\mathbf{b}_{1} \equiv \mathbf{b}_{2} \equiv \mathbf{b}_{0}\left(\bmod m^{\prime}\right) \\
\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0 \\
p \nmid N\left(\mathbf{b}_{1}\right) N\left(\mathbf{b}_{2}\right)}} \frac{g_{\mathbf{b}_{1} g_{\mathbf{b}_{2}}}}{f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p, p} \operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)},  \tag{11.13}\\
& T_{12}:=\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\
p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \frac{1}{p_{1} p_{2}} \sum_{\substack{\left.\left.\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\
\mathbf{b}_{1} \equiv \mathbf{b}_{2} \equiv \mathbf{b}_{0}\left(\bmod m^{\prime}\right) \\
\wedge \\
p_{1} \nmid \mathbf{m}_{1}, \mathbf{b}_{2}\right) \neq 0 \\
p_{1}\right)}} \frac{g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}} D_{\left.\mathbf{b}_{1}, \mathbf{b}_{2}\right), p_{2} \nmid N\left(\mathbf{b}_{2}\right)}^{\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)}}{} . \tag{11.14}
\end{align*}
$$

Proof. Let $\eta_{5}:=\eta_{4}^{3}$. We wish to replace $\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime \prime}$ with a quantity which doesn't depend on $\mathbf{b}_{1}, \mathbf{b}_{2}$ by splitting $\mathcal{C}_{B}$ into $O\left(\eta_{5}^{-4} \eta_{1}^{4}\right)$ smaller hypercubes of side length $\eta_{5} B$. We see that $\operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime \prime}\right)$ depends continuously on the components of $\mathbf{b}_{1}$ and $\mathbf{b}_{2}$, and that $\operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime \prime}\right)$ is always of size $O\left(A^{2}\right)$. Moreover, if we restrict $\mathbf{b}_{1}, \mathbf{b}_{2}$ to hypercubes of side length $\eta_{5} B$
then $\operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime}\right)$ varies by $O\left(\eta_{5} A^{2}\right)$ as $\mathbf{b}_{1}, \mathbf{b}_{2}$ vary within these hypercubes. Thus we see that

$$
\begin{align*}
T_{8} & =\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\
p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{b}_{1} \equiv \mathbf{b}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{B}=\left(\mathbf{b}_{0}\left(\bmod m^{\prime}\right) \\
p_{1} \nmid N\left(\mathbf{b}_{1}\right), p_{2} \nmid N\left(\mathbf{b}_{2}\right) \\
\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0\right.}} \frac{g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}} \operatorname{vol}\left(\mathcal{R}_{\mathbf{b}_{1}, \mathbf{b}_{2}}^{\prime \prime}\right)}{f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}} \operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)} \\
& <T_{9}+\eta_{5}^{-4} A^{2} \sup _{\mathcal{C}_{1}, \mathcal{C}_{2}}\left|T_{10}\right|, \tag{11.15}
\end{align*}
$$

where

$$
\begin{aligned}
& T_{10}=T_{10}\left(\mathcal{C}_{1}, \mathcal{C}_{2}\right):=\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\
p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\
\mathbf{b}_{1} \equiv \mathbf{b}_{2} \equiv \mathbf{b}_{0}\left(\bmod m^{\prime}\right) \\
\wedge_{1}\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0 \\
p_{1} \nmid N\left(\mathbf{b}_{1}\right), p_{2} \nmid N\left(\mathbf{b}_{2}\right)}} \frac{g_{\mathbf{b}_{1} g_{\mathbf{b}_{2}}}}{} .
\end{aligned}
$$

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

$$
\begin{equation*}
T_{10}=T_{11}+T_{12}, \tag{11.16}
\end{equation*}
$$

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 $\left.\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)=\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) / D_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)$ we need to show that $f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}=$ $p_{1} p_{2}$ in $T_{12}$ to obtain the desired expression. We first note that since $p_{1} \nmid$ $N\left(\mathbf{b}_{1}\right)$ the multiplication-by- $\mathbf{b}_{1}$ matrix $M_{\mathbf{b}_{1}}$ is invertible $\left(\bmod p_{1}\right)$. This means that for every $\mathbf{x}\left(\bmod p_{1}\right)$ there is a unique $\mathbf{a}\left(\bmod p_{1}\right)$ such that $\mathbf{x}=$ $\mathbf{a} \diamond \mathbf{b}_{1}\left(\bmod p_{1}\right)$, and so $\mathbf{v}_{p_{1}} \cdot\left(\mathbf{a} \diamond \mathbf{b}_{1}\right)=0\left(\bmod p_{1}\right)$ is therefore a non-trivial constraint on the components of $\mathbf{a}\left(\bmod p_{1}\right)$. Similarly since $p_{2} \nmid N\left(\mathbf{b}_{2}\right)$, we see $p_{2} \mid \mathbf{v}_{p_{2}} \cdot\left(\mathbf{a} \diamond \mathbf{b}_{2}\right)$ is a non-trivial constraints on the components of $\mathbf{a}\left(\bmod p_{2}\right)$. From this it follows that we have that $f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p_{1}, p_{2}}=p_{1} p_{2}$, 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 $\mathbf{b}_{1} \propto \mathbf{b}_{2}(\bmod p)$ to $T_{11}$ is

$$
\ll \sum_{p \in\left[P_{1}, P_{2}\right]} \sum_{\mathbf{c}_{1} \propto \mathbf{c}_{2}(\bmod p)} \eta_{4}^{-2}\left(\frac{B^{6}}{p^{7}}+B^{17 / 3}\right) \ll \frac{B^{6} \eta_{4}^{-2}}{P_{1}}+\eta_{4}^{-2} P_{2}^{6} B^{17 / 3} .
$$

Thus we have

$$
\begin{equation*}
T_{11}=T_{11}^{\prime}+O\left(\frac{B^{6} \eta_{4}^{-2}}{P_{1}}+\eta_{4}^{-2} P_{2}^{6} B^{17 / 3}\right) \tag{11.17}
\end{equation*}
$$

where $T_{11}^{\prime}$ counts those terms in $T_{11}$ with $\mathbf{b}_{1} \not \propto \mathbf{b}_{2}(\bmod p)$, or equivalently with $p \nmid D_{\mathbf{b}_{1}, \mathbf{b}_{2}}$.

When $\mathbf{b}_{1} \not \propto \mathbf{b}_{2}(\bmod p)$, we see that the constraints $\left(\mathbf{a} \diamond \mathbf{b}_{1}\right)_{4}=$ $0(\bmod p)$ and $\left(\mathbf{a} \diamond \mathbf{b}_{2}\right)_{4}=0(\bmod p)$ are two linearly independent linear constraints on $\mathbf{a}(\bmod p)$. In particular, the index $f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p, p}=\left[\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right.$ : $\left.\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}, p, p}\right]$ simplifies to give
$\frac{1}{f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p, p}}=\frac{\#\left\{\mathbf{a}(\bmod p):\left(\mathbf{a} \diamond \mathbf{b}_{1}\right)_{4}=\left(\mathbf{a} \diamond \mathbf{b}_{2}\right)_{4}=\mathbf{v} \cdot\left(\mathbf{a} \diamond \mathbf{b}_{1}\right)=\mathbf{v} \cdot\left(\mathbf{a} \diamond \mathbf{b}_{2}\right)=0(\bmod p)\right\}}{p^{2}}$.
We separate the above count according to the rank of the multiplication-by-a matrix $M_{a}(\bmod p)$. Thus

$$
\begin{equation*}
\frac{1}{f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p, p}}=\sum_{i=0}^{4} \frac{1}{p^{2}} \widetilde{S}_{i}\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \tag{11.18}
\end{equation*}
$$

where $\widetilde{S}_{i}\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)$ counts those $\mathbf{a}(\bmod p)$ such that $M_{\mathbf{a}}$ has rank $i$ and satisfies $\left(\mathbf{a} \diamond \mathbf{b}_{1}\right)_{4}=\left(\mathbf{a} \diamond \mathbf{b}_{2}\right)_{4}=\mathbf{v} \cdot\left(\mathbf{a} \diamond \mathbf{b}_{1}\right)=\mathbf{v} \cdot\left(\mathbf{a} \diamond \mathbf{b}_{2}\right)=0(\bmod p)$.

First we consider $\widetilde{S}_{4}$.

## Lemma 11.8.

$$
\sum_{\mathbf{c}_{1}, \mathbf{c}_{2}(\bmod p)} \frac{1}{p^{2}} \widetilde{S}_{4}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right) \ll p^{6}
$$

Proof. In this case $M_{\mathbf{a}}$ has rank 4, and so is invertible $(\bmod p)$. Given any choice of $\mathbf{c}_{1}(\bmod p)$ with $p \nmid N\left(\mathbf{c}_{1}\right)$, we see that $\mathbf{a} \diamond \mathbf{c}_{1}=M_{\mathbf{c}_{1}} \mathbf{a}$ where the multiplication-by-c $\mathbf{c}_{1}$ matrix $M_{\mathbf{c}_{1}}$ has determinant $N\left(\mathbf{c}_{1}\right)$, and so is invertible $(\bmod p)$. Therefore, given any choice of $\mathbf{x}(\bmod p)$, there is a unique choice of $\mathbf{a}(\bmod p)$ with $p \nmid N(\mathbf{a})$ such that $\mathbf{a} \diamond \mathbf{c}_{1} \equiv$ $\mathbf{x}(\bmod p)$. Similarly, since we only consider a with $M_{\mathbf{a}}$ is invertible, given any choice of $\mathbf{y}(\bmod p)$ there is then a unique choice of $\mathbf{c}_{2}(\bmod p)$ such that $\mathbf{a} \diamond \mathbf{c}_{2} \equiv \mathbf{y}(\bmod p)$. Since there are $O\left(p^{4}\right)$ choices of $\mathbf{x}, \mathbf{y}(\bmod p)$ with $\mathbf{x}_{4}=\mathbf{y}_{4}=0$ and $\mathbf{v} \cdot \mathbf{x}=\mathbf{v} \cdot \mathbf{y}=0(\bmod p)$, there are therefore $O\left(p^{4}\right)$ choices of $\mathbf{a}, \mathbf{c}_{2}(\bmod p)$ such that $p \nmid N(\mathbf{a})$ and $\left(\mathbf{a} \diamond \mathbf{c}_{1}\right)_{4}=\left(\mathbf{a} \diamond \mathbf{c}_{2}\right)_{4}=$ $\mathbf{v} \cdot\left(\mathbf{a} \diamond \mathbf{c}_{1}\right)=\mathbf{v} \cdot\left(\mathbf{a} \diamond \mathbf{c}_{2}\right)=0(\bmod p)$. Thus we have that

$$
\sum_{\mathbf{c}_{1}, \mathbf{c}_{2}(\bmod p)} \frac{1}{p^{2}} \widetilde{S}_{4}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right) \ll p^{6}
$$

as required.
Now we consider $\widetilde{S}_{2}$ and $\widetilde{S}_{3}$.

## Lemma 11.9.

$$
\sum_{\mathbf{c}_{1}, \mathbf{c}_{2}(\bmod p)} \frac{1}{p^{2}}\left(\widetilde{S}_{2}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)+\widetilde{S}_{3}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)\right) \ll p^{6} .
$$

Proof. Since $M_{\mathbf{a}}$ is not invertible $(\bmod p)$ and has determinant $N(\mathbf{a})$, we see that $p \mid N(\mathbf{a})$ and so $p \mid N\left(\mathbf{a} \diamond \mathbf{c}_{1}\right)=N(\mathbf{a}) N\left(\mathbf{c}_{1}\right)$. Since $f\left(x_{1}, x_{2}, x_{3}\right)$ is an irreducible polynomial which splits into two linear factors over a quadratic extension, and $N\left(x_{1} \nu_{1}+x_{2} \nu_{2}+x_{3} \nu_{3}\right)$ 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 $\left(x_{1}, x_{2}, x_{3}\right)(\bmod p)$ such that $f\left(x_{1}, x_{2}, x_{3}\right)=N\left(x_{1} \nu_{1}+x_{2} \nu_{2}+x_{3} \nu_{3}\right)=$ $0(\bmod p)$. Thus there are $O\left(p^{2}\right)$ choices of $\mathbf{x}, \mathbf{y}$ with $p \mid N(\mathbf{x}), N(\mathbf{y})$ and $x_{4}=y_{4}=\mathbf{v} \cdot \mathbf{x}=\mathbf{v} \cdot \mathbf{y}=0(\bmod p)$. Given $\mathbf{c}_{1}$ with $p \nmid N\left(\mathbf{c}_{1}\right)$ and $\mathbf{x}$ and $\mathbf{y}$ as above, here is a unique $\mathbf{a}(\bmod p)$ such that $\mathbf{a} \diamond \mathbf{c}_{1} \equiv \mathbf{x}(\bmod p)$, and there are $O\left(p^{2}\right)$ choices of $\mathbf{c}_{2}$ such that $\mathbf{a} \diamond \mathbf{c}_{2} \equiv \mathbf{y}(\bmod p)$ provided $M_{\mathbf{a}}$ has rank 2 or 3 . Putting this together gives the result.

Lemma 11.10.

$$
S_{0}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right) \ll 1 .
$$

Proof. The only a such that $M_{\mathbf{a}}$ has rank 0 is the vector $\mathbf{0}(\bmod p)$.
Finally, we need to consider the situation where $M_{\mathbf{a}}$ has rank 1, which is slightly more complicated.
Lemma 11.11.

$$
\sum_{\mathbf{c}_{1}, \mathbf{c}_{2}(\bmod p)} \frac{1}{p^{2}} \widetilde{S}_{1}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right) \ll p^{6}
$$

Proof. If $M_{\mathbf{a}}$ has rank 1 , then there are $p^{3}$ choices of $\mathbf{b}(\bmod p)$ such that $M_{\mathbf{a}} \mathbf{b}=\mathbf{0}(\bmod p)$. On the other hand, let $\mathfrak{a}=\left(a_{1} \nu_{1}+a_{2} \nu_{2}+a_{3} \nu_{3}+a_{4} \nu_{4}\right)$ and $\mathfrak{b}=\left(b_{1} \nu_{1}+b_{2} \nu_{2}+b_{3} \nu_{3}+b_{4} \nu_{4}\right)$. If $M_{\mathbf{a}} \mathbf{b}=\mathbf{0}(\bmod p)$, then the ideal $\mathfrak{a b}$ is a multiple of $(p)$, and so $\mathfrak{b}$ is a multiple of $(p) / \operatorname{gcd}(\mathfrak{a},(p))$. Therefore for there to be $p^{3}$ choices of $\mathfrak{b}(\bmod p)$, 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 a such that $M_{\mathbf{a}}$ has rank 1 .

Since the rank is unchanged by replacing a with $\lambda \mathbf{a}$ for any non-zero scalar $\lambda$, we see all such 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 $\left(\mathbf{a}^{(0)} \diamond \mathbf{c}_{2}\right)_{4} \equiv \mathbf{v}$. $\left(\mathbf{a}^{(0)} \diamond \mathbf{c}_{2}\right) \equiv 0(\bmod p)$ are non-trivial on $\mathbf{c}_{2}(\bmod p)$, and call $\mathbf{a}^{(0)}$ 'exceptional' if the constraints are trivial on $\mathbf{c}_{2}(\bmod p)$. We see that if $\mathbf{a}^{(0)}$ is normal, then there are $O\left(p^{3}\right)$ choices of $\mathbf{c}_{2}(\bmod p)$ and so $O\left(p^{4}\right)$ choices of $\left(\mathbf{c}_{2}, \mathbf{a}\right)(\bmod p)$ with a a multiple of $\mathbf{a}^{(0)}$.

We now prove that when $p$ is large enough, there are no exceptional $\mathbf{a}^{(0)}$.

If $\left(\mathbf{a}^{(0)} \diamond \mathbf{c}\right)_{4} \equiv 0(\bmod p) \forall \mathbf{c}$, 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 $\mathbf{a}^{(0)}=$ $\left(a_{1}^{(0)}, a_{2}^{(0)}, a_{3}^{(0)}, a_{4}^{(0)}\right)$ and $\nu_{i} \nu_{j}=\sum_{k=1}^{4} \lambda_{i j k} \nu_{k}$, we get

$$
\sum_{i=1}^{4} \lambda_{i j 4} a_{i}^{(0)} \equiv 0(\bmod p) \quad j=1,2,3,4
$$

This implies that $p \mid \operatorname{det}\left(\lambda_{i j 4}\right)_{1 \leq i, j \leq 4}$ 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 $\mu_{1}, \mu_{2}, \mu_{3}, \mu_{4}$ such that

$$
\mu_{1}\left(\begin{array}{l}
\lambda_{114} \\
\lambda_{214} \\
\lambda_{314} \\
\lambda_{414}
\end{array}\right)+\mu_{2}\left(\begin{array}{l}
\lambda_{124} \\
\lambda_{224} \\
\lambda_{324} \\
\lambda_{424}
\end{array}\right)+\mu_{3}\left(\begin{array}{l}
\lambda_{134} \\
\lambda_{234} \\
\lambda_{334} \\
\lambda_{434}
\end{array}\right)+\mu_{4}\left(\begin{array}{l}
\lambda_{144} \\
\lambda_{244} \\
\lambda_{344} \\
\lambda_{444}
\end{array}\right)=0,
$$

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 $p \in\left[P_{1}, P_{2}\right]$.

Thus, we have that

However, we have

This gives the result.
We're now in a position to simplify our sum.
Lemma 11.12. Let

$$
T_{11}^{\prime}:=\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\ p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\ \mathbf{b}_{1} \equiv \mathbf{b}_{2} \equiv \mathbf{b}_{0}(\bmod m) \\ \wedge\left(\mathbf{b}_{1}, \mathbf{b}_{\mathbf{2}}\right) \neq 0 \\ p \nmid N\left(\mathbf{b}_{1}\right) N\left(\mathbf{b}_{2}\right) D_{\mathbf{b}_{1}, \mathbf{b}_{2}}}} \frac{g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}}}{f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p, p} \operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)} .
$$

Then we have

$$
T_{11}^{\prime} \ll \frac{X^{o(1)} B^{6}}{P_{1}}+X^{o(1)} P_{2}^{7} B^{17 / 3}
$$

Proof. Firstly, by splitting $\mathbf{b}_{1}, \mathbf{b}_{2}$ into residue classes $(\bmod p)$, we have that

$$
T_{11}^{\prime}=\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\ p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{c}_{1}, \mathbf{c}_{2}(\bmod p) \\ \mathbf{c}_{1} \not \propto \mathbf{c}_{2} \\ N\left(\mathbf{c}_{1}\right) N\left(\mathbf{c}_{2}\right) \neq 0(\bmod p)}} \sum_{\substack{\left.\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\ \mathbf{b}_{1} \equiv \mathbf{b}_{2} \equiv \mathbf{b}_{0}(\bmod m) \\ \mathbf{A ( b}_{1}, \mathbf{b}_{2}\right) \neq 0 \\ \mathbf{b}_{1} \equiv \mathbf{c}_{1}(\bmod p) \\ \mathbf{b}_{2} \equiv \mathbf{c}_{2}(\bmod p)}} \frac{g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}}}{f_{\mathbf{b}_{1}, \mathbf{b}_{2}, p, p} \operatorname{det}\left(\Lambda_{\left.\mathbf{b}_{1}, \mathbf{b}_{2}\right)}\right)} .
$$

Using our expression 11.18, we see that this is given by

$$
\sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\ p \equiv 1\left(\bmod D_{f}\right)}} \sum_{\substack{\mathbf{c}_{1}, \mathbf{c}_{2}(\bmod p) \\ \mathbf{c}_{1} \notin \mathbf{c}_{2} \\ N\left(\mathbf{c}_{1}\right) N\left(\mathbf{c}_{2}\right) \neq 0(\bmod p)}} \sum_{j=0}^{4} \frac{\widetilde{S}_{j}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)}{p^{2}} \sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\ \mathbf{b}_{1} \equiv \mathbf{b}_{2} \equiv \mathbf{b}_{0}(\bmod m) \\ \wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0 \\ \mathbf{b}_{1} \equiv \mathbf{c}_{1}(\bmod p) \\ \mathbf{b}_{2} \equiv \mathbf{c}_{2}(\bmod p)}} \frac{g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}}}{\operatorname{det}\left(\Lambda_{\left.\mathbf{b}_{1}, \mathbf{b}_{2}\right)}\right)} .
$$

Using Lemma 11.11 we get

where
$T\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right):=\widetilde{S}_{0}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)+E_{1}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)+\widetilde{S}_{2}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)+\widetilde{S}_{3}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)+\widetilde{S}_{4}\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)$.
By Lemma 11.5. we have that

$$
\quad \sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\ \mathbf{b}_{1} \equiv \mathbf{b}_{2} \equiv \mathbf{b}_{0}(\bmod m)}} \frac{\left|g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}}\right|}{\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)} \ll \frac{\eta_{4}^{-2} B^{6}}{p^{8}}+\eta_{4}^{-2} B^{17 / 3}
$$

Lemmas $11.10,11.11,11.9,11.8$ show that

$$
\sum_{\mathbf{c}_{1}, \mathbf{c}_{2}(\bmod p)} \frac{T\left(\mathbf{c}_{1}, \mathbf{c}_{2}\right)}{p^{2}} \ll p^{6} .
$$

Thus we see that the term $T_{11}^{\prime} 11.19$ is

$$
\ll \eta_{4}^{-2} \sum_{\substack{p \in\left[P_{1}, P_{2}\right] \\ p \equiv 1\left(\bmod D_{f}\right)}} p^{6}\left(\frac{B^{6}}{p^{8}}+B^{17 / 3}\right) \ll \frac{\eta_{4}^{-2} B^{6}}{P_{1}}+\eta_{4}^{-2} B^{17 / 3} P_{2}^{7} .
$$

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

$$
T_{12} \ll\left|S_{s e p}\right|+\frac{X^{o(1)} B^{6}}{P_{1}}+X^{o(1)} P_{2}^{7} B^{17 / 3}
$$

where, $S_{\text {sep }}$ is given by

$$
S_{s e p}:=\sum_{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}} \sum_{\mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2}} \frac{g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}} D_{\mathbf{b}_{1}, \mathbf{b}_{2}}}{\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)} .
$$

Proof. We wish to reintroduce terms with $p_{1} \nmid N\left(\mathbf{b}_{1}\right)$ and $p_{2} \nmid N\left(\mathbf{b}_{2}\right)$ so that the inner sum is independent of $p_{1}, p_{2}$. There are $O\left(p_{1}^{3}\right)$ choices of $\mathbf{c}_{1}\left(\bmod p_{1}\right)$ such that $p_{1} \mid N\left(\mathbf{c}_{1}\right)$. Thus, by Lemma 11.5, we see that the terms with $p_{1} \mid N\left(\mathbf{b}_{1}\right)$ contribute a total

$$
\begin{aligned}
& \sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\
p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \frac{1}{p_{1} p_{2}} \sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\
\mathbf{b}_{1} \equiv \mathbf{b}_{2}=\mathbf{b}_{0}(\bmod m) \\
\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0 \\
p_{1} \mid N\left(\mathbf{b}_{1}\right)}} \frac{\left|g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}}\right| D_{\mathbf{b}_{1}, \mathbf{b}_{2}}}{\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)} \\
& \ll \sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\
p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \frac{1}{p_{1} p_{2}} \sum_{\substack{\mathbf{c}_{1}, \mathbf{c}_{2}\left(\bmod \\
p_{1} \mid N\left(\mathbf{c}_{1}\right)\right.}} \sum_{\substack{\left.p_{1}\right)}} \frac{\left|g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}}\right| D_{\mathbf{b}_{1}, \mathbf{b}_{2}}}{\wedge\left(\mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2}, \mathbf{b}_{2}\right)} \\
& \ll \sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\
p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \frac{\eta_{4}^{-2}}{p_{1} p_{2}} p_{1}^{7}\left(\frac{B^{6}}{p_{1}^{8}}+B^{17 / 3}\right) \\
& \ll \frac{\eta_{4}^{-2} B^{6}}{P_{1}}+\eta_{4}^{-2} P_{2}^{7} B^{17 / 3} .
\end{aligned}
$$

Similarly, we see that terms $p_{2} \mid N\left(\mathbf{b}_{2}\right)$ contribute a total $O\left(B^{6} / P_{1}+\right.$ $\left.P_{2}^{7} B^{17 / 3}\right)$. Thus we find that

$$
\begin{gathered}
T_{12}=\left(\sum_{\substack{p_{1}, p_{2} \in\left[P_{1}, P_{2}\right] \\
p_{1} \equiv p_{2} \equiv 1\left(\bmod D_{f}\right)}} \frac{1}{p_{1} p_{2}}\right)\left(\sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\
\mathbf{b}_{1} \equiv \mathbf{b}_{2} \equiv \mathbf{b}_{0}(\bmod m) \\
\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \neq 0}} \frac{g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}} D_{\mathbf{b}_{1}, \mathbf{b}_{2}}}{\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)}\right) \\
\\
+O\left(\frac{\eta_{4}^{-2} B^{6}}{P_{1}}+\eta_{4}^{-2} P_{2}^{7} B^{17 / 3}\right) .
\end{gathered}
$$

Noting that the sum over $p_{1}, p_{2}$ is $O(1)$, this gives the result.
Thus it remains to bound $S_{\text {sep }}$.

### 11.8 Reduction to small residue classes and small boxes

We first show that the contribution to $S_{\text {sep }}$ from terms with $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}>$ $(\log B)^{K_{2}}$ or $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \leq B^{2} /(\log B)^{K_{2}}$ is negligible if $K_{2}$ is large compared with $K_{1}$.
Lemma 11.14. Let $K_{2}>0$ We have

$$
\sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2} \\ \wedge\left(\mathbf{b}_{2}, \mathbf{b}_{2}\right)>0}}^{{\max \left(B^{2} / \wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right), D_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)>(\log B)^{K_{2}}} \frac{\left|g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}}\right|}{\operatorname{det}\left(\Lambda_{\mathbf{b}_{1}, \mathbf{b}_{2}}\right)}} \ll \frac{\eta_{4}^{-2} B^{6}}{(\log X)^{K_{2}}} .
$$

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
$\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \ll B^{4 / 3}$ is $O\left(\eta_{4}^{-2} B^{17 / 3}\right)$, and the contribution from terms with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \sim B^{2} / C$ (for $C=2^{j} \ll B^{2 / 3}$ ) and $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d$ is

$$
\ll \eta_{4}^{-2} \frac{d C}{B^{2}}\left(B+\frac{B^{4}}{C^{3} d^{3}}\right) B^{4}
$$

Thus we see that the total contribution is

$$
\ll \eta_{4}^{-2} B^{17 / 3}+\eta_{4}^{-2} \sum_{C=2^{j} \ll B^{2 / 3}} \sum_{\substack{d \leq B \\ \max (d, C)>(\log B)^{K_{2}}}} d C\left(B^{3}+\frac{B^{6}}{C^{3} d^{3}}\right) \ll \frac{\eta_{4}^{-2} B^{6}}{(\log B)^{K_{2}}} .
$$

Thus we just need to consider $D_{\mathbf{b}_{1}, \mathbf{b}_{2}} \leq(\log x)^{K_{2}}$ and $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \geq$ $B^{2} /(\log x)^{K_{2}}$.
Lemma 11.15. Imagine that for every cube $\mathcal{C} \subseteq[1, B]^{4}$, every and any c $(\bmod d)$ we have

$$
\sum_{\substack{\mathbf{b} \in \mathbb{Z}^{4} n \mathcal{C} \\ \mathbf{b} \equiv \mathbf{c}(\bmod d)}} g_{\mathbf{b}} \ll{ }_{K} \eta_{4}^{5000} B^{4} .
$$

Then we have

$$
S_{\text {sep }} \ll K_{K} \eta_{4}^{20} B^{6}
$$

Proof. Let $\eta_{6}=\eta_{4}^{30}$. By Lemma 11.14 the contribution to $S_{\text {sep }}$ from terms with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)<\eta_{6} B^{2}$ or from $D_{\mathbf{b}_{1}, \mathbf{b}_{2}}>\eta_{6}^{-1}$ is $O\left(\eta_{4}^{20} B^{6}\right)$. Thus we may focus on the remaining terms.

Since $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)$ is continuous in $\mathbf{b}_{1}, \mathbf{b}_{2}$ we see that if a pair of cubes $\mathcal{C}_{1}^{\prime}, \mathcal{C}_{2}^{\prime}$ of side length $\eta_{6}^{2} B$ contains a point with $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right) \geq \eta_{6} B^{2}$, then in fact for all $\mathbf{b}_{1}^{\prime} \in \mathcal{C}_{1}^{\prime}$ and $\mathbf{b}_{2} \in \mathcal{C}_{2}^{\prime}$ we have $\wedge\left(\mathbf{b}_{1}^{\prime}, \mathbf{b}_{2}^{\prime}\right)=\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)\left(1+O\left(\eta_{6}\right)\right)$. Thus we may replace $\wedge\left(\mathbf{b}_{1}, \mathbf{b}_{2}\right)$ with

$$
\wedge\left(\mathcal{C}_{1}^{\prime}, \mathcal{C}_{2}^{\prime}\right):=\sup _{\mathbf{x} \in \mathcal{C}_{1}^{\prime}, \mathbf{y} \in \mathcal{C}_{2}^{\prime}} \wedge(\mathbf{x}, \mathbf{y})
$$

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

$$
S_{\text {sep }} \ll \eta_{4}^{20} B^{6}+\frac{\eta_{6}^{-9}}{B^{2}} \sum_{d \leq \eta_{6}^{-1}} d \sup _{\substack{\mathcal{C}_{1}^{\prime}, \mathcal{C}_{2}^{\prime}}} \sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}^{\prime}, \mathbf{b}_{2} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2}^{\prime} \\ D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d}} g_{\mathbf{b}_{1}} g_{\mathbf{b}_{2}} .
$$

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

$$
\begin{aligned}
\mathbf{1}_{D_{\mathbf{b}_{1}, \mathbf{b}_{2}}=d} & =\sum_{e \mid D_{\mathbf{b}_{1}, \mathbf{b}_{2}} / d} \mu(e) \\
& =\sum_{e \leq \eta_{6}^{-20}} \mu(e) \mathbf{1}_{\mathbf{b}_{1} \propto \mathbf{b}_{2}(\bmod d e)}+O\left(\eta_{6}^{-20} \mathbf{1}_{D_{\mathbf{b}_{1}, \mathbf{b}_{2}} \geq \eta_{6}^{-20}}\right) .
\end{aligned}
$$

By Lemma 11.4 the contribution of the second term to $S_{\text {sep }}$ is $O\left(\eta_{4}^{20} B^{6}\right)$. Thus we see that

$$
\begin{equation*}
S_{\text {sep }} \ll \eta_{4}^{20} B^{6}+\frac{\eta_{6}^{-31}}{B^{2}} \sup _{\substack{\mathcal{C}_{1}^{\prime}, \mathcal{C}_{2}^{\prime} \\ d e \ll \eta_{6}^{-21}}}\left|S_{\text {sep }}^{\prime}\right| \tag{11.20}
\end{equation*}
$$

where

$$
S_{s e p}^{\prime}:=\sum_{\substack{\mathbf{b}, \lambda_{1}, \lambda_{2}(\bmod d e)}}\left(\sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}^{\prime}, \mathbf{b}_{1} \equiv \lambda_{1} \mathbf{b}(\bmod d e) \\ \mathbf{b}_{1} \equiv \mathbf{b}_{0}(\bmod m)}} g_{\mathbf{b}_{1}}\right)\left(\sum_{\substack{\mathbf{b}_{\mathbf{2}} \in \mathbb{Z}^{4} \cap \mathcal{C}_{2}^{\prime}, \mathbf{b}_{2} \equiv \lambda_{2} \mathbf{b}(\bmod d e) \\ \mathbf{b}_{2} \equiv \mathbf{b}_{0}(\bmod m)}} g_{\mathbf{b}_{2}}\right) .
$$

By assumption of the lemma, we have that

$$
\sum_{\substack{\mathbf{b}_{1} \in \mathbb{Z}^{4} \cap \mathcal{C}_{1}^{\prime}, \mathbf{b}_{1} \equiv \lambda_{1} \mathbf{b}(\bmod d e) \\ \mathbf{b}_{1} \equiv \mathbf{b}_{0}(\bmod m)}} g_{\mathbf{b}_{1}} \ll \eta_{4}^{5000} B^{4} .
$$

Substituting this in then gives $\left|S_{\text {sep }}\right| \ll \eta_{4}^{50} B^{6}+\eta_{4}^{5000} \eta_{6}^{-160} B^{6} \ll \eta_{4}^{50} B^{6}$.

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

$$
\sum_{\substack{\mathbf{b} \in \mathbb{Z}^{4} \cap \mathcal{C} \\ \mathbf{b} \equiv \mathbf{c}(\bmod d)}}\left(\mathbf{1}_{\mathcal{R}}(\mathbf{b})-\widetilde{\mathbf{1}}_{\mathcal{R}}(\mathbf{b})\right)<_{K} \frac{B^{4}}{(\log B)^{K}} .
$$

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 $\mathbf{1}_{\mathcal{R}}(b)$. 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 $\mathbf{1}_{\mathcal{R}}(b)$, giving an explicit main term and an error term which is $O_{K}\left(B^{4} /(\log B)^{K}\right)$. 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 $O_{\overparen{K}}\left(B^{4} /(\log B)^{K}\right)$.

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 $\eta_{4}$ is chosen sufficiently large, we may replace $g_{\mathbf{b}}$ with $\mathbf{1}_{\mathcal{R}}\left(\mathfrak{b} / \mathfrak{c}^{\prime}\right)-\widetilde{\mathbf{1}}_{\mathcal{R}}\left(\mathfrak{b} / \mathfrak{c}^{\prime}\right)$ at the cost of an acceptable error term whenever $\mathfrak{c}^{\prime} \mid \mathfrak{b}$. We note that $\mathfrak{c}^{\prime} \mid \mathfrak{b}$ is determined by a congruence condition on $\mathbf{b}\left(\bmod N\left(\mathfrak{c}^{\prime}\right)\right)$, and recall than $N\left(\mathfrak{c}^{\prime}\right) \ll(\log X)^{o(1)}$. 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 $\left|\widetilde{\mathcal{A}}\left(X_{0}\right)\right| \asymp \eta_{1}^{3} X_{0}^{3}$. 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

$$
T_{1}(\mathcal{R})=\sum_{\mathcal{C} \in C l_{K}} \sum_{\substack{\mathbf{a}_{0}, \mathbf{b}_{0}\left(\bmod m^{\prime}\right) \\ N(\mathfrak{c})\left(\mathbf{a}_{0} \diamond \mathbf{b}_{0}\right)_{i} \equiv\left(\mathbf{v}_{0}\right)_{i}\left(\bmod m^{\prime}\right)}} T_{3}(\mathcal{R})+O\left(X^{3+\epsilon} / P_{1}\right),
$$

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

$$
\begin{gathered}
T_{3}(\mathcal{R})^{2} \ll X^{o(1)} A^{4}\left(A^{3} B^{3}+A B^{7} P_{2}^{2}+A^{2} B^{17 / 3} P_{2}^{7}+\frac{A^{2} B^{6}}{P_{1}}\right) \\
+A^{4}\left(\eta_{4} A^{2} B^{6}+\eta_{4}^{-12} A^{2} \cdot \eta_{4}^{20} B^{6}\right)
\end{gathered}
$$

Since $\prod_{i=1}^{3} X_{i} \gg A^{3} B^{3}(\log X)^{-K}$, this gives the result provided

$$
A<B^{3-\epsilon}, \quad B P_{2}^{2}<A^{1-\epsilon}, \quad P_{2}^{21}<B^{1-\epsilon},
$$

and the constant $K_{1}$ defining $\eta_{4}$ is taken sufficiently large in terms of $K$. (Here we used that the second inequality implies 11.8).) After taking $\epsilon$ 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 $\tau \leq \min \left(4-2 \theta_{1}^{\prime}-\cdots-2 \theta_{\ell^{\prime}}^{\prime}, \theta_{1}+\cdots+\theta_{\ell^{\prime}}-1\right) / 100$. 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. Erdôs. 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):6780, 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


[^0]:    ${ }^{1}$ 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

[^1]:    ${ }^{2}$ We can check that $P_{1}(X)+\left(r_{1} r_{2}+r_{3} r_{4}\right)$ and $P_{2}(X)+\left(r_{1} r_{2}+r_{3} r_{4}\right)\left(X+\sum_{i<j} r_{i} r_{j}\right)$ have coefficients which are symmetric integer polynomials in the $r_{i}$, and so are in $\mathbb{Z}[X]$. Since $r_{1} r_{2}+r_{3} r_{4} \in \mathbb{Z}$, it follows that $P_{1}(X)$ and $P_{2}(X)$ are in $\mathbb{Z}[X]$.

[^2]:    ${ }^{3}$ If $\Delta_{1}=\Delta_{2}=0$ then the roots of $r_{1}+r_{2}$ and $r_{1} r_{2}$ are in $\mathbb{Q}$. This contradicts the fact that $\left[\mathbb{Q}\left(r_{1}\right): \mathbb{Q}\right]=4$.

[^3]:    ${ }^{4}$ In [1] and 4] this form corresponds to the form $q_{4}$.

[^4]:    ${ }^{5}$ 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 $m$.

