

On the representation of primes by cubic polynomials in two variables

D.R. Heath-Brown

Mathematical Institute, Oxford

B.Z. Moroz

Max-Planck-Institut für Mathematik, Bonn

1. Introduction and statement of the main results

The goal of this paper is to give a proof of the following theorem, which may be regarded as an instance of Schinzel's Hypothesis; it implies, in particular, a hypothesis introduced in a recent paper of the first author (see [2, Hypothesis 4]).

Theorem 1. *Let $f_0(\vec{x})$ be a binary cubic form with integral rational coefficients irreducible in $\mathbb{Z}[\vec{x}]$. For $d \in \mathbb{Z}$ and $\vec{\gamma} \in \mathbb{Z}^2$, let the positive integer γ_0 be chosen so that $f(\vec{x}) = \gamma_0^{-1} f_0(\vec{\gamma} + d\vec{x})$ is a primitive polynomial with integral rational coefficients. Suppose, moreover, that no prime divides $f(\vec{a})$ for every \vec{a} in \mathbb{Z}^2 . Then the set $f(\mathbb{Z}^2)$ contains infinitely many rational primes.*

We shall use the technique developed in [3], and then applied in [4] to treat a general binary cubic form; consequently, the reader is advised to familiarize himself with the contents of those papers before studying the present one. As in [3, 4], we shall actually obtain an asymptotic formula for the relevant number of primes. Note that we cannot handle every binary cubic polynomial which splits over \mathbb{Q} . In particular our methods do not suffice to treat the polynomial

$$N_{\mathbb{Q}(\sqrt[3]{2}, \vec{x})/\mathbb{Q}(\vec{x})}(x_1 + x_2\sqrt[3]{2} + \sqrt[3]{4}) = x_1^3 - 6x_1x_2 + 2x_2^3 + 4, \quad \vec{x} := (x_1, x_2).$$

The reasons for this failure are subtle - the Type I sums can be handled satisfactorily, but not the Type II sums.

In what follows, we shall retain the notational conventions introduced in [4, § 1]. Let $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$, and \mathbb{N} stand for the fields of complex, real, rational numbers, the ring of rational integers, and the set of positive rational integers, respectively. Let k be a cubic number field; as in [4], let $\mathfrak{o}, \mathcal{I}, P$, and \mathcal{P} denote respectively the ring of integers of k , the monoid of integral ideals in k , the set of rational primes, and the set of prime ideals in \mathfrak{o} . Given a sequence D of rational integers and a sequence \mathcal{D} of ideals in \mathcal{I} , let $D_a = \{c : c \in D, a|c\}$ and $\mathcal{D}_a = \{\mathfrak{c} : \mathfrak{c} \in \mathcal{D}, \mathfrak{a}|\mathfrak{c}\}$ for $a \in \mathbb{N}$ and $\mathfrak{a} \in \mathcal{I}$. In formulae, we shall sometimes use the abbreviation $(a, b) := \text{h.c.f.}(a, b)$.

Let us fix a \mathbb{Z} -submodule F of \mathfrak{o} of rank 2, an integer d in \mathbb{N} , and a vector $\vec{\gamma}$ in \mathbb{Z}^2 . As in [4], let $F = \{a_1\omega_1 + a_2\omega_2 : \vec{a} \in \mathbb{Z}^2\}$, so that $k = \mathbb{Q}(\theta_0)$ with $\theta_0 := \omega_2\omega_1^{-1}$. For $\vec{u} \in \mathbb{Z}^2$, we shall sometimes write $u = u_1\omega_1 + u_2\omega_2$; in particular, $\gamma = \gamma_1\omega_1 + \gamma_2\omega_2$. Let $\mathfrak{d} = (\gamma, d\omega_1, d\omega_2)$ be the ideal in \mathfrak{o} generated by dF and γ , and let

$$f(\vec{x}) = N_{k(\vec{x})/\mathbb{Q}(\vec{x})}(\gamma + dx)N\mathfrak{d}^{-1}. \quad (1.1)$$

Clearly, $f(\vec{x}) \in \mathbb{Z}[\vec{x}]$ and the polynomial $f(\vec{x})$ is irreducible in $\mathbb{Q}(\vec{x})$; moreover, it follows from the general theory (see, for instance, [7, chapter II]) that $f(\vec{x})$ is a primitive polynomial. Let $\varepsilon(f)$ denote the highest common factor of the integer values $\{f(\vec{a}) : \vec{a} \in \mathbb{Z}^2\}$ of f . Write, for brevity, $\eta := (\log X)^{-c}$, where c is a suitable positive constant defined as in [3, 4], and consider the square

$$I(X) := \{\vec{u} : \vec{u} \in \mathbb{R}^2, X < u_1, u_2 \leq X(1 + \eta)\}.$$

Let

$$\pi(f, X) := \# \{p : p \in P, p = f(\vec{a}), \vec{a} \in I(X)\}.$$

Let $h_f := d^3 N(\mathfrak{d}^{-1}(\omega_1 + \omega_2))$, so that $f(\vec{a}) = h_f X^3(1 + O(\eta))$ for $\vec{a} \in I(X)$, cf. [4, Lemma 2.3]. Without loss of generality, it may be assumed that $h_f > 0$. We can now state our main result.

Theorem 2. *If $\varepsilon(f) = 1$, then*

$$\pi(f, X) = \sigma_1(f) \frac{\eta^2 X^2}{3 \log X} \{1 + O((\log \log X)^{-1/6})\} \quad (1.2)$$

as $X \rightarrow \infty$, with $\sigma_1(f) > 0$ given by (3.1).

Theorem 1 follows from Theorem 2 because the polynomial f considered in Theorem 1 may be defined by an equation of the form (1.1).

Remark 1. In [4, § 2] it has been observed that $\varepsilon(f_0) \in \{1, 2\}$ and that if $\varepsilon(f_0) = 2$, then $f_0(\vec{x}) = 2g(\vec{y})$, where $x_1 = 2y_1$, $x_2 = y_2$, and g is a

binary cubic form irreducible in $\mathbb{Z}[\bar{y}]$ with $\varepsilon(g) = 1$. It will be shown here (see Lemma 2.4) that $\varepsilon(f) \in \{1, 2, 3, 6\}$ and, moreover, $\varepsilon(f) = \varepsilon(f_0)$ if $\text{h.c.f.}(6, d)=1$.

As an application of our theorem we have the following results about rational points on cubic surfaces. We remark that unconditional results of the type given by Corollary 1.2 are few and far between.

Corollary 1.1 *Suppose that a_1, a_2, a_3, a_4, a_5 are integers coprime to 3, and assume that none of them is divisible by the square of any prime $p = 2 \pmod{3}$. Then if*

$$\sum_{i=1}^5 a_i x_i^3 = 0$$

has non-zero p -adic solutions for every p , it will have non-zero integral solutions, providing that the Selmer Conjecture holds.

Proof. This follows from [2, Theorem 4], since Hypothesis 4 introduced in [2] is a special case of Theorem 2 stated above.

Remark 2. For precise formulation of the Selmer (Parity) Conjecture see [2, Hypothesis 1].

Corollary 1.2 *Let a and b be coprime rational integers satisfying one of the following congruence conditions:*

$$a \text{ or } b = \pm 2 \text{ or } \pm 3 \pmod{9}, \quad (1.3)$$

or

$$a = \pm b \pmod{9}. \quad (1.4)$$

Then there is a nontrivial rational point on the surface

$$x_0^3 + 2x_1^3 + ax_2^3 + bx_3^3 = 0.$$

Proof. The result is trivial if a/b is a rational cube. Otherwise the corollary will be an easy consequence of our theorem and a result of Satgé [6, Proposition 3.3]. The latter states that the curve

$$x_0^3 + 2x_1^3 = pZ^3$$

has a non-trivial rational point for any prime $p = 2 \pmod{9}$. Under the hypotheses of the corollary we can find integers a_0, b_0 such that either $aa_0^3 + bb_0^3 = 2 \pmod{9}$, in the case of (1.3), or $27|aa_0^3 + bb_0^3$ and $(aa_0^3 + bb_0^3)/27 = 2 \pmod{9}$ in case (1.4). If we choose

$$f(x, y) = a(a_0 + 3x)^3 + b(b_0 + 3y)^3$$

or

$$f(x, y) = \frac{a(a_0 + 81x)^3 + b(b_0 + 81y)^3}{27}$$

in the two cases, our Theorem 2 produces a prime $p = f(x, y)$; by construction $p \equiv 2 \pmod{9}$, and the result follows.

Remark 3. The reader will note that neither Corollary 1, nor Corollary 2 can be deduced from our previous results on representation of primes by binary cubic forms obtained in [4]. In both cases the applications require congruence conditions on the primes to be represented.

2. Some subsidiary estimates

As in [4], let $\theta = \theta_0 N(\omega_1(\omega_1, \omega_2)^{-1})$; write $i(\theta) = (\mathfrak{o} : \mathbb{Z}[\theta])$. From now on we shall assume, without loss of generality, that $\text{h.c.f.}(\gamma_1, \gamma_2, d) = 1$ and let $C = i(\theta)N(\omega_1\omega_2)d$. For $\vec{u} \in \mathbb{Z}^2$, let $\mathfrak{A}_u(\gamma) := (\gamma + ud)\mathfrak{d}^{-1}$, so that $f(\vec{x}) = N_{k(\vec{x})/\mathbb{Q}(\vec{x})}\mathfrak{A}_x(\gamma)$. Let

$$\mathcal{A} = \{\mathfrak{A}_a(\gamma) : \vec{a} \in I(X) \cap \mathbb{Z}^2, \text{h.c.f.}(\gamma_1 + a_1d, \gamma_2 + a_2d) = 1\}.$$

Let further

$$\mathcal{R} = \{R : R \in \mathcal{I}, \mu(R)^2 = 1, \mu\left(\frac{NR}{N((R, C))}\right)^2 = 1\}.$$

By [4, Lemma 2.2] (cf. also [3, Lemma 3.1]), if $\mathfrak{p}_i | \mathfrak{B}$, $\mathfrak{p}_i | p$, $\mathfrak{p}_i \in \mathcal{P}$, $i = 1, 2$, for some \mathfrak{B} in \mathcal{A} and some p in P and if p is non-singular, that is if p does not divide $i(\theta)N(\omega_1\omega_2)$, then $\mathfrak{p}_1 = \mathfrak{p}_2$ and $N\mathfrak{p}_1 = p$. Therefore, as it has been remarked in [4, p.261],

$$(\{R : R \in \mathcal{I}, \mu(R)^2 = 1\} \cap \mathcal{A}) \subseteq \mathcal{R}.$$

Let $A = \{N\mathfrak{a} \mid \mathfrak{a} \in \mathcal{A}\}$, then

$$A = \{f(\vec{a}) : \vec{a} \in I(X) \cap \mathbb{Z}^2, \text{h.c.f.}(\gamma_1 + a_1d, \gamma_2 + a_2d) = 1\}.$$

For $R \in \mathcal{R}$, let $r := NR$ and

$$\sigma(R, X; \gamma, \vec{\beta}) = \# \{\vec{u} : \vec{u} \in \mathbb{Z}^2 \cap I(X, \vec{\beta}), R | \mathfrak{A}_u(\gamma)\}, \quad (2.1)$$

where $I(X, \vec{\beta}) := \{\vec{u} : \vec{u} + \vec{\beta} \in I(X)\}$, so that $I(X) = I(X, \vec{0})$. Further, let

$$\mathfrak{m}(R, \gamma) = \{\vec{u} : \vec{u} \in \mathbb{Z}^2, \vec{u} \bmod r, R | \mathfrak{A}_u(\gamma)\},$$

$$m(R, \gamma) = \frac{1}{r} \# \mathfrak{m}(R, \gamma),$$

and

$$\sigma_0(R, a; \gamma) = \sum_{\vec{u} \in \mathfrak{m}(R, \gamma)} e_r(\vec{a}\vec{u}),$$

so that

$$m(R, \gamma) = \frac{\sigma_0(R, 0; \gamma)}{r}.$$

As in [3, pp.28-29] and [4, p.261], it follows that

$$\sigma(R, X; \gamma, \vec{\beta}) = r^{-2} \sum_{\substack{\vec{a} \bmod r, \vec{x} \in I(X, \vec{\beta}) \\ \vec{u} \in \mathfrak{m}(R, \gamma)}} e_r(\vec{a}(\vec{u} - \vec{x}))$$

and therefore

$$\sigma(R, X; \gamma, \vec{\beta}) = r^{-2} \sum_{\substack{\vec{a} \bmod r \\ \vec{x} \in I(X, \vec{\beta})}} \sigma_0(R, a; \gamma) e_r(-\vec{a}\vec{x}). \quad (2.2)$$

Lemma 2.1. *The sum $\sigma_0(R, a; \gamma)$ is weakly multiplicative, that is*

$$\sigma_0(ST, a; \gamma) = \sigma_0(S, a; \gamma) \sigma_0(T, a; \gamma)$$

as soon as $\text{h.c.f.}(N_{k/\mathbb{Q}}S, N_{k/\mathbb{Q}}T) = 1$.

Proof. Suppose that $\text{h.c.f.}(N_{k/\mathbb{Q}}S, N_{k/\mathbb{Q}}T) = 1$. By the Chinese Remainder Theorem,

$$\mathfrak{m}(ST, \gamma) = \mathfrak{m}(S, \gamma) \times \mathfrak{m}(T, \gamma).$$

The assertion of the lemma follows from this relation and the definition of $\sigma_0(R, a; \gamma)$.

By definition,

$$\mathcal{A}_R = \{\mathfrak{A}_a : \vec{a} \in I(X) \cap \mathbb{Z}^2, \text{ h.c.f.}(\gamma_1 + a_1d, \gamma_2 + a_2d) = 1, R|\mathfrak{A}_a(\gamma)\}.$$

For $R \in \mathcal{R}$, let

$$[\mathcal{A}_R] := \frac{\eta^2 X^2 m(R, \gamma)}{r} \sum_{(\delta, d)=1, \delta \in \mathbb{N}} \frac{\mu(\delta)}{\delta^2} \cdot \frac{N((R, \delta))}{m((R, \delta), \gamma)}, \quad (2.3)$$

and let

$$\# \mathcal{A}_R = [\mathcal{A}_R] + \rho_1(R, X). \quad (2.4)$$

Lemma 2.2. *For any positive integer l , there is a constant $c(l)$ such that*

$$\sum_{\substack{Q < NR \leq 2Q \\ R \in \mathcal{R}}} \tau(R)^l |\rho_1(R, X)| \ll (Q + XQ^{1/2} + X^{3/2})(\log QX)^{c(l)}.$$

Proof. Clearly,

$$\# \mathcal{A}_R = \sum_{\delta \in \mathbb{N}} \mu(\delta) \# \mathcal{A}_R^{(\delta)}, \quad (2.5)$$

where

$$\mathcal{A}_R^{(\delta)} := \{\vec{a} : \vec{a} \in I(X) \cap \mathbb{Z}^2, \delta | \text{h.c.f.}(\gamma_1 + a_1 d, \gamma_2 + a_2 d), R | \mathfrak{A}_a(\gamma)\}.$$

Since $\text{h.c.f.}(\gamma_1, \gamma_2, d) = 1$, the summation in (2.5) may be restricted by the condition $\text{h.c.f.}(\delta, d) = 1$.

Suppose that $R \in \mathcal{R}$ and let $R_1^{(\delta)} = \frac{R}{(R, \delta)}$ for $\delta \in \mathbb{N}$. It follows from Lemma 2.1 that

$$m(R, \gamma) = m((R, \delta), \gamma) m(R_1^{(\delta)}, \gamma). \quad (2.6)$$

Assuming further that $\text{h.c.f.}(\delta, d) = 1$ and $\mu(\delta)^2 = 1$, let $\vec{\beta}^{(\delta)}$ be defined by the conditions:

$$\delta | (\vec{\gamma} + \vec{\beta}^{(\delta)} d), \quad 0 \leq \beta_1^{(\delta)}, \beta_2^{(\delta)} < \delta.$$

It can be easily seen that

$$m(R_1^{(\delta)}, \gamma) = m(R_1^{(\delta)}, \frac{\gamma + \beta^{(\delta)} d}{\delta}). \quad (2.7)$$

On substituting equations (2.6) and (2.7) in (2.3), one obtains

$$[\mathcal{A}_R] := \frac{\eta^2 X^2}{r} \sum_{(\delta, d)=1, \delta \in \mathbb{N}} \frac{\mu(\delta)}{\delta^2} m(R_1^{(\delta)}, \frac{\gamma + \beta^{(\delta)} d}{\delta}) N((R, \delta)). \quad (2.8)$$

Moreover, equation (2.5) may be rewritten as follows

$$\# \mathcal{A}_R = \sum_{\delta \in \mathbb{N}, (\delta, d)=1} \mu(\delta) \# \mathcal{B}_R^{(\delta)},$$

where

$$\mathcal{B}_R^{(\delta)} := \{\vec{b} : \vec{b} \in I(\frac{X}{\delta}, \frac{\beta^{(\delta)}}{\delta}) \cap \mathbb{Z}^2, R | \delta \mathfrak{A}_b(\frac{\gamma + \beta^{(\delta)} d}{\delta})\}.$$

In view of (2.1), this gives

$$\# \mathcal{A}_R = \sum_{\delta \in \mathbb{N}, (\delta, d)=1} \mu(\delta) \sigma(R_1^{(\delta)}, \frac{X}{\delta}; \frac{\gamma + \beta^{(\delta)} d}{\delta}, \frac{\beta^{(\delta)}}{\delta}). \quad (2.9)$$

As in [3, p.29] and [4, p.261], it follows from (2.2) that

$$\sigma(R, X; \gamma, \vec{\beta}) = \frac{\eta^2 X^2 m(R, \gamma)}{r} + \rho(R, X; \gamma, \vec{\beta}), \quad (2.10)$$

with

$$\rho(R, X; \gamma, \vec{\beta}) = r^{-2} \sum_{\substack{\vec{a} \bmod r, \vec{a} \neq \vec{0} \\ \vec{x} \in I(X, \vec{\beta})}} \sigma_0(R, a; \gamma) e_r(-\vec{a}\vec{x}) + O\left(\frac{Xm(R, \gamma)}{r}\right).$$

In view of (2.8) and (2.9), we conclude that (2.4) holds with

$$\rho_1(R, X) = \sum_{\delta \in \mathbb{N}, (\delta, d)=1} \mu(\delta) \rho(R_1^{(\delta)}, \frac{X}{\delta}; \frac{\gamma + \beta^{(\delta)}d}{\delta}, \frac{\beta^{(\delta)}}{\delta}). \quad (2.11)$$

Since $m(S, \gamma) = 1$ as soon as $\text{h.c.f.}(S, C) = 1$, it follows from (2.6) that $m(R, \gamma) = m((R, C), \gamma) = O(1)$. Therefore

$$\rho(R, X; \gamma, \vec{\beta}) = \Sigma_0 + O\left(\frac{X}{r}\right), \quad (2.12)$$

with

$$\Sigma_0 = r^{-2} \sum_{\substack{\vec{a} \bmod r, \vec{a} \neq \vec{0} \\ \vec{x} \in I(X, \vec{\beta})}} \sigma_0(R, a; \gamma) e_r(-\vec{a}\vec{x}).$$

Let

$$\Sigma_1 = \sum_{\substack{Q < NR \leq 2Q \\ R \in \mathcal{R}}} \tau(R)^l |\rho(R, X; \gamma, \vec{\beta})|.$$

It follows from (2.12) that

$$\Sigma_1 \ll \Sigma_{11} + O(X(\log Q)^{c(l)}), \quad (2.13)$$

where

$$\Sigma_{11} := \sum_{\substack{Q < NR \leq 2Q \\ R \in \mathcal{R}}} \tau(R)^A |\Sigma_0|.$$

Clearly,

$$|\Sigma_0| \leq r^{-2} \sum_{\vec{a} \bmod r, \vec{a} \neq \vec{0}} |\sigma_0(R, a; \gamma)| \left| \sum_{\vec{x} \in I(X, \vec{\beta})} e_r(-\vec{a}\vec{x}) \right|;$$

therefore it follows from Lemma 2.1 that

$$|\Sigma_0| \ll \sum_{\vec{a} \in \Pi_1} f_X(R, a; \gamma),$$

where

$$f_X(R, a; \gamma) := \frac{|\sigma_0(R_1, a; \gamma)|}{r^2} \min\{X, \frac{r}{|a_1|}\} \min\{X, \frac{r}{|a_2|}\}, \quad R_1 := \frac{R}{(R, C)},$$

and

$$\Pi_1 = \{\vec{a} : \vec{a} \in \mathbb{Z}^2, \vec{a} \neq 0, |a_1|, |a_2| \leq r/2\},$$

cf. [4, (3.6)]. This gives

$$\Sigma_{11} \ll \Sigma_{12} + \Sigma_{13}, \quad (2.14)$$

with

$$\Sigma_{1j} = \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \vec{a} \in \Pi_j}} \tau(R)^l f_X(R, a; \gamma), \quad j = 2, 3,$$

where

$$\Pi_2 = \{\vec{a} : \vec{a} \in \Pi_1, a_1 a_2 = 0\}, \quad \Pi_3 = \{\vec{a} : \vec{a} \in \Pi_1, a_1 a_2 \neq 0\}.$$

As in [3, p.30] and [4, p.262], it follows that

$$\Sigma_{12} \ll X \sum_{0 < a \leq Q} \frac{1}{a} \sum_{\substack{Q < r \leq 2Q \\ R_1 | a}} \tau(R)^l \ll X \sum_{0 < a \leq Q} \frac{\tau(a)^{c_1(l)}}{a};$$

thus

$$\Sigma_{12} \ll X (\log Q)^{c(l)}. \quad (2.15)$$

Clearly,

$$\Sigma_{13} \leq \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \vec{a} \in \Pi_3}} \tau(R)^l \frac{|\sigma_0(R_1, a; \gamma)|}{|a_1 a_2|}.$$

Suppose that $\mathfrak{p} \in \mathcal{R}$, $N\mathfrak{p} = p$, $p \in P$, and $C \neq 0 \pmod p$, then

$$|\sigma_0(\mathfrak{p}, a; \gamma)| = \left| \sum_{\vec{u} \pmod p, \mathfrak{p} | \gamma + u d} e_p(\vec{u} \vec{a}) \right| = \left| \sum_{\vec{v} \pmod p, \mathfrak{p} | v} e_p(\vec{v} \vec{a}) \right|.$$

Therefore the scaling argument in [3, § 5; 4, § 3] shows that

$$\sigma_0(R_1, \vec{a}; \gamma) \neq 0 \Rightarrow a_2 \omega_1 = a_1 \omega_2 \pmod{R_1},$$

cf. [4, (3.7)]. This gives

$$\Sigma_{13} \leq \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \vec{a} \in \Omega}} \tau(R)^l \frac{|\sigma_0(R_1, a; \gamma)|}{|a_1 a_2|},$$

where

$$\Omega = \{\vec{a} : \vec{a} \in \mathbb{Z}^2, 1 \leq |a_1|, |a_2| \leq Q, a_2 \omega_1 = a_1 \omega_2 \pmod{R_1}\};$$

since

$$|\sigma_0(R_1, a; \gamma)| \ll m(R_1, \gamma) r \ll Q,$$

it follows that

$$\Sigma_{13} \leq Q \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \vec{a} \in \Omega}} \frac{\tau(R)^l}{|a_1 a_2|}.$$

Thus

$$\Sigma_{13} \ll Q (\log Q)^{c(l)}, \quad (2.16)$$

as in [3, p.30] and [4, pp.262-263]. Relations (2.13-16) give

$$\Sigma_1 \ll (X + Q) (\log Q)^{c(l)}. \quad (2.17)$$

Let

$$\Sigma_2 = \sum_{\substack{Q < NR \leq 2Q \\ R \in \mathcal{R}}} \tau(R)^l |\rho_1(R, X)|$$

and

$$g_X(R, \delta; \gamma) := |\rho(R_1^{(\delta)}, \frac{X}{\delta}; \frac{\gamma + \beta^{(\delta)} d}{\delta}, \frac{\vec{\beta}^{(\delta)}}{\delta})|.$$

In view of (2.11),

$$\Sigma_2 \leq \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \delta \in \Omega_1}} \tau(R)^l g_X(R, \delta; \gamma), \quad (2.18)$$

where

$$\Omega_1 := \{\delta : \delta \in \mathbb{N}, \text{h.c.f.}(\delta, d) = 1\}.$$

For $\Delta > 0$, let

$$\Omega_1^+ := \{\delta : \delta \in \Omega_1, \delta > \Delta\}, \quad \Omega_1^- := \Omega_1 \setminus \Omega_1^+.$$

It follows from (2.18) that

$$\Sigma_2 \leq \Sigma_{21} + \Sigma_{22}, \quad (2.19)$$

where

$$\Sigma_{21} = \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \delta \in \Omega_1^+}} \tau(R)^l g_X(R, \delta; \gamma)$$

and

$$\Sigma_{22} = \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \delta \in \Omega_1^-}} \tau(R)^l g_X(R, \delta; \gamma).$$

Further, it follows from (2.10) that

$$\Sigma_{21} \leq \Sigma_{23} + \Sigma_{24}, \quad (2.20)$$

with

$$\Sigma_{23} = \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \delta \in \Omega_1^+}} \tau(R)^l \sigma(R_1^{(\delta)}, \frac{X}{\delta}; \frac{\gamma + \beta^{(\delta)}d}{\delta}, \frac{\beta^{(\delta)}}{\delta})$$

and

$$\Sigma_{24} = \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \delta \in \Omega_1^+}} \tau(R)^l \frac{\eta^2 X^2}{\delta^2 N R_1^{(\delta)}} m(R_1^{(\delta)}, \frac{\gamma + \beta^{(\delta)}d}{\delta}).$$

Since $m(R, \gamma) = O(1)$, we have

$$\Sigma_{24} \ll \eta^2 X^2 \sum_{\substack{Q < r \leq 2Q \\ R \in \mathcal{R}, \delta > \Delta}} \frac{\tau(R)^l N((R, \delta))}{\delta^2 N R}.$$

The argument proceeds as in [4, p.264]. One first obtains the following estimate

$$\Sigma_{24} \ll \eta^2 X^2 \Delta^{-1} (\log Q)^{c(l)}. \quad (2.21)$$

Then we let

$$R_0 := \text{h.c.f.}(R, C), \quad R = R_1 R_0, \quad \mathfrak{A}_1 = \text{h.c.f.}(R_1, \delta), \quad R_1 = \mathfrak{A}_1 \mathfrak{A}_2$$

and conclude that

$$\Sigma_{23} \ll \sum_{\delta \in \Omega_1^+, N\mathfrak{A}_1|\delta} \tau(\mathfrak{A}_1)^l \Sigma_{25}(\mathfrak{A}_1), \quad (2.22)$$

where

$$\Sigma_{25}(\mathfrak{A}_1) = \sum_{Q < N(\mathfrak{A}_1 \mathfrak{A}_2 R_0) \leq 2Q} \tau(\mathfrak{A}_2)^l \sigma(\mathfrak{A}_2, \frac{X}{\delta}; \frac{\gamma + \beta^{(\delta)} d}{\delta}, \frac{\beta^{(\delta)}}{\delta}).$$

Moreover, the definition (2.1) of $\sigma(R, X; \gamma, \vec{\beta})$ shows that, as in [4, p.264], one may apply relation [4, (3.8)] to obtain the following upper bound:

$$\Sigma_{25}(\mathfrak{A}_1) \ll X^2 \delta^{-2} (\log X)^{c_1(l)}.$$

Therefore (2.22) gives

$$\Sigma_{23} \ll \sum_{\delta > \Delta, N\mathfrak{A}_1|\delta} \tau(\mathfrak{A}_1)^l X^2 \delta^{-2} (\log X)^{c_1(l)};$$

thus

$$\Sigma_{23} \ll X^2 \Delta^{-1} (\log X)^{c(l)}. \quad (2.23)$$

On the other hand (cf. [4, p.264]),

$$\Sigma_{22} \ll \sum_{\delta \in \Omega_1^-, NR_1|\delta} \tau(R)^l \Sigma_{26}(R), \quad (2.24)$$

with

$$\Sigma_{26}(R) = \sum_{\substack{Q < N(RS) \leq 2Q, \\ RS \in \mathcal{R}}} \tau(S)^l |\rho(S, \frac{X}{\delta}; \frac{\gamma + \beta^{(\delta)} d}{\delta}, \frac{\beta^{(\delta)}}{\delta})|.$$

It follows from the relations (2.24) and (2.17) that

$$\Sigma_{22} \ll \sum_{\delta \leq \Delta, NR_1|\delta} \tau(R)^l (\frac{X}{\delta} + \frac{Q}{NR}) (\log Q)^{c_2(l)};$$

where in the above notation $R = R_1 R_0$. As in [3, § 5], this gives

$$\Sigma_{22} \ll \Delta (X + Q) (\log Q)^{c(l)} \quad (2.25)$$

for $\Delta \ll X$. Put

$$\Delta = 1 + \min\{X^{1/2}, XQ^{-1/2}\};$$

the asserted estimate

$$\Sigma_2 \ll (Q + XQ^{1/2} + X^{3/2})(\log QX)^{c(l)}$$

follows from relations (2.19)-(2.21), (2.23), and (2.25). This concludes the proof of Lemma 2.2.

Let now

$$[A_q] = \mu(q) \sum_{\substack{R|q, q|NR \\ R \in \mathcal{R}}} \mu(R) [\mathcal{A}_R] \quad (2.26)$$

and

$$\rho_2(q, X) = \mu(q) \sum_{\substack{R|q, q|NR \\ R \in \mathcal{R}}} \mu(R) \rho_1(R, X)$$

for $q \in \mathbb{N}$.

Lemma 2.3 *If $\mu(q)^2 = 1$, then*

$$\# A_q = [A_q] + \rho_2(q, X); \quad (2.27)$$

moreover, for any positive integer l , there is a constant $c(l)$ such that

$$\sum_{Q < q \leq 2Q} \tau(q)^A \mu(q)^2 |\rho_2(q, X)| \ll (Q + XQ^{1/2} + X^{3/2})(\log QX)^{c(l)}. \quad (2.28)$$

Proof. As in [3, pp.32-33] and [4, p.265], assuming q be square-free, we deduce from the identity

$$\mu(q) \sum_{\substack{R|\mathfrak{A}, R|q \\ q|NR}} \mu(R) = \begin{cases} 1, & q|N\mathfrak{A}, \\ 0, & \text{otherwise} \end{cases}$$

that

$$\# A_q = \mu(q) \sum_{\substack{R|q, q|NR \\ R \in \mathcal{R}}} \mu(R) \# \mathcal{A}_R.$$

Therefore equation (2.27) follows from (2.4). The estimate (2.28) follows from Lemma 2.2 in exactly the same way as the corresponding estimate in [4, Lemma 3.3].

Let

$$\zeta_d(s) = \zeta(s) \prod_{p \in P, p|d} \left(1 - \frac{1}{p^s}\right)$$

for $s \in \mathbb{C}$. As in [3, p.5] and [4, p.266], let $\nu_p := \{\mathfrak{p} : \mathfrak{p} \in \mathcal{P}, N\mathfrak{p} = p\}$ stand for the number of prime ideals of the first degree in k lying above p .

Lemma 2.4 *There are a multiplicative function $\Gamma(q)$ and a positive real number c_0 satisfying the following conditions:*

- (i) $0 \leq \Gamma(p) \leq 1$ for $p \in P$;
- (ii) $1 - \Gamma(p) \geq c_0$ as soon as $p > 3$, $p \in P$;
- (iii) if $\mu(q)^2 = 1$, then

$$[A_q] = \frac{\eta^2 X^2}{\zeta_d(2)} \Gamma(q). \quad (2.29)$$

- (iv) if $C \not\equiv 0 \pmod{p}$, then

$$\Gamma(p) = \frac{\nu_p}{p+1}.$$

Moreover, $\varepsilon(f) \in \{1, 2, 3, 6\}$ and

$$1 - \Gamma(p) = 0 \Leftrightarrow p|\varepsilon(f)$$

for $p = 2, 3$.

Proof. Let $R \in \mathcal{R}$. Since $m(R, \gamma) = m(R_0, \gamma)$, it follows from the definition (2.3) that

$$[\mathcal{A}_R] = \frac{\eta^2 X^2}{\zeta_d(2) NR} \tilde{m}(R, \gamma) \quad (2.30)$$

with

$$\tilde{m}(R, \gamma) = m(R_0, \gamma) \prod_{p \in P_0(R, d)} \left(1 - \frac{1}{p^2}\right)^{-1} \left(1 - \frac{N((R, p))}{p^2 m((R, p), \gamma)}\right), \quad (2.31)$$

where

$$P_0(R, d) = \{p : p \in P, p|NR, d \not\equiv 0 \pmod{p}\}.$$

On letting

$$\Gamma(q) = \mu(q) \sum_{\substack{R|q, q|NR \\ R \in \mathcal{R}}} \frac{\mu(R)}{NR} \tilde{m}(R, \gamma),$$

one deduces equation (2.29) from relations (2.26) and (2.30). Clearly,

$$\Gamma(q) = \prod_{p \in P, p|q} \Gamma(p)$$

and

$$\Gamma(p) = - \sum_{\substack{R|p, p|NR \\ R \in \mathcal{R}}} \frac{\mu(R)}{NR} \tilde{m}(R, \gamma) \quad (2.32)$$

for $p \in P$. Let

$$b(R) := p^2 m(R, \gamma) NR^{-1} \quad (2.33)$$

and note that

$$b(R) = \# \{ \vec{u} : \vec{u} \in \mathbb{Z}^2, 0 \leq u_1, u_2 < p, R|\mathfrak{A}_u(\gamma) \}, \quad (2.34)$$

if $R|p$, $p \in P$; in particular, $b(1) = p^2$. One concludes from (2.34) that

$$\sum_{R|p} \mu(R) b(R) = \# \{ \vec{u} : \vec{u} \in \mathbb{Z}^2, 0 \leq u_1, u_2 < p, \text{h.c.f.}(\mathfrak{A}_u(\gamma), p) = 1 \}. \quad (2.35)$$

Suppose first $C \neq 0 \pmod{p}$. Then

$$\Gamma(p) = \frac{\nu_p}{p+1}$$

and, consequently, $0 \leq \Gamma(p) \leq 3/4$ for $p \in P$ since $\nu_2 \leq 2$ when 2 does not divide $i(\theta)$ (cf. [5]).

Suppose now that $p|C$ but $d \neq 0 \pmod{p}$; then it follows from (2.31-33) that

$$\Gamma(p) = \frac{1}{1-p^2} \sum_{\substack{R|p, R \neq 1 \\ R \in \mathcal{R}}} \mu(R) (b(R) - 1).$$

Since $b(1) = p^2$, the last equation may be rewritten as follows:

$$\Gamma(p) = \frac{1}{1-p^2} \sum_{R|p} \mu(R) b(R) + 1.$$

Moreover, since $d \neq 0 \pmod{p}$, it follows from (2.35) that

$$\sum_{R|p} \mu(R) b(R) = \# \{ \vec{u} : \vec{u} \in \mathbb{Z}^2, 0 \leq u_1, u_2 < p, \text{h.c.f.}(\tilde{\mathfrak{A}}_u(\gamma), p) = 1 \},$$

where

$$\tilde{\mathfrak{A}}_u(\gamma) := (u_1 \omega_1 + u_2 \omega_2) (\text{h.c.f.}(\omega_1, \omega_2))^{-1}.$$

Hence $\Gamma(p)$ depends neither on d , nor on γ , if p does not divide d ; therefore all the assertions of the lemma follow from [4, Lemma 3.4] in this case.

Let now $p|d$, then it follows from (2.31) that $\tilde{m}(R, \gamma) = m(R_0, \gamma)$ for $R|p$; therefore equation (2.32) may be rewritten as follows:

$$\Gamma(p) = - \sum_{\substack{R|p, p|NR \\ R \in \mathcal{R}}} \mu(R) \frac{m(R, \gamma)}{NR},$$

or

$$1 - \Gamma(p) = \frac{1}{p^2} \sum_{R|p} \mu(R) b(R). \quad (2.36)$$

Hence $0 \leq 1 - \Gamma(p) \leq 1$, in view of (2.35); this proves (i). Let

$$d = p^{\mu_0} d_0, \quad p = \mathfrak{p}^e \mathfrak{q}, \quad \gamma = \mathfrak{p}^{\mu_1} \mathfrak{b}_1, \quad \text{h.c.f.}(\omega_1, \omega_2) = \mathfrak{p}^{\mu_2} \mathfrak{b}_2$$

with $\mathfrak{p} \in \mathcal{P}$, $d_0 \mathfrak{b}_1 \mathfrak{b}_2 \mathfrak{q} \neq 0 \pmod{\mathfrak{p}}$. Then $\text{h.c.f.}(\mathfrak{A}_u(\gamma), \mathfrak{p}) = 1$ unless $\mu_1 \geq e\mu_0 + \mu_2$; moreover, if $\mu_1 \geq e\mu_0 + \mu_2$, then

$$\# \{ \vec{u} : \vec{u} \in \mathbb{Z}^2, 0 \leq u_1, u_2 < p, \mathfrak{p} | \mathfrak{A}_u(\gamma) \} \leq p.$$

Hence

$$\# \{ \vec{u} : \vec{u} \in \mathbb{Z}^2, 0 \leq u_1, u_2 < p, \text{h.c.f.}(\mathfrak{A}_u(\gamma), p) \neq 1 \} \leq 3p;$$

therefore it follows from (2.35) and (2.36) that

$$1 - \Gamma(p) \geq 1 - \frac{3}{p} > 0$$

for $p > 3$; this proves (ii). Moreover, it is clear also that $\Gamma(p) = 1$ if and only if $\text{h.c.f.}(\mathfrak{A}_u(\gamma), p) \neq 1$ for every \vec{u} in \mathbb{Z}^2 . Thus $\varepsilon(f)$ is divisible by no prime $p > 3$. An analogous argument shows that $\varepsilon(f)$ is square-free. This completes the proof of Lemma 2.4.

3. The sieve bounds

As in [4, (3.17)], let

$$\sigma(f) = \prod_{p \in P} \left(1 + \frac{1}{p}\right) (1 - \Gamma(p));$$

in view of Lemma 2.4(iv), the product $\sigma(f)$ converges (cf. [4, Lemma 3.4]). Let

$$\sigma_1(f) = \sigma(f) \prod_{p \in P, p|d} \left(1 - \frac{1}{p^2}\right)^{-1}, \quad (3.1)$$

$h_{f_0} = f_0(1, 1)$, $h_f = d^3 h_{f_0}$, and $\kappa = \sigma_1(f)\eta(h_f X)^{-1}$. In what follows, it will be assumed that $\sigma(f) \neq 0$ (and therefore $\kappa \neq 0$).

Let

$$\mathcal{B} = \{\mathfrak{A} : \mathfrak{A} \in \mathcal{I}, h_f X^3 < N\mathfrak{A} \leq h_f X^3(1 + \eta)\},$$

and $B = \{N\mathfrak{A} : \mathfrak{A} \in \mathcal{B}\}$. Write, for brevity, $\tau := (\log \log X)^{-1/6}$. The asymptotic formula (1.2) of Theorem 2 is equivalent to the following estimate to be proved along the lines of [3, 4]:

$$\pi(\mathcal{A}) = \kappa\pi(\mathcal{B}) + O\left(\frac{\eta^2 X^2}{\log X}\tau\right). \quad (3.2)$$

Lemmata 3.5, 3.6, and 4.1 in [4] can be taken over verbatim. Let us prove the analogue of [4, Lemma 4.2] (cf. also [3, Lemma 3.5]). We adopt the sieve notation introduced in [4, § 4].

Lemma 3.1 *We have*

$$\sum_{0 \leq n \leq n_0} |T^{(n)}(\mathcal{A}) - \kappa T^{(n)}(\mathcal{B})| \ll \tau \frac{\eta^2 X^2}{\log X}.$$

Proof. Without loss of generality, it may be assumed that

$$p \geq X^\tau \Rightarrow C \not\equiv 0 \pmod{p}. \quad (3.3)$$

Let

$$j(q) = \mu(q) q \sum_{R|q, q|NR} \frac{\mu(R)}{NR} = q \prod_{p \in P, p|q} \left(1 - \prod_{\mathfrak{p} \in \mathcal{P}, \mathfrak{p}|p} \left(1 - \frac{1}{N\mathfrak{p}}\right)\right),$$

cf. [4, Lemma 3.6]. Equation [4, (4.9)] gives

$$\begin{aligned} T^{(n)}(\mathcal{B}) &= \phi(k) h_f \eta X^3 \prod_{p < X^\tau} \left(1 - \frac{j(p)}{p}\right) \Sigma_5^{(n)} \{1 + O(\exp(-\tau^{-1}))\} \\ &\quad + O(X^{3-\tau/3}), \end{aligned} \quad (3.4)$$

where $\phi(k)$ stands for the residue of the zeta-function $\zeta_k(s)$ of k at $s = 1$ (cf. [4, p.258]) and

$$\Sigma_5^{(n)} = \sum_{\substack{X^\tau \leq p_n < \dots < p_1 < X^{1-\tau} \\ p_1 \dots p_n < X^{1+\tau}}} \frac{j(p_1 \dots p_n)}{p_1 \dots p_n}.$$

In view of (3.3), it follows from [4, Lemma 2.2] that

$$S(\mathcal{A}_{\lambda(\mathfrak{p})}, X^\tau) = S(A_{p_1 \dots p_n}, X^\tau)$$

for $\vec{\mathfrak{p}} \in J_n(\mathcal{A})$ with $N\mathfrak{p}_i = p_i$, $p_i \in P$, $1 \leq i \leq n$, and $\lambda(\vec{\mathfrak{p}}) = \prod_{i=1}^n \mathfrak{p}_i$. Therefore

$$T^{(n)}(\mathcal{A}) = \sum_{\substack{X^\tau \leq p_n < \dots < p_1 < X^{1-\tau} \\ p_1 \dots p_n < X^{1+\tau}}} S(A_{p_1 \dots p_n}, X^\tau), \quad T^{(0)}(\mathcal{A}) = S(\mathcal{A}, X^\tau). \quad (3.5)$$

By the ‘Fundamental Lemma’, [1, Theorem 7.1], with ‘ $\omega(p)$ ’ = $p\Gamma(p)$, ‘ X ’ = $\frac{\eta^2 X^2}{\zeta_d(2)}$, ‘ ξ ’ = $X^{1/6}$, and ‘ z ’ = X^τ , it follows from Lemmata 2.3 and 2.4 that

$$S(A_q, X^\tau) = M(q)\{1 + O(\exp(-\tau^{-1}))\} + O(E(q)),$$

where

$$M(q) = \Gamma(q) \prod_{p < X^\tau} (1 - \Gamma(p)) \frac{\eta^2 X^2}{\zeta_d(2)}$$

and

$$E(q) = \sum_{\substack{\delta < X^{1/3} \\ p|\delta \Rightarrow p < X^\tau}} \mu(\delta)^2 \tau(\delta)^2 |\rho_2(q\delta, X)|.$$

This gives

$$\begin{aligned} T^{(n)}(\mathcal{A}) &= \frac{\eta^2 X^2}{\zeta_d(2)} \prod_{p < X^\tau} (1 - \Gamma(p)) \Sigma_4^{(n)} (1 + O(\exp(-\tau^{-1}))) \\ &\quad + \rho_3(X) \end{aligned} \quad (3.6)$$

with

$$\Sigma_4^{(n)} = \sum_{\substack{X^\tau \leq p_n < \dots < p_1 < X^{1-\tau} \\ p_1 \dots p_n < X^{1+\tau}}} \Gamma(p_1 \dots p_n)$$

and

$$\rho_3(X) = \sum_{q < X^{4/3+\tau}} \mu(q)^2 \tau(q)^2 |\rho_2(q, X)|.$$

It follows from (2.28) that $\rho_3(X) \ll X^{7/4}(\log X)^c$. Moreover, as in [3, p.67], it follows from (2.28) that

$$\prod_{p < X^\tau} (1 - \Gamma(p)) = \sigma(f)\zeta(2) \prod_{p < X^\tau} \left(1 - \frac{1}{p}\right) (1 + O((\log X^\tau)^{-2})),$$

cf. [3, (6.7)], and

$$\prod_{p < X^\tau} \left(1 - \frac{j(p)}{p}\right) = \phi(k)^{-1} \prod_{p < X^\tau} \left(1 - \frac{1}{p}\right) (1 + O((\log X^\tau)^{-2})),$$

cf. [3, (6.9)]. Combining these estimates, one deduces from (3.6) and (3.4) that

$$\begin{aligned} T^{(n)}(\mathcal{A}) = & \frac{\eta^2 X^2 \sigma(f) \zeta(2)}{\zeta_d(2)} \prod_{p < X^\tau} \left(1 - \frac{1}{p}\right)^{\Sigma_4^{(n)}} (1 + O(\exp(-\tau^{-1}))) (1 + O((\log X^\tau)^{-2})) \\ & + O(X^{7/4} (\log X)^c) \end{aligned} \quad (3.7)$$

and

$$\begin{aligned} T^{(n)}(\mathcal{B}) = & h_f \eta X^3 \prod_{p < X^\tau} \left(1 - \frac{1}{p}\right)^{\Sigma_5^{(n)}} (1 + O(\exp(-\tau^{-1}))) (1 + O((\log X^\tau)^{-2})) \\ & + O(X^{3-\tau/3}). \end{aligned} \quad (3.8)$$

The assertion of the lemma can be deduced from the relations (3.7) and (3.8) in exactly the same way as the analogous estimate in [3, § 6].

Neither the formulation, nor the proof of the analogues of [3, Lemmata 3.6 and 3.7] (cf. also [4, Lemmata 4.4 and 5.1]) need be changed. For the reader's convenience, we reproduce the assertions of these Lemmata to be deduced as in [3, § 7] from a variant of Selberg's upper bound sieve, see [1, Theorem 4.1].

Lemma 3.2 *We have*

$$S_j(\mathcal{A}) + \kappa S_j(\mathcal{B}) \ll \tau \frac{\eta^2 X^2}{\log X}$$

for $j = 3, 5, 6$ or 7 .

Lemma 3.3 *We have*

$$\sum_{n \geq 3} |U^{(n)}(\mathcal{D}) - \hat{U}^{(n)}(\mathcal{D})| \ll \frac{\eta^2 X^2}{\log X} \xi \tau^{-4},$$

$$|U_1^{(n)}(\mathcal{D}) - \hat{U}_1^{(n)}(\mathcal{D})| \ll \frac{\eta^2 X^2}{\log X} \xi \tau^{-3}$$

for $n = 1$ and 2 ,

$$|S_4(\mathcal{D}) - \hat{S}_4(\mathcal{D})| \ll \frac{\eta^2 X^2}{\log X} \xi \tau^{-3},$$

and

$$|U_2^{(1)}(\mathcal{D}) - \hat{U}_2^{(1)}(\mathcal{D})| \ll \frac{\eta^2 X^2}{\log X} \xi \tau^{-4},$$

where \mathcal{D} stands for either of the sequences \mathcal{A}, \mathcal{B} .

Remark 4. Lemmata 3.1-3 may be regarded as formal corollaries of Lemmata 2.3 and 2.4, defining the ‘level of distribution’ of the sequence \mathcal{A} . We expect analogous assertions to be provable for other sequences of ideals in k with the same level of distribution, in particular, for the sequence arising if a general cubic polynomial in $\mathbb{Z}[x_1, x_2]$ completely decomposable over \mathbb{C} is studied. As it has been stressed in [3, § 2], the real novelty of the method developed in [3] is the ‘Type II’ estimates to be treated in the next section.

4. The Type II estimates

The strategy of the Type II estimates was outlined in [3, pp.9-10] and explained in detail in [3, pp.14-21]. Let us retain the notations introduced in [4, pp.271-273]; in particular, each of the relevant sums $U(\mathcal{A})$, $V(\mathcal{A})$ is decomposed as follows (cf. [4, p.273]):

$$U(\mathcal{A}) = U_e(\mathcal{A}) + U_g(\mathcal{A}), \quad V(\mathcal{A}) = V_e(\mathcal{A}) + V_g(\mathcal{A}).$$

We start with following analogue of [3, Lemma 3.9; 4, Lemma 5.2].

Lemma 4.1 *In notation of [4, § 5], suppose that $\vec{m} \in \iota(n)$ and $\nu \in \iota_1(n)$. Then there is a constant c , depending at most on f and such that*

$$U_e(\mathcal{A}) - \kappa U(\mathcal{B}) \ll M^{-1} \eta^{5/2} X^2 (\log X)^c,$$

where $M = \prod_{i=1}^{n+1} m_i$. Moreover,

$$V_e(\mathcal{A}) - \kappa V(\mathcal{B}) = O(\eta^{5/2} X^2 (\log X)^c),$$

and

$$\sum_{n \geq 3} |\hat{U}_e^{(n)}(\mathcal{A}) - \kappa \hat{U}^{(n)}(\mathcal{B})| = O(\eta^{5/2} X^2 (\log X)^c).$$

Proof. For $n \geq 0$, let $\vec{m} \in \iota(n)$ and $\nu \in \iota_1(n)$. As in [3, § 10] and [4, p.274], one can deduce from [3, (8.3)] and [4, (3.8)] in the case $n > 0$ and from (2.30) in conjunction with Lemma 2.2 when $n = 0$ that, for a suitable constant c_1 ,

$$U_e(\mathcal{A}) = \sum_{\mathfrak{A} \in \mathcal{R}, N\mathfrak{A} < L} a(\mathfrak{A}, \mathfrak{D}) \# \mathcal{A}_{\mathfrak{A}\mathfrak{D}} + O\left(\frac{\eta^{5/2} X^2}{M} (\log X)^{c_1}\right), \quad (4.1)$$

where $L = X^{\tau/2}$ and

$$a(\mathfrak{A}, \mathfrak{D}) = b_{\mathfrak{A}} \frac{w'(h_f X^3 / N(\mathfrak{A}))}{M(\xi \log X)^{n+1}} \mu(\mathfrak{D}) \log \frac{L}{N\mathfrak{D}}.$$

It follows from the definitions that

$$w'(t) \neq 0 \Rightarrow X^{1+\tau} \leq t < X^{3/2-\tau},$$

since

$$(1 + \tau)\xi^{-1} \leq \sum_{i=1}^{n+1} m_i \leq \left(\frac{3}{2} - \tau\right)\xi^{-1} - (n + 1)$$

when $\vec{m} \in \iota(n)$ $\nu \in \iota_1(n)$, cf. [4, § 5]. Therefore it may be assumed that the summation in (4.1) is subject to the additional condition

$$N(\mathfrak{A}\mathfrak{D}) \ll X^{2-\tau/2}. \quad (4.2)$$

It follows from (2.4) and (2.30) that

$$\# \mathcal{A}_{\mathfrak{A}\mathfrak{D}} = \frac{\eta^2 X^2}{\zeta_d(2) N(\mathfrak{A}\mathfrak{D})} \tilde{m}(\mathfrak{A}\mathfrak{D}, \gamma) + \rho_1(\mathfrak{A}\mathfrak{D}, X). \quad (4.3)$$

As in [3, p.62] and [4, p.274], one deduces from (4.1)-(4.3) and Lemma 2.2 that, for some c_2 ,

$$\begin{aligned} U_e(\mathcal{A}) &= \frac{\eta^2 X^2}{\zeta_d(2) M(\xi \log X)^{n+1}} \sum_{\mathfrak{A} \in \mathcal{R}} b_{\mathfrak{A}} \frac{w'(h_f X^3 / N\mathfrak{A})}{N\mathfrak{A}} \tilde{m}(\mathfrak{A}, \gamma) \Sigma_6 \\ &+ O\left(\frac{\eta^{5/2} X^2}{M} (\log X)^{c_2}\right) \end{aligned}$$

with

$$\Sigma_6 = \sum_{\mathfrak{D} \in \mathcal{R}, N\mathfrak{D} < L} \frac{\mu(\mathfrak{D})}{N\mathfrak{D}} \tilde{m}(\mathfrak{D}, \gamma) \log \frac{L}{N\mathfrak{D}}.$$

As in [3, p.62-63] and [4, p.274], it follows now from Perron's formula that

$$\Sigma_6 = \prod_{p \in P} \left(1 - \frac{1}{p}\right)^{-1} (1 - \Gamma(p)) + O(\exp(-c_3(\log L)^{1/2})),$$

with $c_3 > 0$. In view of (3.1), one concludes that

$$U_e(\mathcal{A}) = \frac{\sigma(f)\eta^2 X^2 \zeta(2)}{\zeta_d(2)} \Sigma_7 (1 + O(\exp(-c(\log L)^{1/2})))$$

$$+ O(M^{-1}\eta^{5/2}X^2(\log X)^c),$$

where

$$\Sigma_7 = \sum_{\mathfrak{A} \in \mathcal{R}} b_{\mathfrak{A}} \frac{w'(h_f X^3/N(\mathfrak{A}))}{M(\xi \log X)^{n+1}} N(\mathfrak{A})^{-1} \tilde{m}(\mathfrak{A}, \gamma).$$

Since

$$\tilde{m}(\mathfrak{A}, \gamma) = \prod_{\mathfrak{p} \in \mathcal{P}, \mathfrak{p}|\mathfrak{A}} (1 + N(\mathfrak{p})^{-1})^{-1}$$

when $b_{\mathfrak{A}} \neq 0$, one can conclude the proof of the lemma along the lines of [3, § 10; 4, § 5].

As a consequence of Lemmata 3.1-3.3, Lemma 4.1, and the analogue of [4, Lemma 4.1], one obtains the following analogue of [4, Proposition 5.1].

Proposition 4.1 *We have*

$$\begin{aligned} \pi(\mathcal{A}) - \kappa\pi(\mathcal{B}) &\ll \tau \frac{\eta^2 X^2}{\log X} + \eta^{5/2} X^2 (\log X)^c \\ &+ \sum_{n \geq 3} |\hat{U}_g^{(n)}(\mathcal{A})| + \sum_{n=1,2} |\hat{U}_{1,g}^{(n)}(\mathcal{A})| + |\hat{S}_{4,g}(\mathcal{A})| + |\hat{U}_{2,g}^{(1)}(\mathcal{A})|. \end{aligned}$$

As has been explained at the end of [3, § 3] and noted in [4, p.287], Theorem 2 and therefore Theorem 1 can be deduced from Proposition 4.1 and the following analogue of [4, Proposition 6.1].

Proposition 4.2 *In the notation of [4, § 6], let $\mathcal{C} \subseteq \mathbb{R}^3$ be a cube of side $S_0 \geq L^2$, and suppose that $c_i \ll V^{1/3}$, $1 \leq i \leq 3$, and $N\check{c} \gg V$ for $\vec{c} \in \mathcal{C}$.*

(i) There is a positive constant c depending at most on f and such that the following estimate

$$\sum_{\substack{\beta = \alpha \bmod q \\ \hat{\beta} \in \mathcal{C}, \beta \in A^{(0)}}} g_{(\beta)} \ll V \exp(-c\sqrt{\log L})$$

holds uniformly in a range $1 < q \leq (\log X)^l$ for any $l > 0$, any class A of ideal numbers, and any ideal number α in A .

(ii) If a bound of the form

$$\sum_{\substack{\beta = \alpha \bmod q \\ \hat{\beta} \in \mathcal{C}, \beta \in A^{(0)}}} g_{(\beta)} \ll V \exp(-c\sqrt{\log L}), \quad c > 0, \quad (4.4)$$

holds uniformly in a range

$$1 < q \leq Q_1 \leq \exp(\sqrt[3]{\log X})$$

for any class A of ideal numbers and any ideal number α in A , then

$$\sum_{\substack{\mathfrak{a}\mathfrak{b} \in \mathcal{A} \\ V < N\mathfrak{b} \leq 2V}} b_{\mathfrak{a}}g_{\mathfrak{b}} \ll X^2 Q_1^{-1/160} (\log X)^c$$

for $X^{1+\tau} \ll V \ll X^{3/2-\tau}$, with a suitable positive constant c depending at most on f .

Only the second assertion (ii) needs a new proof. Choose V as in (ii), and let

$$\Sigma_8(V) := \sum_{\mathfrak{a}\mathfrak{b} \in \mathcal{A}, V < N\mathfrak{b} \leq 2V} b_{\mathfrak{a}}g_{\mathfrak{b}}.$$

We have

$$\Sigma_8(V) = \sum_{\substack{\mathfrak{a}\mathfrak{b} = \mathfrak{A}_a(\gamma), \vec{a} \in R \\ V < N\mathfrak{b} \leq 2V}} b_{\mathfrak{a}}g_{\mathfrak{b}}\Psi(\vec{a}),$$

where $\Psi : \mathbb{R}^2 \rightarrow \{0, 1\}$ is the characteristic function of the square $I(X)$ and

$$R := \{\vec{a} : \vec{a} \in \mathbb{Z}^2, \text{h.c.f.}(\gamma_1 + a_1d, \gamma_2 + a_2d) = 1\}.$$

As in [4], let \mathcal{Q} stand for the set of those integral ideals in \mathfrak{o} which are not divisible by a rational prime; then

$$\Sigma_8(V) = \sum_{\substack{\mathfrak{a}\mathfrak{b} = \mathfrak{A}_a(\gamma), \vec{a} \in \mathbb{Z}^2 \\ V < N\mathfrak{b} \leq 2V, \{\mathfrak{a}, \mathfrak{b}\} \subset \mathcal{Q}}} b_{\mathfrak{a}}g_{\mathfrak{b}}\Psi(\vec{a}) \sum_{b \in \Delta_a(X)} \mu(b)$$

with

$$\Delta_a(X) := \{b : b \in \mathbb{N}, b \ll X, b \mid \text{h.c.f.}(\gamma_1 + a_1d, \gamma_2 + a_2d)\}.$$

Let $b \in \Delta_a(X)$. Then $\text{h.c.f.}(b, d) = 1$ since, by assumption, $\text{h.c.f.}(\gamma_1, \gamma_2, d) = 1$; therefore $b \mid \mathfrak{A}_a(\gamma)$. As in [3, § 11; 4, § 6], it follows now that

$$\Sigma_8(V) = \sum_{\substack{\mathfrak{a}\mathfrak{b} = \mathfrak{A}_a(\gamma), \{\mathfrak{a}, \mathfrak{b}\} \subset \mathcal{Q} \\ \vec{a} \in \mathbb{Z}^2, V < N\mathfrak{b} \leq 2V}} b_{\mathfrak{a}}g_{\mathfrak{b}}\Psi(\vec{a}) + O(X^{2-\tau/2}(\log X)^c) \quad (4.5)$$

for some c . In the notation of [4, § 6], equation (4.5) may be rewritten as follows:

$$\Sigma_8(V) = \sum_{\substack{\varphi(\vec{a})=\delta\alpha\beta, (\alpha)\in\mathcal{Q} \\ \vec{a}\in\mathbb{Z}^2, V<N\beta\leq 2V}} b_{(\alpha)}G(\beta)\Psi(\vec{a}) + O(X^{2-\tau/2}(\log X)^c),$$

where now $\varphi(\vec{a}) := \gamma + d \cdot a$ and $\mathfrak{d} = (\delta)$. Proceeding as in [3, pp.67-68] and [4, p.279], we let

$$\psi(\vec{a}_1, \vec{a}_2; \beta_1, \beta_2) = \text{card } \{\alpha : (\alpha) \in \mathcal{Q}, \varphi(\vec{a}_i) = \delta\alpha\beta_i, i = 1, 2\}$$

and conclude that

$$\Sigma_8(V) \ll X^{2-\tau/2}(\log X)^c + (X^3/V)^{1/2}\Sigma_9^{1/2}, \quad (4.6)$$

where

$$\Sigma_9 = \Sigma_{10} + O(X^2(\log X)^c), \quad (4.7)$$

with

$$\Sigma_{10} := \sum_{\substack{\beta_1 \neq \beta_2, \vec{a}_i \in \mathbb{Z}^2, \\ V < N\beta_i \leq 2V, i=1,2}} G(\beta_1)G(\beta_2)\Psi(\vec{a}_1)\Psi(\vec{a}_2)\psi(\vec{a}_1, \vec{a}_2; \beta_1, \beta_2). \quad (4.8)$$

For $\vec{b} \in \mathbb{Z}^3$, let

$$D(\vec{b}) := h.c.f.(b_1, b_2, b_3), [\vec{b}] = D(\vec{b})^{-1}\vec{b}.$$

As in [4, p.279], one concludes that

$$\psi(\vec{a}_1, \vec{a}_2; \beta_1, \beta_2) = 1 \Rightarrow \text{cl } \beta_1 = \text{cl } \beta_2. \quad (4.9)$$

Let us recall that, for each class A of ideal numbers in k , we have defined [4, p.277] an invertible \mathbb{Q} -linear transformation

$$h_A : \beta \mapsto \hat{\beta}, h_A : A \rightarrow \mathbb{Q}^3$$

such that the image $h_A(A^{(0)})$ of the lattice

$$A^{(0)} = \{\alpha : \alpha \in A, (\alpha) \in \mathcal{I}(k)\}$$

of the integral ideal numbers in A is a sublattice of \mathbb{Z}^3 of finite index (equal to $|\det h_A|$). The following lemma is our analogue of [4, Lemma 6.2]. It can be deduced from relations (4.6)-(4.9) along the lines of [3, § 11; 4, § 6].

Lemma 4.2 *Let $1 \ll Y \ll X^{\tau/3}$. There is a constant c , depending at most on f and a class B of ideal numbers, such that*

$$\Sigma_8(V) \ll X^2 Y^{-1/2} (\log X)^c + X^{3/2} V^{-1/2} \Sigma_{11}^{1/2}, \quad (4.10)$$

with

$$\Sigma_{11} := \sum_{\beta_1, \beta_2, \vec{a}_1, \vec{a}_2} G(\beta_1) G(\beta_2) \Psi(\vec{a}_1) \Psi(\vec{a}_2) \psi(\vec{a}_1, \vec{a}_2; \beta_1, \beta_2), \quad (4.11)$$

subject to the conditions

$$D(\hat{\beta}_1 \wedge \hat{\beta}_2) > V X^{-1} Y^{-1}; \quad \vec{a}_i \in \mathbb{Z}^2, \quad \beta_i \in B^{(0)}, \quad V < N\beta_i \leq 2V \text{ for } i = 1, 2.$$

Moreover, if $\psi(\vec{a}_1, \vec{a}_2; \beta_1, \beta_2) = 1$, then

$$\vec{a}_i d + \vec{\gamma} = \nu D(\hat{\beta}_1 \wedge \hat{\beta}_2)^{-1} \vec{h}_i(\beta_1, \beta_2) \quad (4.12)$$

with $\nu \in \{\pm 1\}$, $\vec{h}_i := (h_{i1}, h_{i2})$, the functions h_{ij} being defined by [4, (6.4)] for $i, j = 1, 2$.

Let us substitute relation (4.12) into the definition (4.11). This gives

$$\Sigma_{11} = \sum_{\beta_1, \beta_2, \nu} G(\beta_1) G(\beta_2) \Psi\left(\frac{\nu D^{-1} \vec{h}_1(\beta_1, \beta_2) - \vec{\gamma}}{d}\right) \Psi\left(\frac{\nu D^{-1} \vec{h}_2(\beta_1, \beta_2) - \vec{\gamma}}{d}\right) \quad (4.13)$$

subject to the conditions:

$$D(\hat{\beta}_1 \wedge \hat{\beta}_2) > V X^{-1} Y^{-1}$$

and

$$\beta_i \in B^{(0)}, \quad V < N\beta_i \leq 2V, \quad \nu \vec{\gamma} = D^{-1} \vec{h}_i(\beta_1, \beta_2) \pmod{d}$$

for $\nu \in \{\pm 1\}$, $i = 1, 2$; here $D := D(\hat{\beta}_1 \wedge \hat{\beta}_2)$. Let

$$\begin{aligned} U(y, \nu) &= \{(\hat{\beta}_1, \hat{\beta}_2) : \beta_i \in B^{(0)}, \quad V < N\beta_i \leq 2V, \\ y(Xd + \gamma_j) &< \nu h_{ij}(\beta_1, \beta_2) \leq y(X(1 + \eta)d + \gamma_j) \text{ for } i, j = 1, 2\} \end{aligned}$$

for $y > 0$, $\nu \in \{\pm 1\}$; further, let

$$\begin{aligned} U_0(n, \nu) &= \{(\hat{\beta}_1, \hat{\beta}_2) : (\hat{\beta}_1, \hat{\beta}_2) \in U(n, \nu), \\ D(\hat{\beta}_1 \wedge \hat{\beta}_2) &= n, \quad \nu \vec{\gamma} = n^{-1} \vec{h}_i(\beta_1, \beta_2) \pmod{d} \text{ for } i = 1, 2\} \end{aligned}$$

for $n \in \mathbb{N}$. As in [3, p.72; 4, p.280], let us subdivide the range of summation in Σ_{11} into subintervals

$$I_m := (\frac{m-1}{T}\Delta, \frac{m}{T}\Delta], \text{ with } T \ll X^{2\tau/3}, T < m \leq 2T, \Delta \ll VX^{-1}.$$

Let

$$\Sigma_{12}(m, \Delta) = \sum_{d_1 \in I_m} \left| \sum_{(\hat{\beta}_1, \hat{\beta}_2) \in U_0(d_1, \nu)} G(\beta_1)G(\beta_2) \right|. \quad (4.14)$$

As in the cited works (cf. [4, (6.6), (6.7)]), it follows from equation (4.13) that

$$\Sigma_{11} \ll (\log X) T \Sigma_{12}(m, \Delta), \quad (4.15)$$

for at least one triple (m, Δ, ν) . Proceeding with our argument, let us cover the region of summation $U_0(d_1, \nu)$ in (4.14) by means of cubes $\mathfrak{C}(\vec{n}) = \mathcal{C}_1(\vec{n}) \times \mathcal{C}_2(\vec{n})$ defined as in [4, § 6]. Relations (4.10), (4.14-16) lead to the following inequality (cf. [3, (12.8); 4, (6.9)]):

$$\Sigma_8(V) \ll X^2 Y^{-1/2} (\log X)^c + X^{3/2} V^{-1/2} Y^7 \Sigma_{13}^{1/2} (\log X)^c$$

with

$$\Sigma_{13} = \sum_{d_1 \in I_m} \left| \sum_{(\hat{\beta}_1, \hat{\beta}_2) \in U_1(\mathfrak{C}; d_1, \nu)} G(\beta_1)G(\beta_2) \right|,$$

where

$$\begin{aligned} U_1(\mathfrak{C}; d_1, \nu) &= \{(\hat{\beta}_1, \hat{\beta}_2) : (\hat{\beta}_1, \hat{\beta}_2) \in \mathfrak{C}, D(\hat{\beta}_1 \wedge \hat{\beta}_2) = d_1, \\ \beta_i \in B^{(0)}, \nu \vec{\gamma} &= d_1^{-1} \vec{h}_i(\beta_1, \beta_2) \pmod{d} \text{ for } i = 1, 2\} \end{aligned}$$

and \mathfrak{C} is a suitable class I cube, in the sense of [3, p.73; 4, p.281]. Let

$$\begin{aligned} U_2(\mathfrak{C}; d_1, d_2, \nu) &= \{(\hat{\beta}_1, \hat{\beta}_2) : (\hat{\beta}_1, \hat{\beta}_2) \in \mathfrak{C}, d_1 d_2 \mid \hat{\beta}_1 \wedge \hat{\beta}_2, \\ \beta_i \in B^{(0)}, \nu \vec{\gamma} &= d_1^{-1} \vec{h}_i(\beta_1, \beta_2) \pmod{d} \text{ for } i = 1, 2\} \end{aligned}$$

and let

$$\Sigma_{14} = \sum_{(\hat{\beta}_1, \hat{\beta}_2) \in U_2(\mathfrak{C}; d_1, d_2, \nu)} G(\beta_1)G(\beta_2).$$

The argument used in [3, § 12] and [4, pp.281-283] to deduce [3, Lemma 12.2] and its analogue [4, (6.11)] leads to the following conclusion.

Lemma 4.3 *Suppose that $1 \ll Y \ll X^{\tau/3}$, and let $d_0 := X^{-1} V Y^{15} + V^{1/6}$. There is a constant c , depending at most on f , such that*

$$\Sigma_8(V) \ll X^2 Y^{-1/2} (\log X)^c + X^{3/2} V^{-1/2} Y^7 \Sigma_{15}^{1/2} (\log X)^c, \quad (4.16)$$

where

$$\Sigma_{15} = \sum_{d_1 \in I_m, d_1 d_2 < d_0} |\Sigma_{14}| \quad (4.17)$$

and \mathfrak{C} is a suitable class I cube.

5. Completion of the proof of Proposition 4.2 and Theorem 2

The functions

$$\vec{h}_i(\beta_1, \beta_2) = \vec{h}_i(h_B^{-1}(\hat{\beta}_1), h_B^{-1}(\hat{\beta}_2))$$

may be regarded as polynomials in $\hat{\beta}_1$ and $\hat{\beta}_2$ with rational coefficients. We write them with a common denominator as

$$\vec{h}_i(\beta_1, \beta_2) = d^{*-1} \vec{H}_i(\hat{\beta}_1, \hat{\beta}_2),$$

where each \vec{H}_i is a vector of three integral polynomials. We note that the common denominator d^* will only depend on the field k and the choice of the bases made in [4, p. 277]. Moreover, we note from the definition [4; (6.4)] that $\vec{h}_i(\beta, \lambda\beta)$ vanishes identically for $i = 1, 2$, whence

$$\vec{H}_i(\hat{\beta}, \lambda\hat{\beta}) = 0 \quad (i = 1, 2) \tag{5.1}$$

identically.

The conditions

$$\nu\vec{\gamma} = d_1^{-1}\vec{h}_i(\beta_1, \beta_2) \pmod{d} \quad \text{for } i = 1, 2$$

are now equivalent to a pair of congruences

$$d_1 d^* \nu\vec{\gamma} = \vec{H}_i(\hat{\beta}_1, \hat{\beta}_2) \pmod{d_1 d d^*}.$$

In order to separate the variables in the equation (4.17), let us replace the condition $d_1 d_2 \mid \hat{\beta}_1 \wedge \hat{\beta}_2$ by the condition that $\hat{\beta}_2 = \lambda \hat{\beta}_1 \pmod{d_1 d_2}$ for some integer λ , which is necessarily coprime to $d_1 d_2$, cf. [3, pp. 70, 78]; it may clearly be assumed that $1 \leq \lambda \leq d_1 d_2$.

Since our conditions are now all modulo $d_{12} := d_1 d_2 d d^*$, we can pick out the admissible vectors $\hat{\beta}_i$ by using orthogonality for the function

$$e_l(x) := \exp(2\pi i x / l)$$

and taking $l = d_{12}$. In this way we find that

$$\Sigma_{14} = \frac{1}{d_{12}^6} \sum_{\lambda, \beta_i, \vec{b}_i, \hat{\eta}_i} e_{d_{12}}(\vec{b}_1(\hat{\beta}_1 - \hat{\eta}_1) + \vec{b}_2(\hat{\beta}_2 - \hat{\eta}_2)) G(\beta_1) G(\beta_2)$$

subject to the conditions:

$$\hat{\eta}_2 = \lambda \hat{\eta}_1 \pmod{d_1 d_2}, \quad 1 \leq \lambda \leq d_1 d_2, \quad (\lambda, d_1 d_2) = 1, \quad 0 \leq b_{ij}, \hat{\eta}_{ij} < d_{12},$$

$$d_1 d^* \nu \vec{\gamma} = \vec{H}_i(\hat{\eta}_1, \hat{\eta}_2) \pmod{d_1 d d^*}, \quad \beta_i \in B^{(0)}, \quad \hat{\beta}_i \in \mathcal{C}_i,$$

where $\mathfrak{C} = \mathcal{C}_1 \times \mathcal{C}_2$, $\hat{\eta}_i = (\hat{\eta}_{i1}, \hat{\eta}_{i2}, \hat{\eta}_{i3})$, for $1 \leq j \leq 3$ and $i = 1, 2$. Given $\mathcal{D} \subset \mathbb{R}^3$ and $\alpha \in \mathbb{R}^3$, let

$$\sigma_l(\alpha, \mathcal{D}) = \sum_{\hat{\beta} \in \mathcal{D} \cap \mathbb{Z}^3, \beta \in B^{(0)}} e_l(\alpha \hat{\beta}) G(\beta),$$

whence

$$\Sigma_{14} = \frac{1}{d_{12}^6} \sum_{\lambda, \vec{b}_i, \hat{\eta}_i} e_{d_{12}}(-\vec{b}_1 \hat{\eta}_1 - \vec{b}_2 \hat{\eta}_2) \sigma_{d_{12}}(\vec{b}_1, \mathcal{C}_1) \sigma_{d_{12}}(\vec{b}_2, \mathcal{C}_2),$$

with $\lambda, \hat{\eta}_1, \hat{\eta}_2$ subject to the same conditions as before. We proceed to write $\hat{\eta}_2 = \lambda \hat{\eta}_1 + d_1 d_2 \hat{\eta}_3$, where $\hat{\eta}_3$ runs over integer vectors modulo dd^* for which

$$d_1 d^* \nu \vec{\gamma} = \vec{H}_i(\hat{\eta}_1, \lambda \hat{\eta}_1 + d_1 d_2 \hat{\eta}_3) \pmod{d_1 d d^*}.$$

According to (5.1) the right hand side depends only on the congruence classes of $\hat{\eta}_1$ and $\hat{\eta}_3$ modulo dd^* . We therefore put $\hat{\eta}_1 = \hat{\eta}_4 + dd^* \hat{\eta}_5$, where $\hat{\eta}_{4i}$ runs over integer vectors modulo dd^* and $\hat{\eta}_{5i}$ runs over integer vectors modulo $d_1 d_2$. The sum Σ_{14} now becomes

$$\Sigma_{14} = \frac{1}{d_{12}^6} \sum_{\lambda, \vec{b}_i} S(\lambda, \vec{b}_1, \vec{b}_2) \sigma_{d_{12}}(\vec{b}_1, \mathcal{C}_1) \sigma_{d_{12}}(\vec{b}_2, \mathcal{C}_2), \quad (5.2)$$

with \vec{b}_1, \vec{b}_2 and λ running over the same set as before, and

$$S(\lambda, \vec{b}_1, \vec{b}_2) = \sum_{\hat{\eta}_3, \hat{\eta}_4, \hat{\eta}_5} e_{d_1 d_2} \left(-(\vec{b}_1 + \lambda \vec{b}_2) \hat{\eta}_5 \right) e_{d_{12}} \left(-(\vec{b}_1 + \lambda \vec{b}_2) \hat{\eta}_4 - d_1 d_2 \vec{b}_2 \hat{\eta}_3 \right)$$

with

$$0 \leq \hat{\eta}_{3i} < dd^*, \quad 0 \leq \hat{\eta}_{4i} < dd^*, \quad 0 \leq \hat{\eta}_{5i} < d_1 d_2 \quad \text{for } 1 \leq i \leq 3,$$

subject to the condition

$$d_1 d^* \nu \vec{\gamma} = \vec{H}_i(\hat{\eta}_4, \lambda \hat{\eta}_4 + d_1 d_2 \hat{\eta}_3 d_1 d d^*) \pmod{d_1 d d^*}.$$

We may therefore perform the summation over $\hat{\eta}_5$ to deduce that

$$S(\lambda, \vec{b}_1, \vec{b}_2) = 0$$

unless

$$\vec{b}_1 + \lambda \vec{b}_2 = 0 \pmod{d_1 d_2}$$

in which case we have the trivial bound

$$S(\lambda, \vec{b}_1, \vec{b}_2) \ll (d_1 d_2)^3,$$

on recalling that $d_{12} \ll d_1 d_2$.

We now deduce from (5.2) that

$$\Sigma_{14} \ll (d_1 d_2)^{-3} \sum_{\lambda, \vec{b}_i} |\sigma_{d_{12}}(\vec{b}_1, \mathcal{C}_1) \sigma_{d_{12}}(\vec{b}_2, \mathcal{C}_2)|,$$

where the sum is now subject to the condition

$$1 \leq \lambda \leq d_1 d_2, (\lambda, d_1 d_2) = 1, 0 \leq b_{ij} < d_{12}$$

and

$$\vec{b}_1 + \lambda \vec{b}_2 = 0 \pmod{d_1 d_2}.$$

An application of Cauchy's inequality then yields

$$\Sigma_{14} \ll (d_1 d_2)^{-3} \left\{ \sum_{\vec{b}_1} |\sigma_{d_{12}}(\vec{b}_1, \mathcal{C}_1)|^2 N_1 \right\}^{1/2} \left\{ \sum_{\vec{b}_2} |\sigma_{d_{12}}(\vec{b}_2, \mathcal{C}_2)|^2 N_2 \right\}^{1/2}$$

where N_1 is the number of pairs λ, \vec{b}_2 which can correspond to a given vector \vec{b}_1 , and similarly for N_2 . Clearly we have $N_1, N_2 \ll d_1 d_2$, and it therefore follows that

$$\Sigma_{14} \ll (d_1 d_2)^{-2} \max_{i=1,2} \sum_{\vec{b}} |\sigma_{d_{12}}(\vec{b}, \mathcal{C}_i)|^2,$$

where \vec{b} runs over integer vectors modulo d_{12} .

We then have

$$\Sigma_{14} \ll (d_1 d_2)^{-2} \left\{ \sum_{\vec{b}} |\sigma_{d_{12}}(\vec{b}, \mathcal{C}_1)|^2 + \sum_{\vec{b}} |\sigma_{d_{12}}(\vec{b}, \mathcal{C}_2)|^2 \right\},$$

which, in conjunction with (4.17), produces the upper bound

$$\Sigma_{15} \ll \sum_{\substack{d_1 \in I_m, d_1 d_2 < d_0 \\ \vec{b} \pmod{d_{12}}}} \frac{1}{(d_1 d_2)^2} |\sigma_{d_{12}}(\vec{b}, \mathcal{C}_0)|^2 \quad (5.3)$$

with $\mathcal{C}_0 \in \{\mathcal{C}_1, \mathcal{C}_2\}$, cf. [3, p.78; 4, p.283]. Proposition 4.2 can be deduced from Lemma 4.3 and relation (5.3) along the lines of [3, § 13; 4, § 6].

On suitably adjusting the parameters η and Q_1 , [3, p.21; 4, p.287], one concludes the proof of Theorems 1 and 2 as in the cited works.

References

- [1] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London, 1974.
- [2] D.R. Heath-Brown, The solubility of diagonal cubic Diophantine equations, *Proceedings of the London Mathematical Society* (3), 79 (1999), 241-259.
- [3] D.R. Heath-Brown, Primes represented by $x^3 + 2y^3$, *Acta Mathematica*, 186 (2001), 1-84.
- [4] D.R. Heath-Brown and B.Z. Moroz, Primes represented by binary cubic forms, *Proceedings of the London Mathematical Society* (3), 84 (2002), 257-288.
- [5] P. Llorente and E. Nart, Effective determination of the decomposition of the rational primes in a cubic field, *Proc. of the American Math. Soc.*, 87 (1983), 579-585.
- [6] P. Satgé, Un analogue du calcul de Heegner, *Invent. Math.*, 87 (1987), 425-439.
- [7] H. Weyl, *Algebraic theory of numbers*, Princeton University Press, Princeton, 1940.