Primes represented by binary cubic forms

D.R. Heath-Brown
Mathematical Institute, Oxford

B.Z. Moroz
Max-Planck-Institut für Mathematik, Bonn

1 Introduction

Recently the first of the authors [2] proved the following theorem.

There are infinitely many primes of the form $a^3 + 2b^3$ with integer a, b. More specifically, there is a positive constant c such that, if

$$\eta = \eta(X) = (\log X)^{-c},$$

then the number of such primes with $X < a, b \leq X(1+\eta)$ is

$$\sigma_0 \, \frac{\eta^2 X^2}{3 \log X} \, \{1 + O((\log\log X)^{-1/6})\}$$

as $X \to \infty$, where

$$\sigma_0 = \prod_p (1 - \frac{\nu_p - 1}{p})$$

and ν_p denotes the number of solutions of the congruence $x^3 \equiv 2 \mod p$.

Our goal in the present paper is to treat a general binary cubic form, making use of the technique developed in [2]. The main result of this paper can be stated as follows.

Theorem 1.1 *Let $f(x)$ be a binary cubic form with integral rational coefficients irreducible in $\mathbb{Z}[x]$. There are infinitely many primes of the form $f(a)$ with $a \in \mathbb{Z}^2$ unless $f(a)$ is divisible by 2 for each a in $\mathbb{Z}^2$, in which case there are infinitely many primes of the form $\frac{1}{2} f(a)$ with $a \in \mathbb{Z}^2$.*

In point of fact, we shall obtain an asymptotic formula for the relevant number of primes as in [2]. The proof follows the pattern set up in [2]. Large

parts of the argument in [2] carry over almost verbatim. We shall not repeat these, but rather, emphasize those points where additional work is necessary. In consequence, the reader is advised to familiarize himself with [2] before studying the present paper. The most novel parts of the present paper are to be found in sections 2, 6, and 7.

Notation. As usual, $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ stand for the fields of complex, real, rational numbers, and the ring of rational integers, respectively; A^* denotes the group of invertible elements in a commutative ring A. We write $\#\,\mathfrak{M}$ to denote the cardinality of the set $\mathfrak{M}$. The letters μ and τ denote the Möbius and the divisor functions respectively; sometimes we write, for brevity, $\tau(\alpha)$ for the number of divisors of the ideal (α) over a field which will be clear from the context, and similar for μ. Let $e_q(x) := \exp(2\pi i x/q)$. If a denotes the array $(a_1, \ldots, a_n)$, for instance $a \in \mathbb{R}^n$, we let a_i stand for the $i-$th coordinate, and write $ab := \sum_{i=1}^n a_i b_i$ for $\{a, b\} \subset \mathbb{R}^n$; let $\partial_i f(x) := \frac{\partial_i f(x_1,\ldots,x_n)}{\partial x_i}$. Notation $a_1 = a_2 \mod R$, or simply $a_1 = a_2(R)$, means that R divides $a_1 - a_2$. In what follows, X denotes a sufficiently large positive real number; the implied constants in upper estimates and asymptotic formulae depend at most on the coefficients of the form f. We shall maintain the convention introduced in [2], according to which c (respectively $c(A)$) denotes a positive absolute (resp. depending only on A) constant, potentially different at each occurence. Let $\eta := (\log X)^{-c}$, where c is a suitable positive constant defined as in [2].

2 General set-up; the statement of the main result

Let K be a number field of degree $n = r_1 + 2r_2$ over $\mathbb{Q}$, and let $\sigma_i : K \to \mathbb{C}$, $1 \le i \le n$, be the distinct isomorphic embeddings of K into $\mathbb{C}$ numbered in such a way that $\sigma_i(K) \subset \mathbb{R}$ if and only if $i \le r_1$, and $\alpha^{(i+r_2)} = \bar{\alpha}^{(i)}$ for $r_1 < i \le r_1 + r_2$, where $\alpha^{(i)} := \sigma_i(\alpha)$ for $\alpha \in K$. Let $\mathfrak{o}(K),\ D(K),\ h(K),\ R(K)$, and $\mathcal{I}(K)$ denote the ring of integers, the discriminant, the class number, the regulator matrix of K, and the monoid of integral ideals in K respectively. Let us recall that $R(K) = (a_{ij})_{1 \le i,j \le r+1},\ r := r_1 + r_2 - 1$ with $a_{1j} = 1/n$ for $1 \le j \le r_1$, $a_{1j} = 2/n$ for $j > r_1$, and $a_{ij} = \log|\varepsilon_{i-1}^{(j)}|,\ 2 \le i \le r+1$, $1 \le j \le r+1$, where $\{\varepsilon_i : 1 \le i \le r\}$ is a set of fundamental units of K, cf. [7], p.94. Finally, let

$$\zeta_K(s) = \sum_{\mathfrak{A} \in \mathcal{I}(K)} N\mathfrak{A}^{-s}$$

be the zeta-function of K, and let $\phi(K) = 2^r \pi^{r_2} D(K)^{-1/2} h(K) |\det\ R(K)|$ be the residue of $\zeta_K(s)$ at $s = 1$, see for instance [7, p.129].

Let k be a cubic number field, that is an extension of $\mathbb{Q}$ with $[k : \mathbb{Q}] = 3$; write, for brevity, $\mathfrak{o} := \mathfrak{o}(k)$. We fix a $\mathbb{Z}$-submodule F of $\mathfrak{o}$ of rank 2, and write $F = \{a_1\omega_1 + a_2\omega_2 : a \in \mathbb{Z}^2\}$, so that $k = \mathbb{Q}(\theta_0), \theta_0 := \omega_2\omega_1^{-1}$. Let $\mathfrak{d} = (\omega_1, \omega_2)$ be the ideal in $\mathfrak{o}$ generated by F, and let

$$f(x) = N_{k(x)/\mathbb{Q}(x)}(x_1\omega_1 + x_2\omega_2)N\mathfrak{d}^{-1}.$$

Let $\varepsilon(f)$ denote the highest common factor of the integer values $\{f(a) : a \in \mathbb{Z}^2\}$ of f, and let $h_f = f(1, 1)$. Without loss of generality, it may be assumed that $h_f > 0$. The following lemmata are to be proved at the end of this section.

Lemma 2.1 *$f(x)$ is an integral binary cubic form irreducible in $\mathbb{Z}[x]$, in particular primitive, and any such form is of this shape. Moreover, $\varepsilon(f) = 1$ unless each of the four integers $N(\mathfrak{d}^{-1}\omega_1), N(\mathfrak{d}^{-1}\omega_2), N(\mathfrak{d}^{-1}(\omega_1 \pm \omega_2))$ is even, in which case $\varepsilon(f) = 2$.*

Let $\theta = \theta_0 N(\omega_1\mathfrak{d}^{-1})$, and let $\nu = (\mathfrak{o} : \mathbb{Z}[\theta])$. A rational prime, resp. a prime ideal in $\mathfrak{o}$, dividing $\nu N(\omega_1\omega_2)$ is said to be *singular*. Let P, P_0, $\mathcal{P}$, and $\mathcal{P}_0$ denote the set of rational primes, the set of singular rational primes, the set of prime ideals in $\mathfrak{o}$, and the set of singular prime ideals in $\mathfrak{o}$, respectively; the sets P_0 and $\mathcal{P}_0$ being finite, write $C = \prod_{p \in P_0} p$. Let $I(X)$ denote the square $X < x_1, x_2 \leq X(1 + \eta)$ in $\mathbb{R}^2$. Given $a \in \mathbb{Z}^2$, let $\mathfrak{A}_a := (a_1\omega_1 + a_2\omega_2)\mathfrak{d}^{-1}$; let

$$\mathcal{A}_0 = \{\mathfrak{A}_a :\ a \in \mathbb{Z}^2, (a_1, a_2) = 1\},$$

and let

$$\mathcal{A} = \{\mathfrak{A}_a :\ \mathfrak{A}_a \in \mathcal{A}_0, a \in I(X)\}.$$

Lemma 2.2 *Suppose that $\mathfrak{p}_i|\mathfrak{B}$, $\mathfrak{p}_i|p$, $\mathfrak{p}_i \in \mathcal{P}$ for some $\mathfrak{B}$ in $\mathcal{A}_0$, and some p in P, $i = 1, 2$. If p is not singular, then $\mathfrak{p}_1 = \mathfrak{p}_2$ and $N\mathfrak{p}_1 = p$.*

Lemma 2.3 *Suppose that $\{\mathfrak{A}_a, \mathfrak{A}_b\} \subseteq \mathcal{A}$. Then $f(a) = h_f X^3(1 + O(\eta))$ and $\mathfrak{A}_a = \mathfrak{A}_b \Rightarrow a = b$.*

As an immediate consequence of these two lemmata, one obtains the following result.

Corollary 2.1 *If $\mathfrak{A}_a \in \mathcal{A}$, then $f(a) \in P \Leftrightarrow \mathfrak{A}_a \in \mathcal{P}$.*

We are now ready to state our main result. Let

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

be the number of rational primes p of the form $p = f(a)$ with $a \in I(X)$. By Corollary 2.1,

$$\pi(\mathcal{A}) = \text{card}\ (\mathcal{A} \cap \mathcal{P}). \tag{2.1}$$

Theorem 2.1 *Let f be a binary cubic form irreducible in $\mathbb{Z}[x]$ with $\varepsilon(f) = 1$; suppose $f(1,1) > 0$. Then*

$$\pi(\mathcal{A}) = \sigma(f)\ \frac{\eta^2 X^2}{3 \log X}\ \{1 + O((\log\log X)^{-1/6})\} \tag{2.2}$$

as $X \to \infty$, with $\sigma(f) > 0$.

Corollary 2.2 *Let f be a binary cubic form irreducible in $\mathbb{Z}[x]$ with $\varepsilon(f) = 2$; suppose $f(2,1) > 0$. Then the number of rational primes p of the form $p = \frac{1}{2}f(a)$ with $b(a) \in I(X)$, where $b_1(a) = \frac{1}{2}a_1,\ b_2(a) = a_2$, is equal to*

$$\sigma(f)\ \frac{\eta^2 X^2}{3 \log X}\ \{1 + O((\log\log X)^{-1/6})\}.$$

Proof. It suffices to remark that if $\varepsilon(f) = 2$ then $f(x) = 2g(y)$, where $x_1 = 2y_1,\ x_2 = y_2$, and g is a binary cubic form irreducible in $\mathbb{Z}[x]$ with $\varepsilon(g) = 1$. Since $f(2,1) = 2g(1,1)$, the assertion follows from Theorem 2.1 applied to g.

We conclude this section by proving Lemmata 2.1-3. Let us begin with Lemma 2.1. The binary cubic form $f(x)$ is integral, for each of the coefficients of the form $N_{k(x)/\mathbb{Q}(x)}(x_1\omega_1 + x_2\omega_2)$ is divisible by $N\mathfrak{d}$. Since $k = \mathbb{Q}(\theta_0)$, the form $f(x)$ is $\mathbb{Q}-$irreducible. If

$$p | \text{h.c.f.}(N(\mathfrak{d}^{-1}\omega_1), N(\mathfrak{d}^{-1}\omega_2), N(\mathfrak{d}^{-1}(\omega_1 \pm \omega_2)))$$

and $p \in P$, then $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where

$$\mathfrak{p}_1 | \omega_1\mathfrak{d}^{-1}, \mathfrak{p}_2 | \omega_2\mathfrak{d}^{-1}, \mathfrak{p}_3 | (\omega_1 \pm \omega_2)\mathfrak{d}^{-1},\ \mathfrak{p}_i \in \mathcal{P},\ 1 \le i \le 3,$$

and it follows that $p = 2$; moreover, the coefficients of $x_1^2x_2$ and of $x_1x_2^2$ in $f(x)$ are easily seen to be odd in this case. It follows therefore that f is primitive. Conversely, let $f(x)$ be an integral binary cubic form irreducible in $\mathbb{Z}[x]$, then $f(x) = aN_{k(x)/\mathbb{Q}(x)}(x_1 + \eta x_2)$ with $a \in \mathbb{Z},\ \eta \in k$. Suppose $m\eta \in \mathfrak{o},\ m \in \mathbb{Z}$, and let $g(x) = N_{k(x)/\mathbb{Q}(x)}(mx_1 + \omega x_2)N\mathfrak{d}^{-1}$, where $\omega = m\eta,\ \mathfrak{d} = (m, \omega)$. Since $g(x)$ is an integral binary cubic form irreducible in $\mathbb{Z}[x]$, it follows that

$f = g$. Clearly, $\varepsilon(f) \neq 0 \bmod 4$. Moreover, the above argument shows also that $\varepsilon(f) = 2$ if and only if the following condition holds:

$$2 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ \mathfrak{p}_i \in \mathcal{P},\ \mathfrak{p}_i \neq \mathfrak{p}_j,\ \mathfrak{p}_i\mathfrak{d}|\omega_i, 1 \leq i < j \leq 3,\ \mathfrak{p}_3\mathfrak{d}|(\omega_1 + \omega_2).$$

This completes the proof of Lemma 2.1.

Suppose now that $\mathfrak{p}_1, \mathfrak{p}_2|\mathfrak{A}_a,\ \mathfrak{A}_a \in \mathcal{A}_0$. Then if $n = -a_1a_2^{-1} \bmod p$ with $n \in \mathbb{Z}$, we will have

$$\theta_0 = -a_1a_2^{-1} = n\ (\mathfrak{p}_i),\ (i = 1, 2).$$

Since $\mathfrak{p}_1, \mathfrak{p}_2|p$, and p is non-singular, it follows that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ do not divide ν. Thus $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$. Let $\varphi(u) = N_{k(u)/\mathbb{Q}(u)}(u - \theta)$ be the characteristic polynomial of θ_0, so that

$$\varphi(n) = -a_2^{-3}N(\mathfrak{d}^{-1}\omega_1)^{-1}N(\mathfrak{A}_a) = 0 \bmod p.$$

It follows from a theorem of Dedekind (see, for instance [5, Lemma 1]) that the ideal $(p, \theta_0 - n)$ is prime. Since both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ divide $(p, \theta_0 - n)$ we deduce that $\mathfrak{p}_1 = \mathfrak{p}_2$, as Lemma 2.2 asserts.

Finally, let $\mathfrak{A}_a \in \mathcal{A}$. Then $f(a) = X^3f(a/X)$ and $a_i/X = 1 + O(\eta),\ i = 1, 2$, so that $f(a) = h_fX^3(1 + O(\eta))$ since $h_f > 0$. Suppose $\mathfrak{A}_a = \mathfrak{A}_b$ and let

$$\alpha = (a_1\omega_1 + a_2\omega_2)(b_1\omega_1 + b_2\omega_2)^{-1}, \tag{2.3}$$

then $\alpha \in \mathfrak{o}^*$. It follows from (2.3) that

$$\text{Tr } \alpha = (a_1\partial_1 f(b) + a_2\partial_2 f(b))f(b)^{-1},$$

and therefore

$$\text{Tr } \alpha = (b_1\partial_1 f(b) + b_2\partial_2 f(b))f(b)^{-1} + O(\eta X f(b)^{-1}(|\partial_1 f(b)| + |\partial_2 f(b)|)),$$

or Tr $\alpha = 3 + O(\eta)$. Since Tr $\alpha \in \mathbb{Z}$, it follows that Tr $\alpha = 3$; analogously, Tr $\alpha^{-1} = 3$. Thus $\alpha = 1$, and Lemma 2.3 follows.

3 Preparatory lemmata; calculation of $\sigma(f)$

Write, for brevity, $\mathcal{I} := \mathcal{I}(k)$. Given a sequence D of rational integers, and a sequence $\mathcal{D}$ of ideals in $\mathcal{I}$, let $D_d = \{c : c \in D, d|c\}$, and $\mathcal{D}_\mathfrak{a} = \{\mathfrak{c} : \mathfrak{c} \in \mathcal{D}, \mathfrak{a}|\mathfrak{c}\}$ for $d \in \mathbb{Z}$, and $\mathfrak{a} \in \mathcal{I}$. Let

$$A = \{f(a) : a \in I(X) \cap\ \mathbb{Z}^2,\ (a_1, a_2) = 1\},$$

or what amounts to the same thing, $A = \{N\mathfrak{a} \mid \mathfrak{a} \in \mathcal{A}\}$. Let

$$\mathcal{R} = \{R : R \in \mathcal{I}, \mu(R)^2 = 1, R = R_0R_1, \mu(NR_1)^2 = 1\},$$

where $R_0 = (R, C)$, so that $(R_1, C) = 1$. It follows from Lemma 2.2 that

$$(\{R : R \in \mathcal{I}, \mu(R)^2 = 1\} \cap \mathcal{A}_0) \subseteq \mathcal{R}.$$

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

$$\sigma(R, X) = \#\{a : a \in \mathbb{Z}^2 \cap I(X), R|\mathfrak{A}_a\},$$

let

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

where $r := NR$, and let

$$\alpha(R) = \frac{1}{r}\,\#\,\mathfrak{m}(R),\ \beta(R) = \frac{1}{r}\,\alpha(R). \tag{3.1}$$

Following [2, § 5] we may conclude that

$$\sigma(R, X) = r^{-2} \sum_{\substack{a \bmod r \\ x \in I(X)}} \sigma_0(R, a) e_r(-ax),$$

where $\sigma_0(R, a) = \sum_{u \in \mathfrak{m}(R)} e_r(au)$. One remarks that the sum $\sigma_0(R, a)$ is weakly multiplicative, that is $\sigma_0(\mathfrak{ab}, a) = \sigma_0(\mathfrak{a}, a)\sigma_0(\mathfrak{b}, a)$, whenever $(N\mathfrak{a}, N\mathfrak{b}) = 1$, and $\alpha(R) = \alpha(R_0)\alpha(R_1) = \alpha(R_0)$ for $R \in \mathcal{R}$. As in [2], it follows that

$$\sigma(R, X) = \frac{\eta^2 X^2}{r}\,\alpha(R_0) + \rho(R, X), \tag{3.2}$$

with

$$\rho(R, X) = \Sigma_0 + O(\frac{X}{r}), \tag{3.3}$$

where

$$\Sigma_0 = r^{-2} \sum_{\substack{a \neq 0 \bmod r \\ x \in I(X)}} \sigma_0(R, a) e_r(-ax). \tag{3.4}$$

Let

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

We prove the following analogue of [2, Lemma 5.1].

Lemma 3.1 *If A is any positive integer, there exists $c(A)$ such that*

$$\Sigma_1 \ll (X+Q)(\log Q)^{c(A)}.$$

Proof. It follows from (3.3) that $\Sigma_1 \leq \Sigma_{11} + \Sigma_{12}$, where

$$\Sigma_{11} \ll X \sum_{Q<NR\leq 2Q} \tau(R)^A NR^{-1} \ll X(\log Q)^{c(A)},$$

and

$$\Sigma_{12} = \sum_{\substack{Q<NR\leq 2Q \\ R\in\mathcal{R}}} \tau(R)^A |\Sigma_0|. \tag{3.5}$$

By (3.4),

$$\Sigma_0 \leq r^{-2} \sum_{a\neq 0 \bmod r} |\sigma_0(R,a)| \, | \sum_{x\in I(X)} e_r(-ax)|.$$

Since $|\sigma_0(R,a)| = |\sigma_0(R_0,a)| \; |\sigma_0(R_1,a)| \leq NR_0^2 \; |\sigma_0(R_1,a)| \ll |\sigma_0(R_1,a)|$, it follows that

$$|\Sigma_0| \ll \sum_{\substack{|a_1|,|a_2|\leq r/2 \\ a\neq 0}} \frac{|\sigma_0(R_1,a)|}{r^2} \min\{X, \frac{r}{|a_1|}\} \min\{X, \frac{r}{|a_2|}\}. \tag{3.6}$$

Further, if $NR_1 = p, \; p\in P, \; a \neq 0 \mod p$, then

$$\sigma_0(R_1,a) = \sum_{tu\in\mathfrak{m}(R_1)} e_p(tua) = \sum_{u\in\mathfrak{m}(R_1)} e_p(tua)$$

as soon as $t \neq 0 \mod p$; therefore

$$\begin{aligned} (p-1)\,\sigma_0(R_1,a) &= \sum_{\substack{u\in\mathfrak{m}(R_1) \\ 1\leq t<p}} e_p(tua) \\ &= p \,\#\,\{u : u\in\mathfrak{m}(R_1), p|ua\} - \#\,\mathfrak{m}(R_1). \end{aligned}$$

If $a_2\omega_1 \neq a_1\omega_2 \mod R_1$, this gives $(p-1)\,\sigma_0(R_1,a) = p - \#\,\mathfrak{m}(R_1) = 0$; in view of the weak multiplicativity of $\sigma_0(R_1,a)$, it follows therefore that

$$a_2\omega_1 \neq a_1\omega_2 \mod R_1 \;\Rightarrow\; \sigma_0(R_1,a) = 0 \tag{3.7}$$

for any R. Let us substitute estimate (3.6) in the equation (3.5) and divide the range of summation over a into two parts, summing first over those a

with $a_1a_2 = 0$ and then over those with $a_1a_2 \neq 0$. This gives $\Sigma_{12} \ll \Sigma_{13}+\Sigma_{14}$, where

$$\Sigma_{13} \ll X \sum_{0<a\leq Q} \frac{1}{a} \sum_{\substack{Q<NR\leq 2Q \\ R_1|a}} \tau(R)^A \ll X \sum_{0<a\leq Q} \frac{\tau(a)^{c_1(A)}}{a} \ll X\ (\log Q)^{c(A)},$$

and

$$\Sigma_{14} = \sum_{\substack{1\leq|a_1|,|a_2|\leq r/2 \\ Q<NR\leq 2Q, R\in\mathcal{R}}} \tau(R)^A\ \frac{|\sigma_0(R_1,a)|}{r^2} \min\{X, \frac{r}{|a_1|}\} \min\{X, \frac{r}{|a_2|}\}.$$

One obtains

$$\Sigma_{14} \ll \sum_{\substack{Q<NR\leq 2Q, R\in\mathcal{R} \\ a\in\Omega}} \tau(R)^A\ \frac{|\sigma_0(R_1,a)|}{|a_1a_2|} \ll Q \sum_{\substack{Q<NR\leq 2Q, R\in\mathcal{R} \\ a\in\Omega}} \frac{\tau(R)^A}{|a_1a_2|},$$

where

$$\Omega = \{a : 1 \leq |a_1|, |a_2| \leq Q,\ a_2\omega_1 = a_1\omega_2 \mod R_1\};$$

this gives

$$\begin{aligned}\Sigma_{14} \ll Q \sum_{1\leq|a_1|,|a_2|\leq Q} \frac{\tau(a_2\omega_1 - a_1\omega_2)^{c_1(A)}}{|a_1a_2|} \\ = Q \sum_M \sum_{\substack{M_1\leq|a_1|\leq 2M_1 \\ M_2\leq|a_2|\leq 2M_2}} (M_1M_2)^{-1}\tau(a_2\omega_1 - a_1\omega_2)^{c_1(A)}\end{aligned}$$

with M_1, M_2 ranging over the set $\{2^m : 1 \leq 2^m \leq Q\}$. Making use of the following analogue of [2, Lemma 4.7]

$$\sum_{\substack{|a_1|\leq x_1,|a_2|\leq x_2 \\ a_1a_2\neq 0}} \tau(a_2\omega_1 - a_1\omega_2)^A \ll x_1x_2\ (\log(x_1x_2))^{c(A)}, \tag{3.8}$$

one obtains

$$\Sigma_{14} \ll Q(\log Q)^{c_1(A)} \sum_M 1 \ll Q(\log Q)^{c(A)}.$$

This concludes the proof of Lemma 3.1.

By definition,

$$\mathcal{A}_R = \{\mathfrak{A}_a : a \in I(X) \cap \mathbb{Z}^2,\ (a_1, a_2) = 1,\ R|\mathfrak{A}_a\}.$$

Assuming $R \in \mathcal{R}$, it follows then that

$$\begin{aligned} \#\,\mathcal{A}_R &= \sum_{d=1}^{\infty} \mu(d)\ \sigma(\frac{R}{(R,d)}, \frac{X}{d}) \\ &= \frac{\eta^2 X^2}{r}\ \alpha(R_0) \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}\ \beta((R,d))^{-1} + \rho_1(R,X), \end{aligned} \tag{3.9}$$

where

$$\rho_1(R,X) = \sum_{d=1}^{\infty} \mu(d)\ \rho(\frac{R}{(R,d)}, \frac{X}{d}). \tag{3.10}$$

Thus

$$\#\,\mathcal{A}_R = \frac{\eta^2 X^2}{r\zeta(2)}\ \alpha(R_0)\ \alpha_1(R) + \rho_1(R,X), \tag{3.11}$$

where

$$\alpha_1(R) = \prod_{p \in P,\ p|r} (1 - \frac{1}{p^2})^{-1}(1 - \frac{1}{p^2\beta((R,p))}). \tag{3.12}$$

Let

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

The following lemma is our analogue of [2, Lemma 3.2].

Lemma 3.2 *If A is any positive integer, there exists $c(A)$ such that*

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

Proof. It follows from (3.10) that $\Sigma_2 \le \Sigma_{21} + \Sigma_{22}$, where

$$\Sigma_{21} = \sum_{\substack{Q < NR \le 2Q \\ R \in \mathcal{R},\ d > \Delta}} \tau(R)^A |\rho(\frac{R}{(R,d)}, \frac{X}{d})|,$$

and

$$\Sigma_{22} = \sum_{\substack{Q < NR \le 2Q \\ R \in \mathcal{R}, d \le \Delta}} \tau(R)^A |\rho(\frac{R}{(R,d)}, \frac{X}{d})|.$$

It follows from (3.2) that $\Sigma_{21} \le \Sigma_{23} + \Sigma_{24}$, where

$$\Sigma_{23} = \sum_{\substack{Q<NR\le 2Q \\ R\in\mathcal{R},\ d>\Delta}} \tau(R)^A |\sigma(\frac{R}{(R,d)}, \frac{X}{d})|,$$

and

$$\begin{aligned}\Sigma_{24} &= \eta^2 X^2 \sum_{\substack{Q<NR\le 2Q \\ R\in\mathcal{R},\ d>\Delta}} \tau(R)^A \ \frac{N((R,d))}{d^2\ NR}\ \alpha(\frac{R_0}{(R_0,d)}) \\ &\ll \eta^2 X^2 \sum_{\substack{Q<NR\le 2Q \\ R\in\mathcal{R},\ d>\Delta}} \frac{\tau(R)^A}{NR}\ \frac{N((R,d))}{d^2}.\end{aligned}$$

Let

$$\mathfrak{A}_1 = (R_1, d),\ R_1 = \mathfrak{A}_1\mathfrak{A}_2,\ d = mN\mathfrak{A}_1.$$

In this notation

$$\begin{aligned}\Sigma_{24} &\ll \eta^2 X^2 \sum_{Q<N(\mathfrak{A}_1\mathfrak{A}_2R_0)\le 2Q} \tau(\mathfrak{A}_1)^A\tau(\mathfrak{A}_2)^A N(\mathfrak{A}_1)^{-2}N(\mathfrak{A}_2)^{-1} \sum_{m>\Delta N(\mathfrak{A}_1)^{-1}} m^{-2} \\ &\ll \eta^2 X^2\Delta^{-1}(\log X)^{c(A)},\end{aligned}$$

and

$$\begin{aligned}\Sigma_{23} &\ll \sum_{\substack{Q<N(\mathfrak{A}_1\mathfrak{A}_2R_0)\le 2Q \\ d>\Delta,\ N(\mathfrak{A}_1)|d}} \tau(\mathfrak{A}_1)^A\tau(\mathfrak{A}_2)^A|\sigma(\frac{R_0}{(R_0,d)}\ \mathfrak{A}_2, \frac{X}{d})| \\ &\le \sum_{d>\Delta,\ N(\mathfrak{A}_1)|d} \tau(\mathfrak{A}_1)^A \sum_{Q<N(\mathfrak{A}_1\mathfrak{A}_2R_0)\le 2Q} \tau(\mathfrak{A}_2)^A|\sigma(\mathfrak{A}_2, \frac{X}{d})| \\ &\ll \sum_{d>\Delta} \tau(d)^{c_1(A)} \sum_{a\in I(X/d)} \tau(\mathfrak{A}_a)^{c_1(A)}.\end{aligned}$$

In view of (3.8), this gives

$$\Sigma_{23} \ll X^2\Delta^{-1}(\log X)^{c(A)};$$

thus

$$\Sigma_{21} \ll \Delta^{-1}\ X^2(\log X)^{c(A)}. \tag{3.13}$$

Let now $\mathfrak{A} = (R, d),\ R = \mathfrak{A}\mathfrak{B}$; with this notation,

$$\Sigma_{22} \leq \sum_{\substack{Q<N(\mathfrak{A}\mathfrak{B})\leq 2Q \\ d\leq\Delta,\ N(\mathfrak{A}_1)|d}} \tau(\mathfrak{A})^A \tau(\mathfrak{B})^A |\rho(\mathfrak{B}, \frac{X}{d})|,$$

where we write $\mathfrak{A} = \mathfrak{A}_0\mathfrak{A}_1$ with $\mathfrak{A}_0 = (\mathfrak{A}, C)$, as at the beginning of this section. Therefore it follows from Lemma 3.1 that

$$\begin{aligned}
\Sigma_{22} &\ll \sum_{d\leq\Delta,\ N(\mathfrak{A}_1)|d} \tau(\mathfrak{A})^A (\frac{Q}{N\mathfrak{A}} + \frac{X}{d})(\log Q)^{c(A)} \\
&\ll \sum_{d\leq\Delta,\ N(\mathfrak{A}_1)|d} \tau(\mathfrak{A}_1)^A (\frac{Q}{N\mathfrak{A}_1} + \frac{X}{d})(\log Q)^{c(A)} \\
&\ll \Delta\ (X+Q)(\log Q)^{c(A)}(\log X).
\end{aligned}$$

As in the proof of [2, Lemma 3.2], we combine this estimate with (3.13) and let $\Delta = 1 + \min\{X^{1/2}\,,\ XQ^{-1/2}\}$ to conclude the proof of the lemma.

To estimate $\#\ A_q$ we start, as in [2, § 5], with the following identity in which $p \in P$:

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

For q square-free, this gives

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

Therefore

$$\#\ A_q = \sum_{\mathfrak{A}\in\mathcal{A},\ q|N\mathfrak{A}} 1 = \mu(q) \sum_{\substack{R|(\mathfrak{A},q),\ q|NR \\ \mathfrak{A}\in\mathcal{A}}} \mu(R) = \mu(q) \sum_{\substack{R|q,\ q|NR \\ R\in\mathcal{R}}} \mu(R)\ \#\ \mathcal{A}_R.$$

On substituting equation (3.11) into the last equation, one obtains

$$\#\ A_q = \gamma(q)\ \frac{\eta^2 X^2}{\zeta(2)} + \rho_2(q, X), \tag{3.14}$$

where

$$\gamma(q) = \mu(q) \sum_{\substack{R|q,\ q|NR \\ R\in\mathcal{R}}} \frac{\mu(R)\alpha(R_0)\ \alpha_1(R)}{NR} = \prod_{p|q} \gamma(p) \tag{3.15}$$

with

$$\gamma(p) = -\sum_{\substack{R|p,\ R\neq 1\\ R\in\mathcal{R}}} \frac{\mu(R)\alpha(R_0)\ \alpha_1(R)}{NR},$$

and

$$\rho_2(q,X) = \mu(q)\sum_{\substack{R|q,\ q|NR\\ R\in\mathcal{R}}} \mu(R)\rho_1(R,X). \tag{3.16}$$

Let

$$\Sigma_3 = \sum_{Q<q\leq 2Q} \tau(q)^A\mu(q)^2|\rho_2(q,X)|.$$

We can now prove an analogue of [2, Lemma 2.1].

Lemma 3.3 *If A is any positive integer, there exists $c(A)$ such that*

$$\Sigma_3 \ll (Q + XQ^{1/2} + X^{3/2})(\log QX)^{c(A)}.$$

Proof. It follows from (3.16) that

$$\Sigma_3 \ll \sum_{\substack{Q<q\leq 2Q\\ R\in\mathcal{R}(q)}} \tau(q)^A\mu(q)^2\ |\rho_1(R,X)| \ll \sum_{\substack{Q<NR\leq 2C^3Q\\ R\in\mathcal{R}}} \tau(R)^{c_1(A)}\ |\rho_1(R,X)|,$$

where

$$\mathcal{R}(q) = \{R : R\in\mathcal{R}, q_0|NR_0, R_0|q_0, NR_1 = q_1, q = q_0q_1, q_0 = (q,C)\}.$$

Therefore the asserted estimate follows from Lemma 3.2.

We let, by definition,

$$\sigma(f) = \prod_{p\in P}(1+\frac{1}{p})(1-\gamma(p)). \tag{3.17}$$

Lemma 3.4 *The infinite product in (3.17) converges, $\gamma(p)\geq 0$ for each p, and there is a positive real number c, depending at most on f, such that $1-\gamma(p)\geq c$ as soon as $p\geq 3$; moreover, $\gamma(2) = 1 \Leftrightarrow \varepsilon(f) = 2$.*

Proof. If p is not singular, that is if it does not divide C, then

$$(1+\frac{1}{p})(1-\gamma(p)) = 1 - \frac{\nu_p - 1}{p}, \tag{3.18}$$

where ν_p denotes the number of prime ideals $\mathfrak{p}$ in $\mathcal{P}$ with $N\mathfrak{p} = p$. It follows from (3.18) that there is a positive real number c, depending at most on f, such that $1 - \gamma(p) \geq c$ for all non-singular primes $p \geq 3$. Moreover, the product in (3.17) differs from the product

$$\prod_{p \in P} (1 - \frac{\nu_p - 1}{p}),$$

convergent in view of the Prime Ideal Theorem, by finitely many factors. Suppose p is singular. It follows from the definitions (3.1) and (3.12) of $\beta(R)$ and $\alpha_1(R)$ that

$$\gamma(p) = - \sum_{\substack{R|p,\, R \neq 1 \\ R \in \mathcal{R}}} \mu(R)\beta(R)\, \alpha_1(R) = \frac{1}{1-p^2} \sum_{\substack{R|p,\, R \neq 1 \\ R \in \mathcal{R}}} \mu(R)(p^2\beta(R) - 1).$$

Let $b(R) = p^2\beta(R)$, then

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

since $\mu(R) \neq 0 \ \Rightarrow \ R \in \mathcal{R}$. It follows from (3.1) that

$$b(R) = \#\, \{u : u \in \mathbb{Z}^2, u \mod p, R|\mathfrak{A}_u\}$$

if $R|p$. Therefore

$$\sum_{R|p} \mu(R)b(R) = \#\, \{u : u \in \mathbb{Z}^2, u \mod p, \text{ h.c.f.}(\mathfrak{A}_u, p) = 1\}.$$

The above quantity is at most p^2, whence $\gamma(p) \geq 0$, and it is strictly positive if and only if $p \nmid \varepsilon(f)$. Since there are only finitely many singular primes, this completes the proof of the lemma.

To state the analogues of [2, Lemma 2.2] and [2, Lemma 3.3], 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 let $B = \{N\mathfrak{A} : \mathfrak{A} \in \mathcal{B}\}$.

Lemma 3.5 *If A is any positive integer, there exists $c(A)$ such that*

$$\sum_{Q < q \leq 2Q} \tau(q)^A \mu(q)^2 \, |\#\, B_q - \phi(k)\, \frac{h_f \eta X^3}{Nq}\, j(q)| \ll X^2 Q^{1/3} (\log Q)^{c(A)},$$

where

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

Lemma 3.6 *If A is any positive integer, there exists $c(A)$ such that*

$$\sum_{Q<NR\leq 2Q} \tau(R)^A\ |\#\ \mathcal{B}_R - \phi(k)\ \frac{h_f\eta X^3}{NR}| \ll X^2 Q^{1/3} (\log Q)^{c(A)}.$$

These two statements can be proved in exactly the same way as Lemma 2.2 and Lemma 3.3 in [2].

4 Sieve methods

Let

$$\pi(\mathcal{B}) = \#\ (\mathcal{B} \cap \mathcal{P}).$$

By the Prime Ideal Theorem,

$$\pi(\mathcal{B}) = \frac{h_f\eta X^3}{3\log X}\ (1 + O(1/\log X)).$$

Therefore (2.2) is equivalent to the following asymptotic formula, to be proved by a version of the sieve method developed in [2],

$$\pi(\mathcal{A}) = \kappa\pi(\mathcal{B}) + O(\frac{\eta^2 X^2}{\log X}\tau), \tag{4.1}$$

where

$$\kappa := \sigma(f)\eta(h_f X)^{-1},\ \tau := (\log\log X)^{-1/6}.$$

We adopt the following notation. Choose a total ordering $\prec$ on $\mathcal{P}$ in such a way that

$$N\mathfrak{p}_1 < N\mathfrak{p}_2\ \Rightarrow \mathfrak{p}_1 \prec \mathfrak{p}_2.$$

Then, given a sequence D of rational integers, and a sequence $\mathcal{D}$ of ideals in $\mathcal{I}$, let

$$S(D, z) = \#\ \{a : a \in D,\ p|a \Rightarrow p \geq z, p \in P\},$$

$$S(\mathcal{D}, z) = \#\ \{\mathfrak{a} : \mathfrak{a} \in \mathcal{D},\ \mathfrak{p}|\mathfrak{a} \Rightarrow N\mathfrak{p} \geq z, \mathfrak{p} \in \mathcal{P}\}$$

and

$$S(\mathcal{D}, \mathfrak{p}_1) = \#\ \{\mathfrak{a} : \mathfrak{a} \in \mathcal{D},\ \mathfrak{p}|\mathfrak{a} \Rightarrow \mathfrak{p} \succeq \mathfrak{p}_1, \mathfrak{p} \in \mathcal{P}\},$$

for any real $z > 1$. Clearly,

$$\pi(\mathcal{D}) = S(\mathcal{D}, h_1 X^{3/2}), \tag{4.2}$$

where $h_1 := 2\sqrt{h_f}$ and $\mathcal{D}$ stands for either of the sequences $\mathcal{A}, \mathcal{B}$. As in [2], we write

$$S(\mathcal{D}, h_1 X^{3/2}) = S_1(\mathcal{D}) - \sum_{i=2}^{5} S_i(\mathcal{D}), \tag{4.3}$$

where

$$S_1(\mathcal{D}) := S(\mathcal{D}, X^\tau),\ S_i(\mathcal{D}) := \sum_{a_i \le N(\mathfrak{p}) < b_i} S(\mathcal{D}_\mathfrak{p}, \mathfrak{p}),\ 2 \le i \le 5,$$

and

$$a_2 = X^\tau,\ a_3 = b_2 = X^{1-\tau},\ a_4 = b_3 = X^{1+\tau},\ a_5 = b_4 = X^{3/2-\tau},\ b_5 = h_1 X^{3/2}.$$

For $\mathfrak{p} \in \mathcal{P}^n$, let $\lambda(\mathfrak{p}) = \prod_{i=1}^n \mathfrak{p}_i$. Let

$$J_n(\mathcal{A}) = \{\mathfrak{p} : \mathfrak{p} \in \mathcal{P}^n, X^\tau \le N\mathfrak{p}_n < \ldots < N\mathfrak{p}_1 < X^{1-\tau}\},$$

and

$$J_n(\mathcal{B}) = \{\mathfrak{p} : \mathfrak{p} \in \mathcal{P}^n, \mathfrak{p}_n \prec \ldots \prec \mathfrak{p}_1,\ N\mathfrak{p}_1 < X^{1-\tau},\ N\mathfrak{p}_n \ge X^\tau\}.$$

One defines

$$T^{(n)}(\mathcal{D}) = \sum_{\substack{\mathfrak{p} \in J_n(\mathcal{D}) \\ N\lambda(\mathfrak{p}) < X^{1+\tau}}} S(\mathcal{D}_{\lambda(\mathfrak{p})}, X^\tau),$$

and

$$U^{(n)}(\mathcal{D}) = \sum_{\substack{\mathfrak{p} \in J_{n+1}(\mathcal{D}) \\ N(\lambda(\mathfrak{p})\mathfrak{p}_{n+1}^{-1}) < X^{1+\tau} \le N\lambda(\mathfrak{p})}} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_{n+1})$$

for $n > 0$; let $T^{(0)}(\mathcal{D}) := S_1(\mathcal{D})$. The combinatorial argument used in [2, § 2] shows that

$$S_2(\mathcal{D}) = \sum_{1 \le n \le n_0} (-1)^{n-1} (T^{(n)}(\mathcal{D}) - U^{(n)}(\mathcal{D})),\ n_0 \ll \tau^{-1}. \tag{4.4}$$

Following [2, § 3] we put

$$U_1^{(1)}(\mathcal{D}) = \sum_{\substack{\mathfrak{p} \in J_2(\mathcal{D}) \\ X^{1+\tau} \le N\lambda(\mathfrak{p}) \le X^{3/2-\tau}}} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_2),$$

$$U_2^{(1)}(\mathcal{D}) = \sum_{\substack{\mathfrak{p}\in J_2(\mathcal{D})\\ N\lambda(\mathfrak{p})\geq X^{3/2+\tau}}} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_2),$$

$$U_1^{(2)}(\mathcal{D}) = \sum_{\substack{\mathfrak{p}\in J_3(\mathcal{D})\\ N(\lambda(\mathfrak{p})\mathfrak{p}_3^{-1})<X^{1+\tau}\leq N\lambda(\mathfrak{p})\leq X^{3/2-\tau}}} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_3),$$

$$S_6(\mathcal{D}) = \sum_{\substack{\mathfrak{p}\in J_2(\mathcal{D})\\ X^{3/2-\tau}\leq N\lambda(\mathfrak{p})\leq X^{3/2+\tau}}} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_2),$$

and

$$S_7(\mathcal{D}) = \sum_{\substack{\mathfrak{p}\in J_3(\mathcal{D})\\ N(\lambda(\mathfrak{p})\mathfrak{p}_3^{-1})<X^{1+\tau},\ N\lambda(\mathfrak{p})\geq X^{3/2-\tau}}} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_3).$$

It follows that

$$U^{(1)}(\mathcal{D}) = U_1^{(1)}(\mathcal{D}) + S_6(\mathcal{D}) + U_2^{(1)}(\mathcal{D}) \tag{4.5}$$

and

$$U^{(2)}(\mathcal{D}) = U_1^{(2)}(\mathcal{D}) + S_7(\mathcal{D}). \tag{4.6}$$

Lemma 4.1 *We have*

$$\begin{aligned}\pi(\mathcal{A}) - \kappa\pi(\mathcal{B}) \ \ll\ & \sum_{0\leq n\leq n_0} |T^{(n)}(\mathcal{A}) - \kappa T^{(n)}(\mathcal{B})| \\ & + |U_1^{(1)}(\mathcal{A}) - \kappa U_1^{(1)}(\mathcal{B})| + |U_2^{(1)}(\mathcal{A}) - \kappa U_2^{(1)}(\mathcal{B})| \\ & + |U_1^{(2)}(\mathcal{A}) - \kappa U_1^{(2)}(\mathcal{B})| + \sum_{3\leq n\leq n_0} |U^{(n)}(\mathcal{A}) - \kappa U^{(n)}(\mathcal{B})| \\ & + \sum_{j=3,5,6,7} (S_j(\mathcal{A}) + \kappa S_j(\mathcal{B})) + |S_4(\mathcal{A}) - \kappa S_4(\mathcal{B})|.\end{aligned}$$

Proof. It follows from the equations (4.2-6).

Lemma 4.2 *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. One may assume that no prime p with $p \geq X^\tau$ is singular; then the analogue of the equation (6.1) in [2] can be proved in exactly the same way as in [2, § 6]. Thus

$$T^{(n)}(\mathcal{A}) = \sum_{\substack{X^\tau \leq p_n < \ldots < p_1 < X^{1-\tau} \\ p_1 \ldots p_n < X^{1+\tau}}} S(A_{p_1 \ldots p_n}, X^\tau),\ T^{(0)}(\mathcal{A}) = S(\mathcal{A}, X^\tau). \quad (4.7)$$

By the 'Fundamental Lemma', [1, Theorem 7.1], with '$\omega(p)$'= $p\gamma(p)$, 'X'= $\frac{\eta^2 X^2}{\zeta(2)}$, '$\xi$'=$X^{1/6}$ and 'z'= X^τ, it follows from (3.14) that

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

where

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

and

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

In view of Lemma 3.3 this gives, cf. [2, equation (6.3)],

$$\begin{aligned} T^{(n)}(\mathcal{A}) &= \frac{\eta^2 X^2}{\zeta(2)} \prod_{p < X^\tau} (1 - \gamma(p)) \Sigma_4 \{1 + O(\exp(-\tau^{-1}))\} \\ &\qquad + O(X^{7/4} (\log X)^c), \end{aligned} \quad (4.8)$$

where

$$\Sigma_4 = \sum_{\substack{X^\tau \leq p_n < \ldots < p_1 < X^{1-\tau} \\ p_1 \ldots p_n < X^{1+\tau}}} \gamma(p_1 \ldots p_n).$$

The analogue of the relation (6.6) in [2] can be deduced from Lemma 3.6 in exactly the same way as in [2, § 6]. This gives

$$\begin{aligned} T^{(n)}(\mathcal{B}) &= \phi(k) h_f \eta X^3 \prod_{p < X^\tau} (1 - \frac{j(p)}{p}) \Sigma_5 \{1 + O(\exp(-\tau^{-1}))\} \\ &\qquad + O(X^{3-\tau/3}), \end{aligned} \quad (4.9)$$

where

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

The upper estimate of Lemma 4.2 can be deduced from the relations (4.8) and (4.9) in exactly the same way as the analogous estimate in [2, § 6].

Lemma 4.3 *Let Q be a set of square-free integers q with $N < q \le 2N$. Suppose that $z \gg X^\tau$ and $N \ll X^{2-\tau}$. Then*

$$\sum_{N\mathfrak{Q}\in Q, \mathfrak{Q}\in\mathcal{I}} S(\mathcal{A}_\mathfrak{Q}, z) \ll \sum_{q\in Q} \frac{\eta^2 X^2}{q \log \min(z, X^{2-\tau}/N)} + X^{2-\tau/5},$$

and

$$\sum_{N\mathfrak{Q}\in Q, \mathfrak{Q}\in\mathcal{I}} S(\mathcal{B}_\mathfrak{Q}, z) \ll \sum_{q\in Q} \frac{\eta X^3}{q \log \min(z, X^{2-\tau}/N)} + X^{3-\tau/5}.$$

This lemma can be proved in exactly the same way as the analogous Lemma 7.1 in [2] because no singular primes enter into discussion. Moreover, neither the formulation, nor the proof of the following analogue of [2, Lemma 3.6] need be changed.

Lemma 4.4 *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.

5 Some approximations

Let $\xi = \tau^5$, and let $J(l) = \{a : a \in \mathbb{R}, X^{l\xi} \le a < X^{(l+1)\xi}\}$; following the approximation procedure introduced in [2], we define two functions $d_n : \mathcal{I} \times \mathbb{Z}^{n+1} \to \mathbb{R}$, and $b_n : \mathcal{I} \times \mathbb{Z}^{n+1} \to \{0, 1\}$. Let

$$d_n(\mathfrak{A}, m) = \prod_{i=1}^{n+1} \frac{\log p_i}{m_i \xi \log X},$$

if

$$\mathfrak{A} = \prod_{i=1}^{n+1} \mathfrak{p}_i, N(\mathfrak{p}_i) = p_i, p_i \in P \cap J(m_i), m_i > 0, 1 \le i \le n+1, \qquad (5.1)$$

and let $d_n(\mathfrak{A}, m) = 0$, if conditions (5.1) do not hold; let

$$b_n(\mathfrak{A}, m) = \begin{cases} 1, & \text{if } \mathfrak{A} \in \mathcal{R},\ \mathfrak{p}|\mathfrak{A} \Rightarrow N(\mathfrak{p}) \geq X^{m_{n+1}\xi},\ \mathfrak{p} \in \mathcal{P}, \\ 0, & \text{otherwise.} \end{cases} \tag{5.2}$$

As in [2, § 3], let

$$\hat{U}^{(m,n)}(\mathcal{D}) = \sum_{\mathfrak{A}\mathfrak{B}\in\mathcal{D}} b_n(\mathfrak{A}, m) d_n(\mathfrak{B}, m); \tag{5.3}$$

further let

$$\hat{U}^{(n)}(\mathcal{D}) = \sum_{m\in\iota(n)} \hat{U}^{(m,n)}(\mathcal{D}) \tag{5.4}$$

for $n \geq 3$,

$$\hat{U}_1^{(n)}(\mathcal{D}) = \sum_{m\in\iota(n)} \hat{U}^{(m,n)}(\mathcal{D}) \tag{5.5}$$

for $n = 1, 2$, and

$$\hat{S}_4(\mathcal{D}) = \sum_{m\in\iota(0)} \hat{U}^{(m,0)}(\mathcal{D}), \tag{5.6}$$

where, as in § 4, $\mathcal{D}$ stands for either of the sequences $\mathcal{A}, \mathcal{B}$ and

$$\begin{aligned} \iota(n) = \{m : m \in \mathbb{Z}^{n+1} \quad &, \quad m_1 > \ldots > m_{n+1} \geq \tau\xi^{-1}, \\ \sum_{i=1}^{n+1} m_i \geq (1+\tau)\xi^{-1} \quad &, \quad \sum_{i=1}^{n+1}(m_i+1) \leq (\frac{3}{2}-\tau)\xi^{-1}, \\ \sum_{i=1}^{n}(m_i+1) \leq (1+\tau)\xi^{-1} \quad &, \quad m_1 + 1 \leq (1-\tau)\xi^{-1}\}, \end{aligned}$$

if $n > 0$;

$$\iota(0) = \{m : m \in \mathbb{Z},\ (1+\tau)\xi^{-1} \leq m \leq (\frac{3}{2}-\tau)\xi^{-1} - 1.$$

Finally, one defines a function $b^{(1)} : \mathcal{I}(k) \times \mathbb{Z}^2 \to \{0, 1\}$ by the equation

$$b^{(1)}(\mathfrak{A}, l) = \begin{cases} 1, & \text{if } \mathfrak{A} = \mathfrak{p}_1\mathfrak{p}_2,\ N(\mathfrak{p}_i) \in J(l_i),\ \mathfrak{p}_i \in \mathcal{P}, i = 1, 2, \\ 0, & \text{otherwise.} \end{cases}$$

Let

$$\hat{U}^{(\nu,n)}(\mathcal{D}) = \sum_{\mathfrak{A}\mathfrak{B}\in\mathcal{D}} b^{(1)}(\mathfrak{A}, l) d_n(\mathfrak{B}, m),\ \nu := (l, m), \tag{5.7}$$

and let

$$\hat{U}_2^{(1)}(\mathcal{D}) = \sum_{(l,m)\in\iota_1(n),\ 0\le n\le n_0} \hat{U}^{(\nu,n)}(\mathcal{D}),\ n_0 \ll \tau^{-1}, \tag{5.8}$$

where

$$\iota_1(n) = \{(l,m) : (l,m) \in \mathbb{Z}^2 \times \mathbb{Z}^{n+1} \quad , \quad m_1 > \ldots > m_{n+1} \ge l_2,$$
$$\tau \le l_2\xi < l_1\xi \le 1-\tau-\xi \quad , \quad (l_1+l_2)\xi \ge 3/2+\tau\}.$$

Lemma 5.1 *We have*

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

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

for $n = 1$ and 2,

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

and

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

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

Being analogous to Lemma 3.7 in [2], this lemma can be proved in exactly the same way. In particular, to deduce an analogue of the estimate (7.6) in [2] one may use the following estimate

$$\text{card}\ \{a_1 : a_1 \in \mathbb{Z}, X < a_1 \le X(1+\eta),\ \mathfrak{B}|(a_1\omega_1 + a_2\omega_2)\mathfrak{d}^{-1}\} \ll 1 + \frac{\eta X}{N(\mathfrak{B})}$$

valid under the assumption that h.c.f.$(\omega_1, \mathfrak{B}) = 1$.

Write now

$$d_n = e_n + g_n, \tag{5.9}$$

where e_n is given by

$$e_n(\mathfrak{A}, m) = \frac{w'(N\mathfrak{A})}{\prod_{i=1}^{n+1}(m_i\xi\log X)} \sum_{\mathfrak{B}|\mathfrak{A},\ N(\mathfrak{B})<L} \mu(\mathfrak{B}) \log\frac{L}{N(\mathfrak{B})}. \tag{5.10}$$

Here

$$L = X^{\tau/2} \tag{5.11}$$

and

$$w(t) = w(t, m) = \int_{G(m,t)} dx$$

with

$$G(m,t) = \{x : x \in \mathbb{R}^{n+1},\ x_i \in J(m_i),\ 1 \le i \le n+1, \prod_{i=1}^{n+1} x_i \le t\}.$$

Let

$$U_e(\mathcal{A}) = \sum_{\mathfrak{A}\mathfrak{B}\in\mathcal{A}} b_{\mathfrak{A}} e_n(\mathfrak{B}, m), \tag{5.12}$$

where $b_{\mathfrak{A}}$ denotes either $b^{(1)}(\mathfrak{A}, l)$, or $b_n(\mathfrak{A}, m)$; on substituting decomposition (5.9) in (5.3) and (5.7), one obtains

$$U(\mathcal{A}) = U_e(\mathcal{A}) + U_g(\mathcal{A}), \tag{5.13}$$

where U stands for any of the symbols $\hat{U}^{(m,n)},\ \hat{U}^{(\nu,n)}$; further, on substituting (5.13) in (5.4-6) and (5.8) we get the decomposition

$$V(\mathcal{A}) = V_e(\mathcal{A}) + V_g(\mathcal{A})$$

with $V \in \{\hat{U}^{(n)},\ \hat{U}_1^{(n)},\ \hat{S}_4,\ \hat{U}_2^{(1)}\}$.

We can now state our analogue of [2, Lemma 3.9].

Lemma 5.2 *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

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

Proof. It follows from (5.12) and (5.10) that

$$U_e(\mathcal{A}) = \frac{1}{M(\xi\log X)^{n+1}} \sum_{\substack{\mathfrak{A}\mathfrak{B}\in\mathcal{A} \\ \mathfrak{C}|\mathfrak{B}, N\mathfrak{C}<L}} b_{\mathfrak{A}} w'(N\mathfrak{B})\mu(\mathfrak{C}) \log\frac{L}{N\mathfrak{C}}\ .$$

Just as in [2, § 10], one can deduce from [2, relation (8.3)] and (3.8) in the case $n > 0$ and from (3.11) in conjunction with Lemma 3.2 when $n = 0$ that

$$U_e(\mathcal{A}) = \sum_{\mathfrak{A}\mathfrak{C}\in\mathcal{R}, N\mathfrak{C}<L} a(\mathfrak{A},\mathfrak{C})|\mathcal{A}_{\mathfrak{A}\mathfrak{C}}| + O(\frac{\eta^{5/2}X^2}{M}(\log X)^c),$$

where

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

It should be remarked that h.c.f.$(\mathfrak{A},\mathfrak{C}) = 1$, as soon as $\mathfrak{A}\mathfrak{C} \in \mathcal{R}, N\mathfrak{C} < L$ and $b_{\mathfrak{A}} \neq 0$. Since it may be assumed that $N(\mathfrak{A}\mathfrak{C}) \leq X^{2-\tau/2}$, it follows from (3.11), Lemma 3.2, and the relation (8.4) in [2] that

$$\begin{aligned} U_e(\mathcal{A}) &= \frac{\eta^2X^2}{\zeta(2)M(\xi\log X)^{n+1}}\sum_{\mathfrak{A}\in\mathcal{R}} b_{\mathfrak{A}}\frac{w'(h_fX^3/N\mathfrak{A})}{N\mathfrak{A}}\ \alpha_1(\mathfrak{A})\ \Sigma_6 \\ &+ O(\frac{\eta^{5/2}X^2}{M}(\log X)^b), \end{aligned}$$

where

$$\Sigma_6 = \sum_{\mathfrak{C}\in\mathcal{R}, N\mathfrak{C}<L}\frac{\mu(\mathfrak{C})}{N\mathfrak{C}}\ \alpha(\mathfrak{C}_0)\ \alpha_1(\mathfrak{C})\log\frac{L}{N\mathfrak{C}}\ .$$

It follows from Perron's formula that

$$\Sigma_6 = \frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty} l(s+1)\frac{L^s}{s^2}ds,$$

where

$$l(s) = \sum_{\mathfrak{C}\in\mathcal{R}}\frac{\mu(\mathfrak{C})\ \alpha(\mathfrak{C}_0)\ \alpha_1(\mathfrak{C})}{N\mathfrak{C}^s} = \prod_{p\in P} l_p(s).$$

As in [2], it follows from (3.15) and (3.17) that

$$\begin{aligned} \Sigma_6 &= \mathrm{Res}(l(s+1)L^s s^{-2})_{s=0} + O(\exp(-c(\log L)^{1/2})) \\ &= \phi(k)^{-1}\prod_{p\in P} l_p(1)\prod_{\mathfrak{p}|p,\mathfrak{p}\in\mathcal{P}}(1-\frac{1}{N(\mathfrak{p})})^{-1} + O(\exp(-c(\log L)^{1/2})) \\ &= \prod_{p\in P}(1-\frac{1}{p})^{-1}\sum_{\mathfrak{C}\in\mathcal{R},\mathfrak{C}|p}\frac{\mu(\mathfrak{C})\ \alpha(\mathfrak{C}_0)\ \alpha_1(\mathfrak{C})}{N\mathfrak{C}} + O(\exp(-c(\log L)^{1/2})) \\ &= \prod_{p\in P}(1-\frac{1}{p})^{-1}(1-\gamma(p)) + O(\exp(-c(\log L)^{1/2})) \\ &= \sigma(f)\zeta(2) + O(\exp(-c(\log L)^{1/2})), \end{aligned}$$

with $c > 0$, where $\mathrm{Res}(u(s))_{s=0}$ stands for the residue of $u(s)$ at $s = 0$. This gives

$$U_e(\mathcal{A}) = \sigma(f)\eta^2 X^2 \Sigma_7 \{1 + O(\exp\{-c(\log L)^{1/2}\})\} + O(M^{-1}\eta^{5/2} X^2 (\log X)^c),$$

where

$$\Sigma_7 = \sum_{\mathfrak{A}\in\mathcal{R}} b_{\mathfrak{A}} \frac{w'(h_f X^3/N(\mathfrak{A}))}{M(\xi \log X)^{n+1}} N(\mathfrak{A})^{-1} \alpha_1(\mathfrak{A}),$$

and, moreover,

$$\alpha_1(\mathfrak{A}) = \prod_{\mathfrak{p}\in\mathcal{P},\mathfrak{p}|\mathfrak{A}} (1 + N(\mathfrak{p})^{-1})^{-1}$$

as soon as $b_{\mathfrak{A}} \neq 0$. As in [2, § 10], it follows now that

$$U_e(\mathcal{A}) = \sigma(f)\eta^2 X^2 \Sigma_8 + O(M^{-1}\eta^{5/2} X^2 (\log X)^c), \tag{5.14}$$

where

$$\Sigma_8 = \sum_{\mathfrak{A}\in\mathcal{R}} b_{\mathfrak{A}} \frac{w'(h_f X^3/N(\mathfrak{A}))}{M(\xi \log X)^{n+1}} N(\mathfrak{A})^{-1}.$$

The analysis of $U(\mathcal{B})$ goes through along the lines of [2, § 10] and gives

$$U(\mathcal{B}) = h_f \eta X^3 \Sigma_8 + O(\frac{\eta^2 X^3}{M}). \tag{5.15}$$

A comparison of (5.14) and (5.15) then establishes the first part of Lemma 5.2. The second part of the lemma can be proved in the same way as at the end of [2, § 10].

The following proposition is an immediate consequence of Lemmata 4.1, 4.2, 4.4, 5.1, and 5.2.

Proposition 5.1 *We have*

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

6 The type II estimates

To complete the proof of Theorem 2.1 we have to estimate the sums $U_g(\mathcal{A})$, and $V_g(\mathcal{A})$. We shall establish the analogues of [2, Lemma 3.8] and [2, Lemma 3.10], following the plan of the proof of these results in [2]. These considerations require techniques from E. Hecke's multidimensional arithmetic, [3],

[4], [6]. Since, as it was once remarked, [7, p.v], 'to improve upon Hecke, in a treatment along classical lines of the theory of algebraic numbers, would be a futile and impossible task', we shall describe the properties of the ideal numbers following [3] rather closely.

Let K be a number field of degree $n = r_1 + 2r_2$ over $\mathbb{Q}$, as at the beginning of § 2. The class group of K being finite, one can choose ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ so that every (non-zero) fractional ideal $\mathfrak{A}$ has a unique decomposition

$$\mathfrak{A} = (\alpha)\mathfrak{a}_1{}^{l_1} \ldots \mathfrak{a}_t^{l_t},\ \alpha \in K^*,\ l \in \mathbb{Z}^t,\ 0 \leq l_j < h_j;$$

let

$$\mathfrak{a}_j^{h_j} = (\alpha_j),\ 1 \leq j \leq t,\ h(K) = \prod_{j=1}^{t} h_j.$$

Let $L = K(\beta_1, \ldots, \beta_t)$, where β_j satisfies the equation $\beta_j^{h_j} = \alpha_j$, and suppose the complex numbers $\beta_j^{(i)},\ 1 \leq j \leq t$, are chosen to satisfy the equations

$$(\beta_j^{(i)})^{h_j} = \alpha_j^{(i)},\ 1 \leq i \leq n,$$

and

$$\beta_j^{(i+r_2)} = \overline{\beta_j^{(i)}}, r_1 < i \leq r_1 + r_2.$$

Let $\mathfrak{I}(K) = \{0\} \cup \mathfrak{I}(K)^*$, where $\mathfrak{I}(K)^*$ stands for the subgroup of L^* generated by K^* and $\{\beta_j : 1 \leq j \leq t\}$; by definition, $\mathfrak{I}(K)$ is the domain of ideal numbers of K. The factor-group $\mathfrak{I}(K)^*/\mathfrak{o}(K)^*$ is clearly isomorphic to the group of fractional ideals of K. For $\beta \in \mathfrak{I}(K)$, let (β) denote the corresponding ideal in K; let $N\beta := \prod_{i=1}^{n} \beta^{(i)}$, then $|N\beta| = N(\beta)$. Moreover,

$$(\beta) \in \mathcal{I}(K) \Leftrightarrow \beta \in \mathfrak{o}(L).$$

Two ideal numbers α, β are said to lie in the same class if the corresponding ideals $(\alpha), (\beta)$ belong to the same class of ideals; thus the domain of ideal numbers $\mathfrak{I}(K)$ splits into $h(K)$ classes. A class of ideal numbers, say A, has an integral basis $\{w_1, \ldots, w_n\}$, so that

$$A = \{a_1 w_1 + \ldots + a_n w_n : a \in \mathbb{Q}^n\},$$

and

$$A \cap \mathfrak{o}(L) = \{a_1 w_1 + \ldots + a_n w_n : a \in \mathbb{Z}^n\};$$

moreover, the discriminant of an integral basis of A is equal to $D(K)$, the discriminant of K. For any α in A, one may note that $\{w_i : 1 \leq i \leq n\}$ is a $\mathbb{Q}$-basis of A if and only if $\{\alpha^{-1} w_i : 1 \leq i \leq n\}$ is a basis of $K|\mathbb{Q}$. This

simple observation is implicit in our considerations; it shows, in particular, that there is a unique basis $\{\tilde{w}_i : 1 \le i \le n\}$ of A^{-1} defined by the condition $\mathrm{Tr}(w_i\tilde{w}_j) = \delta_{ij}$, where

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{otherwise;} \end{cases}$$

these two bases are said to be dual to each other. In what follows, cl $\mathfrak{a}$ and cl α stand for the class of ideals containing $\mathfrak{a}$ and for the class of ideal numbers containing α, respectively. The following analogue of [2, Lemma 4.6] can be proved along the same lines as that lemma.

Lemma 6.1 *Let $x \ge y \ge 2$ be given, and let α, β be two integral ideal numbers of K with cl α = cl β. Suppose that h.c.f.$(\alpha, \beta) \ll 1$, and there is an integer r such that*

$$|\alpha^{(j)}|,\ |\beta^{(j)}| \le x^r,\ 1 \le j \le n.$$

Then given any positive integer l, there is a positive constant $c(l, r)$ such that

$$\sum_{\substack{|m|\le x,\ |n|\le y \\ n\ne 0}} \tau(m\alpha + n\beta)^l \ll xy(\log x)^{c(l,r)}.$$

Let now $K = k$; let, for brevity, $\mathfrak{I} := \mathfrak{I}(k)$, and $g_{\mathfrak{A}} := g_n(\mathfrak{A}, m)$. Let $\mathfrak{d} = (\delta),\ \delta \in \mathfrak{I}$; choose an integral basis $\{w_1,\ w_2,\ w_3\}$ of cl δ^{-1} and a basis $\{\omega_1,\ \omega_2\}$ of the $\mathbb{Z}-$module F (cf. § 2) in such a way that $\omega_1\delta^{-1} = w_1,\ \omega_2\delta^{-1} = bw_2$ with $b \in \mathbb{Z}$. Let us fix an integral basis in each class A of ideal numbers of k subject, when $A =$ cl δ^{-1}, to the above condition. Given $\beta \in \mathfrak{I}$, let $b_i = \mathrm{Tr}(\beta v_i\tilde{w}_3)$, where $\{v_1,\ v_2,\ v_3\}$ is the fixed integral basis of cl $(\beta\delta)^{-1}$, so that $\beta v_i = a_{i1}w_1 + a_{i2}w_2 + b_iw_3$; write $\hat{\beta} = (b_1,\ b_2,\ b_3)$. The restriction h_A of the map $h : \beta \mapsto \hat{\beta}$ to a class A of ideal numbers is easily seen to be an invertible $\mathbb{Q}-$linear transformation $h_A : A \to \mathbb{Q}^3$; moreover,

$$\{h_A(\beta) : \beta \in A,\ (\beta) \in \mathcal{I}(k)\}$$

is a sublattice of $\mathbb{Z}^3$ of finite index (equal to det h_A). We extend this map to an $\mathbb{R}-$linear transformation $h_A : A_{\mathbb{R}} \to \mathbb{R}^3$, where $A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R}$, by letting

$$h_A(\sum_{i=1}^{3} a_i\bar{w}_i) = \sum_{i=1}^{3} a_i h_A(\bar{w}_i),\ a \in \mathbb{R}^3,$$

where $\{\bar{w}_1, \bar{w}_2, \bar{w}_3\}$ is the fixed integral basis of A. Write

$$\hat{\beta} := h_A(\beta),\ \beta^{(j)} := \sum_{i=1}^{3} a_i\bar{w}_i^{(j)},\ N\beta = \prod_{j=1}^{3} \beta^{(j)},\ \mathrm{Tr}\ \beta = \sum_{j=1}^{3} \beta^{(j)}$$

for $\beta \in A_{\mathbb{R}},\ \beta = \sum_{i=1}^{3} a_i \bar{w}_i$; we write further $\check{x} := h_A^{-1}(x)$ for $x \in \mathbb{R}^3$ and let

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

The following proposition is our analogue of (the conjunction of) [2, Lemma 3.8] and [2, Lemma 3.10].

Proposition 6.1 *Let $\mathcal{C} \subseteq \mathbb{R}^3$ be a cube of side $S_0 \geq L^2$, and suppose that $a_i \ll V^{1/3}, 1 \leq i \leq 3$, and $N\check{a} \gg V$ for $a \in \mathcal{C}$.*

(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

$$\sum_{\substack{\beta = \alpha \bmod q \\ \hat{\beta} \in \mathcal{C},\ \beta \in A^{(0)}}} g_{(\beta)} \ll V \exp(-c\sqrt{\log L}),\ c > 0, \tag{6.1}$$

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

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

for $X^{1+\tau} \ll V \ll X^{3/2-\tau}$, with a suitable positive constant c depending at most on f; here notation $b_{\mathfrak{a}}$ has the same meaning as in equation (5.12).

In this section we shall prove (ii). Choose V as in (ii), and let $\Psi : \mathbb{R}^2 \to \{0, 1\}$ be the characteristic function of the square $I(X)$; let

$$\Sigma_9(V) := \sum_{\substack{\mathfrak{ab} \in \mathcal{A} \\ V < N\mathfrak{b} \leq 2V}} b_{\mathfrak{a}} g_{\mathfrak{b}}.$$

We have

$$\Sigma_9(V) = \sum_{\substack{\mathfrak{ab}=\mathfrak{A}_a, V<N\mathfrak{b}\leq 2V \\ a\in\mathbb{Z}^2,\,(a_1,a_2)=1}} b_{\mathfrak{a}} g_{\mathfrak{b}} \Psi(a).$$

The argument at the beginning of § 11 in [2] shows that

$$\Sigma_9(V) = \sum_{\substack{\mathfrak{ab}=\mathfrak{A}_a, V<N\mathfrak{b}\leq 2V \\ a\in\mathbb{Z}^2,\,\{\mathfrak{a},\mathfrak{b}\}\subset\mathcal{Q}}} b_{\mathfrak{a}} g_{\mathfrak{b}} \Psi(a) + O(X^{2-\tau/2}(\log X)^c), \tag{6.2}$$

where $\mathcal{Q}$ stands for the set of those integral ideals in $\mathfrak{o}$ which are not divisible by a rational prime. An integral ideal number β is said to be primitive if $(\beta) \in \mathcal{Q}$. Clearly, if $\hat{\beta}$ is a primitive vector then β is primitive. Without loss of generality, we may assume in what follows that $k \subset \mathbb{R}$. If $r = 1$, let $\mathcal{Q}_0$ denote the set of primitive ideal numbers β satisfying the conditions:

$$\beta = (N\beta)^{1/3}\varepsilon_0^z,\ -1/2 < z \leq 1/2,\ \beta > 0,$$

where ε_0 is the fundamental unit of k with $\varepsilon_0 > 1$. If k is a totally real cubic field, i.e. if $r = 2$, we choose two multiplicatively independent fundamental units $\varepsilon_1, \varepsilon_2$ of k with $N\varepsilon_1 = N\varepsilon_2 = 1$, and let $\mathcal{Q}_0$ be the set of primitive ideal numbers β defined by the conditions:

$$|\beta^{(j)}| = (N\beta)^{1/3}\ |\varepsilon_1^{(j)}|^{z_1}|\varepsilon_2^{(j)}|^{z_2},\ -1/2 < z_1, z_2 \leq 1/2,\ 1 \leq j \leq 3,\ N\beta > 0,$$

where $\beta^{(1)} = \beta$. Let

$$G(\beta) = \begin{cases} g_{(\beta)}, & \text{if } \beta \in \mathcal{Q}_0 \\ 0, & \text{otherwise.} \end{cases}$$

Equation (6.2) can now be rewritten as follows:

$$\Sigma_9(V) = \sum_{\substack{\varphi(a)=\delta\alpha\beta,\,(\alpha)\in\mathcal{Q} \\ a\in\mathbb{Z}^2,\,V<N\beta\leq 2V}} b_{(\alpha)} G(\beta)\Psi(a) + O(X^{2-\tau/2}(\log X)^c),$$

where $\varphi(a) := a_1\omega_1 + a_2\omega_2$. As in [2], an application of Cauchy's inequality yields

$$\Sigma_9(V) \ll X^{2-\tau/2}(\log X)^c + (X^3/V)^{1/2}\Sigma_{10}^{1/2},$$

where

$$\Sigma_{10} = \sum_{(\alpha)\in\mathcal{Q}} \Big| \sum_{\substack{\varphi(a)=\delta\alpha\beta \\ a\in\mathbb{Z}^2,\, V<N\beta\le 2V}} G(\beta)\Psi(a)\Big|^2$$

$$= \sum_{\substack{a_i\in\mathbb{Z}^2,\, i=1,2 \\ V<N\beta_1, N\beta_2\le 2V}} G(\beta_1)G(\beta_2)\Psi(a_1)\Psi(a_2)\psi(a_1,a_2;\beta_1,\beta_2),$$

with

$$\psi(a_1,a_2;\beta_1,\beta_2) = \text{card}\,\{\alpha : (\alpha)\in\mathcal{Q},\ \varphi(a_i)=\delta\alpha\beta_i,\ i=1,2\},$$

so that ψ takes values in $\{0,1\}$. Further, as in [2], one may remove the diagonal terms in Σ_{10} and write

$$\Sigma_{10} = \Sigma_{11} + O(X^2(\log X)^c),$$

where

$$\Sigma_{11} = \sum_{\substack{\beta_1\ne\beta_2,\, a_i\in\mathbb{Z}^2, \\ V<N\beta_i\le 2V,\, i=1,2}} G(\beta_1)G(\beta_2)\Psi(a_1)\Psi(a_2)\psi(a_1,a_2;\beta_1,\beta_2).$$

For $b\in\mathbb{Z}^3$, let $d(b) := h.c.f.(b_1,b_2,b_3)$ and let $[b] = d(b)^{-1}b$. Suppose $\psi(a_1,a_2;\beta_1,\beta_2)=1$, then

$$\delta\alpha\beta_i = a_{i1}\omega_1 + a_{i2}\omega_2 = \delta(a_{i1}w_1 + a_{i2}(bw_2)),$$

or

$$\alpha\beta_i = a_{i1}w_1 + a_{i2}(bw_2),\ i=1,2.$$

Therefore

$$\sum_{j=1}^{3}\alpha_j b_j^{(i)} = 0,$$

where $\{v_1,v_2,v_3\}$ is the fixed integral basis of $\text{cl}(\beta_i\delta)^{-1}$, and

$$b_j^{(i)} := \text{Tr}(v_j\beta_i\tilde{w}_3),\ \alpha=\alpha_1v_1+\alpha_2v_2+\alpha_3v_3,\ i=1,2.$$

Thus $\vec{\alpha} = c[\hat{\beta}_1\wedge\hat{\beta}_2]$ with some integer c, where

$$\hat{\beta}_i = (b_1^{(i)}, b_2^{(i)}, b_3^{(i)}),\ \vec{\alpha} = (\alpha_1,\ \alpha_2,\ \alpha_3).$$

Since $(\alpha) \in \mathcal{Q}$, the vector $\vec{\alpha}$ is primitive and, consequently, $c = \pm 1$. Thus (cf. [2, § 11])

$$\text{cl } \beta_1 = \text{cl } \beta_2,\ \alpha \in \text{cl}(\delta\beta_1)^{-1},\ \vec{\alpha} = \pm[\hat{\beta}_1 \wedge \hat{\beta}_2]. \tag{6.3}$$

Let

$$h_{i1}(\beta_1, \beta_2) = \text{Tr}(\beta_i\beta_{12}\tilde{w}_1),\ h_{i2}(\beta_1, \beta_2) = b^{-1}\text{Tr}(\beta_i\beta_{12}\tilde{w}_2), \tag{6.4}$$

where $\beta_{12} = \sum_{j=1}^{3}(\hat{\beta}_1 \wedge \hat{\beta}_2)_j v_j$; then $a_i = \pm\, d^{-1}h_i(\beta_1, \beta_2)$ with $h_i := (h_{i1}, h_{i2})$, $d := d(\hat{\beta}_1 \wedge \hat{\beta}_2),\ i = 1, 2$. since α is primitive if and only if $\vec{\alpha}$ is primitive, we produce exactly the required set of ideal numbers α in this way.

The argument leading to the proof of Lemma 11.2 in [2] results in the following analogous statement.

Lemma 6.2 *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*

$$\Sigma_9(V) \ll X^2Y^{-1/2}(\log X)^c + X^{3/2}V^{-1/2}\Sigma_{12}^{1/2},$$

with

$$\Sigma_{12} = \sum_{\beta_1,\beta_2,a_1,a_2} G(\beta_1)G(\beta_2)\Psi(a_1)\Psi(a_2)\psi(a_1, a_2; \beta_1, \beta_2),$$

subject to the conditions

$$a_i \in \mathbb{Z}^2,\ \beta_i \in B^{(0)},\ V < N\beta_i \le 2V,\ i = 1, 2,\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) > VX^{-1}Y^{-1}.$$

The argument at the beginning of [2, § 12] shows that

$$\Sigma_{12} = 2\sum_{\beta_1,\beta_2} G(\beta_1)G(\beta_2)\Psi(d^{-1}h_1(\beta_1, \beta_2))\Psi(d^{-1}h_2(\beta_1, \beta_2)) \tag{6.5}$$

subject to the conditions

$$\beta_i \in B^{(0)},\ V < N\beta_i \le 2V,\ i = 1, 2,\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) > VX^{-1}Y^{-1}.$$

For $y > 0$, let

$$\begin{aligned} U(y) &= \{(\hat{\beta}_1, \hat{\beta}_2) : \beta_i \in B^{(0)},\ V < N\beta_i \le 2V, \\ yX &< h_{ij}(\beta_1, \beta_2) \le yX(1 + \eta),\ i, j = 1, 2\}. \end{aligned}$$

With this notation, equation (6.5) may be rewritten as follows:

$$\Sigma_{12} = 2 \sum_{\substack{(\hat{\beta}_1,\hat{\beta}_2)\in U(d) \\ d>VX^{-1}Y^{-1}}} G(\beta_1)G(\beta_2),\ d := d(\hat{\beta}_1 \wedge \hat{\beta}_2).$$

Subdividing the range of summation over d into subintervals

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

one obtains

$$\Sigma_{12} \ll (\log X)\ T\ \Sigma_{13}(m,\Delta) \tag{6.6}$$

for at least one pair (m,Δ), where

$$\Sigma_{13}(m,\Delta) = \sum_{d_1 \in I_m} | \sum_{\substack{(\hat{\beta_1},\hat{\beta_2}) \in\ U(d_1) \\ d(\hat{\beta_1} \wedge \hat{\beta_2}) = d_1}} G(\beta_1)G(\beta_2)|. \tag{6.7}$$

The argument proceeds, as in [2, § 12]. One must prove, for example, that the cubic polynomials $h_{ij},\ i,j = 1,2$, are non-singular in the relevant region. As in [2, § 12], we do it for the polynomial h_{11}, the rest being analogous.

Let $\mathcal{E}$ stand for the set of the three distinct embeddings $\sigma : k \hookrightarrow \mathbb{C}$, and let $\beta_{i\sigma} := \sigma(\beta_i),\ i = 1,2,\ \sigma \in \mathcal{E}$; write, for brevity, $s_j := b_j^{(1)},\ t_j := b_j^{(2)}$, so that

$$s_j = \mathrm{Tr}(\beta_1 v_j \tilde{w}_3),\ t_j = \mathrm{Tr}(\beta_2 v_j \tilde{w}_3),\ 1 \leq j \leq 3, \hat{\beta_1} = (s_1,s_2,s_3),\ \hat{\beta_2} = (t_1,t_2,t_3).$$

It follows from (6.4) that

$$h_{11}(\beta_1,\beta_2) = \mathrm{Tr}(\beta_1 \tilde{w}_1(v_1(s_2t_3 - s_3t_2) + v_2(s_3t_1 - s_1t_3) + v_3(s_1t_2 - s_2t_1))).$$

Let $\rho \in \mathcal{E}$; we have

$$\begin{aligned}(\rho\tilde{w}_3)^{-1}\frac{\partial h_{11}}{\partial \beta_{2\rho}} &= (s_2\rho v_3 - s_3\rho v_2)\mathrm{Tr}(\beta_1\tilde{w}_1v_1) \\ &+ (s_3\rho v_1 - s_1\rho v_3)\mathrm{Tr}(\beta_1\tilde{w}_1v_2) + (s_1\rho v_2 - s_2\rho v_1)\mathrm{Tr}(\beta_1\tilde{w}_1v_3).\end{aligned}$$

On writing

$$\mathrm{Tr}(\beta_1\tilde{w}_jv_i) = \sum_{\sigma\in\mathcal{E}} \beta_{1\sigma}\sigma(\tilde{w}_jv_i),\ 1 \leq i \leq 3,\ j = 1,3,$$

substituting this identity in the previous equation, and rearranging the terms in the resulting sum, one obtains

$$(\rho\tilde{w}_3)^{-1}\frac{\partial h_{11}}{\partial \beta_{2\rho}} = \beta_{1\sigma}\beta_{1\tau}(\sigma\tilde{w}_3\tau\tilde{w}_1 - \sigma\tilde{w}_1\tau\tilde{w}_3)D(v),$$

where $\mathcal{E} = \{\rho, \sigma, \tau\}$, and where $D(v) := \det(\tau(v),\ \sigma(v),\ \rho(v))$. Therefore

$$\sum_{\rho \in \mathcal{E}} (\rho \tilde{w}_3)^{-1} (\rho \tilde{w}_2) \beta_{1\rho} \frac{\partial h_{11}}{\partial \beta_{2\rho}} = -(N\beta_1) D(v) D(\tilde{w}) = \pm N\beta_1$$

since the discriminant of a class of ideal numbers is equal to the field discriminant, and we may conclude, as in [2, § 12], that

$$|\nabla h_{11}(n)| \gg T^2, n := (n_1, \dots, n_6), \tag{6.8}$$

for $(\hat{\beta}_1, \hat{\beta}_2) \in U(d),\ d \in I_m$, where

$$s_i = V^{1/3}\ \frac{n_i}{T},\ t_i = V^{1/3}\ \frac{n_{i+3}}{T},\ 1 \le i \le 3,$$

assuming $n_j \ll T,\ 1 \le j \le 6$. For $r = 1$ we may handle the cubic polynomials $\beta_i^3 - (N\beta_i)\varepsilon^{\pm 3/2}$ in the same way. Thus, for $r = 1$ we may follow [2]. We cover the region of summation in (6.7) by means of cubes

$$\begin{aligned} \mathcal{C}(n) &= \{(\hat{\beta}_1, \hat{\beta}_2) :\ V^{1/3}\ \frac{n_i - 1}{T} < s_i \le V^{1/3}\ \frac{n_i}{T}, \\ V^{1/3}\ \frac{n_{i+3} - 1}{T} &< t_i \le V^{1/3}\ \frac{n_{i+3}}{T},\ 1 \le i \le 3\}, \end{aligned}$$

and say that a cube $\mathcal{C}(n)$ is of class I if it lies completely inside $U(d)$ for each $d \in I_m$, and of class II if there is at least one $d \in I_m$ for which $U(d) \cap \mathcal{C}(n) \neq \emptyset$ but $\mathcal{C}(n)$ does not lie inside $U(d)$. Making use of the estimate (6.8) and its analogues, one deduces from Lemma 4.9 in [2] that there are $O(T^5)$ class II cubes if $r = 1$.

If $r = 2$, one has to consider a condition of the form

$$|\beta_1^j| = (N\beta_1)^{1/3} |\varepsilon_1^j|^{1/2} |\varepsilon_2^j|^{z_2},\ \ (j = 1, 2 \text{ and } 3).$$

This can be expressed as an equation of the form

$$A \log |\beta_{1\rho}| + B \log |\beta_{1\tau}| + C \log |\beta_{1\sigma}| = 0,$$

where A, B, C are non-zero constants (involving $\log |\varepsilon_i|$ etc.). Such an equation can be handled directly, without appealing to Lemma 4.9 in [2].

It then follows from Lemma 6.2 that there is a class I cube $\mathcal{C}$ such that

$$\Sigma_9(V) \ll X^2 Y^{-1/2} (\log X)^c + X^{3/2} V^{-1/2} Y^7 \Sigma_{14}^{1/2} (\log X)^c, \tag{6.9}$$

where

$$\Sigma_{14} = \sum_{d_1 \in I_m} \Big| \sum_{\substack{(\hat{\beta}_1, \hat{\beta}_2) \in \mathcal{C} \\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) = d_1}} G(\beta_1) G(\beta_2) \Big|,$$

cf. relation (12.8) in [2]. Further,

$$\Sigma_{14} = \sum_{d_1 \in I_m} |\sum_{d=1}^{\infty} \mu(d) \sum_{\substack{(\hat{\beta}_1, \hat{\beta}_2) \in \mathcal{C} \\ d_1 d | \hat{\beta}_1 \wedge \hat{\beta}_2}} G(\beta_1) G(\beta_2)|,$$

and it follows that

$$\Sigma_{14} \leq \sum_{\substack{1 \leq H < \infty \\ v \in \hat{\mathbb{Z}^3}}} \Sigma_{15}(H, v),$$

where H runs through the powers of 2, and $\hat{\mathbb{Z}^3}$ stands for the set of primitive vectors in $\mathbb{Z}^3$; here

$$\Sigma_{15}(H, v) := \sum_{d_1 \in I_m} | \sum_{\substack{d_1 d | r,\ rv \in \mathcal{C} \\ H < d_1 d \leq 2H}} \mu(d) \sum_{\hat{\beta}_1 \wedge \hat{\beta}_2 = rv} G(\beta_1) G(\beta_2)|.$$

Moreover, the argument in [2,§12] shows that

$$\Sigma_{15}(H, v) \ll (\log X)^2 \sum_{\substack{\hat{\beta}_i \in \Lambda,\ \beta_i \in \mathcal{Q} \\ i=1,2,\ \gamma \in \Gamma}} \tau(\gamma)^6, \tag{6.10}$$

where Λ is a lattice generated by z_1, z_2 such that

$$\{z_1, z_2\} \subset \mathbb{Z}^3,\ z_1 \wedge z_2 = v,\ |z_1| \leq |z_2| \ll V^{1/3},$$

and

$$\Gamma = \{\beta_1, \beta_2, b_1 c_2 - b_2 c_1\},\ \hat{\beta}_i = b_i z_1 + c_i z_2,\ i = 1, 2,$$

so that $r = \pm(b_1 c_2 - b_2 c_1)$. To estimate the sum in the right hand side of (6.10), we may apply Lemma 6.1; the argument used at the end of [2, § 12] leads then to the following analogue of Lemma 12.2 in [2]:

$$\Sigma_9(V) \ll X^2 Y^{-1/2} (\log X)^c + X^{3/2} V^{-1/2} Y^7 \Sigma_{16}^{1/2} (\log X)^c, \tag{6.11}$$

where

$$\Sigma_{16} = \sum_{\substack{d_1 \in I_m \\ d_1 d < d_0}} | \sum_{\substack{(\hat{\beta}_1, \hat{\beta}_2) \in \mathcal{C} \\ d_1 d | \hat{\beta}_1 \wedge \hat{\beta}_2}} G(\beta_1) G(\beta_2)| \tag{6.12}$$

with $d_0 := X^{-1}VY^{15} + V^{1/6}$. Further, the sum Σ_{16} can be estimated as in [2, § 13]. Given a cube $\mathcal{D}$ in $\mathbb{R}^3$ and a point a in $\mathbb{Z}^3$, let

$$\sigma(a; G, \mathcal{D}) = \sum_{\hat{\beta} \in \mathcal{D} \cap \mathbb{Z}^3} \exp(2\pi i a\hat{\beta}) G(\beta).$$

One first obtains an analogue of the estimate (13.2) in [2]:

$$\Sigma_{16} \ll XY \frac{\log V}{V} \sum_{q \le d_0} \frac{\tau(q)}{q} \sum_{b \in \mathcal{J}(q),\, i=1,2} |\sigma(q^{-1}b; G, \mathcal{C}_i)|^2, \tag{6.13}$$

where $\mathcal{J}(q) = \{b : b \in \mathbb{Z}^3,\ b \bmod q,\ h.c.f.(b_1, b_2, b_3, q) = 1\}$, and the cube $\mathcal{C}$ in (6.12) is regarded as a product $\mathcal{C}_1 \times \mathcal{C}_2$ of the two 3-dimensional cubes, in a natural way. An application of the large sieve argument in the form of Lemma 13.1 in [2] allows then to deduce from (6.13) that, cf. estimate (13.4) in [2],

$$\Sigma_{16} \ll \Sigma_{17} + XV(YQ_0^{-1/2} + Y^{46}X^{-\tau/2})(\log X)^c.$$

where

$$\Sigma_{17} = XY \frac{\log V}{V} \sum_{q \le Q_0} \frac{\tau(q)}{q} \sum_{b \in \mathcal{J}(q),\, i=1,2} |\sigma(q^{-1}b; G, \mathcal{C}_i)|^2.$$

Clearly,

$$\sigma(q^{-1}b; G, \mathcal{C}) = \sum_{\substack{c \bmod q \\ c \in \mathbb{Z}^3}} \exp(\frac{2\pi i bc}{q}) \sum_{\substack{\hat{\beta} \in \mathcal{C} \\ \hat{\beta} = c \bmod q}} G(\beta).$$

Moreover, on recalling that

$$B^{(0)} = \{\beta \in B : (\beta) \in \mathcal{I}(k)\},$$

we see that

$$\sum_{\substack{\hat{\beta} \in \mathcal{C} \\ \hat{\beta} = c \bmod q}} G(\beta) = \sum_{\substack{\hat{\beta} \in \mathcal{C},\, \beta \in B^{(0)} \\ \hat{\beta} = c \bmod q}} g_{(\beta)} \sum_{d | \beta} \mu(d),$$

so that

$$\sigma(q^{-1}b; G, \mathcal{C}) \ll \sum_{\substack{c \bmod q \\ c \in \mathbb{Z}^3, d \ge 1}} \Big| \sum_{\substack{\hat{\beta} \in \mathcal{C},\, \beta \in B^{(0)} \\ d | \beta,\, \hat{\beta} = c \bmod q}} g_{(\beta)} \Big|. \tag{6.14}$$

Since $\beta \mapsto \hat{\beta}$ is an invertible transformation, whose matrix depends at most on f and B, the conditions $d|\beta$ and $\hat{\beta} = c \bmod q$ are equivalent to a set of congruence conditions on $\hat{\beta}$ modulo $[q, d]$, cf. [2, § 13]; consequently, the inner sum in (6.14) can be bounded above with the help of (6.1). To conclude the proof of (ii) in Proposition 6.1 as in [2, § 13] we need the following analogue of Lemma 4.5 in [2].

Lemma 6.3 *Let $\mathcal{C} = (a_1, a_1 + s_0] \times (a_2, a_2 + s_0] \times (a_3, a_3 + s_0]$ be a cube of side s_0, and suppose that $\max |a_i| \le s_0^l$ for some positive constant l. Then there is a constant $c(l)$ such that*

$$\sum_{\hat{\beta} \in \mathcal{C}, \beta \in A^{(0)}} \tau(\beta)^2 \ll s_0^3 (\log s_0)^{c(l)}.$$

The proof of this lemma coincides with the proof of Lemma 4.5 in [2, § 4].

7 Completion of the proof of Proposition 6.1 and Theorem 2.1

Part (i) of Proposition 6.1, to be proved in this section, is our analogue of Lemma 3.8 in [2]. As in [2], we begin by considering the function $e_n(\mathfrak{A}, m)$.

Lemma 7.1 *In notation of Proposition 6.1, let*

$$I = \frac{1}{|\det\ h_A|} \int_{\mathcal{C}} w'(N\check{x})\, dx,$$

and suppose $\alpha \in A^{(0)}$; let $\varepsilon(\alpha, q) = 1$ if α and q are coprime, and $\varepsilon(\alpha, q) = 0$ otherwise. The following asymptotic formula

$$\sum_{\substack{\beta = \alpha \bmod q \\ \hat{\beta} \in \mathcal{C},\ \beta \in A^{(0)}}} e_n((\beta), m) \;=\; \phi(k)^{-1} M^{-1} (\xi \log X)^{-n-1} I \frac{\varepsilon(\alpha, q)}{\varphi_k(q)}$$

$$+ O(S_0^3 M^{-1} \tau(q)^c \exp(-c\sqrt{\log L})),$$

holds uniformly for $1 \le q \le L^{1/6}$. Here $M = \prod_{i=1}^{n+1} m_i$ as in Lemma 5.2, φ_k stands for the Euler function over the field k, and c is a positive constant depending at most on f.

This lemma can be proved along the lines of the proof of Lemma 8.1 in [2].

Turning to the analysis of $d_n(\mathfrak{A}, m)$, let us note that for any $q \leq L^{1/6}$ we have

$$\sum_{\substack{\beta = \alpha \bmod q \\ \hat{\beta} \in \mathcal{C},\, \beta \in (\mathrm{cl}\ \alpha)^{(0)}}} d_n((\beta), m) = 0$$

whenever α and q have a common factor, since in this case (β) will be a product of prime ideals $\mathfrak{p}$ with $N(\mathfrak{p}) \geq X^{\tau} \geq L > N(q)$. Thus we can assume that $h.c.f.(\alpha, q) = 1$. It suffices therefore to prove the following analogue of Lemma 9.2 in [2].

Proposition 7.1 *Let $l > 0,\ \alpha \in A,\ q \in \mathbb{Z}$, and suppose that $h.c.f.(\alpha, q) = 1$. The following asymptotic formula*

$$\begin{aligned} \sum_{\substack{\beta = \alpha \bmod q \\ \hat{\beta} \in \mathcal{C},\, \beta \in A^{(0)}}} d_n((\beta), m) &= \phi(k)^{-1} M^{-1} \varphi_k(q)^{-1} (\xi \log X)^{-n-1} I \\ &+ O(V\ \exp(-c\sqrt{\log L})), \end{aligned}$$

holds uniformly for $1 \leq q \leq (\log X)^l$, where c is a positive constant depending at most on f.

Proof. Let

$$\mathfrak{I}(q) = \{\alpha : \alpha \in \mathfrak{I},\ h.c.f.(\alpha, q) = 1\},$$

let $\mathfrak{I}_1(q) = \mathfrak{I}(q) \cap k$, and let

$$\mathfrak{I}_0(q) = \{\alpha : \alpha \in k,\ \alpha = 1 \bmod q\},$$

where $h.c.f.(\alpha, q) = 1$ means that $(\alpha) = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n(\mathfrak{p})}$ with $n(\mathfrak{p}) \in \mathbb{Z},\ n(\mathfrak{p}) = 0$ for $\mathfrak{p} | q$. Let H denote the set of characters of the factor-group $\mathfrak{I}_1(q)/\mathfrak{I}_0(q)$; write $d_{\mathfrak{A}} := d_n(\mathfrak{A}, m)$ for $\mathfrak{A} \in \mathcal{I}(k)$. It follows that

$$\sum_{\substack{\beta = \alpha \bmod q \\ \hat{\beta} \in \mathcal{C},\, \beta \in A^{(0)}}} d_n((\beta), m) = \varphi_k(q)^{-1} \sum_{\chi \in H} \bar{\chi}(\alpha) \sum_{\hat{\beta} \in \mathcal{C},\, \beta \in A^{(0)}} d_{(\beta)} \chi(\beta), \tag{7.1}$$

where each χ is extended to a character of the group $\mathfrak{I}(q)$; since $\beta\alpha^{-1} \in k^*$, the sum in the right hand side of (7.1) does not depend on the chosen extension. As usual, let $\{\alpha\}$ denote the fractional part of a real number α. For $\beta \in A_{\mathbb{R}}$ and $\chi \in H$, choose functions as follows. When $r = 1$ let

$$\psi_1(\beta) = \frac{\log |\beta|}{\log |\varepsilon_0|},\ \exp(2\pi i \psi_2(\beta)) = \frac{\beta^{(2)}}{|\beta^{(2)}|} \exp(-2\pi i \theta \psi_1(\beta))$$

with $\frac{\varepsilon_0^{(2)}}{|\varepsilon_0^{(2)}|} = \exp(2\pi i\theta)$, and let

$$\chi(\varepsilon_0) = \exp(2\pi it),\ 0 \le t < 1,\ \nu_0(\chi,\beta) = \exp(-2\pi it\{\psi_1(\beta)\}).$$

If $r = 2$, let ψ_1, ψ_2 be defined by the equation $l(\beta)R(k)^{-1} = l(\psi)$, where

$$l(\beta) := (\log|\beta^{(1)}|, \log|\beta^{(2)}|, \log|\beta^{(3)}|),\ l(\psi) := (\log|N\beta|, \psi_1(\beta), \psi_2(\beta)),$$

with $R(k)$ denoting the regulator matrix of k as in § 2, and let

$$\nu_0(\chi,\beta) = \exp(-2\pi i(t_1\{\psi_1(\beta)\} + t_2\{\psi_2(\beta)\})),$$

where

$$\chi(\varepsilon_j) = \exp(2\pi it_j),\ 0 \le t_j < 1,\ j = 1, 2.$$

Now let

$$\nu(\chi,\beta) = \chi(\beta)(\frac{\beta}{|\beta|})^s\nu_0(\chi,\beta),$$

where $\chi(-1) = (-1)^s,\ s = 0, 1$. The characters $\lambda_j(\alpha) = \exp(2\pi i\psi_j(\alpha)),\ j = 1, 2$, generate the group of Grössencharacters of k. Let

$$H(u) = \begin{cases} 1 - \Delta^{-1}||u||, & ||u|| \le \Delta, \\ 0, & ||u|| \ge \Delta, \end{cases}$$

where $||u|| := \min\{|u - n| : n \in \mathbb{Z}\}$ for $u \in \mathbb{R}$. Following [2], let us introduce a weight function $W(\beta;\Delta,x)$, defined for $0 < \Delta < \frac{1}{2},\ x \in \mathbb{R}^3,\ (\beta) \in \mathcal{I}(k)$ by

$$W(\beta;\Delta,x) = H(\psi_1(\beta) - \psi_1(\check{x}))H(\psi_2(\beta) - \psi_2(\check{x})),$$

and consider the sum

$$\Sigma(\chi,x) = \sum_{\substack{N\check{x} < N(\beta) \le N\check{x} + \Delta V \\ \beta \in A^{(0)}}} d_{(\beta)}\nu(\chi,\beta)W(\beta;\Delta,x),$$

where $x \in \mathcal{C}$, so that $V \ll N\check{x} \ll V$. Clearly,

$$\Sigma(\chi,x) = \frac{1}{h(k)}\sum_{\nu_1}\bar{\nu_1}(A)\sum_{N\check{x} < N(\beta) \le N\check{x} + \Delta V} d_{(\beta)}\nu_1((\beta))\nu(\chi,\beta)W(\beta;\Delta,x), \tag{7.2}$$

where ν_1 ranges over the characters of the class group of k.

Lemma 7.2 *Let $x \in \mathcal{C}$ and suppose that $q \leq (\log L)^l$. Then*

$$\Sigma(\chi, x) = \varepsilon(\chi) m(x) \frac{\Delta^2}{M} (\xi \log X)^{-n-1} + O_l(\Delta^{-2} M^{-1} V \exp(-c\sqrt{\log L})), \tag{7.3}$$

where

$$m(x) = w(N\check{x} + \Delta V) - w(N\check{x})$$

and $\varepsilon(\chi) = h(k)^{-1}$ or 0 depending on whether χ is trivial or not.

Proof. The asymptotic formula (7.3) can be deduced from (7.2) along the lines of the proof of Lemma 9.3 in [2]; if the character χ is trivial, the contribution to the main term comes from the summand in (7.2) with $\nu_1 = 1$.

Let now

$$\Sigma'(\chi, x) = \nu_0(\chi, \beta)^{-1} \Sigma(\chi, x),$$

and let

$$\mathfrak{j} = \int_{\mathcal{C}} \Sigma'(\chi, x) dx.$$

Following [2], one deduces from Lemma 7.2 that

$$\begin{aligned} \mathfrak{j} \;\; = \;\; & \varepsilon(\chi) \frac{\Delta^3 V}{M} (\xi \log X)^{-n-1} |\det \; h_A| I + O(\Delta^4 V^2 M^{-1}) \\ & + O_l(\Delta^{-2} M^{-1} V S_0^3 \exp(-c\sqrt{\log L})). \end{aligned} \tag{7.4}$$

Lemma 7.3 *Let $\alpha \in \mathfrak{I}$, and suppose that $W(\alpha; \Delta, x) \neq 0$, and that*

$$N\check{x} < N(\alpha) \leq N\check{x} + \Delta V, \; V \ll N(\alpha) \ll V.$$

Then $(\alpha) = (\beta)$ for some $\beta \in \mathfrak{I}$ with $\hat{\beta} = (1 + O(\Delta))x$. Moreover, there exists $y \in \mathbb{R}^3$ and $\varepsilon \in \mathfrak{o}^*$ such that $\check{x} = \check{y}\varepsilon$ and $\hat{\alpha} = (1 + O(\Delta))y$.

An analogue of Lemma 7.3 is valid for any number field; its proof is an exercise in the multidimensional arithmetic of E.Hecke, [3], [4], [6], and we omit it here; one can also prove this lemma by a direct calculation, generalising the proof of Lemma 9.5 in [2]. Denoting by c the constant implicit in the $O-$ symbols of Lemma 7.3, let

$$\mathcal{C}' = \{t : t \in \mathbb{R}^3, \; |t - x| \leq cV^{1/3}\Delta \text{ for some } x \in \mathcal{C}\}.$$

It follows from Lemma 7.3 that

$$\Sigma'(x) = \sum_{\substack{\hat{\beta} \in \mathcal{C}', \, \beta \in A^{(0)} \\ N\check{x} < N\beta \leq N\check{x} + \Delta V}} d_{(\beta)} \chi(\beta) W(\beta; \Delta, x)(1 + O(\Delta)),$$

and therefore

$$\mathfrak{j} = \sum_{\hat{\beta}\in\mathcal{C}',\ \beta\in A^{(0)}} d_{(\beta)}\chi(\beta)(1+O(\Delta)) \int_{x\in\mathcal{C},\ N\check{x}<N\beta\le N\check{x}+\Delta V} W(\beta;\Delta,x)dx.$$

As in [2], it now follows that

$$\mathfrak{j} = \sum_{\hat{\beta}\in\mathcal{C},\ \beta\in A^{(0)}} d_{(\beta)}\chi(\beta)(1+O(\Delta))I_0(\beta) + O(\Delta^4 V^2 \log X),$$

where

$$I_0(\beta) = \int_{x\in\mathcal{F},\ N\check{x}<N\beta\le N\check{x}+\Delta V} W(\beta;\Delta,x)dx,$$

and $\mathcal{F}$ is a fundamental domain of the group of units $\mathfrak{o}^*$ in $\mathbb{R}^3$. If $r=1$, the integral $I_0(\beta)$ can be evaluated in the same way as in [2]; if $r=2$, to evaluate this integral one makes a substitution

$$\check{x} \mapsto l(\check{x})R(k)^{-1} = (\log|N\check{x}|, \psi_1(\check{x}), \psi_2(\check{x})).$$

This gives $I_0(\beta) = \Delta^3 V\phi(k)h(k)^{-1}|\det\ h_A|$ in either case; therefore

$$\mathfrak{j} = \Delta^3 V\phi(k)h(k)^{-1}|\det\ h_A| \sum_{\hat{\beta}\in\mathcal{C},\ \beta\in A} d_{(\beta)}\chi(\beta)(1+O(\Delta)) + O(\Delta^4 V^2\log X). \tag{7.5}$$

On comparing relations (7.1), (7.4), and (7.5) one concludes the proof of Proposition 7.1 along the lines of [2, § 9]. This completes the proof of Proposition 6.1.

As it has been explained at the end of [2, § 3], Theorem 2.1 and therefore Theorem 1.1 can be deduced from Proposition 5.1 and Proposition 6.1 by a suitable choice of the parameters η and Q_1.

Acknowledgement. The visits of the second author to Oxford have been supported through the EEC program "Arithmetic Algebraic Geometry"; this financial assistance and the hospitality of the Mathematical Institute at the University of Oxford during these visits are gratefully acknowledged.

References

[1] H. Halberstam and H.-E. Richert, *Sieve methods,* Academic Press, London, 1974.

[2] D.R. Heath-Brown, Primes represented by x^3+2y^3, Acta Mathematica, to appear.

[3] E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, *Math. Z.,* 6 (1920), 11-51.

[4] J.P.Kubilius, On some problems in geometry of prime numbers (in Russian), *Math. Sb. of the USSR,* 31 (1952), 507-542.

[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] T. Mitsui, Generalized prime number theorem, *Jap. J. Math.,* 26 (1956), 1-42.

[7] A.Weil, *Basic number theory,* Springer-Verlag, 1973.

Subject classification: 11N32 (11N36, 11R44)

Authors' addresses
D.R. Heath-Brown,
Mathematical Institute,
24-29, St. Giles',
Oxford OX1 3LB,
ENGLAND

B.Z. Moroz,
Max-Planck-Institute Für Mathematik,
Vivatgasse 7,
D-53111 Bonn,
GERMANY