SERRE'S PROBLEM ON THE DENSITY OF ISOTROPIC FIBRES IN CONIC BUNDLES

by

E. Sofos

Abstract. — Let $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a non-singular conic bundle over $\mathbb{Q}$ having n non-split fibres and denote by $N(\pi, B)$ the cardinality of the fibres of Weil height at most B that possess a rational point. Serre showed in 1990 that a direct application of the large sieve yields

$$N(\pi, B) \ll B^2 (\log B)^{-n/2}$$

and raised the problem of proving that this is the true order of magnitude of $N(\pi, B)$ under the necessary assumption that there exists at least one smooth fibre with a rational point. We solve this problem for all non-singular conic bundles of rank at most 3. Our method comprises the use of Hooley neutralisers, estimating divisor sums over values of binary forms, and an application of the Rosser–Iwaniec sieve.

Contents

1. Introduction

The asymptotic distribution of the members of a family of varieties that have a rational point has been the focus of intensive investigation during recent years. There are families of Fano varieties over $\mathbb{Q}$ where the percentage of fibres with a $\mathbb{Q}$-point exists and is positive. Poonen and Voloch [**PV04**] have verified this in the case of hypersurfaces on the condition that the Brauer-Manin obstruction is the only obstruction to the Hasse principle for

2000 ***Mathematics Subject Classification.*** — 14G05; 14D10, 11N36, 11G35.

rational points on certain varieties. Research on this theme has subsequently flourished; the interested reader is referred to the recent work of Loughran and Smeets [**LS15**] and the thorough list of references it provides. It is noteworthy that families of conics were excluded from the Poonen-Voloch results since in this case the percentage is expected to vanish. Our aim in this paper is to focus on this exceptional case.

The exceptional behavior, first noticed by Serre [**Ser90**], can be explained, for example, through [**BCF**$^+$**15**, Th.1.2] of Bhargava, Cremona, Fisher, Jones, and Keating, where it is stated that the probability that a quadratic form in 3 variables over $\mathbb{Z}_p$ is isotropic is given by

$$\rho_3(p) = 1 - \frac{p}{2(p+1)^2}.$$

Owing to the Hasse principle, this suggests that the percentage of isotropic planar conics over $\mathbb{Q}$ with coefficients of size B should vanish asymptotically as $B \to \infty$ and, more precisely, it should decrease like

$$\prod_{p \leqslant B} \rho_3(p) \asymp (\log B)^{-1/2}.$$

Serre [**Ser90**] used the large sieve to prove upper bounds of the aforementioned order of magnitude and raised the problem of verifying that this is the correct order of magnitude. Obtaining precise lower bounds is a genuinely harder problem, since one needs a method for finding rational points. There are fewer difficulties when the generic fibre satisfies the Hasse principle, however, even in this case, there have been only very special cases in which the problem has been solved. More specifically, Hooley [**Hoo93**] and Guo [**Guo95**] proved the correct lower bound for the case of diagonal planar conics, and later, Hooley [**Hoo07**] proved a similar result in the case of general planar conics.

Let $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a non-singular conic bundle over $\mathbb{Q}$. A singular fibre $\pi^{-1}(\mathfrak{m})$ above a closed point $\mathfrak{m} \in \mathbb{P}^1_{\mathbb{Q}}$ is called *split* if both of its components are defined over the residue field $\mathbb{Q}(\mathfrak{m})$ and *non-split* otherwise. Denoting the set of non-split fibres by $M(\pi)$, and letting

$$n = \sharp M(\pi),$$

Serre's problem reads as follows: *assuming that there exists a smooth $\mathbb{Q}$-isotropic fibre of π, then verify that the quantity*

$$N(\pi, B) := \sharp\Big\{x \in \mathbb{P}^1_{\mathbb{Q}} : H(x) \leqslant B, \pi^{-1}(x) \text{ has a rational point}\Big\}$$

satisfies

$$N(\pi, B) \asymp \frac{B^2}{(\log B)^{n/2}}, \tag{1.1}$$

where H is the usual Weil height on $\mathbb{P}^1_{\mathbb{Q}}$. It should be noted that Loughran [**Lou13**] has stated a broader and more precise form of (1.1) that he furthermore verified in specific situations. Following Skorobogatov [**Sko96**], we let

$$r(\pi) = \sum_{\mathfrak{m} \in M(\pi)} [\mathbb{Q}(\mathfrak{m}) : \mathbb{Q}]$$

denote the *rank* of the fibration π. As a special case of [**Lou13**, Cor.1.4] the estimate (1.1) is promoted to an asymptotic formula when $r(\pi) = 2$ and $n = 1$, and the proof uses harmonic analysis on toric varieties. Our main theorem settles Serre's problem in cases where one lacks such a structure.

Theorem 1.1. — *Let $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a non-singular conic bundle over $\mathbb{Q}$ of rank $r(\pi) \leqslant 3$ and assume that there exists a smooth fibre with a rational point. Then*

$$N(\pi, B) \asymp \frac{B^2}{(\log B)^{n/2}}.$$

The existence assumption is obviously necessary for the lower bound. However, in the case $r(\pi) = 3$ it becomes redundant. Indeed, when $r(\pi) = 3$, X becomes birational to a quintic del Pezzo surface by the work of Iskovskih [**Isk79**, Th.5] and therefore the theorem of Enriques [**Enr97**] combined with [**Man86**, Th.29.4] reveals that X is $\mathbb{Q}$-rational, and in particular it has at least one smooth fibre with a $\mathbb{Q}$-point.

In what follows we outline the proof of Theorem 1.1 as well as the structure of the paper. Constructing indicator functions that detect the isotropic fibres is a key novel ingredient of the proof of Theorem 1.1. It allows the transformation of $N(\pi, B)$ into an average of arithmetic functions over values of binary forms (see (3.6) and (3.8)). The construction will be brought to life in §3.

The next step takes place in §4 and regards the most important technical device of our paper, namely **Hooley neutralisers**. Using the approach expounded by Hooley [**Hoo74**] allows us to extirpate certain awkward arithmetic functions apparent in (3.6), by introducing new weights coming from a combinatorial sieve. This reduces the problem to one of estimating asymptotically specific divisor sums, with an error term that exhibits a power saving.

A precise definition of the divisor sums at hand is supplied in (4.1). They are of shape

$$\sum_{|s|,|t|\leqslant B} \prod_{i=1}^{n} \sum_{d_i | \Delta_i(s,t)} \left(\frac{F_i(s,t)}{d_i} \right),$$

where $(\frac{\cdot}{\cdot})$ denotes the Jacobi symbol, $F_i \in \mathbb{Z}[s,t]$ are forms of even degree, $\Delta_i \in \mathbb{Z}[s,t]$ are irreducible forms with $\sum_i \deg(\Delta_i) \leqslant 3$, and the summation is over coprime integers s and t, satisfying certain congruence conditions. There is a large volume of literature that builds on the seminal work of S. Daniel [**Dan99**] to evaluate similar averages. However, his approach allows a power saving in the error term only in the case $\sum_i \deg(\Delta_i) \leqslant 3$, which is the only element in our proof of Theorem 1.1 obstructing its generalisation to all non–singular conic bundles with a smooth $\mathbb{Q}$-isotropic fibre. We shall state our result regarding divisor sums in Theorem 4.5 and its proof will be the sole aim in §5.

A confluence of entirely new features appear in §5 for the first time in the context of divisor sums over values of binary forms. Initially, one is faced with the presence of the forms F_i rather than fixed integers. This poses added difficulties that require serious

modification of Daniel's approach (see Proposition 3.2). A further novel feature of our treatment lies in the fact that our method is uniform in the factorisation of the form $\prod_i \Delta_i$ over $\mathbb{Q}$ (see Lemma 5.9). Lastly, we will prove that the modulus defining the aforementioned congruence conditions on s and t is allowed to assume values up to a positive power of B. This *level of distribution* result is the most advanced new component of our work; we shall put it into form in Theorem 4.5.

The Rosser-Iwaniec sieve enters the stage during §6 and it is the final step in the proof of Theorem 1.1. As is surely familiar to sieve experts, the use of sieve weights precludes the possibility of obtaining an asymptotic for $N(\pi, B)$ in Theorem 1.1.

Acknowledgements. — The problem was suggested during the 2014 AIM Workshop *'Rational and integral points on higher-dimensional varieties'* by Daniel Loughran to whom we are grateful for numerous conversations. We are furthermore indebted to Roger Heath–Brown for valuable discussions. This investigation was performed while the author was a postdoctoral researcher at Leiden and the support of its university is greatly appreciated.

Notation. — For any $k, k' \in \mathbb{Z}$ we shall denote their greatest common divisor and least common multiple by $\gcd(k, k')$ and $[k, k']$ respectively. The set of all primitive integer vectors in $\mathbb{Z}^k$ will be denoted by $\mathbb{Z}^k_{\text{prim}}$, while the p-adic valuation of an integer k will be denoted by $\nu_p(k)$. As usual, we let $\tau(k)$ denote the number of positive divisors of any non-zero integer k. Each $\mathbf{x} \in \mathbb{R}^k$ has a supremum norm which will be denoted by $\|\mathbf{x}\|$, and similarly, for a bounded set $\mathscr{C} \subset \mathbb{R}^k$ we shall represent the supremum of $\left\{\|\mathbf{x}\| : \mathbf{x} \in \mathscr{C}\right\}$ by $\|\mathscr{C}\|_\infty$. Given a polynomial $f \in \mathbb{R}[x_1, \dots, x_k]$ we shall denote the maximum absolute value of its coefficients by $\langle f \rangle$.

The data associated to the conic bundle apparent in Theorem 1.1 will be considered constant throughout. This is taken to mean that, although each implied constant in the big O notation will depend on several quantities related to π, we shall avoid recording these dependencies. The list of the said quantities consists of

$$\Delta, \Delta_i, F_i, \mathscr{R}, W, W_i, f_i \in \mathscr{U}, s_0, t_0,$$

whose meaning will become evident in due course. Any other dependencies of the implied constants on further parameters will be explicitly specified via the use of a subscript. The symbol ε will be used for a small positive parameter and its value may vary, allowing, for example, inequalities of the form $x^\varepsilon \ll_\varepsilon x^{\varepsilon/2}$.

2. Preliminaries

We shall follow closely the geometric setup for conic bundles as given in [**BSJ14**, §2.2]. The fibre of π above the point $[s, t] \in \mathbb{P}^1_{\mathbb{Q}}$ is of the shape $Q_{s,t} = 0$, where

$$Q_{s,t}(\mathbf{x}) = \sum_{i,j=1}^{3} f_{ij}(s, t) x_i x_j \tag{2.1}$$

and all f_{ij} are binary integer forms. The non-singularity of X shows that the discriminant of $Q_{s,t}$, defined through

$$\Delta(s,t) = \frac{1}{2}\det\left(\frac{\partial^2 Q_{s,t}(\mathbf{x})}{\partial x_i \partial x_j}\right),$$

is separable. We shall assume that all principal minors of the matrix $(f_{ij}) \in (\mathbb{Z}[s,t])^{3\times 3}$ are forms of even degree, say $d_i \in 2\mathbb{Z}_{\geqslant 0}$ for $i = 1, 2, 3$.

The fact that we are interested in lower bounds of the correct order of magnitude for $N(\pi, B)$ allows us to assume with no loss of generality, that the fibre at infinity is smooth, a fact equivalent to $t \nmid \Delta(s,t)$ in $\mathbb{Z}[s,t]$. It furthermore allows us to assume that all singular fibres are non-split, since contracting one line in any split singular fibre does not affect the order of magnitude of $N(\pi, B)$. We have the factorisation

$$\Delta(s,t) = \prod_{i=1}^{n}\Delta_i(s,t), \tag{2.2}$$

where the forms Δ_i are irreducible over $\mathbb{Z}[s,t]$ and coprime in pairs; they are in correspondence with the singular fibres of π. For each $i = 1, \dots, n$ we fix a root $\theta_i \in \overline{\mathbb{Q}}$ of $\Delta_i(x,1) = 0$ once and for all for the rest of this paper. The fact that each singular fibre is non-split implies that non of the lines comprising the singular fibre above $[\theta_i, 1]$ is defined over the residue field $\mathbb{Q}(\theta_i)$.

Let us recall that in the notation of [**BSJ14**, §2.2], the morphism

$$(s,t;\mathbf{x}) \mapsto (s/t; [x_1 t^{-d_1/2}, x_2 t^{-d_2/2}, x_3 t^{-d_3/2}])$$

maps each $(s,t;\mathbf{x}) \in \mathbb{A}^5$ with $Q_{s,t}(\mathbf{x}) = 0, \mathbf{x} \neq \mathbf{0}$ and $(s,t) \neq \mathbf{0}$ to a point on the variety $S_1 \subset \mathbb{A}^1 \times \mathbb{P}^2$ given by $Q_{u,1}(\mathbf{x}) = 0$. This reveals that there exists an integer d that makes the following identity valid,

$$t^d Q_{s,t}(\mathbf{x}) = Q_{s/t,1}(x_1 t^{-d_1/2}, x_2 t^{-d_2/2}, x_3 t^{-d_3/2}). \tag{2.3}$$

3. Construction of the detectors

Owing to the assumptions of Theorem 1.1 there exist $(s_0, t_0) \in \mathbb{Z}^2_{\text{prim}}$ and $\mathbf{y} \in \mathbb{Z}^3_{\text{prim}}$ such that $Q_{s_0,t_0}(\mathbf{y}) = 0$ and $\Delta(s_0, t_0) \neq 0$. The implicit function theorem for the $\mathbb{R}$-morphism $\pi : X(\mathbb{R}) \to \mathbb{P}^1(\mathbb{R})$ provides a set $C \subset \mathbb{R}^2$ of non-empty interior that contains both $\mathbf{0}, (s_0, t_0)$ and that is closed under scalar multiplication, such that whenever $(s,t) \in C$ then $Q_{s,t} = 0$ is smooth and has a real point. Observe that given any finite set of lines of $\mathbb{R}^2$ all of which pass through the origin but none through (s_0, t_0), there exists a box inside C that contains (s_0, t_0) and not intersecting any of the lines. This shows that there exists a box of non-empty interior $\mathscr{R} \subset C$ such that if $(s,t) \in \mathbb{R}^2 \cap B\mathscr{R}$ and $B \in \mathbb{R}_{>1}$ then $\Delta(s,t) \neq 0, Q_{s,t}(\mathbb{R}) \neq \varnothing$ and

$$\Delta_i(s,t)\Delta_i(s_0,t_0) > 0 \text{ if } \Delta_i \text{ is linear.} \tag{3.1}$$

In a similar fashion, the non-archimedean analogue of the implicit function theorem can be used for each $p \leqslant D_0$ to provide large integers κ_p such that

$$\text{if } (s,t) \equiv (s_0,t_0) \pmod{p^{\kappa_p}} \text{ then } Q_{s,t}(\mathbb{Q}_p) \neq \varnothing. \tag{3.2}$$

We define the symbol $\mathscr{H}_p(s,t)$ for all primes p and any $(s,t) \in \mathbb{Z}^2_{\text{prim}}$ with $\Delta(s,t) \neq 0$ to be 1 or -1 according to if the conic $Q_{s,t}(\mathbf{x}) = 0$ is soluble over $\mathbb{Q}_p$ or not. Therefore letting for any $B > 1$,

$$\mathscr{B} := \left\{ (s,t) \in \mathbb{Z}^2_{\text{prim}} \cap B\mathscr{R} : (s,t) \equiv (s_0,t_0) \left(\text{mod } \prod_{p \leqslant D_0} p^{\kappa_p} \right) \right\},$$

allows us to deduce via the Hasse principle that

$$N(\pi, B) \gg \sum_{(s,t) \in \mathscr{B}} \prod_{\substack{p \mid \Delta(s,t) \\ p > D_0}} \left(\frac{1 + \mathscr{H}_p(s,t)}{2} \right), \tag{3.3}$$

given that $Q_{s,t}(\mathbf{x}) = 0$ has a $\mathbb{Q}_p$-point whenever $p \nmid \Delta(s,t)$.

It is important to highlight that (3.3) gives us the freedom to choose D_0 arbitrarily large. The idea of restricting to congruences modulo the integer

$$W = \prod_{p \leqslant D_0} p^{n_p},$$

where $n_p \geqslant \kappa_p$, comes from sieve theory. We shall often enlarge the size of D_0 and n_p with no further mention, this will allow us to deal with complications arising from the effect of small primes. We shall always choose W to depend solely on the coefficients of the forms $f_{ij}(s,t)$ in (2.1) and in particular W will be independent of the counting parameter B.

Owing to the vanishing of $\Delta(\theta_i, 1)$, the form $Q_{\theta_i,1}(\mathbf{x})$ is singular and thus $\nabla Q_{\theta_i,1}(\mathbf{v}) = 0$ for some non-zero vector $\mathbf{v} \in \mathbb{Z}[\theta_i]^3$. Fixing some $1 \leqslant \ell_i \leqslant 3$ satisfying $v_{\ell_i} \neq 0$ allows us to consider the discriminant of the binary quadratic form $Q_{s,t}(x_{\ell_i} = 0)$. This discriminant, henceforth called $F_i(s,t)$, is a binary form in $\mathbb{Z}[s,t]$ and has even degree owing to the assumption that the matrix of the quadratic form $Q_{s,t}(\mathbf{x})$ has principal minors of even degree. It is important to note that the construction of F_i is not unique since it depends on the choice of ℓ_i. We can however make a choice of ℓ_i following the algorithm above, and fix this choice once and for all for the rest of this paper.

For any $N \in \mathbb{N}$ and any field K of characteristic not 2, we let $Q \in K[x_1, \dots, x_N]$ be any quadratic form. Then for all $\mathbf{x} \in K^N$, we have $4Q(\mathbf{x}) = 2Q(\mathbf{x}) + \nabla Q(\mathbf{x}) \cdot \mathbf{x}$, where $\cdot$ denotes the inner product in K^N. Therefore we obtain that

$$\text{if } \ \nabla Q(\mathbf{x}) = 0, \ \text{ then } \ Q(\mathbf{x}) = 0. \tag{3.4}$$

Let us next prove that the fact that the singular fibre above $[\theta_i, 1]$ is not a double line implies $\text{Res}(\Delta_i, F_i) \neq 0$. Indeed, assuming with no loss of generality that $\ell_i = 1$ and

considering the transformation $\mathbf{y} = T_i^{-1}\mathbf{x}$, where

$$T_i := \begin{pmatrix} v_1 & 0 & 0 \\ v_2 & v_1 & 0 \\ v_3 & 0 & v_1 \end{pmatrix},$$

shows that

$$\begin{aligned} Q_{\theta_i,1}(\mathbf{x}) &= Q_{\theta_i,1}(v_1(0,y_2,y_3) + y_1\mathbf{v}) \\ &= v_1^2 Q_{\theta_i,1}(0,y_2,y_3) + y_1^2 Q_{\theta_i,1}(\mathbf{v}) + y_1 v_1(\nabla Q_{\theta_i,1}(\mathbf{v})\cdot(0,y_2,y_3)) \\ &= v_1^2 Q_{\theta_i,1}(0,y_2,y_3). \end{aligned}$$

We have made use of $Q_{\theta_i,1}(\mathbf{v}) = 0$, which is implied by $\nabla Q_{\theta_i,1}(\mathbf{v}) = 0$ and of (3.4) for

$$N = 3, K = \mathbb{Q}(\theta_i), Q = Q_{\theta_i,1}, \mathbf{x} = \mathbf{v}.$$

The calculation above reveals that there exists an invertible transformation defined over $\mathbb{Q}(\theta_i)$ that transforms the singular fibre above $[\theta_i, 1]$ into the binary quadratic form

$$Q_{\theta_i,1}(0,y_2,y_3) = 0.$$

Since our conic bundle is non-singular, each singular fibre is not a double line and therefore the discriminant of the said quadratic form, $F_i(\theta_i,1)$, must be non-zero. However, if $\mathrm{Res}(\Delta_i, F_i) = 0$ then the irreducibility of Δ_i would yield that $\Delta_i | F_i$ in $\mathbb{Z}[s,t]$ and therefore $F_i(\theta_i,1) = 0$, a contradiction. Let us record here the obvious observation that since the singular fibre above $[\theta_i,1]$ is non-split, we have that

$$F_i(\theta_i,1) \notin \mathbb{Q}(\theta_i)^2 \quad \text{for all} \quad i = 1,\dots,n. \tag{3.5}$$

Proposition 3.1 **(Detectors).** — *There exists a large positive constant D_0, that depends at most on the coefficients of the equation $Q_{s,t} = 0$ which defines the conic bundle, such that, whenever $(s,t) \in \mathbb{Z}^2_{prim}$ with $\Delta(s,t) \neq 0$ and $p > D_0$ is a prime that divides $\Delta(s,t)$, then there exists a unique $i \in \{1,\dots,n\}$ satisfying $p|\Delta_i(s,t)$ and*

$$\mathscr{H}_p(s,t) = \left(\frac{F_i(s,t)}{p}\right)^{\nu_p(\Delta_i(s,t))}.$$

Proof. — Recalling (2.2) and taking D_0 large enough so that W includes all prime divisors of the resultant of Δ_i and Δ_j for all $i \neq j$, immediately yields that there exists a unique index $i \in \{1,\dots,n\}$ such that $p|\Delta_i(s,t)$. The fact that $t \nmid \Delta(s,t)$ in $\mathbb{Z}[s,t]$ implies that $\Delta_i(1,0) \neq 0$. Enlarging D_0 allows us to assume that $p \nmid \Delta_i(1,0)$ and therefore the coprimality of s and t reveals that $p \nmid t$. We therefore obtain that $\Xi_p := s/t \pmod p$ is defined and, in light of (2.3), $Q_{s,t} = 0$ has a $\mathbb{Q}_p$-point if and only if $Q_{\Xi_p,1} = 0$ does. Noting that $\Delta_i(\Xi_p,1) \equiv 0 \pmod p$, allows us to confirm that the map $\psi : \mathbb{Z}[x]/(\Delta_i(x,1)) \to \mathbb{Z}/p\mathbb{Z}$, given by

$$h(x) + (\Delta_i(x,1)) \mapsto h(\Xi_p) \pmod p,$$

is well-defined and a ring homomorphism.

Taking a larger value for D_0 allows us to obtain the coprimality of p and $\psi(v_{\ell_i})2\mathrm{Res}(\Delta_i, F_i)$ and hence the matrix $\psi(T_i) \in (\mathbb{Z}/p\mathbb{Z})^{3\times 3}$ is invertible. Therefore applying ψ to the equality

$Q_{\theta_i,1}(\mathbf{x}) = v_{\ell_i}^2 Q_{\theta_i,1}(0, y_2, y_3)$ shows that $Q_{\Xi_p,1}$ can be transformed over $\mathbb{Z}/p\mathbb{Z}$ into the binary quadratic form $Q_{\Xi_p,1}(0, y_2, y_3)$. Due to $p \nmid \mathrm{Res}(\Delta_i, F_i)$, its discriminant $F_i(\Xi_p, 1)$, is not divisible by p and we can therefore diagonalise it into $c(z_1^2 - F_i(\Xi_p, 1)z_2^2)$ for some $c \in \mathbb{Z}/p\mathbb{Z}$ with $p \nmid c$. We have therefore shown that $Q_{\Xi_p,1} = 0$ is equivalent over $\mathbb{Q}_p$ to

$$c(z_1^2 - F_i(\Xi_p, 1)z_2^2) + c' z_3^2 = 0$$

for some $c' \in p\mathbb{Z}_p$. Noting that the p-adic valuation of $\Delta(\Xi_p, 1)$ is $\nu_p(\Delta_i(s,t))$, we deduce that $\nu_p(c') = \nu_p(\Delta_i(s,t))$ and therefore a standard computation reveals that the p-adic Hilbert symbol of $z_1^2 = F_i(\Xi_p, 1)z_2^2 - \frac{c'}{c} z_3^2$ equals

$$\left(\frac{F_i(\Xi_p, 1)}{p}\right)^{\nu_p(\Delta_i(s,t))}.$$

Bringing together the observations $s \equiv \Xi_p t \pmod p$ and $2 | \deg(F_i)$ finishes the proof of our proposition. ∎

Introducing for each $(s,t) \in \mathscr{B}$ and $i \in \{1, \dots, n\}$ the entities

$$r_i^*(s,t) := \prod_{\substack{p | \Delta_i(s,t) \\ p > D_0}} \left(1 + \left(\frac{F_i(s,t)}{p}\right)\right)$$

and combining Proposition 3.1 with (3.3) yields that $N(\pi, B)$ is

$$\gg \sum_{(s,t)\in\mathscr{B}} \prod_{i=1}^{n} \prod_{\substack{p | \Delta_i(s,t) \\ p > D_0}} \frac{1}{2}\left(1 + \left(\frac{F_i(s,t)}{p}\right)^{\nu_p(\Delta_i(s,t))}\right) \geqslant \sum_{(s,t)\in\mathscr{B}} \prod_{i=1}^{n} r_i^*(s,t) 2^{-\sharp\{p | \Delta_i(s,t) : p > D_0\}}.$$

Define for any $k \in \mathbb{Z} - \{0\}$ and $z \in \mathbb{R} \cap (D_0, \infty)$ the function

$$\omega(k; z) := \sharp\{p | k : D_0 < p \leqslant z\}.$$

Furthermore, whenever $z \in \mathbb{R} \cap (D_0, B)$ we define

$$\varpi := \left(\frac{\log z}{\log B}\right) 100n(n+1),$$

which will eventually be a small positive constant. Let us recall that for the integer $j = \sharp\{p | k : p > D_0\}$ we have $j \leqslant (\log k)/(\log D_0)$. The inequality $|\Delta_i(s,t)| \ll B^{\deg(\Delta_i)}$ therefore reveals that

$$N(\pi, B) \gg \sum_{(s,t)\in\mathscr{B}} \prod_{i=1}^{n} \frac{r_i^*(s,t)}{2^{\omega(\Delta_i(s,t); z)}}. \tag{3.6}$$

Before the end of this section we record a result which will facilitate the application of the hyperbola trick in §5. For any integer $n \in \mathbb{Z} - \{0\}$ define

$$n^\dagger := \prod_{\substack{p | n \\ p > D_0}} p^{\nu_p(n)}.$$

Proposition 3.2. — *For all $(s,t) \in \mathscr{B}$ and $i = 1, \dots, n$ we have*

$$\left(\frac{F_i(s,t)}{\Delta_i(s,t)^\dagger}\right) = 1.$$

Proof. — Notice that for all (s,t) under consideration the conic $Q_{s,t}(\mathbf{x}) = 0$ is smooth and is soluble over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p satisfying $p \leqslant D_0$ or $p \nmid \Delta(s,t)$. By Hilbert's reciprocity formula we obtain

$$\prod_{\substack{p \mid \Delta(s,t) \\ p > D_0}} \mathscr{H}_p(s,t) = 1 \tag{3.7}$$

and hence Proposition 3.1 yields that

$$\prod_{i=1}^{n} \left(\frac{F_i(s,t)}{\Delta_i(s,t)^\dagger}\right) = 1.$$

Noting that the rank $r(\pi) = \sum_{i=1}^n \deg(\Delta_i)$ is at most 3 shows that the vector $(\deg(\Delta_i))_{i=1}^n$ can only be one of the following, $(3), (2,1), (1,1,1), (2), (1,1)$ or (1). In the first case, the proof of our claim is furnished immediately by (3.7), while in the two remaining cases, (3.7) shows that it suffices to prove $\left(\frac{F_i(s,t)}{\Delta_i(s,t)^\dagger}\right) = 1$ for each i with Δ_i linear.

Indeed, let $\Delta_i(s,t) = a_i s - b_i t$ be such a form, where a_i, b_i are integers with $(a_i, b_i) \neq \mathbf{0}$. Letting $c_i := F_i(b_i, a_i)$, we observe that there exists a polynomial $g_i \in \mathbb{Z}[x,y]$ such that

$$a_i^{\deg(F_i)} F_i(x,y) = y^{\deg(F_i)} c_i + \Delta_i(x,y) g_i(x,y),$$

as can be shown by a Taylor expansion for example. Specialising to $(x,y) = (s,t)$ and using that $2 | \deg(F_i)$, we obtain the equality

$$\left(\frac{F_i(s,t)}{\Delta_i(s,t)^\dagger}\right) = \left(\frac{c_i}{\Delta_i(s,t)^\dagger}\right).$$

To continue our argument, we augment W by assuming that $4c_i\Delta_i(s_0,t_0) | W$. Note that for all (s,t) in our lemma there exist $(s',t') \in \mathbb{Z}^2$ such that $(s,t) = (s_0,t_0) + W(s',t')$ and hence we have that

$$\Delta_i(s,t) = \Delta_i(s_0,t_0)\left(1 + \frac{W}{\Delta_i(s_0,t_0)}\Delta_i(s',t')\right).$$

The integer in the parenthesis is positive due to (3.1). Noting that $\Delta_i(s_0,t_0) | W$ shows that $\Delta_i(s_0,t_0)^\dagger = 1$, and therefore

$$\Delta_i(s,t)^\dagger = 1 + \frac{W}{\Delta_i(s_0,t_0)}\Delta_i(s',t') \equiv 1 \,(\mathrm{mod}\ 4c_i).$$

Now quadratic reciprocity reveals the validity of

$$\left(\frac{c_i}{\Delta_i(s,t)^\dagger}\right) = \left(\frac{\Delta_i(s,t)^\dagger}{c_i}\right),$$

which equals $(\frac{1}{c_i}) = 1$, and therefore our proof is hereby concluded. ∎

We shall now record an explicit formula for $N(\pi, B)$ which is valid for non-singular conic bundles of any rank. This formula is not used in the present paper but can be helpful in future work in the area. Let us define for any index $i = 1, \dots, n$ and all $(s,t) \in \mathbb{Z}^2_{\text{prim}}$ satisfying $\Delta(s,t) \neq 0$ the arithmetic functions

$$\widetilde{r}_i(s,t) := \prod_{\substack{p \mid \Delta_i(s,t) \\ p > D_0}} (1 + \mathscr{H}_p(s,t)),$$

which, by Lemma 3.1, fulfil

$$\widetilde{r}_i(s,t) = \sum_{\substack{d_i \mid \Delta_i(s,t)^\flat \\ \gcd(d_i, \Delta_i(s,t)/d_i)=1}} \left(\frac{F_i(s,t)}{d_i} \right).$$

Introducing for any $D > 0$ the set

$$\mathrm{Sol}(D) := \{(s,t) \in \mathbb{Z}^2 : Q_{s,t} = 0 \text{ isotropic over } \mathbb{R} \text{ and } \mathbb{Q}_p \text{ for all } p \leqslant D\},$$

allows us to deduce via the Hasse principle that

$$N(\pi, B) = \frac{1}{2} \sum^{*}_{\substack{|s|,|t| \leqslant B \\ \Delta(s,t) \neq 0 \\ (s,t) \in \mathrm{Sol}(D_0)}} \prod_{i=1}^{n} \frac{\widetilde{r}_i(s,t)}{2^{\sharp\{p \mid \Delta_i(s,t)^\flat\}}} + \sum_{\substack{1 \leqslant i \leqslant n \\ \deg(\Delta_i)=1}} 1, \tag{3.8}$$

since the only degenerate fibres contributing towards $N(\pi, B)$ are the ones defined over $\mathbb{Q}$.

We next sketch how one could deal with the conditions on the summation over s, t imposed by the set $\mathrm{Sol}(D_0)$. We can see, for example, by diagonalising $Q_{s,t} = 0$ over $\mathbb{R}$ and using the Hilbert symbol over $\mathbb{R}$, that there is a finite union of open, disjoint, and non-empty sets $\mathscr{R}_j \subset \mathbb{R}^2$ such that $Q_{s,t} = 0$ has a real point if and only if $(s,t) \in \bigcup_j \mathscr{R}_j$. To deal with p-adic solubility for the small primes $p \leqslant D_0$, we can observe that for each prime $p \geqslant 2$, whenever $p^\alpha \| \Delta(\sigma, \tau)$ and $(s,t) \equiv (\sigma, \tau) \pmod{p^{\alpha+1}}$, then $Q_{s,t} = 0$ has a $\mathbb{Q}_p$-point if and only if $Q_{\sigma,\tau} = 0$ has, and therefore one can then partition the sum over s, t in sets defined (mod $p^{\alpha+1}$) for all $p \leqslant D_0$ and $\alpha \in \mathbb{Z}_{\geqslant 0}$. The periodic property we mentioned can be inferred by observing that a smooth conic $Q = 0$ has a p-adic point if and only if its p-adic Hardy-Littlewood density is positive and that the limit [**Sof14**, Eq.(1.2)] defining the p-adic density stabilises as soon as $n \geqslant \nu_p(\Delta_Q) + 1$, in the notation of [**Sof14**].

4. Introducing the Hooley neutralisers

4.1. Construction of the neutraliser. — It is tempting to use the formula

$$\frac{1}{2^{\omega(k)}} = \sum_{d \mid k} \frac{\mu(d)}{\tau(d)}$$

to turn the sum (3.6) into a sum of the form

$$\sum_{d_i \ll B^{\deg(\Delta_i)}} \frac{\mu(d_1)\cdots\mu(d_n)}{\tau(d_1)\cdots\tau(d_n)} \sum_{\substack{(s,t)\in\mathscr{B}\\ d_i \mid \Delta(s,t)}} r_1^*(s,t)\cdots r_n^*(s,t).$$

Alas, this action will place us in a quandary owing to the magnitude of the range of summation of each variable $d = d_1, \dots, d_n$. Hooley's neutraliser trick consists of employing sieve functions $\lambda_d^{\pm}$ that imitate the Möbius function $\mu(d)$, yet at the same time, having a small support.

With an eye to future applications we supply a general version of his artifice in the next proposition. Before proceeding, we recall the sole required property of the sequence $(\lambda_d^{\pm})_{d\in\mathbb{N}}$, namely

$$\lambda_1^{\pm} = 1 \quad \text{and} \quad \lambda_d^- \leqslant 0 \leqslant \lambda_d^+ \quad \text{for all } d \neq 1.$$

Proposition 4.1. — *Assume that $\mathscr{P}_1, \dots, \mathscr{P}_n$ are sets of primes and that we are given functions $f_1, \dots, f_n : \mathbb{N} \to \mathbb{R}$ satisfying the following properties,*
(1) *f_i multiplicative,*
(2) *$f_i(\mathbb{N}) \subset \mathbb{R}_{>0}$,*
(3) *$m \in \mathbb{N}, p$ prime $\Rightarrow f_i(p^m) = f_i(p)$,*
(4) *$p \in \mathscr{P}_i \Rightarrow f_i(p) < 1$,*
(5) *$p \notin \mathscr{P}_i \Rightarrow f_i(p) = 1$.*
Define the multiplicative functions $\widehat{f}_i : \mathbb{N} \to \mathbb{R}$ by $\widehat{f}_i(k) := \prod_{p\mid k}(1 - f_i(p))$. Then for all $\mathbf{k} \in \mathbb{N}^n$ with $gcd(k_i, k_j) = 1$ for all $i \neq j$ we have

$$\sum_{\substack{d_i\mid k_i\\ p\mid d_i \Rightarrow p\in\mathscr{P}_i\\ d_i \text{ squarefree}}} \lambda^-_{d_1\cdots d_n} \prod_{i=1}^n \widehat{f}_i(d_i) \leqslant \prod_{i=1}^n f_i(k_i) \leqslant \sum_{\substack{d_i\mid k_i\\ p\mid d_i \Rightarrow p\in\mathscr{P}_i\\ d_i \text{ squarefree}}} \lambda^+_{d_1\cdots d_n} \prod_{i=1}^n \widehat{f}_i(d_i).$$

Proof. — Let n_i be squarefree integers composed entirely of primes in $\mathscr{P}_i$ for all $i = 1, \dots, n$ and assume that they are coprime in pairs. Then by (1) and (2) we get

$$1 = \prod_{i=1}^n \frac{\widehat{f}_i(1)}{f_i(1)} = \sum_{\substack{\mathbf{m}\in\mathbb{N}^n\\ m_i\mid n_i}} \left(\prod_{i=1}^n \frac{\widehat{f}_i(m_i)}{f_i(m_i)}\right) \delta(m_1\cdots m_n),$$

where δ is the characteristic function of $\{1\}$. Noting that $\frac{\widehat{f}_i(m_i)}{f_i(m_i)} > 0$ due to (2) and (4), we deduce that

$$\sum_{\substack{\mathbf{m}\in\mathbb{N}^n\\ m_i\mid n_i}} \left(\prod_{i=1}^n \frac{\widehat{f}_i(m_i)}{f_i(m_i)}\right) \left(\sum_{d\mid m_1\cdots m_n} \lambda_d^-\right) \leqslant 1 \leqslant \sum_{\substack{\mathbf{m}\in\mathbb{N}^n\\ m_i\mid n_i}} \left(\prod_{i=1}^n \frac{\widehat{f}_i(m_i)}{f_i(m_i)}\right) \left(\sum_{d\mid m_1\cdots m_n} \lambda_d^+\right).$$

Each d in the sum can be written uniquely as $d_1 \cdots d_n$, where $d_i | m_i | n_i$, and therefore writing $m_i = d_i d_i^*$ allows us to transform the sums over $\mathbf{m}$ into

$$\sum_{\substack{\mathbf{d}\in\mathbb{N}^n\\ d_i|n_i\\ \gcd(d_i,d_j)=1}} \lambda^{\pm}_{d_1\cdots d_n} \sum_{\substack{\mathbf{m}\in\mathbb{N}^n\\ d_i|m_i\\ m_i|n_i}} \left(\prod_{i=1}^n \frac{\widehat{f}_i(m_i)}{f_i(m_i)}\right) = \sum_{\substack{\mathbf{d}\in\mathbb{N}^n\\ d_i|n_i\\ \gcd(d_i,d_j)=1}} \lambda^{\pm}_{d_1\cdots d_n} \prod_{i=1}^n \left(\sum_{\substack{d_i^*\in\mathbb{N}\\ d_i^*|\frac{n_i}{d_i}}} \frac{\widehat{f}_i(d_i d_i^*)}{f_i(d_i d_i^*)}\right).$$

Note that $m_i | n_i$ implies that m_i is squarefree and hence $\gcd(d_i, d_i^*) = 1$. By (1) we get

$$\sum_{\substack{d_i^*\in\mathbb{N}\\ d_i^*|\frac{n_i}{d_i}}} \frac{\widehat{f}_i(d_i d_i^*)}{f_i(d_i d_i^*)} = \frac{\widehat{f}_i(d_i)}{f_i(d_i)} \sum_{\substack{d_i^*\in\mathbb{N}\\ d_i^*|\frac{n_i}{d_i}}} \frac{\widehat{f}_i(d_i^*)}{f_i(d_i^*)},$$

and furthermore an easy computation reveals that the sum over d_i^* equals $f_i(\frac{n_i}{d_i})^{-1}$ owing to the definition of $\widehat{f}_i$. One also has that $\gcd(d_i, \frac{n_i}{d_i}) = 1$ since n_i is squarefree, and hence (1) shows that $f_i(n_i) = f_i(d_i) f_i(n_i/d_i)$. We obtain that

$$\frac{\widehat{f}_i(d_i)}{f_i(d_i)} \sum_{\substack{d_i^*\in\mathbb{N}\\ d_i^*|\frac{n_i}{d_i}}} \frac{\widehat{f}_i(d_i^*)}{f_i(d_i^*)} = \frac{\widehat{f}_i(d_i)}{f_i(n_i)},$$

which proves the claim of our proposition in the case that each n_i is squarefree and composed only by primes in $\mathscr{P}_i$.

We shall need (3) to prove our proposition in its full generality. Given any positive integers $k_1, \ldots, k_n$ as in the statement of our proposition, define

$$n_i := \prod_{\substack{p|k_i\\ p\in\mathscr{P}_i}} p.$$

Observe that by (1), (3) and (5) we have $f_i(k_i) = f_i(n_i)$ and hence

$$\prod_{i=1}^n f_i(k_i) = \prod_{i=1}^n f_i(n_i) \leqslant \sum_{d_i|n_i} \lambda^{\pm}_{d_1\cdots d_n} \prod_{i=1}^n \widehat{f}_i(d_i) = \sum_{\substack{d_i|k_i\\ p|d_i\Rightarrow p\in\mathscr{P}_i\\ d_i \text{ squarefree}}} \lambda^{\pm}_{d_1\cdots d_n} \prod_{i=1}^n \widehat{f}_i(d_i),$$

which concludes our proof. ∎

Lemma 4.2. — *Assume that $n \in \mathbb{N}$, $z \in \mathbb{R}_{>D_0}$ and let $P(z) = \prod_{D_0<p\leqslant z} p$. Whenever $\mathbf{k} \in (\mathbb{Z} - \{0\})^n$ with $gcd(k_i, k_j) = 1$ for all $i \neq j$, we have*

$$\prod_{i=1}^n 2^{-\omega(k_i;z)} \geqslant \sum_{\substack{d_i|(k_i,P(z))\\ gcd(d_i,d_j)=1, i\neq j}} \frac{\lambda^{-}_{d_1\cdots d_n}}{\tau(d_1)\cdots\tau(d_n)}.$$

Proof. — Let $\mathscr{P}_i$ be the set of primes in the interval $(D_0, z]$ and define the multiplicative function $f_i(n)$ through

$$f_i(p^m) = \begin{cases} \frac{1}{2} & \text{if } p|P(z), \\ 1 & \text{otherwise,} \end{cases}$$

for all primes p and $m \in \mathbb{N}$. The conditions of Proposition 4.1 are met and it is straightforward to check that

$$\widehat{f}_i(d) = \begin{cases} 2^{-\omega(d)} & \text{if } d|P(z), \\ 0 & \text{otherwise,} \end{cases}$$

something which finalises our proof. ∎

Define for each $i = 1, \dots, n$,

$$\mathscr{A}_i := \langle \Delta_i \rangle (1 + \deg(\Delta_i)) \, \|\mathscr{R}\|_\infty^{\deg(\Delta_i)}$$

and observe that for each $(s,t) \in \mathscr{B}$ and $i = 1, \dots, n$, we have $|\Delta_i(s,t)| \leqslant \mathscr{A}_i B^{\deg(\Delta_i)}$. Injecting Lemma 4.2 into (3.6) produces the following result.

Lemma 4.3. — *Assume that* $\varpi > \frac{\log D_0}{\log B} 100n(n+1)$ *and let us define*

$$\mathscr{D} := \left\{ \mathbf{d} \in \mathbb{N}^n : \begin{array}{l} d_i \leqslant \mathscr{A}_i B^{\deg(\Delta_i)}, \mu(d_i)^2 = 1, p|d_i \Rightarrow p \leqslant B^{\frac{\varpi}{100n(n+1)}}, \\ gcd(d_i, W) = 1, gcd(d_i, d_j) = 1, i \neq j \end{array} \right\}$$

and for $\mathbf{d} \in \mathscr{D}$ *let*

$$M_{\mathbf{d}}^*(B) := \sum_{\substack{(s,t) \in \mathscr{B} \\ d_i | \Delta_i(s,t)}} \prod_{i=1}^n r_i^*(s,t).$$

Then we have

$$N(\pi, B) \gg \sum_{\mathbf{d} \in \mathscr{D}} \frac{\lambda^-_{d_1 \cdots d_n}}{\tau(d_1) \cdots \tau(d_n)} M_{\mathbf{d}}^*(B),$$

where the implied constant is allowed to depend on ϖ.

4.2. Transition to r functions. — Our aim in this section is to replace the r^* functions by functions that are amenable to divisor sum techniques. To this aim let us define for all $(s,t) \in \mathscr{B}$, $i = 1, \dots, n$, and $m \in \mathbb{N}$ with $m|\Delta_i(s,t)$ the function

$$r_i(s,t;m) := \sum_{\substack{k | \Delta_i(s,t)/m \\ \gcd(k,W)=1}} \left(\frac{F_i(s,t)}{k} \right).$$

For any $a \in \mathbb{Z} - \{0\}$, the Jacobi symbol $(\frac{a}{k})$ is multiplicative with respect to k, and therefore, whenever $A \in \mathbb{Z} - \{0\}$, we are provided with

$$\prod_{\substack{p|A \\ p \nmid W}} \left(1 + \left(\frac{a}{p} \right) \right) = \sum_{\substack{m^2 | A \\ \gcd(m,W)=1}} \mu(m) \sum_{\substack{k | A/m^2 \\ \gcd(k,W)=1}} \left(\frac{a}{k} \right),$$

which implies that for all $(s,t)\in\mathscr{B}$ and $i=1,\dots,n$, one has

$$r_i^*(s,t)=\sum_{\substack{m_i^2|\Delta_i(s,t)\\ \gcd(m_i,W)=1}}\mu(m_i)r_i(s,t;m_i^2).$$

Letting

$$\mathscr{M}:=\left\{\mathbf{m}\in\mathbb{N}^n:\ \begin{array}{l} m_i\leqslant \mathscr{A}_i^{1/2}B^{\deg(\Delta_i)/2}, \mu(m_i)^2=\gcd(m_i,W)=1,\\ \gcd(m_i,m_j)=\gcd(m_i,d_j)=1, i\neq j\end{array}\right\}$$

and defining for $(\mathbf{d},\mathbf{m})\in\mathscr{D}\times\mathscr{M}$,

$$S_{\mathbf{d}}(B;\mathbf{m}):=\sum_{\substack{(s,t)\in\mathscr{B}\\ [m_i^2,d_i]|\Delta_i(s,t)}}\prod_{i=1}^n r_i(s,t;m_i^2), \tag{4.1}$$

allows us to infer the validity of

$$M_{\mathbf{d}}^*(B)=\sum_{\mathbf{m}\in\mathscr{M}}\mu(m_1\cdots m_n)S_{\mathbf{d}}(B;\mathbf{m}). \tag{4.2}$$

Let us define for all $Y\in\mathbb{R}_{\geqslant}1$ and $\mathbf{d}\in\mathscr{D}$,

$$M_{\mathbf{d}}(B,Y):=\sum_{\substack{\mathbf{m}\in\mathscr{M}\\ \|\mathbf{m}\|\leqslant Y}}\mu(m_1\cdots m_n)S_{\mathbf{d}}(B;\mathbf{m}).$$

Lemma 4.4. — *We have for all $Y\in\mathbb{R}\cap(1,B^{1/2})$, $\mathbf{d}\in\mathscr{D}$ and any $\varepsilon>0$,*

$$M_{\mathbf{d}}^*(B)=M_{\mathbf{d}}(B,Y)+O_\varepsilon\left(\frac{B^{2+\varepsilon}}{Y}\right).$$

Proof. — Each m_i in (4.2) satisfies $m_i^2\leqslant|\Delta_i(s,t)|\leqslant\mathscr{A}_iB^{\deg(\Delta_i)}$ and hence the familiar estimate $\tau(n)\ll_\varepsilon B^\varepsilon$ shows that

$$M_{\mathbf{d}}^*(B)-M_{\mathbf{d}}(B,Y)\ll B^\varepsilon\sum_{i=1}^n\sum_{\substack{\mathbf{m}\in\mathscr{M}\\ m_i>Y}}L(\mathbf{m}), \tag{4.3}$$

where

$$L(\mathbf{m}):=\sharp\Big\{(s,t)\in\mathbb{Z}^2_{\mathrm{prim}}\cap B\mathscr{R}:m_i^2|\Delta_i(s,t)\Big\}.$$

We next show that $L(\mathbf{m})$ is contained in a union of at most $\ll_\varepsilon B^\varepsilon$ lattices in $\mathbb{Z}^2$ of determinant $m_1^2\cdots m_n^2$. This is trivially the case if there exists a prime p dividing one of the m_i such that $\Delta_i(s,t)\equiv 0\,(\mathrm{mod}\ p^2)$ has no solution with $(s,t)\in\mathbb{Z}^2_{\mathrm{prim}}$. In the opposite case, for each such prime p there exist at most

$$\sharp\{\xi\ \big(\mathrm{mod}\ p^2\big):\Delta_i(\xi,1)\equiv 0\ \big(\mathrm{mod}\ p^2\big)\ \text{ or }\ \Delta_i(1,\xi)\equiv 0\ \big(\mathrm{mod}\ p^2\big)\}\ll_\varepsilon B^\varepsilon$$

values of ξ such that all (s,t) in the aforementioned set belong in the lattice determined by the condition $s\equiv\xi t\,(\mathrm{mod}\ p^2)$ or $t\equiv\xi s\,(\mathrm{mod}\ p^2)$ and whose determinant is p^2. Noting

that $\mathbf{m} \in \mathscr{M}$ and hence the integers m_i are coprime in pairs, we can combine these lattices in a single lattice Λ of determinant $m_1^2 \cdots m_n^2$. The estimate

$$\sharp\Big\{\mathbb{Z}^2 \cap \Lambda \cap B\mathscr{R}\Big\} \ll \frac{B^2 \operatorname{vol}(\mathscr{R})}{|\det(\Lambda)|} + 1$$

reveals that

$$L(\mathbf{m}) \ll_\varepsilon B^\varepsilon \left(\frac{B^2}{m_1^2 \cdots m_n^2} + 1\right),$$

which, once injected into (4.3), provides the proof of our lemma by virtue of the fact that

$$m_i \leqslant \mathscr{A}_i^{1/2} B^{\deg(\Delta_i)/2}$$

for each $\mathbf{m} \in \mathscr{M}$. ■

Our aim in §5 is to evaluate the sums $S_{\mathbf{d}}(B; \mathbf{m})$. We choose to state the end result of §5 here and explore its implications regarding $M_{\mathbf{d}}^*(B)$ immediately.

Before stating the result some notation is required. Let us introduce the following set of multiplicative functions

$$\mathscr{U} := \Big\{f : \mathbb{N} \to \mathbb{R}_{>0} : f(n) = \prod_{p|n}(1 + g(p)) \text{ where } g(p) \ll_f p^{-1}\Big\}.$$

Notice that $\mathscr{U}$ is a group under pointwise multiplication with identity given by the constant function $f(n) = 1$. Furthermore, for each element $f \in \mathscr{U}$ there exists $a > 0$, such that for all $\varepsilon > 0$ we have

$$f(n) \ll \tau(n)^a \ll_\varepsilon n^\varepsilon. \tag{4.4}$$

We shall find it convenient to define for each $m \in \mathbb{N}$ and $f \in \mathscr{U}$ the function

$$f(n, m) = \sum_{\substack{d|n \\ \gcd(d,m)=1}} \mu(d)^2 g(d), \tag{4.5}$$

notice that for all $(f(n), m) \in \mathscr{U} \times \mathbb{N}$ we have $f(n, m) \in \mathscr{U}$. It is straightforward to verify

$$f\left(\prod_{i=1}^r n_i\right) = f(n_1) \prod_{i=2}^r f\left(n_i, \prod_{j=1}^{i-1} n_j\right) \tag{4.6}$$

for all $\mathbf{n} \in \mathbb{N}^r$ and $f \in \mathscr{U}$, while the property

$$f(\gcd(n, m)) = \frac{f(n)f(m)}{f(nm)} \quad (n, m \in \mathbb{N}, f \in \mathscr{U}), \tag{4.7}$$

is obviously valid.

Let us define for all $d \in \mathbb{N}$ coprime to W and each $i = 1, \dots, n$,

$$\tau_i(d) := \sum_{\substack{\xi \pmod d \\ \Delta_i(\xi,1) \equiv 0 \pmod d}} 1, \qquad \varrho_i(d) := \sum_{\substack{\xi \pmod d \\ \Delta_i(\xi,1) \equiv 0 \pmod d}} \left(\frac{F_i(\xi, 1)}{d}\right).$$

Extending both functions to $\mathbb{N}$ by letting them vanish when the argument has a prime divisor $p \leqslant D_0$, allows one to show that both τ_i and ϱ_i are multiplicative. Assuming that D_0 is large enough, Hensel's lemma can be utilised to prove that for all primes $p > D_0$ and $k \in \mathbb{N}$ we have

$$|\varrho_i(p^k)| \leqslant \tau_i(p^k) = \tau_i(p) \leqslant \deg(\Delta_i),$$

and therefore there exists $A_i > 1$ such that for all $\varepsilon > 0$ and $d \in \mathbb{N}$, the estimates

$$\tau_i(d), \varrho_i(d) \ll \tau(d)^{A_i} \ll_\varepsilon d^\varepsilon \tag{4.8}$$

hold. Defining the arithmetic functions

$$\sigma_i(d) := \prod_{p|d} \left(\tau_i(p) + \sum_{k=0}^{\infty} \varrho_i(p^{k+1}) p^{-k} \right) \quad \text{and} \quad \tau_i^\sharp(d) := \prod_{p|d} \left(\tau_i(p) + \sum_{k=1}^{\infty} \varrho_i(p^k) p^{-k} \right), \tag{4.9}$$

enables us to state the main result of §5.

Theorem 4.5. — *There exist functions $g_i, h_i \in \mathscr{U}$ and a positive constant c, such that for each $(\mathbf{d}, \mathbf{m}) \in \mathscr{D} \times \mathscr{M}$, we have*

$$S_{\mathbf{d}}(B; \mathbf{m}) = cB^2 \left(\prod_{i=1}^{n} \frac{\sigma_i(d_i)}{g_i(d_i) d_i} \right) \left(\prod_{i=1}^{n} \frac{\tau_i^\sharp(m_i/gcd(d_i, m_i))}{h_i(m_i, d_i) m_i^2 gcd(d_i, m_i)^{-1}} \right) + O\Big(\|\mathbf{d}\|^n B^{\frac{19}{20}} \Big),$$

where the implied constant is independent of $B, \mathbf{d}$ and $\mathbf{m}$.

Using Theorem 4.5 we can now deduce the following result.

Proposition 4.6. — *There exist $u_i \in \mathscr{U}, c' > 0$, such that one has for all $\mathbf{d} \in \mathscr{D}$,*

$$M_{\mathbf{d}}^*(B) = c' B^2 \left(\prod_{i=1}^{n} \frac{\sigma_i(d_i)}{d_i} u_i(d_i) \right) + O\Big(\|\mathbf{d}\|^n B^{2 - \frac{1}{50n}} \Big),$$

where the implied constant is independent of B and $\mathbf{d}$.

Proof. — Letting

$$A(\mathbf{d}) = \sum_{\substack{\mathbf{m} \in \mathscr{M} \\ \|\mathbf{m}\| \leqslant Y}} \mu(m_1 \cdots m_n) \prod_{i=1}^{n} \frac{\tau_i^\sharp(m_i/\gcd(d_i, m_i))}{h_i(m_i, d_i) m_i^2} \gcd(d_i, m_i),$$

and using Lemma 4.4 with $Y = B^{\frac{1}{20(1+n)}}$, allows us to infer upon employing Proposition 4.5, that $M_{\mathbf{d}}^*(B)$ equals

$$cB^2 \left(\prod_{i=1}^{n} \frac{\sigma_i(d_i)}{g_i(d_i) d_i} \right) A(\mathbf{d}), \tag{4.10}$$

up to an admissible error term. Define the constants

$$\eta(p) = \sum_{i=1}^{n} \frac{\tau_i^\sharp(p)}{h_i(p)} \quad \text{and} \quad \eta_j(p) = p + \sum_{i \neq j} \frac{\tau_i^\sharp(p)}{h_i(p)}.$$

Using (4.8) provides the estimate

$$\sum_{m>Y}\frac{\tau_i^\sharp(m/\gcd(d,m))}{h_i(m,d)m^2}\gcd(d,m)\ll_\varepsilon \sum_{m>Y}\frac{m^\varepsilon}{m^2}\gcd(d,m)\ll_\varepsilon d^\varepsilon Y^{\varepsilon-1},$$

which shows that the condition $\|\mathbf{m}\|\leqslant Y$ in $A(\mathbf{d})$ can be removed harmlessly. We therefore end up with a series whose Euler product is

$$\prod_{p\nmid W}\Big(1-\frac{\eta(p)}{p^2}\Big)\prod_{i=1}^n\prod_{p\mid d_i}\frac{1-\frac{\eta_i(p)}{p^2}}{1-\frac{\eta(p)}{p^2}}=c''\prod_{i=1}^n h_i'(d_i),\ \text{say.}$$

The estimates $\eta(p)\ll 1$ and $\eta_i(p)\ll p$ imply that, once W is enlarged, we can safely assume $c''>0$ and $h_i'\in\mathscr{U}$. Letting $c'=cc''$ and $u_i=h_i'/g_i$ completes our proof. ■

5. Evaluation of the ensuing divisor sums

Our aim in §5 is to prove Theorem 4.5.

5.1. Auxiliary results. — We may use Hensel's lemma to deduce that for all $\nu\in\mathbb{N}$ and primes $p>D_0$,

$$\varrho_i(p^\nu)=\begin{cases}\varrho_i(p) & \text{if } \nu \text{ is odd,}\\ \tau_i(p) & \text{otherwise,}\end{cases}\tag{5.1}$$

from which we infer that the function

$$R_i(p,z):=\sum_{\nu=1}^\infty \varrho_i(p^\nu)z^\nu,\tag{5.2}$$

defined for $z\in\mathbb{C}$ with $|z|\leqslant 2^{-1/2}$ and primes p, satisfies

$$R_i(p,z)=z\frac{\varrho_i(p)+z\tau_i(p)}{1-z^2}.\tag{5.3}$$

We can similarly prove the identity

$$\sigma_i(p)=\tau_i(p)+\varrho_i(p)+\frac{p\tau_i(p)+\varrho_i(p)}{p^2-1}.\tag{5.4}$$

For a fixed $i=1,\dots,n$ we let $c=\Delta_i(1,0)$ and we immediately see that $\theta:=\theta_i/\Delta_i(1,0)$ is a root of the irreducible integer polynomial $\Delta_i(x,c)/c$, and hence an algebraic integer. Therefore, letting

$$k=\mathbb{Q}(\theta)\text{ and }K=\mathbb{Q}(\theta,\sqrt{F_i(\theta,c)}),$$

we see that $\mathbb{Q}(\theta_i)=\mathbb{Q}(\theta)$, thus leading to $[K:k]=2$ via (3.5). The non-trivial irreducible representation of $\mathrm{Gal}(K/k)$ gives rise to the entire Artin L-function

$$L_i(s)=\prod_{\mathfrak{p}\trianglelefteq\mathscr{O}_k}\big(1-\chi(\mathfrak{p})N_k(\mathfrak{p})^{-s}\big)^{-1},$$

that does not vanish at $s=1$ and where $\chi(\mathfrak{p})$ is 0 if $\mathfrak{p}$ is ramified in K and 1 or -1 according to if $\mathfrak{p}$ is split or inert in $\mathscr{O}_K$. Enlarging W allows us to use the well-known principle of Dedekind, according to which, linear factors $x-\xi \in \mathbb{F}_p[x]$ of $\Delta_i(x,c)$ parametrise the linear prime ideals $\mathfrak{p}_\xi$ above p. The map $\mathbb{Z}[\theta]/(p,\theta-\xi) \to \mathscr{O}_k/\mathfrak{p}_\xi\mathscr{O}_k$, given by

$$h(\theta)+(p,\theta-\xi) \mapsto h(\theta)+\mathfrak{p}_\xi\mathscr{O}_k,$$

is an isomorphism, and therefore the image of $F_i(\theta,c)$ is a square in $\mathscr{O}_k/\mathfrak{p}_\xi\mathscr{O}_k \simeq \mathbb{F}_p$ if and only if the prime $\mathfrak{p}_\xi$ splits in K. Noting that $\deg(F_i)$ is even, we are led to

$$\sum_{\substack{\mathfrak{p}|(p)\\ N_k(\mathfrak{p})=p}} \chi(\mathfrak{p}) = \sum_{\substack{\xi (\mathrm{mod}\ p)\\ \Delta_i(\xi,c)\equiv 0 (\mathrm{mod}\ p)}} \left(\frac{F_i(\xi,c)}{p}\right) = \varrho_i(p). \tag{5.5}$$

Letting

$$P_i(s) := \prod_{p\nmid W} \left(1+R_i(p,p^{-s})\right), \tag{5.6}$$

we see that the analytic properties of the function $G_i = P_i L_i^{-1}$ are determined solely by prime ideals with $N_k(\mathfrak{p}) < p^2$. In particular this enables us to show that G_i is holomorphic in the region $\Re(s) > \frac{1}{2}$ and that for any $\varepsilon > 0$ it satisfies $G_i(s) \asymp_\varepsilon 1$ whenever $\Re(s) > \frac{1}{2}+\varepsilon$. We may thus deduce that

$$P_i(1) \neq 0 \tag{5.7}$$

and that for all $\varepsilon > 0$,

$$P_i(s) \ll_\varepsilon |\Im(s)|^{\frac{\deg(\Delta_i)}{2}(1-\Re(s))+\varepsilon}, \text{ whenever } \frac{1}{2} < \Re(s) \leqslant 1, \tag{5.8}$$

the last property being due to the convexity bound [**IK04**, Eq.(5.20)] applied to $L_i(s)$.

Observe that (5.5) and the prime number theorem for the L-function $L_i(s)$ reveal that

$$\sum_{p<z} \frac{\varrho_i(p)}{p} = \sum_{N_k(\mathfrak{p})<z} \frac{\chi(\mathfrak{p})}{N_k(\mathfrak{p})} + b_i + O\left(\frac{1}{\log z}\right) = b_i' + O\left(\frac{1}{\log z}\right), \tag{5.9}$$

for some constants b_i and b_i', both independent of z. We similarly have

$$\tau_i(p) = \sum_{\substack{\mathfrak{p}|(p)\\ N_k(\mathfrak{p})=p}} 1$$

and therefore the prime number theorem for the Dedekind zeta function of k leads to the estimate

$$\sum_{p<z} \frac{\tau_i(p)}{p} = \log\log z + b_i'' + O\left(\frac{1}{\log z}\right), \tag{5.10}$$

for some constant b_i'' independent of z.

5.2. Preparations. — Recall the definition of the divisor sums $S_{\mathbf{d}}(B;\mathbf{m})$, introduced in (4.1). The fact $\Delta_i(s_0,t_0)\neq 0$ guarantees that for each prime p the sequence $\nu_p(\Delta_i(s,t))$ stabilises when $(s,t)\in\mathscr{B}$ and $(s,t)\equiv(s_0,t_0)\,(\mathrm{mod}\ p^n)$ for $n\to\infty$. Therefore enlarging W allows us to define integers W_i, independent of s and t, composed of primes $p\leqslant D_0$ such that if $(s,t)\equiv(s_0,t_0)\,(\mathrm{mod}\ W)$ then $\Delta_i(s,t)^\dagger=|\Delta_i(s,t)|/W_i$. Defining for all $(\mathbf{d},\mathbf{m})\in\mathscr{D}\times\mathscr{M}$, $\mathbf{v}\in(\mathbb{R}_{\geqslant 1})^n$ and ordered $\boldsymbol{\psi}\in\{0,1\}^n$, the entities

$$Q_i:=\left(\frac{\mathscr{A}_iB^{\deg(\Delta_i)}}{m_i^2W_i}\right)^{1/2}, \tag{5.11}$$

$$\mathscr{K}:=\left\{\mathbf{k}\in\mathbb{N}^n:\ \begin{array}{l}1\leqslant k_i\leqslant Q_i,\gcd(k_i,W)=1,\\ \gcd(k_i,d_jm_jk_j)=1,i\neq j\end{array}\right\},$$

$$\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{v})=\bigcap_{i=1}^n\Big\{(s,t)\in\mathbb{R}^2\cap B\mathscr{R}:|\Delta_i(s,t)|\geqslant\psi_iv_im_i^2Q_iW_i\Big\},$$

and

$$\omega_{\boldsymbol{\psi}}(\mathbf{v})=\mathrm{vol}(\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{v})), \tag{5.12}$$

we have the following result.

***Lemma 5.1* (Hyperbola trick).** — *For each $(\mathbf{d},\mathbf{m})\in\mathscr{D}\times\mathscr{M}$ we have*

$$S_{\mathbf{d}}(B;\mathbf{m})=\sum_{\boldsymbol{\psi}\in\{0,1\}^n}\sum_{\substack{\mathbf{k}\in\mathscr{K}\\(1-\psi_i)k_i\neq Q_i}}\sum_{\substack{(s,t)\in\mathscr{B}\cap\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\\q_i|\Delta_i(s,t)}}\prod_{i=1}^n\left(\frac{F_i(s,t)}{k_i}\right),$$

where $q_i=[d_i,k_im_i^2]$.

Proof. — The p-adic stability property alluded to earlier, reveals that for all $(s,t)\in\mathscr{B}$ one has $r_i(s,t;m_i^2)=r_i(s,t;m_i^2W_i)$, and hence letting

$$r_i^{(0)}(s,t)=\sum_{\substack{k_i|\frac{\Delta_i(s,t)}{m_i^2W_i}\\k_i<Q_i}}\left(\frac{F_i(s,t)}{k_i}\right)\quad\text{and}\quad r_i^{(1)}(s,t)=\sum_{\substack{k_i^*|\frac{\Delta_i(s,t)}{m_i^2W_i}\\k_i^*\leqslant\frac{|\Delta_i(s,t)|}{Q_im_i^2W_i}}}\left(\frac{F_i(s,t)}{k_i^*}\right),$$

we are driven via Proposition 3.2 towards

$$r_i(s,t;m_i^2)=\sum_{k_ik_i^*=\frac{|\Delta_i(s,t)|}{m_i^2W_i}}\left(\frac{F_i(s,t)}{k_i}\right)=r_i^{(0)}(s,t)+r_i^{(1)}(s,t)\,.$$

The proof of our lemma is furnished upon injecting this equality into (4.1) and noticing that $[[d_i,m_i^2],k_im_i^2]=[d_i,k_im_i^2]$ due to the fact that both d_i and m_i are squarefree integers. ∎

Let us define for $\boldsymbol{\psi}\in\{0,1\}^n,\mathbf{k}\in\mathscr{K}$ and $\boldsymbol{\xi}\in\prod_{i=1}^n(\mathbb{Z}/q_i\mathbb{Z})$ the set

$$\mathscr{L}_{\boldsymbol{\psi}}(\mathbf{k},\boldsymbol{\xi}):=\sharp\left\{(s,t)\in\mathbb{Z}^2_{\mathrm{prim}}\cap\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k}):\ \begin{array}{l}(s,t)\equiv(s_0,t_0)\,(\mathrm{mod}\ W)\,,\\ s\equiv\xi_it\,(\mathrm{mod}\ q_i)\end{array}\right\}.$$

***Lemma 5.2* (Partitioning in lattices).** — *For each* $(\mathbf{d},\mathbf{m})\in\mathscr{D}\times\mathscr{M}$ *we have*

$$S_{\mathbf{d}}(B;\mathbf{m})=\sum_{\boldsymbol{\psi}\in\{0,1\}^n}\sum_{\substack{\mathbf{k}\in\mathscr{K}\\(1-\psi_i)k_i\neq Q_i}}\sum_{\substack{\xi_i(\mathrm{mod}\ q_i)\\ \Delta_i(\xi_i,1)\equiv 0(\mathrm{mod}\ q_i)}}\prod_{i=1}^{n}\left(\frac{F_i(\xi_i,1)}{k_i}\right)\mathscr{L}_{\boldsymbol{\psi}}(\mathbf{k},\boldsymbol{\xi})\,.$$

Proof. — As in the beginning of the proof of Lemma 3.1, one sees that $\gcd(q_i,W)=1$ and $q_i|\Delta_i(s,t)$ imply that $s/t\,(\mathrm{mod}\ q_i)$ is well-defined. We deduce that for all (s,t) appearing in the statement of Lemma 5.1 we have $s\equiv\xi_i t\,(\mathrm{mod}\ q_i)$ for all $i=1,\dots,n$, where ξ_i is an integer satisfying the condition $\Delta_i(\xi_i,1)\equiv 0\,(\mathrm{mod}\ q_i)$. The property $k_i|q_i$ validates the equality

$$\left(\frac{F_i(s,t)}{k_i}\right)=\left(\frac{F_i(\xi_i t,t)}{k_i}\right)=\left(\frac{t^{\deg(F_i)}F_i(\xi_i,1)}{k_i}\right),$$

and the fact that $2|\deg(F_i)$ shows that

$$\left(\frac{t^{\deg(F_i)}F_i(\xi_i,1)}{k_i}\right)=\left(\frac{F_i(\xi_i,1)}{k_i}\right),$$

an observation which concludes our proof. ■

5.3. Point counting in primitive lattices. — We call a lattice $G\subset\mathbb{Z}^2$ *primitive* if the only integers fulfilling $G\subset\delta\mathbb{Z}^2$ are $\delta=\pm1$.

Lemma 5.3. — *Let* $\mathbf{A}\in\mathbb{Z}^{2\times 2}$ *be an upper triangular matrix of non-zero determinant and consider the lattice given by* $G=\{\mathbf{Ay}:\mathbf{y}\in\mathbb{Z}^2\}$. *We shall let its determinant and first successive minimum be denoted by* $\det(G)$ *and* $\lambda_1(G)$ *respectively. Assume that* $\mathscr{V}\subset\mathbb{R}^2$ *is a bounded measurable set whose boundary is piecewise differentiable and that* $\mathbf{x}_0\in\mathbb{Z}^2$ *and* $q\in\mathbb{Z}$ *are such that* $gcd(\mathbf{x}_0,q)=1$ *and* $gcd\,(\det(G),q)=1$.

(1) *The estimate*

$$\sharp\Big\{\mathbf{x}\in\mathscr{V}\cap G:\mathbf{x}\equiv\mathbf{x}_0\,(\mathrm{mod}\ q)\Big\}=\frac{\mathrm{vol}(\mathscr{V})}{\det(G)}\frac{1}{q^2}+O\left(1+\frac{\partial(\mathscr{V})}{\lambda_1(G)q}\right)$$

holds with an absolute implied constant.

(2) *If* G *is primitive then the quantity* $\sharp\Big\{\mathbf{x}\in\mathbb{Z}^2_{prim}\cap\mathscr{V}\cap G:\mathbf{x}\equiv\mathbf{x}_0\,(\mathrm{mod}\ q)\Big\}$ *equals*

$$\frac{\mathrm{vol}(\mathscr{V})}{\zeta(2)\det(G)q^2}\prod_{p|\det(G)}\left(1+\frac{1}{p}\right)^{-1}\prod_{p|q}\left(1-\frac{1}{p^2}\right)^{-1}$$

up to an error

$$\ll\frac{\tau(\det(G))}{\lambda_1(G)}\left(\|\mathscr{V}\|_\infty+\frac{\partial(\mathscr{V})}{q}\log\left(1+\|\mathscr{V}\|_\infty\right)+\frac{\mathrm{vol}(\mathscr{V})}{q^2}\frac{1}{1+\|\mathscr{V}\|_\infty}\right),$$

with an absolute implied constant.

Proof. — (1) Defining $\mathbf{y}_0$ through $\det(G)\mathbf{y}_0 \equiv \mathbf{A}^{\mathrm{adj}}\mathbf{x}_0 \pmod q$ and letting $\mathbf{y} = \mathbf{y}_0 + q\mathbf{z}$ we see that the quantity under consideration is $\sharp\{\mathbf{z} \in \mathbb{Z}^2 : \mathbf{A}\mathbf{z} \in (\mathscr{V} - \mathbf{A}\mathbf{y}_0)/q\}$. Our proof is then concluded by observing that the region $(\mathscr{V} - \mathbf{A}\mathbf{y}_0)/q$ has volume $\frac{\mathrm{vol}(\mathscr{V})}{q^2}$ and length of boundary $\frac{\partial(\mathscr{V})}{q}$.
(2) We shall deploy Möbius inversion to detect the coprimality condition and due to $\gcd(\mathbf{x}, q) = 1$ and $\mathbf{x} \equiv \mathbf{x}_0 \pmod q$, we only need to ensure that $\mathbf{x}$ is coprime to integers coprime to q. Sieving out multiples of $\det(G)q$, we see that the quantity under consideration equals

$$\sum_{\substack{m\in\mathbb{N}\\ \gcd(m,\det(G)q)=1}} \mu(m)\sharp\Big\{\mathbf{y} \in \mathbb{Z}^2 : m|\mathbf{M}\mathbf{y}, \gcd(\mathbf{A}\mathbf{y}, \det(G)) = 1, \mathbf{y} \equiv \mathbf{y}_0 \pmod q, \mathbf{A}\mathbf{y} \in \mathscr{V}\Big\}.$$

Due to $\gcd(m, \det(G)) = 1$, the condition $m|\mathbf{A}\mathbf{y}$ is equivalent to $m|\mathbf{y}$ and, letting $\mathbf{y} = m\mathbf{z}$, we obtain

$$\sum_{\gcd(m,\det(G)q)=1} \mu(m)\sharp\Big\{\mathbf{z} \in \mathbb{Z}^2 : \gcd(\mathbf{A}\mathbf{z}, \det(G)) = 1, \mathbf{z} \equiv \overline{m}\mathbf{y}_0 \pmod q, \mathbf{A}\mathbf{z} \in \mathscr{V}/m\Big\}.$$

Notice that in order for the inner quantity to be non-zero we must have $\lambda_1(G) \leqslant \|\mathscr{V}\|_\infty/m$. Removing the condition $\gcd(\mathbf{A}\mathbf{z}, \det(G)) = 1$ reveals that the quantity under consideration equals

$$\sum_{k|\det(G)} \mu(k) \sum_{\substack{m\leqslant\|\mathscr{V}\|_\infty/\lambda_1(G)\\ \gcd(m,\det(G)q)=1}} \mu(m)\sharp\Big\{\mathbf{z} \in \mathbb{Z}^2 : k|\mathbf{A}\mathbf{z}, \mathbf{z} \equiv \overline{m}\mathbf{y}_0 \pmod q, \mathbf{A}\mathbf{z} \in \frac{\mathscr{V}}{m}\Big\}.$$

The set $G(k) := \Big\{\mathbf{A}\mathbf{z} : \mathbf{z} \in \mathbb{Z}^2, k|\mathbf{A}\mathbf{z}\Big\}$ is a sublattice of $G = \Big\{\mathbf{A}\mathbf{z} : \mathbf{z} \in \mathbb{Z}^2\Big\}$, whose first successive minimum $\lambda_1(G(k))$ satisfies $k\lambda(G) \leqslant \lambda(G(k))$, since if $\mathbf{v}$ is a minimal non-zero integer vector of $G(k)$ then $k|\mathbf{v}$ and furthermore $\mathbf{v}/k \in G$. Assume that $\mathbf{A}$ is given by

$$\mathbf{A} = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}. \tag{5.13}$$

We shall prove $\det(G(k)) = k\det(G)$ by making use of (5.13). Indeed, factorising the squarefree integer k, known to divide $\det(G)$, as $k = k_1k_2$, where k_1 has all of the prime factors of k dividing a_1, and using the primitivity of the lattice, makes apparent that the property $k|\mathbf{A}\mathbf{z}$ is equivalent to

$$k_1|z_2 \ \ \& \ \ z_1 \equiv bz_2 \pmod{k_2},$$

where $a_1b \equiv a_2 \pmod{k_2}$. Writing $z_2 = k_1u_1$ and $z_1 = bk_1u_1 + k_2u_2$ for some $\mathbf{u} \in \mathbb{Z}^2$, and bringing into play the matrix

$$\mathbf{A}' := \begin{pmatrix} (a_1b + a_2)k_1 & a_1k_2 \\ a_3k_1 & 0 \end{pmatrix},$$

gives birth to $\mathbf{A}\mathbf{z} = \mathbf{A}'\mathbf{u}$. This equality allows us to acquire the desired result

$$\det(G(k)) = \det(\mathbf{A}') = k\det(G).$$

We next have

$$\begin{aligned}&\sharp\Big\{\mathbf{z}\in\mathbb{Z}^2 : k|\mathbf{Az}, \mathbf{z}\equiv \overline{m}\mathbf{y}_0 \,(\mathrm{mod}\ q)\,, \mathbf{Az}\in \mathscr{V}/m\Big\}\\ =&\sharp\Big\{\mathbf{u}\in\mathbb{Z}^2 : \mathbf{u}\equiv \mathbf{AA}'^{\mathrm{adj}}\overline{a_1a_3km}\mathbf{y}_0 \,(\mathrm{mod}\ q)\,, \mathbf{A}'\mathbf{u}\in \mathscr{V}/m\Big\}\end{aligned}$$

and therefore the first part of the present lemma confirms that

$$\begin{aligned}&\sharp\Big\{\mathbf{x}\in\mathbb{Z}^2_{\mathrm{prim}} : \mathbf{x}\equiv \mathbf{x}_0 \,(\mathrm{mod}\ q)\,, \mathbf{x}\in \mathscr{V}\Big\}\\ =&\sum_{k|\det(G)}\mu(k)\sum_{\substack{m\leqslant \|\mathscr{V}\|_\infty/\lambda_1(G)\\ \gcd(m,\det(G)q)=1}}\mu(m)\left(\frac{\mathrm{vol}(\mathscr{V})}{k\det(G)}\frac{1}{m^2q^2}+O\left(1+\frac{\partial(\mathscr{V})}{\lambda_1(G(k))mq}\right)\right).\end{aligned}$$

Using the inequality $k\lambda_1(G)\leqslant\lambda_1(G(k))$ shows that the error term above is

$$\begin{aligned}&\ll\sum_{k|\det(G)}\sum_{m\leqslant\|\mathscr{V}\|_\infty/\lambda_1(G)}\left(1+\frac{\partial(\mathscr{V})}{\lambda_1(G)qkm}\right)\\ &=\tau(\det(G))\frac{\|\mathscr{V}\|_\infty}{\lambda_1(G)}+\tau(\det(G))\frac{\partial(\mathscr{V})}{\lambda_1(G)q}\log\left(1+\|\mathscr{V}\|_\infty\right),\end{aligned}$$

while the main term equals

$$\begin{aligned}&\frac{\mathrm{vol}(\mathscr{V})}{\det(G)\,q^2}\sum_{k|\det(G)}\frac{\mu(k)}{k}\sum_{\substack{m\leqslant\|\mathscr{V}\|_\infty/\lambda_1(G)\\ \gcd(m,\det(G)q)=1}}\frac{\mu(m)}{m^2}=\\ &\frac{\mathrm{vol}(\mathscr{V})}{\zeta(2)\det(G)\,q^2}\sum_{k|\det(G)}\frac{\mu(k)}{k}\prod_{p|\det(G)q}\left(1-\frac{1}{p^2}\right)^{-1}+O\left(\frac{\mathrm{vol}(\mathscr{V})}{\det(G)}\frac{\lambda_1(G)\tau(\det(\Lambda))}{q^2\|\mathscr{V}\|_\infty}\right),\end{aligned}$$

hence, utilising $\frac{1}{\det(G)}\ll\frac{1}{\lambda_1(G)^2}$ delivers the proof of our claim. ∎

5.4. Error term. — Recall the definition of $\omega_{\boldsymbol{\psi}}$ in (5.12) and define the multiplicative function

$$f_0(k)=\prod_{p|k}\left(1+\frac{1}{p}\right)^{-1}.$$

Lemma 5.4. — *There exists $c_0>0$ such that*

$$\mathscr{L}_{\boldsymbol{\psi}}(\mathbf{k},\boldsymbol{\xi})=c_0\ \omega_{\boldsymbol{\psi}}(\mathbf{k})\prod_{i=1}^{n}\frac{f_0(m_ik_id_i)gcd(d_i,k_im_i)}{m_i^2k_id_i}+O\left(\frac{\tau(m_1^2d_1k_1\dots m_n^2d_nk_n)}{\lambda_1(G_{\mathbf{k}})}B\log B\right),$$

where $G_{\mathbf{k}}$ denotes the lattice

$$G_{\mathbf{k}}:=\Big\{(s,t)\in\mathbb{Z}^2 : s\equiv\xi_it\,(\mathrm{mod}\ k_i)\ \textit{for all } i=1,\dots,n\Big\}.$$

Proof. — By the Chinese remainder theorem there exists an integer ξ such that $q_i|\xi-\xi_i$ for all $i=1,\dots,n$. This shows that $(\xi,1)$ is on the lattice $G_{\mathbf{q}}$, which is therefore primitive. Observing that the condition $s\equiv \xi t \,(\mathrm{mod}\, q_1\cdots q_n)$ is equivalent to (s,t) lying within $\{\mathbf{Ay}:\mathbf{y}\in\mathbb{Z}^2\}$ with

$$\mathbf{A}=\begin{pmatrix} q_1\cdots q_n & \xi \\ 0 & 1\end{pmatrix},$$

allows us to use part (2) of Lemma 5.3 to evaluate $\mathscr{L}_{\boldsymbol{\psi}}(\mathbf{k},\boldsymbol{\xi})$. The main term will be

$$\frac{\omega_{\boldsymbol{\psi}}(\mathbf{k})}{\zeta(2)\det(G_{\mathbf{q}})W^2}\prod_{p|\det(G_{\mathbf{q}})}\Big(1+\frac{1}{p}\Big)^{-1}\prod_{p|W}\Big(1-\frac{1}{p^2}\Big)^{-1},$$

and once we define $c_0:=W^{-2}\prod_{p\nmid W}\left(1-\frac{1}{p^2}\right)$ and use that $\det(G_{\mathbf{q}})=q_1\cdots q_n$, we see that it equals $c_0\omega_{\boldsymbol{\psi}}(\mathbf{k})\frac{f_0(q_1)}{q_1}\cdots\frac{f_0(q_n)}{q_n}$. To show that this is the main term stated in our lemma, observe that the integers d_i and m_i are squarefree, and hence $q_i=m_i^2k_id_i/\gcd(d_i,k_im_i)$, which implies that $f_0(q_i)=f_0(m_ik_id_i)$.

By part (2) of Lemma 5.3 we see that the error term in the present lemma is

$$\ll \frac{\tau(q_1\cdots q_n)}{\lambda_1(G_{\mathbf{q}})}\left(\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty+\frac{\log\left(1+\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty\right)}{W\partial(\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k}))^{-1}}+\frac{\mathrm{vol}(\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k}))}{W^2(1+\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty)}\right),$$

with an absolute implied constant. The inequality $\mathrm{vol}(\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k}))/(1+\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty)\ll B$ is valid when $\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})$ is empty. In the opposite case, there exists some $\mathbf{x}\in\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\subset B\mathscr{R}$, which must necessarily be non-zero, and hence $\|\mathbf{x}\|_\infty\geqslant B\inf\{\|\mathbf{y}\|_\infty:\mathbf{y}\in\mathscr{R}\}\gg B$. This implies that $\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty\gg B$, and therefore $\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\subset B\mathscr{R}$ confirms the validity of

$$\frac{\mathrm{vol}(\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k}))}{1+\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty}\leqslant\frac{\mathrm{vol}(B\mathscr{R})}{1+\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty}\ll B.$$

The region $\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})$ is a subset of the box $B\mathscr{R}$ which is cut out by at most 6 planar curves, each of degree at most 3, namely the curves given by $|\Delta_i(s,t)|=\psi_ik_ie_iQ_iW_i$. This fact reveals that $\partial(\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k}))\ll\partial(B\mathscr{R})\ll B$ and hence

$$\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty+\frac{\partial(\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k}))}{W}\log\left(1+\|\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{k})\|_\infty\right)\ll B\log B.$$

To finish our proof we observe that $\lambda_1(G_{\mathbf{k}})\geqslant\lambda_1(G_{\mathbf{q}})$ can be inferred from $k_i|q_i$. ∎

Define for all $(\mathbf{d},\mathbf{m})\in\mathscr{D}\times\mathscr{M}$, $\boldsymbol{\psi}\in\{0,1\}^n$, the squarefree integers

$$d_i':=\frac{d_i}{\gcd(d_i,m_i)},m_i':=\frac{m_i}{\gcd(d_i,m_i)},d_i'':=\prod_{\substack{p|d_i\\ p\nmid m_ik_i}}p,m_i'':=\prod_{\substack{p|m_i\\ p\nmid k_i}}p$$

and let

$$T_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m}):=\sum_{\substack{\mathbf{k}\in\mathscr{K}\\ (1-\psi_i)k_i\neq Q_i}}\omega_{\boldsymbol{\psi}}(\mathbf{k})\prod_{i=1}^n\frac{\varrho_i(k_i)}{k_i}f_0(k_i,d_im_i)\gcd(k_i,d_i')\tau_i(d_i''m_i'').\tag{5.14}$$

The proof of the following result is inspired by an argument of Daniel [**Dan99**, Lem. 3.2].

Lemma 5.5. — *For each* $(\mathbf{d},\mathbf{m})\in\mathscr{D}\times\mathscr{M}$ *and* $\varepsilon>0$, *we have*

$$S_{\mathbf{d}}(B;\mathbf{m})=c_0\left(\prod_{i=1}^{n}\frac{f_0(d_im_i)}{d_im_i^2}gcd(d_i,m_i)\right)\left(\sum_{\boldsymbol{\psi}\in\{0,1\}^n}T_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})\right)+O_\varepsilon\Big(B^{\frac{7}{4}+\varepsilon}\Big).$$

Proof. — Using (5.1) in conjunction with $\gcd(m_i^2k_i,d_i'')=1$, allows us to procure the validity of

$$\sum_{\substack{\xi_i \pmod{q_i}\\ \Delta_i(\xi_i,1)\equiv 0 \pmod{q_i}}}\left(\frac{F_i(\xi_i,1)}{k_i}\right)=\varrho_i(k_i)\tau_i(d_i''m_i'').$$

The error term in our lemma is of order $\ll_\varepsilon B^{1+\varepsilon}\sum_{k_i\leqslant Q_i}\lambda_1(G_{\mathbf{k}})^{-1}$, as one can deduce upon congregation of Lemmas 5.2, 5.4 and the estimate (4.8). The fact that the integers k_i are coprime in pairs shows that the lattice $G_{\mathbf{k}}$ has determinant $k_1\cdots k_n$. Therefore, by Minkowski's theorem, its first successive minimum satisfies

$$\lambda_1(G_{\mathbf{k}})\ll(k_1\cdots k_n)^{1/2}\ll B^{3/4},$$

from which we immediately infer that the sum over k_i is

$$\ll\sum_{\substack{\mathbf{v}\in\mathbb{Z}^2\\ \Delta(\mathbf{v})\neq 0\\ \|\mathbf{v}\|\ll B^{3/4}}}\frac{1}{\|\mathbf{v}\|}\prod_{i=1}^{n}\tau(|\Delta_i(\mathbf{v})|)+\sum_{\substack{1\leqslant i\leqslant n\\ \deg(\Delta_i)=1}}Q_i.$$

The last term is the contribution of the primitive (due to the minimality property of the first successive minimum) non-zero vectors $\mathbf{v}$ that are zeros of some Δ_i. The number of such vectors is twice the number of linear forms dividing Δ, if any. Observe that if Δ_j is linear then the available values $k_i\leqslant Q_i, i\neq j$, with $\mathbf{v}=\lambda_1(G_{k_1,\dots,k_n})$ are $O(1)$ in cardinality, since $k_i|\Delta_i(\mathbf{v})$ and $\Delta_i(\mathbf{v})\neq 0$ assumes finitely many values. Our proof is now brought into conclusion upon deploying the estimate $\sum_{0<\|\mathbf{v}\|\leqslant z}\|\mathbf{v}\|^{-1}\ll z$. ■

5.5. Main term. — Our aim in this section is to estimate the average $T_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})$. In contrast to all prior treatments of similar sums, we provide a uniform treatment for all $\boldsymbol{\psi}\in\{0,1\}^n$.

Recall the definition of Q_i and $\omega_{\boldsymbol{\psi}}$ provided in (5.11) and (5.12) respectively.

Lemma 5.6. — (1) *For all* $\boldsymbol{\psi}\in\{0,1\}^n$ *we have* $\omega_{\boldsymbol{\psi}}(1,\dots,1)=B^2\operatorname{vol}(\mathscr{R})+O(B^{3/2}\|\mathbf{m}\|)$.
(2) *For all* i *with* $\psi_i\neq 0$ *and each* $v_i\geqslant 1$ *we have*

$$|\omega_{\boldsymbol{\psi}}(\mathbf{v}+\mathbf{e_i})-\omega_{\boldsymbol{\psi}}(\mathbf{v})|\ll B\|\mathbf{m}\|\log B\begin{cases}B^{1/2} & \text{if } \deg(\Delta_i)=1,\\ v_i^{-1+2/\deg(\Delta_i)} & \text{otherwise.}\end{cases}$$

(3) *The support of* $\omega_{\boldsymbol{\psi}}$ *is contained in* $\Big\{\mathbf{v}\in(\mathbb{R}_{\geqslant 1})^n : 1\leqslant v_i\leqslant Q_i \text{ whenever } i\in\operatorname{supp}(\boldsymbol{\psi})\Big\}$.
(4) *For all* $\mathbf{v}$ *we have* $\omega_{\boldsymbol{\psi}}(\mathbf{v})\ll B^2$.

Proof. — (1) Our statement is obvious if $\boldsymbol{\psi} = \mathbf{0}$ and if $\boldsymbol{\psi} \neq \mathbf{0}$ we shall show that for all i in the support of $\boldsymbol{\psi}$ we have, upon denoting $z_i = m_i W_i^{1/2} \mathscr{A}_i^{1/2} B^{\deg(\Delta_i)/2}$, that

$$\operatorname{vol}\left((s,t) \in B\mathscr{R} : |\Delta_i(s,t)| < z_i\right) \ll m_i B^{3/2}. \tag{5.15}$$

Our claim will then follow from

$$\left|\omega_{\boldsymbol{\psi}}(1,\dots,1) - B^2 \operatorname{vol}(\mathscr{R})\right| \leqslant \sum_{i \in \operatorname{supp}(\boldsymbol{\psi})} \operatorname{vol}\left((s,t) \in B\mathscr{R} : |\Delta_i(s,t)| < z_i\right).$$

If $\deg(\Delta_i) \geqslant 3$, then $\beta_i = \operatorname{vol}\left((s,t) \in \mathbb{R}^2 : |\Delta_i(s,t)| < 1\right) < \infty$, and therefore

$$\operatorname{vol}\left((s,t) \in B\mathscr{R} : |\Delta_i(s,t)| < z_i\right) \leqslant \beta_i z_i^{2/\deg(\Delta_i)} \ll m_i B,$$

we can also treat similarly the case when Δ_i is quadratic and irreducible in $\mathbb{R}[s,t]$. If Δ_i is linear, then a linear change of variables shows that

$$\operatorname{vol}\left((s,t) \in B\mathscr{R} : |\Delta_i(s,t)| < z_i\right) \ll B z_i \ll m_i B^{3/2},$$

which is sufficient. The last remaining case is when Δ_i is quadratic and splits over $\mathbb{R}$, in this case it can be transformed into st. Denoting by $\mathscr{R}'$ the image of $\mathscr{R}$ under this transformation, we observe that the volume of $\{(s,t) \in B\mathscr{R}' : |st| < z_i\}$ is

$$\ll \operatorname{vol}\left((s,t) \in B\mathscr{R}' : |s| < 1\right) + |z_i| \int_{1 \leqslant |s| \ll B} \frac{\mathrm{d}s}{|s|} \ll B + m_i B \log B,$$

which is sufficient for our proof.
(2) In the case that $\deg(\Delta_i) \geqslant 3$, we can follow the notation of the proof of part (1) to obtain

$$\operatorname{vol}\left((s,t) \in B\mathscr{R} : v_i \leqslant \frac{|\Delta_i(s,t)|}{z_i} < v_i + 1\right) \leqslant \beta_i z_i^{\frac{2}{\deg(\Delta_i)}} \left((v_i+1)^{\frac{2}{\deg(\Delta_i)}} - v_i^{\frac{2}{\deg(\Delta_i)}}\right),$$

which by the mean value theorem is $\ll B m_i^{2/\deg(\Delta_i)} v_i^{1-2/\deg(\Delta_i)}$. The remaining cases $\deg(\Delta_i) = 1$ or 2, are treated in a similar fashion.
(3) It flows directly from the fact that $|\Delta_i(s,t)| \leqslant \mathscr{A}_i B^{\deg(\Delta_i)}$ for all $(s,t) \in B\mathscr{R}$.
(4) This part is a direct consequence of the inclusion $\mathscr{R}_{\boldsymbol{\psi}}(\mathbf{v}) \subset B\mathscr{R}$. ■

Lemma 5.7. — *Assume that $h \in \mathscr{U}$, b is coprime to W and define $\gamma_i = 2/(4+\deg(\Delta_i))$. Then there exist $W_1 \in W\mathbb{N}, c \in \mathbb{R}_{>0}$ and $h_1 \in \mathscr{U}$, such that for all $0 < \varepsilon < \gamma_i$ and $x > 0$, we have*

$$\sum_{\substack{k \leqslant x \\ gcd(k, bW_1)=1}} \frac{\varrho_i(k)}{k} h(k) = c h_1(b) + O_\varepsilon\left(\frac{(bx)^\varepsilon}{x^{\gamma_i}}\right),$$

where the implied constant is independent of b and x.

Proof. — We shall begin by proving our claim in the case $x \geqslant 1$. Define the arithmetic function $g_k : \mathbb{N} \to \mathbb{R}$ by

$$g_k := \begin{cases} h(k)\varrho_i(k) & \text{if } \gcd(k, bW) = 1, \\ 0 & \text{otherwise} \end{cases}$$

and denote its Dirichlet series by $F_g(s)$. Multiplying W by sufficiently large primes produces a multiple W_1 of W and then by (5.3) we have that for all $z \in \mathbb{C}$ with $|z| \leqslant 2^{-1/2}$ and $p \nmid W_1$ one has $R_i(p,z) \ll |z|$. The fact that $h \in \mathscr{U}$ shows that in the same range for z and for all primes $p \nmid bW_1$, one has

$$\left(\sum_{m=1}^{\infty} g_{p^m} z^m\right)(1+R_i(p,z)))^{-1} = (1+h(p)R_i(p,z))\,(1+R_i(p,z))^{-1} = 1+O\left(\frac{|z|}{p}\right),$$

which reveals that the product

$$\Phi_b(s) := \prod_{p \nmid bW_1} \frac{\sum_{m=1}^{\infty} g_{p^m} p^{-ms}}{1+R_i(p,p^{-s})},$$

defined for all $b \in \mathbb{N}$ with $\gcd(b,W)=1$, converges absolutely in the region $\Re(s) > \frac{1}{2}$. The bound

$$\frac{\sum_{m=1}^{\infty} g_{p^m} p^{-ms}}{1+R_i(p,p^{-s})} = 1+O(p^{-3/2})$$

then proves that $\Phi_b(s)$ has no zero in the same region.

Recalling definition (5.6) enables us to see that the following factorisation is valid in the region $\Re(s) > 1$,

$$F_g(s) = \Phi_b(s)P_i(s)\prod_{p|b}\left(1+R_i(p,p^{-s})\right)^{-1},$$

and therefore by analytic continuation it is also valid for $\Re(s) > \frac{1}{2}$. This shows that F_g may be extended to $\Re(s) > \frac{1}{2}$ and that, owing to (5.8), it satisfies the bound

$$F_g(s) \ll_{\varepsilon} b^{\varepsilon}(1+|\Im(s)|)^{\frac{\deg(\Delta_i)}{2}(1-\Re(s))+\varepsilon}, \frac{1}{2} < \Re(s) < 1. \tag{5.16}$$

Enlarging W ensures that the quantities

$$c = \prod_{p \nmid W}\left(1+h(p)R_i(p,p^{-1})\right), h_1(n) = \prod_{p|n}\left(1+h(p)R_i(p,p^{-1})\right)^{-1}$$

satisfy $c > 0$ and $h_1 \in \mathscr{U}$, once the factorisation $c = \Phi_1(1)P_i(1)$ and (5.7) have been combined. Letting $G(x) := \sum_{k \leqslant x} g_k$, a computation involving Euler products reveals that the constant $F_g(1) = \sum_{k=1}^{\infty} g_k/k = \int_1^{\infty} G(u)/u^2 \mathrm{d}u$ equals $ch_1(b)$.

Our aim for the rest of this proof is to show that $G(x) \ll_{\varepsilon} b^{\varepsilon}x^{1-\gamma_i+\varepsilon}$, by partial summation this would be sufficient for our lemma. The fact that $F_g(s)$ converges for $\Re(s) > \frac{1}{2}$ immediately proves such an estimate, save for the dependence on b. However, Making this dependence explicit is the main point of our lemma; this requirement makes using contour integration indispensable.

Letting $x \geqslant 1$ be a half-integer and using [**MV07**, Cor.5.3] with $\sigma_0 = 1+1/\log x$ and $T = x^{\gamma_i}$, gives

$$G(x) = \frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} F_g(s)\frac{x^s}{s}\mathrm{d}s + O\left(R_0(\max_{k\leqslant 2x}|g_k|) + \frac{x}{T}\sum_{k=1}^{\infty}\frac{|g_k|}{k^{\sigma_0}}\right),$$

where

$$R_0 := \sum_{\substack{\frac{x}{2}<n<2x \\ n\neq x}} \min\left(1, \frac{x}{T|x-n|}\right)$$

satisfies $R_0 \ll 1 + \frac{x\log x}{T}$, as shown for example in [**MV07**, p.g. 180]. By (4.4) and (4.8) we deduce that there exists $A > 0$ such that

$$|\varrho_i(k)h(k)| \ll \tau(k)^A.$$

This shows that

$$\sum_{k=1}^{\infty} \frac{|g_k|}{k^{\sigma_0}} \ll \zeta(\sigma_0)^{2^A},$$

and therefore the bound $\zeta(1+\delta) \ll \delta^{-1}$, valid for all $\delta > 0$, yields

$$G(x) = \frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} F_g(s)\frac{x^s}{s}\mathrm{d}s + O_\varepsilon\left(\frac{x^{1+\varepsilon}}{T}\right). \tag{5.17}$$

Taking advantage of the fact that F_g has no poles in the rectangle enclosed by the points $\sigma_0 \pm iT$ and $\frac{1}{2} + \varepsilon \pm iT$ we may replace the vertical line of integration in (5.17) by two horizontal and a vertical line. An easy computation that makes use of (5.16) allows us to provide satisfactory upper bounds for the contribution coming from the three remaining segments, thus finalising the proof in the range $x \geqslant 1$. In the remaining case $0 < x < 1$ we notice that the sum over k in the statement of our lemma contains no terms and therefore the estimates $c \ll 1$ and $h(b) \ll_\varepsilon b^\varepsilon$ prove that our claim remains valid in the region $x < 1$. ■

Our next result regards averages of certain non-multiplicative functions that will appear in the forthcoming estimation of $T_{\mathbf{d},\psi}(B;\mathbf{m})$. Recall definition (4.9).

Lemma 5.8. — *Suppose we are given a function $h \in \mathscr{U}$ and integers d, m and k_0 satisfying*

$$1 = gcd(k_0, dm) = gcd(k_0 dm, W) = \mu(d)^2 = \mu(m)^2$$

and define the integers

$$d' = \prod_{\substack{p|d \\ p\nmid m}} p, m' = \prod_{\substack{p|m \\ p\nmid d}} p.$$

There exist $h_j \in \mathscr{U}$ and a constant $c > 0$ such that for all $0 < \varepsilon < \gamma_i, x \geqslant 1$, we have

$$\sum_{\substack{k\leqslant x \\ gcd(k,Wk_0)=1}} \frac{\varrho_i(k)}{k} h(k, dm')\tau_i\left(\frac{dm'}{gcd(k, dm')}\right) gcd(k, d') =$$

$$ch_1(k_0)h_2(d)h_3(m')\sigma_i(d)\tau_i^\sharp(m') + O_\varepsilon\left(\frac{(dmk_0x)^\varepsilon}{x^{\gamma_i}}\right).$$

Proof. — Writing $\delta_1=\gcd(k,d),\delta_2=\gcd(k,m')$ transforms our sum into

$$\sum_{\substack{\delta_1|d\\ \delta_2|m'}}\tau_i\left(\frac{d}{\delta_1}\right)\tau_i\left(\frac{m'}{\delta_2}\right)\delta_2^{-1}\sum_{\substack{l\leqslant x/(\delta_1\delta_2)\\ \gcd(l,Wk_0dm'/(\delta_1\delta_2))=1}}\frac{\varrho_i(\delta_1\delta_2 l)}{l}h(l,\delta_1\delta_2).$$

For each $\delta\in\mathbb{N}$ we define the set $\mathbb{M}(\delta)\subset\mathbb{N}$ comprising of all positive integers whose prime factors divide δ and we allow $1\in\mathbb{M}(\delta)$. Then each natural l can be decomposed uniquely as $l=l_1l_2l'$ where $l_j\in\mathbb{M}(\delta_j)$ and l' is coprime to $\delta_1\delta_2$, thus leading to the equality of the sum over l with

$$\sum_{l_j\in\mathbb{M}(\delta_j)}\frac{\varrho_i(\delta_1l_1)}{l_1}\frac{\varrho_i(\delta_2l_2)}{l_2}\sum_{\substack{l'\leqslant x/(l_1l_2)\\ \gcd(l',Wk_0dm')=1}}\frac{\varrho_i(l')}{l'}h(l').$$

Lemma 5.7 provides a function $h_1\in\mathscr{U}$, a constant $c>0$ and a multiple of W, which we identify here with W itself, such that the sum over l' equals

$$ch_1(k_0dm')+O_\varepsilon\left(\frac{(k_0dmx)^\varepsilon}{x^{\gamma_i}}(l_1l_2)^{\gamma_i}\right).$$

The estimate (4.8) reveals the validity of $\varrho_i(\delta_jl_j)\ll_\varepsilon(\delta_jl_j)^\varepsilon\leqslant(dml_j)^\varepsilon$. This shows that

$$\sum_{l_j\in\mathbb{M}(\delta_j)}\frac{\varrho_i(\delta_1l_1)}{l_1}\frac{\varrho_i(\delta_2l_2)}{l_2}\ll_\varepsilon(dm)^{2\varepsilon}\prod_{p|\delta_1\delta_2}\frac{1}{1-p^{\varepsilon-1}},$$

and the proof of our lemma follows upon noting that

$$\sum_{l_j\in\mathbb{M}(\delta_j)}\frac{\varrho_i(\delta_jl_j)}{l_j}=\prod_{p|\delta_j}\left(\sum_{k=0}^{\infty}\frac{\varrho_i(p^{k+1})}{p^k}\right),j=1,2.$$

■

Recall (5.14) and define

$$T^\natural_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m}):=\sum_{\mathbf{k}\in\mathscr{K}}\omega_{\boldsymbol{\psi}}(\mathbf{k})\prod_{i=1}^n\frac{\varrho_i(k_i)}{k_i}f_0(k_i,d_im_i)\gcd(k_i,d_i')\tau_i(d_i''m_i''). \tag{5.18}$$

One has

$$T^\natural_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})-T_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})=\sum_{\mathbf{k}\in\mathscr{K}}{}^*\omega_{\boldsymbol{\psi}}(\mathbf{k})\prod_{i=1}^n\frac{\varrho_i(k_i)}{k_i}f_0(k_i,d_im_i)\gcd(k_i,d_i')\tau_i(d_i''m_i''),$$

where $\sum^*$ is over $\mathbf{k}$ with $k_i=Q_i$ if $\psi_i=0$ and $1\leqslant k_i\leqslant Q_i$ if $\psi_i=1$. The third part of Lemma 5.6 in conjunction with (4.8) then leads to

$$T^\natural_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})-T_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})\ll_\varepsilon\|\boldsymbol{\psi}\|B^{\frac{3}{2}+\varepsilon}\|\mathbf{d}\|^n. \tag{5.19}$$

A gambit is on offer in the proof of the ending lemma of the present section; we use iterated partial summation instead of the more natural multidimensional partial summation to deal with the factor $\omega_{\boldsymbol{\psi}}(\mathbf{k})$ present in $T_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})$. While this approach complicates the

argument, it has the advantage of providing a uniform treatment for all vectors $\boldsymbol{\psi}$ and forms Δ_i.

Lemma 5.9. — *There exist $c_1 > 0$ and multiplicative functions $\mathbb{A}_{j,i} \in \mathscr{U}$, such that*

$$T^{\natural}_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m}) = c_1 B^2 \left(\prod_{i=1}^{n} \mathbb{A}_{1,i}(d_i)\sigma_i(d_i)\, \tau_i^{\sharp}(m_i')\, \mathbb{A}_{2,i}(m_i,d_i) \right) + O\Big(\|\mathbf{m}\| B^{\frac{19}{20}} \Big),$$

where the implied constant is independent of $B, \mathbf{d}, \mathbf{m}$ and $\boldsymbol{\psi}$.

Proof. — Letting $\mathscr{K}_i = \Big\{ k_i \in \mathbb{N} \cap [1, Q_i] : \gcd(k_i, W\prod_{j<i} d_j m_j k_j) = 1 \Big\}$ allows us to express $T^{\natural}_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})$ in the form

$$\sum_{k_1 \in \mathscr{K}_1} \frac{\varrho_1(k_1) f_0(k_1, d_1 m_1) \tau_1(d_1'' m_1'')}{\gcd(k_1, d_1')^{-1} k_1} \cdots \sum_{k_n \in \mathscr{K}_n} \frac{\varrho_n(k_n) f_0(k_n, d_n m_n) \tau_n(d_n'' m_n'')}{\gcd(k_n, d_n')^{-1} k_n} \omega_{\boldsymbol{\psi}}(\mathbf{k}). \tag{5.20}$$

Let us note that for all $\mathbb{A} \in \mathscr{U}$ and $d, m, k \in \mathbb{Z}$, the identity

$$\mathbb{A}(dmk) = \mathbb{A}(d)\mathbb{A}(m,d)\mathbb{A}(k,dm) \tag{5.21}$$

holds due to (4.6). We shall make repeated use of Lemma 5.7 to study the sum over $k_n, k_{n-1}, \dots, k_1$ and at every step of this process, products of multiplicative functions in $\mathscr{U}$ evaluated at several combinations of products and quotients of the integers d_i, m_i, k_i and $\gcd(d_i, m_i)$ will enter the stage. Therefore, using the coprimality conditions imprinted in the definitions of $\mathscr{D}, \mathscr{M}, \mathscr{K}$ and (4.7), we shall always use of (5.21) and the group law in $\mathscr{U}$ to rewrite these terms in the succinct form

$$\left(\prod_{i=1}^{n} \mathbb{A}_{1,i}(d_i) \right) \left(\prod_{i=1}^{n} \mathbb{A}_{2,i}(m_i, d_i) \right) \left(\prod_{i=1}^{n} \mathbb{A}_{3,i}(k_i, d_i m_i) \right), \tag{5.22}$$

for some $\mathbb{A}_{i,j} \in \mathscr{U}$. While at each successive stage the values of the functions $\mathbb{A}_{i,j}$ will vary, this will, however, leave unspoilt the validity of our lemma.

We begin by applying Lemma 5.8 for $i = n$, $d = d_n$, $m = m_n$ and

$$k_0 = \prod_{i=1}^{n-1} d_i m_i k_i.$$

Denoting for all $t \in \mathbb{R} \cap [1, 2Q_n]$,

$$S(t) := \sum_{\substack{k_n \leqslant t \\ \gcd(k_n, W k_0) = 1}} \frac{\varrho_n(k_n) f_0(k_n, d_n m_n) \tau_n(d_n'' m_n'')}{\gcd(k_n, d_n')^{-1} k_n},$$

and taking under consideration the inequalities $d_i, m_i, k_i \ll B^n$ we deduce that

$$S(t) = c_n \sigma_n(d_n)\, \tau_n^{\sharp}(m_n')\, \gamma + O_{\varepsilon}\big(B^{\varepsilon} t^{-\gamma_n} \big),$$

where

$$\gamma = h_1 \left(\prod_{j \neq n} d_j m_j k_j \right) h_2(d_n) h_3(m_n, d_n)$$

for a constant $c_n > 0$ and functions $h_i \in \mathscr{U}$, all of which are independent of B, d_i, m_i and k_i. The integers $d_i m_i k_i$ are coprime in pairs, and hence letting

$$\mathbb{A}_{1,i} = \mathbb{A}_{2,i} = \mathbb{A}_{3,i} = h_1, i \neq n \text{ and } \mathbb{A}_{1,n} = h_2, \mathbb{A}_{2,n} = h_3, \mathbb{A}_{3,n} = 1,$$

allows us to see that γ is of the shape (5.22).

Define for fixed $k_1, \dots, k_{n-1}$ the function $\omega_n(x) := \omega_{\boldsymbol{\psi}}(k_1, \dots, k_{n-1}, x)$ and denote by $S_\omega(t)$ the sum one obtains by replacing $\varrho_n(k_n)$ in the definition of $S(t)$ by $\varrho_n(k_n)\omega_n(k_n)$. If $\psi_n = 0$ then the definition of $\omega_{\boldsymbol{\psi}}(\mathbf{v})$ implies

$$S_\omega(Q_n) = \omega_{(\psi_1,\dots,\psi_{n-1},0)}(k_1, \dots, k_{n-1}, 1)S(Q_n),$$

while if $\psi_n = 1$ then letting $z := [Q_n] + 1$ and observing that $\omega_n(z) = 0$, by part (3) of Lemma 5.6 and the discrete version of partial summation we are provided with

$$S_\omega(Q_n) = \sum_{\substack{t\in\mathbb{N}\\ 1\leqslant t\leqslant z-1}} S(t)(\omega_n(t) - \omega_n(t+1)),$$

which equals

$$\omega_n(1)c_n\sigma_n(d_n)\,\tau_n^\sharp(m_n')\,\gamma + O_\varepsilon\left(B^\varepsilon \sum_{\substack{t\in\mathbb{N}\\ 1\leqslant t\leqslant z-1}} \frac{|\omega_n(t+1) - \omega_n(t)|}{t^{\gamma_n}}\right).$$

Employing part (2) of Lemma (5.6) for $i = n, \mathbf{v} = (k_1, \dots, k_{n-1}, t)$ and letting

$$\omega_{n-1}(t) = \omega_{(\psi_1,\dots,\psi_{n-1},0)}(k_1, \dots, k_{n-2}, t, 1),$$

a simple computation reveals that

$$S_\omega(Q_n) = \omega_{n-1}(k_{n-1})c_n\sigma_n(d_n)\,\tau_n^\sharp(m_n')\,\gamma + O_\varepsilon\left(\|\mathbf{m}\|B^{1+\frac{4}{4+\deg(\Delta_n)}+\varepsilon}\right),$$

regardless of the value of ψ_n. Letting

$$\gamma' = c_n\sigma_n(d_n)\,\tau_n^\sharp(m_n')\left(\prod_{i=1}^n \mathbb{A}_{1,i}(d_i)\right)\left(\prod_{i=1}^n \mathbb{A}_{2,i}(m_i, d_i)\right)$$

and noting that $S_\omega(Q_n)$ is the sum over k_n in (5.20), we deduce that, up to an admissible error term, $T^\natural_{\mathbf{d},\boldsymbol{\psi}}(B;\mathbf{m})$ equals

$$\gamma' \sum_{k_1\in\mathscr{K}_1} \frac{\varrho_1(k_1)}{k_1}\tau_1(d_1''m_1'')\gcd(k_1, d_1')(\mathbb{A}_0\mathbb{A}_{3,1})(k_1, d_1m_1)\dots \sum_{k_{n-1}\in\mathscr{K}_{n-1}} \frac{\varrho_{n-1}(k_{n-1})}{k_{n-1}}\times$$
$$\times\, \tau_1(d_{n-1}''m_{n-1}'')\gcd(k_{n-1}, d_{n-1}')(\mathbb{A}_0\mathbb{A}_{3,n-1})(k_{n-1}, d_{n-1}m_{n-1})\omega_{n-1}(k_{n-1}).$$

Repeating this process inductively to evaluate the sum over $k_{n-1}, \dots, k_1$, yields the desired result upon using part (1) of Lemma 5.6. ■

Perusing (5.19), Lemmas 5.5, 5.9, and letting

$$c = 2^n c_0 c_1, g_i = (\mathbb{A}_0\mathbb{A}_{1,i})^{-1}, h_i = (\mathbb{A}_0\mathbb{A}_{2,i})^{-1},$$

allows us to achieve the anticipated catharsis of the verification of Theorem 4.5.

6. Employing the Rosser–Iwaniec sieve

We shall make use of the *Fundamental lemma of sieve theory*; we choose to employ the version of the lemma supplied in [**IK04**, Lem. 6.3].

Lemma 6.1 **(Fundamental lemma of sieve theory).** — *Let $\kappa > 0$ and $y > 1$. There exist two sets of real numbers $\Lambda^+ = (\lambda_d^+)$ and $\Lambda^- = (\lambda_d^-)$ depending only on κ and y with the following properties:*

$$\lambda_1^\pm = 1, \tag{6.1}$$

$$|\lambda_d^\pm| \leqslant 1 \text{ if } 1 < d < y, \tag{6.2}$$

$$\lambda_d^\pm = 0 \text{ if } d \geqslant y, \tag{6.3}$$

and for any integer $n > 1$,

$$\sum_{d|n} \lambda_d^- \leqslant 0 \leqslant \sum_{d|n} \lambda_d^+. \tag{6.4}$$

Moreover, for any multiplicative function $g(d)$ with $0 \leqslant g(p) < 1$ and satisfying the dimension condition

$$\prod_{w \leqslant p < z} (1 - g(p))^{-1} \leqslant \left(\frac{\log z}{\log w}\right)^\kappa \left(1 + \frac{K}{\log w}\right) \tag{6.5}$$

for all $2 \leqslant w < z \leqslant y$ we have

$$\sum_{d|P(z)} \lambda_d^\pm g(d) = \left(1 + O\left(e^{-1/\varpi}\left(1 + \frac{K}{\log z}\right)^{10}\right)\right) \prod_{p<z} (1 - g(p)), \tag{6.6}$$

where $P(z)$ denotes the product of all primes $p < z$ and $\varpi = \log z / \log y$, the implied constant depending only on κ.

Lemma 4.3 and Proposition 4.6 show that if λ_d^- is chosen with respect to $y = B^{\frac{1}{100n(n+1)}}$ then

$$N(\pi, B) \gg B^2 \sum_{\mathbf{d} \in \mathscr{D}} \lambda^-_{d_1 \cdots d_n} \prod_{i=1}^n \frac{\sigma_i(d_i)}{\tau(d_i) d_i} u_i(d_i),$$

where we have made use of (6.2),(6.3) and $\sum_{d_1 \cdots d_n \leqslant y} \|\mathbf{d}\|^n \ll y^{n+1+\varepsilon}$. Therefore Theorem 1.1 would follow from proving that the sum over $\mathbf{d}$ is $\gg (\log B)^{-n/2}$. We shall do so by applying Lemma 6.1 and we begin by verifying its assumptions.

Defining the multiplicative function

$$g(d) = \frac{\mu(d)^2}{d\tau(d)} \mathbf{1}_W(d) \sum_{\substack{\mathbf{d} \in \mathbb{N}^n \\ d_1 \cdots d_n = d \\ \gcd(d_i, d_j) = 1, i \neq j}} \prod_{i=1}^n \sigma_i(d_i) u_i(d_i),$$

where $\mathbf{1}_W$ is the characteristic functions of the integers coprime to W, allows us to write

$$\sum_{\mathbf{d} \in \mathscr{D}} \lambda^-_{d_1 \cdots d_n} \prod_{i=1}^n \frac{\sigma_i(d_i)}{\tau(d_i) d_i} = \sum_{d | P(B^{\varpi/100n(n+1)})} \lambda_d^- g(d)$$

and we shall next show that (6.5) is satisfied with $\kappa = n/2$. We have $g(p) = 0$ for all $p \leqslant D_0$, while in the range $p > D_0$ we have

$$g(p) = \frac{1}{2p} \sum_{i=1}^{n} \sigma_i(p) u_i(p).$$

The estimates $u_i(p), \sigma_i(p) \ll 1$ reveal that $g(p) \ll 1/p$ and hence, enlarging D_0 if necessary, we obtain $g(p) < 1$. The fact that $u_i(p) \geqslant 0$ follows from $u_i \in \mathscr{U}$, thereby showing that the inequality $g(p) \geqslant 0$ is a consequence of $\sigma_i(p) \geqslant 0$. Indeed, by (5.4),

$$\sigma_i(p) = \sum_{\substack{\xi \pmod p \\ \Delta_i(\xi,1) \equiv 0 \pmod p}} \left(1 + \left(\frac{\delta_i(\xi,1)}{p}\right)\right) + O\left(\frac{1}{p}\right),$$

which is a non-negative even integer up to an error $O(\frac{1}{p})$, thus for large p it attains negative values only when $\varrho_i(p) = -\tau_i(p)$. In this case (5.4) reveals that $\sigma_i(p)$ equals $\tau_i(p)(p+1)^{-1}$, which is again non-negative.

Using a Taylor expansion leads us to

$$\log \prod_{p<z} (1 - g(p))^{-1} = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{p<z} g(p)^k$$

whenever $z > D_0$. The estimate $g(p) \ll 1/p$ shows that the sum of all terms with $k \geqslant 2$ equals $c_0 + O(1/z)$ for some constant c_0 independent of z. Let us observe that the sequence

$$a(p) = \sum_{i=1}^{n} (\sigma_i(p) - \tau_i(p) - \varrho_i(p))$$

satisfies $a_i(p) \ll 1/p$, and hence the remaining sum equals

$$\sum_{p<z} g(p) = \frac{1}{2} \sum_{i=1}^{n} \left(\sum_{D_0<p<z} \frac{\tau_i(p)}{p} \right) + \frac{1}{2} \sum_{i=1}^{n} \left(\sum_{D_0<p<z} \frac{\varrho_i(p)}{p} \right) + a + O\left(\frac{1}{z}\right),$$

where $a = \sum_{p>D_0} a_p/p$. By (5.9) and (5.10) we can therefore deduce that

$$\sum_{p<z} g(p) = \frac{n}{2} \log\log z + c_1 + O\left(\frac{1}{\log z}\right),$$

thus infering

$$\prod_{p<z} (1 - g(p))^{-1} = e^{c_0+c_1} (\log z)^{n/2} (1 + O(1/\log z)),$$

from which (6.5) follows in the case $w > D_0$. In the remaining cases $w \leqslant D_0 < z$ and $z < w \leqslant D_0$, the product $\prod_{w \leqslant p<z} (1 - g(p))^{-1}$ equals $\prod_{1+D_0 \leqslant p<z} (1 - g(p))^{-1}$ and 1 respectively; they are $\leqslant (\log z/\log w)^{n/2} (1 + O(1/\log w))$ in both cases. This finishes the

verification of (6.4), we have therefore obtained the validity of

$$\sum_{d|P(B^{\varpi/100n(n+1)})} \lambda_d^- g(d) = \left(1 + O\left(e^{-1/\varpi}\left(1 + \frac{1}{\varpi \log B}\right)^{10}\right)\right) \prod_{p<B^{\varpi/100n(n+1)}} (1 - g(p)).$$

Fixing a suitably small positive value for ϖ ensures that the sum behaves asymptotically as

$$\prod_{p<B^{\varpi/100n(n+1)}} (1 - g(p)) \asymp (\log B)^{-n/2},$$

an estimate which concludes the proof of Theorem 1.1.

References

[BCF+15] M. Bhargava, J. E. Cremona, T. Fisher, N. G. Jones, and J. P. Keating, *What is the probability that a random integral quadratic form in n variables has an integral zero ?*, Internat. Math. Res. Notices (to appear) (2015).

[BSJ14] T. Browning and M. Swarbrick Jones, *Counting rational points on del Pezzo surfaces with a conic bundle structure*, Acta Arith. **163** (2014), no. 3, 271–298.

[Dan99] S. Daniel, *On the divisor-sum problem for binary forms*, J. reine angew. Math. **507** (1999), 107–129.

[Enr97] F. Enriques, *Sulle irrazionalità da cui può farsi dipendere la risoluzione d'un equazione algebrica $f(x, y, z) = 0$ con funzioni razionali di due parametri*, Math. Ann. **49** (1897), 1–23.

[Guo95] C. R. Guo, *On solvability of ternary quadratic forms*, Proc. London Math. Soc. (3) **70** (1995), no. 2, 241–263.

[Hoo74] C. Hooley, *On the intervals between numbers that are sums of two squares. III*, J. reine angew. Math. **267** (1974), 207–218.

[Hoo93] ———, *On ternary quadratic forms that represent zero*, Glasgow Math. J. **35** (1993), no. 1, 13–23.

[Hoo07] ———, *On ternary quadratic forms that represent zero. II*, J. reine angew. Math. **602** (2007), 179–225.

[IK04] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

[Isk79] V. A. Iskovskih, *Minimal models of rational surfaces over arbitrary fields*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 1, 19–43.

[Lou13] D. Loughran, *The number of varieties in a family which contain a rational point*, `http://arxiv.org/abs/1310.6219` (2013).

[LS15] D. Loughran and A. Smeets, *Fibrations with few rational points*, `http://arxiv.org/abs/1511.08027` (2015).

[Man86] Y. I. Manin, *Cubic forms*, second ed., North-Holland Mathematical Library, vol. 4, North-Holland Publishing Co., Amsterdam, 1986.

[MV07] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[PV04] B. Poonen and J. F. Voloch, *Random Diophantine equations*, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, With appendices by Jean-Louis Colliot-Thélène and N. M. Katz, pp. 175–184.

[Ser90] J.-P. Serre, *Spécialisation des éléments de* $\mathrm{Br}_2(\mathbf{Q}(T_1, \dots, T_n))$, C. R. Acad. Sci. Paris Sér. I Math. **311** (1990), no. 7, 397–402.

[Sko96] A. N. Skorobogatov, *Descent on fibrations over the projective line*, Amer. J. Math. **118** (1996), no. 5, 905–923.

[Sof14] E. Sofos, *Uniformly counting rational points on conics*, Acta Arith. **166** (2014), no. 1, 1–14.

E. Sofos, Universiteit Leiden, Mathematisch Instituut Leiden, Snellius building, Niels Bohrweg 1, 2333 CA Leiden, Netherlands. • *E-mail :* e.sofos@math.leidenuniv.nl