Compositio Math. 144 (2008) 1375–1402
doi:10.1112/S0010437X08003692

Binary linear forms as sums of two squares

R. de la Bretèche and T. D. Browning

Abstract

We revisit recent work of Heath-Brown on the average order of the quantity $r(L_1(\mathbf{x}))\cdots r(L_4(\mathbf{x}))$, for suitable binary linear forms $L_1,\dots,L_4$, as $\mathbf{x}=(x_1,x_2)$ ranges over quite general regions in $\mathbb{Z}^2$. In addition to improving the error term in Heath-Brown's estimate, we generalise his result to cover a wider class of linear forms.

1. Introduction

Let $L_1,\dots,L_4\in\mathbb{Z}[x_1,x_2]$ be binary linear forms, and let $\mathcal{R}\subset\mathbb{R}^2$ be any bounded region. This paper is motivated by the question of determining conditions on $L_1,\dots,L_4$ and $\mathcal{R}$ under which it is possible to establish an asymptotic formula for the sum

$$S(X):=\sum_{\mathbf{x}=(x_1,x_2)\in\mathbb{Z}^2\cap X\mathcal{R}} r(L_1(\mathbf{x}))r(L_2(\mathbf{x}))r(L_3(\mathbf{x}))r(L_4(\mathbf{x})),$$

as $X\to\infty$, where $X\mathcal{R}:=\{X\mathbf{x}:\mathbf{x}\in\mathcal{R}\}$. The problem of determining an upper bound for $S(X)$ is substantially easier. In fact our recent investigation [BB06] into the average order of arithmetic functions over the values of binary forms easily gives $S(X)\ll X^2$, provided that no two of $L_1,\dots,L_4$ are proportional. In trying to establish an asymptotic formula for $S(X)$ there is no real loss in generality in restricting one's attention to the corresponding sum in which one of the variables x_1,x_2 is odd. For $j\in\{*,0,1\}$, let us write $S_j(X)$ for the corresponding sum in which x_1 is odd and $x_2\equiv j \bmod 2$, where the case $j=*$ means that no 2-adic restriction is placed on x_2.

Our point of departure is work of Heath-Brown [HB03], which establishes an asymptotic formula for $S_*(X)$ when $L_1,\dots,L_4$ and $\mathcal{R}$ satisfy the following normalisation hypotheses:

(i) $\mathcal{R}$ is an open, bounded and convex region, with a piecewise continuously differentiable boundary;

(ii) no two of $L_1,\dots,L_4$ are proportional;

(iii) $L_i(\mathbf{x})>0$ for all $\mathbf{x}\in\mathcal{R}$; and

(iv) $L_i(\mathbf{x})\equiv x_1 \bmod 4$.

Here, as throughout our work, the index i denotes a generic element of the set $\{1,2,3,4\}$. We will henceforth say that $L_1,\dots,L_4,\mathcal{R}$ 'satisfy NH_0' if these four conditions hold. The first three conditions are all quite natural, and do not impose any serious constraint on $L_1,\dots,L_4,\mathcal{R}$. The fourth condition is more problematic however, especially when it comes to applying the result in other contexts. We will return to this issue shortly. For the moment we concern ourselves with presenting a refinement of Heath-Brown's result. It will be necessary to introduce some more notation first.

Received 14 December 2007, accepted in final form 18 April 2008.
2000 Mathematics Subject Classification 11N37 (primary), 11D25, 11N25 (secondary).
Keywords: rational points of bounded height, binary forms, divisor problem, Manin conjecture, sums of two squares, uniform asymptotic formula.

For given $L_1, \dots, L_4, \mathcal{R}$, we will write

$$L_\infty = L_\infty(L_1, \dots, L_4) := \max_{1 \leqslant i \leqslant 4} \|L_i\|, \tag{1.1}$$

where $\|L_i\|$ denotes the maximum modulus of the coefficients of L_i, and

$$r_\infty = r_\infty(\mathcal{R}) := \sup_{\mathbf{x} \in \mathcal{R}} \max\{|x_1|, |x_2|\}. \tag{1.2}$$

Furthermore, let

$$r' = r'(L_1, \dots, L_4, \mathcal{R}) := \sup_{\mathbf{x} \in \mathcal{R}} \max_{1 \leqslant i \leqslant 4} |L_i(\mathbf{x})|. \tag{1.3}$$

Define the real number

$$\eta := 1 - \frac{1 + \log\log 2}{\log 2}, \tag{1.4}$$

with numerical value $0.086\,071\ldots$, and let χ be the non-principal character modulo 4 defined multiplicatively by

$$\chi(p) := \begin{cases} +1, & \text{if } p \equiv 1 \bmod 4, \\ -1, & \text{if } p \equiv 3 \bmod 4, \\ 0, & \text{if } p = 2. \end{cases}$$

We are now ready to reveal our first result.

Theorem 1. *Assume that $L_1, \dots, L_4, \mathcal{R}$ satisfy NH_0, and let $\varepsilon > 0$. Suppose that $r' X^{1-\varepsilon} \geqslant 1$. Then we have*

$$S_*(X) = 4\pi^4 \operatorname{meas}(\mathcal{R}) X^2 \prod_{p>2} \sigma_p^* + O\left(\frac{L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta - \varepsilon}} \right),$$

where

$$\sigma_p^* := \left(1 - \frac{\chi(p)}{p}\right)^4 \sum_{a,b,c,d=0}^{\infty} \chi(p)^{a+b+c+d} \rho_*(p^a, p^b, p^c, p^d)^{-1} \tag{1.5}$$

and

$$\rho_*(\mathbf{h}) := \det\{\mathbf{x} \in \mathbb{Z}^2 : h_i \mid L_i(\mathbf{x})\} \tag{1.6}$$

as a sublattice of $\mathbb{Z}^2$. Moreover, the product $\prod \sigma_p^*$ is absolutely convergent.

The implied constant in this estimate is allowed to depend upon the choice of ε, a convention that we will adopt for all of the implied constants in this paper. It would be straightforward to replace the term $(\log X)^\varepsilon$ by $(\log\log X)^A$ in the error term, for some explicit value of A. For the purposes of comparison, we note that [HB03, Theorem 1] consists of an asymptotic formula for $S_*(X)$ with error

$$O_{L_1 \dots, L_4, \mathcal{R}}\left(\frac{X^2 (\log\log X)^{15/4}}{(\log X)^{\eta/2}} \right).$$

Here there is an unspecified dependence on $L_1, \dots, L_4, \mathcal{R}$, and η is given by (1.4). Thus Theorem 1 is stronger than [HB03, Theorem 1] in two essential aspects. Firstly, we have been able to obtain complete uniformity in $L_1, \dots, L_4, \mathcal{R}$ in the error term, and secondly, our exponent of $\log X$ is almost twice the size.

Our next result extends Theorem 1 to points running over vectors belonging to suitable sublattices of $\mathbb{Z}^2$. The advantages of such a generalisation will be made clear shortly. For any $\mathbf{D} \in \mathbb{N}^4$, we let

$$\Gamma_{\mathbf{D}} = \Gamma(\mathbf{D}; L_1, \dots, L_4) := \{\mathbf{x} \in \mathbb{Z}^2 : D_i \mid L_i(\mathbf{x})\}. \tag{1.7}$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Then $\Gamma_{\mathbf{D}} \subseteq \mathbb{Z}^2$ is an integer lattice of rank 2. Next, let $\mathbf{d} \in \mathbb{N}^4$ and assume that $d_i \mid D_i$. In particular it follows that $\Gamma_{\mathbf{D}} \subseteq \Gamma_{\mathbf{d}}$. Throughout this paper we will focus our attention on $(\mathbf{d}, \mathbf{D}) \in \mathcal{D}$, where

$$\mathcal{D} := \{(\mathbf{d}, \mathbf{D}) \in \mathbb{N}^8 : 2 \nmid d_i D_i,\ d_i \mid D_i\}. \tag{1.8}$$

For $j \in \{*, 0, 1\}$ the goal is to establish an asymptotic formula for

$$S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}}) := \sum_{\substack{\mathbf{x} \in \Gamma_{\mathbf{D}} \cap X\mathcal{R} \\ 2 \nmid x_1 \\ x_2 \equiv j \bmod 2}} r\left(\frac{L_1(\mathbf{x})}{d_1}\right) r\left(\frac{L_2(\mathbf{x})}{d_2}\right) r\left(\frac{L_3(\mathbf{x})}{d_3}\right) r\left(\frac{L_4(\mathbf{x})}{d_4}\right). \tag{1.9}$$

It is clear that $S_j(X) = S_j(X; (1,1,1,1), \mathbb{Z}^2)$ for each $j \in \{*, 0, 1\}$.

For given $\mathbf{d} \in \mathbb{N}^4$ with odd components, let us say that $L_1, \dots, L_4, \mathcal{R}$ 'satisfy $\mathsf{NH}_0(\mathbf{d})$' if they satisfy the conditions in NH_0, but with (iv) replaced by

(iv)$_{\mathbf{d}}$ $L_i(\mathbf{x}) \equiv d_i x_1 \bmod 4$.

When $d_i \equiv 1 \bmod 4$ for each i, it is clear that (iv)$_{\mathbf{d}}$ coincides with (iv). Let $[a, b]$ denote the least common multiple of any two positive integers a, b. The results that we obtain involve the quantity

$$\rho_0(\mathbf{h}) := \frac{\det \Gamma\big(([D_1, d_1 h_1], \dots, [D_4, d_4 h_4]); L_1, \dots, L_4\big)}{\det \Gamma(\mathbf{D}; L_1, \dots, L_4)}, \tag{1.10}$$

which we will occasionally denote by $\rho_0(\mathbf{h}; \mathbf{D}; L_1, \dots, L_4)$. Specifically, we have local factors

$$\sigma_p := \left(1 - \frac{\chi(p)}{p}\right)^4 \sum_{a,b,c,d=0}^{\infty} \chi(p)^{a+b+c+d} \rho_0(p^a, p^b, p^c, p^d)^{-1}, \tag{1.11}$$

defined for any prime $p > 2$. In view of (1.5) and (1.6), we note that $\rho_0(\mathbf{h}) = \rho_*(\mathbf{h})$ and $\sigma_p = \sigma_p^*$ when $D_i = 1$, since then $\Gamma_{\mathbf{D}} = \mathbb{Z}^2$. Bearing all this notation in mind, we have the following result.

THEOREM 2. *Let $(\mathbf{d}, \mathbf{D}) \in \mathcal{D}$ and assume that $L_1, \dots, L_4, \mathcal{R}$ satisfy $\mathsf{NH}_0(\mathbf{d})$. Let $\varepsilon > 0$ and suppose that $r' X^{1-\varepsilon} \geqslant 1$. Let $j \in \{*, 0, 1\}$. Then we have*

$$S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}}) = \frac{\delta_j \pi^4 \operatorname{meas}(\mathcal{R})}{\det \Gamma_{\mathbf{D}}} X^2 \prod_{p>2} \sigma_p + O\left(\frac{D^{\varepsilon} L_{\infty}^{\varepsilon} r_{\infty} r' X^2}{(\log X)^{\eta - \varepsilon}}\right),$$

where $D := D_1 D_2 D_3 D_4$ and

$$\delta_j := \begin{cases} 2, & \text{if } j = 0, 1, \\ 4, & \text{if } j = *, \end{cases} \tag{1.12}$$

and $L_{\infty}, r_{\infty}, r'$ are given by (1.1), (1.2) and (1.3), respectively. Moreover, the product $\prod \sigma_p$ is absolutely convergent.

Taking $d_i = D_i = 1$ and $j = *$ in the statement of Theorem 2, we retrieve Theorem 1. In fact the proof of Theorem 2 is a rather routine deduction from Theorem 1 and will be carried out in § 6.

We now return to the normalisation conditions (i)–(iv)$_{\mathbf{d}}$ that form the basis of Theorem 2. As indicated above, one of the main motivations behind writing this paper has been to weaken these conditions somewhat. In fact we will be able to replace condition (iv)$_{\mathbf{d}}$ by either of

(iv′)$_{\mathbf{d}}$ the coefficients of L_3, L_4 are all non-zero and there exist integers $k_1, k_2 \geqslant 0$ such that

$$2^{-k_1} L_1(\mathbf{x}) \equiv d_1 x_1 (\mathrm{mod} 4), \quad 2^{-k_2} L_2(\mathbf{x}) \equiv d_2 x_1 (\mathrm{mod} 4),$$

or

(iv″)$_{\mathbf{d}}$ the coefficients of L_3, L_4 are all non-zero and there exist integers $k_1, k_2 \geqslant 0$ such that

$$2^{-k_1} L_1(\mathbf{x}) \equiv d_1 x_1 (\mathrm{mod} 4), \quad 2^{-k_2} L_2(\mathbf{x}) \equiv x_2 (\mathrm{mod} 4).$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Accordingly, we will say that $L_1, \dots, L_4, \mathcal{R}$ 'satisfy $\mathsf{NH}_1(\mathbf{d})$' if they satisfy conditions (i)–(iii) and $(\mathrm{iv}')_{\mathbf{d}}$, and we will say that $L_1, \dots, L_4, \mathcal{R}$ 'satisfy $\mathsf{NH}_2(\mathbf{d})$' if together with (i)–(iii) they satisfy condition $(\mathrm{iv}'')_{\mathbf{d}}$. The condition that none of the coefficients of L_3, L_4 are zero is equivalent to the statement that neither L_3 nor L_4 is proportional to x_1 or x_2. Condition (ii) ensures that no two of $L_1, \dots, L_4$ are proportional, and so if L_3 or L_4 is proportional to one of x_1 or x_2, then there are at least two forms among $L_1, \dots, L_4$ that are not proportional to x_1 or x_2. After a possible relabelling, therefore, one may always assume that the coefficients of L_3, L_4 are non-zero.

The asymptotic formula that we obtain under these new hypotheses is more complicated than Theorem 2, and intimately depends on the coefficients of L_3, L_4. Suppose that

$$L_3(\mathbf{x}) = a_3x_1 + b_3x_2, \quad L_4(\mathbf{x}) = a_4x_1 + b_4x_2, \tag{1.13}$$

and write

$$\mathbf{A} = \begin{pmatrix} a_3 & b_3 \\ a_4 & b_4 \end{pmatrix}$$

for the associated matrix. In particular for $L_1, \dots, L_4$ satisfying any of the normalisation conditions above, we may assume that $\mathbf{A}$ is an integer-valued matrix with non-zero determinant and non-zero entries.

Let $(j,k) \in \{*, 0, 1\} \times \{0, 1, 2\}$. We proceed to introduce a quantity $\delta_{j,k}(\mathbf{A}, \mathbf{d}) \in \mathbb{R}$, which will correspond to the 2-adic density of vectors $\mathbf{x} \in \mathbb{Z}^2$ with $x_1 \equiv 1 \bmod 4$ and $x_2 \equiv j \bmod 2$, for which the corresponding summand in (1.9) is non-zero for $L_1, \dots, L_4, \mathcal{R}$ satisfying $\mathsf{NH}_k(\mathbf{d})$. Let

$$E_n := \{x \in \mathbb{Z}/2^n\mathbb{Z} : \ \exists\, \nu \in \mathbb{Z}_{\geqslant 0},\ 2^{-\nu}x \equiv 1 \bmod 4\}, \tag{1.14}$$

for any $n \in \mathbb{N}$. Then we may set

$$\delta_{j,k}(\mathbf{A}, \mathbf{d}) := \lim_{n\to\infty} \frac{1}{2^{2n-4}} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 : \begin{array}{c} x_1 \equiv 1 \bmod 4 \\ x_2 \equiv j \bmod 2 \\ L_i(\mathbf{x}) \in d_iE_n \end{array} \right\}. \tag{1.15}$$

This limit plainly always exists and is contained in the interval $[0, 4]$. It will ease notation if we simply write $\delta_{j,k}(\mathbf{A})$ for $\delta_{j,k}(\mathbf{A}, \mathbf{d})$ in all that follows. We will calculate this quantity explicitly in § 3. We are now ready to reveal our main result.

Theorem 3. *Let $(\mathbf{d}, \mathbf{D}) \in \mathcal{D}$ and assume that $L_1, \dots, L_4, \mathcal{R}$ satisfy $\mathsf{NH}_k(\mathbf{d})$ for $k \in \{0, 1, 2\}$. Let $\varepsilon > 0$ and suppose that $r'X^{1-\varepsilon} \geqslant 1$. Let $j \in \{*, 0, 1\}$. Then we have*

$$S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}}) = cX^2 + O\left(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r'X^2}{(\log X)^{\eta-\varepsilon}} \right),$$

where

$$c = \delta_{j,k}(\mathbf{A}) \frac{\pi^4 \operatorname{meas}(\mathcal{R})}{\det \Gamma_{\mathbf{D}}} \prod_{p>2} \sigma_p.$$

It is rather trivial to check that $\delta_{j,0}(\mathbf{A}) = \delta_j$, in the notation of (1.12). Hence the statement of Theorem 3 reduces to Theorem 2 when $k = 0$. The proof of Theorem 3 for $k = 1, 2$ uses Theorem 2 as a crucial ingredient, but it will be significantly more complicated than the corresponding deduction of Theorem 2 from Theorem 1. This will be carried out in § 7. The underlying idea is to find appropriate linear transformations that take the relevant linear forms into forms that satisfy the normalisation conditions (i)–$(\mathrm{iv})_{\mathbf{d}}$, thereby bringing the problem in line for an application of Theorem 2. In practice, the choice of transformation depends closely upon the coefficients of L_3, L_4, and a careful case-by-case analysis is necessary.

While interesting in its own right, the study of sums like (1.9) is also related to problems involving the distribution of integer and rational points on algebraic varieties. In fact estimating $S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}})$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

boils down to counting integer points on the affine variety

$$L_i(x_1, x_2) = d_i(s_i^2 + t_i^2), \quad 1 \leqslant i \leqslant 4, \tag{1.16}$$

in $\mathbb{A}^{10}$, with x_1, x_2 restricted in some way. Viewed in this light it might be expected that the constant c in Theorem 3 admits an interpretation as a product of local densities. Our next goal is to show that this is indeed the case.

Let $\boldsymbol{\lambda} \in \mathbb{Z}^4_{\geqslant 0}$ and let $\boldsymbol{\mu} \in \mathbb{Z}^4_{\geqslant 0}$. Given any prime $p > 2$, let

$$N_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p^n) := \#\left\{(\mathbf{x}, \mathbf{s}, \mathbf{t}) \in (\mathbb{Z}/p^n\mathbb{Z})^{10} : \begin{array}{l} L_i(x_1, x_2) \equiv p^{\lambda_i}(s_i^2 + t_i^2) \bmod p^n \\ p^{\mu_i} \mid L_i(x_1, x_2) \end{array}\right\},$$

and define

$$\omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) := \lim_{n\to\infty} p^{-6n-\lambda_1-\cdots-\lambda_4} N_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p^n). \tag{1.17}$$

This corresponds to the p-adic density on a variety of the form (1.16), in which the points are restricted to lie on a certain sublattice of $\mathbb{Z}/p^n\mathbb{Z}$.

Turning to the case $p = 2$, let

$$N_{j,k,\mathbf{d}}(2^n) := \#\left\{(\mathbf{x}, \mathbf{s}, \mathbf{t}) \in (\mathbb{Z}/2^n\mathbb{Z})^{10} : \begin{array}{l} L_i(x_1, x_2) \equiv d_i(s_i^2 + t_i^2) \bmod 2^n \\ x_1 \equiv 1 \bmod 4, \ x_2 \equiv j \bmod 2 \end{array}\right\},$$

for any $(j, k) \in \{*, 0, 1\} \times \{0, 1, 2\}$ and any $\mathbf{d} \in \mathbb{N}^4$ such that $2 \nmid d_1 \cdots d_4$. Here the subscript k indicates that $L_1, \ldots, L_4, \mathcal{R}$ are assumed to satisfy $\mathsf{NH}_k(\mathbf{d})$. The corresponding 2-adic density is given by

$$\omega_{j,k,\mathbf{d}}(2) := \lim_{n\to\infty} 2^{-6n} N_{j,k,\mathbf{d}}(2^n). \tag{1.18}$$

Finally, we let $\omega_{\mathcal{R}}(\infty)$ denote the archimedean density of solutions to the system of equations (1.16), for which $(\mathbf{x}, \mathbf{s}, \mathbf{t}) \in \mathcal{R} \times \mathbb{R}^8$. We will establish the following result in § 2.

THEOREM 4. *We have*

$$c = \omega_{\mathcal{R}}(\infty)\omega_{j,k,\mathbf{d}}(2) \prod_{p>2} \omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p)$$

in the statement of Theorem 3, with

$$\boldsymbol{\lambda} = (\nu_p(d_1), \ldots, \nu_p(d_4)), \quad \boldsymbol{\mu} = (\nu_p(D_1), \ldots, \nu_p(D_4)).$$

It turns out that the system of equations in (1.16) play the role of descent varieties for the pair of equations

$$L_1(x_1, x_2)L_2(x_1, x_2) = x_3^2 + x_4^2, \quad L_3(x_1, x_2)L_4(x_1, x_2) = x_5^2 + x_6^2,$$

for binary linear forms $L_1, \ldots, L_4$ defined over $\mathbb{Z}$. This defines a geometrically integral threefold $V \subset \mathbb{P}^5$, and it is natural to try and estimate the number $N(X)$ of rational points on V with height at most X, as $X \to \infty$. In fact there is a very precise conjecture due to Manin [FMT89] that relates the growth of $N(X)$ to the intrinsic geometry of V. It is easily checked that V is a singular variety with finite singular locus consisting of double points. If $\widetilde{V}$ denotes the minimal desingularisation of V, then the Picard group of $\widetilde{V}$ has rank 1. Moreover, $K_{\widetilde{V}} + 2H$ is effective, where $K_{\widetilde{V}}$ is a canonical divisor and H is a hyperplane section. Thus Manin's conjecture predicts the asymptotic behaviour $N(X) = c_V X^2(1 + o(1))$, as $X \to \infty$, for a suitable constant $c_V \geqslant 0$.

Building on his investigation [HB03, Theorem 1] into the sum $S_*(X)$ defined above, Heath-Brown provides considerable evidence for this conjecture when $L_1, \ldots, L_4, \mathcal{R}$ satisfy a certain normalisation hypothesis, which he labels **NC2**. This coincides with the conditions (i)–(iii) in NH_0, but with (iv) replaced by the condition that

$$L_1(\mathbf{x}) \equiv L_2(\mathbf{x}) \equiv \nu x_1 (\mathrm{mod} 4), \quad L_3(\mathbf{x}) \equiv L_4(\mathbf{x}) \equiv \nu' x_1 (\mathrm{mod} 4),$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

for appropriate $\nu, \nu' = \pm 1$. The outcome of Heath-Brown's investigation is [HB03, Theorem 2]. Under **NC2** this establishes the existence of a constant $c \geqslant 0$ and a function $E(X) = o(X^2)$, such that

$$\sum_{\substack{\mathbf{x} \in \mathbb{Z}^2 \cap X\mathcal{R} \\ x_1 \equiv 1 \bmod 2}} r(L_1(\mathbf{x})L_2(\mathbf{x}))r(L_3(\mathbf{x})L_4(\mathbf{x})) = cX^2 + O(E(X)). \tag{1.19}$$

The explicit value of c is rather complicated to state and will not be given here. One of the features of Heath-Brown's proof is that it does not lead to an explicit error function $E(X)$. An examination of the proof reveals that this can be traced back to an argument involving dominated convergence in the proof of [HB03, Lemma 6.1], thereby allowing Heath-Brown to employ [HB03, Theorem 1], which is not uniform in any of the relevant parameters. Rather than using [HB03, Theorem 1] to estimate the sums $S(d, d')$ that occur in his analysis, however, it is possible to employ our Theorem 2. The advantage in doing so is that the corresponding error term is completely uniform in the parameters d, d', thus circumventing the need for the argument involving dominated convergence. Rather than labouring the details, we will content ourselves with merely recording the outcome of this observation here.

Corollary. *One has $E(X) = X^2(\log X)^{-\eta/3+\varepsilon}$ in (1.19), for any $\varepsilon > 0$.*

In addition to the threefold $V \subset \mathbb{P}^5$ defined above, it transpires that the estimates in this paper can play an important role in analysing the arithmetic of other rational varieties. Indeed, one of the motivating factors behind writing this paper has been to prepare the way for a verification of the Manin conjecture for certain surfaces of the shape

$$x_1x_2 = x_3^2, \quad x_3(ax_1 + bx_2 + cx_3) = x_4^2 + x_5^2,$$

in forthcoming joint work with Emmanuel Peyre. These equations define singular del Pezzo surfaces of degree 4 in $\mathbb{P}^4$, of the type first considered by Iskovskikh. These are arguably the most interesting examples of singular quartic del Pezzo surfaces since they are the only ones for which weak approximation may fail. On solving the first equation in integers, and substituting into the second equation, one is led to consider the family of equations

$$h^2y_1y_2(ay_1^2 + by_2^2 + cy_1y_2) = s^2 + t^2,$$

for h running over a suitable range. Studying the distribution of integer solutions to this system of equations therefore amounts to estimating sums of the shape

$$\sum_{y_1, y_2} r(h^2y_1y_2(ay_1^2 + by_2^2 + cy_1y_2)),$$

uniformly in h. By choosing a, b, c such that $c^2 - 4ab$ is a square, one can show that this sum is related to sums of the sort (1.9), but for which Heath-Brown's original normalisation conditions in NH_0 are no longer met. Thus we have found it desirable to generalise the work of [HB03] to the extent enjoyed in the present paper.

As a final remark we note that further generalisations of our main results seem entirely feasible. For example, one ought to be able to extend the work to deal with analogues of (1.9) in which r is replaced by an r_Δ-function that counts representations as norms of elements belonging to an arbitrary imaginary quadratic field of discriminant Δ.

Notation. Throughout our work $\mathbb{N}$ will denote the set of positive integers. Moreover, we will follow common practice and allow the arbitrary small parameter $\varepsilon > 0$ to take different values at different parts of the argument. All order constants are allowed to depend on ε.

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

2. Interpretation of the constant

Our task in this section is to establish Theorem 4. We begin with some preliminary facts. Let $A \in \mathbb{Z}$ and let $\alpha \in \mathbb{Z}_{\geqslant 0}$. For any prime power p^n, we write

$$S_\alpha(A; p^n) := \#\{(x, y) \in (\mathbb{Z}/p^n\mathbb{Z})^2 : p^\alpha(x^2 + y^2) \equiv A \bmod p^n\}. \tag{2.1}$$

If $\alpha \leqslant n$ then it is not hard to see that

$$S_\alpha(A; p^n) = p^{2\alpha} S_0(A/p^\alpha; p^{n-\alpha}), \tag{2.2}$$

when $\alpha \leqslant \nu_p(A)$ and $S_\alpha(A; p^n) = 0$ otherwise. In the case $\alpha = 0$ we have

$$S_0(A; p^n) = \begin{cases} p^n + np^n(1 - 1/p), & \text{if } \nu_p(A) \geqslant n, \\ (1 + \nu_p(A))p^n(1 - 1/p), & \text{if } \nu_p(A) < n, \end{cases} \tag{2.3}$$

when $p \equiv 1 \bmod 4$. This formula has been employed by Heath-Brown [HB03, § 8] in a similar context. When $p \equiv 3 \bmod 4$, he notes that

$$S_0(A; p^n) = \begin{cases} p^{2[n/2]}, & \text{if } \nu_p(A) \geqslant n, \\ p^n(1 + 1/p), & \text{if } \nu_p(A) < n \text{ and } 2 \mid \nu_p(A), \\ 0, & \text{if } \nu_p(A) < n \text{ and } 2 \nmid \nu_p(A). \end{cases} \tag{2.4}$$

Finally, when $p = 2$ and $n \geqslant 2$, we have

$$S_0(A; 2^n) = \begin{cases} 2^{n+1}, & \text{if } 2^{-\nu_2(A)}A \equiv 1 \bmod 4, \\ 0, & \text{otherwise.} \end{cases} \tag{2.5}$$

Note that Heath-Brown states this formula only for odd A that are congruent to 1 modulo 4, but the general case is easily checked. Indeed, if $\nu = \nu_2(A)$, then one notes that $2 \mid \gcd(x, y)$ in the definition of $S_0(A; 2^n)$ if $\nu \geqslant 2$, and $2 \nmid xy$ if $\nu = 1$. In the former case one therefore has $S_0(A; 2^n) = 4S_0(A/4; 2^{n-2})$, and in the latter case one finds that $S_0(A; 2^n) = 2^{n+1}$.

Let $L_1, \dots, L_4 \in \mathbb{Z}[x_1, x_2]$ be arbitrary linear forms, and recall the definition (1.6) of the determinant $\rho_*(\mathbf{h})$. It follows from the multiplicativity of ρ_* that

$$\frac{1}{\det \Gamma_{\mathbf{D}}} \prod_{p>2} \sigma_p = \prod_{p>2} c_p$$

in the statement of Theorem 3, with

$$c_p = \left(1 - \frac{\chi(p)}{p}\right)^4 \sum_{n_i \geqslant 0} \frac{\chi(p)^{n_1 + \cdots + n_4}}{\rho_*(p^{\max\{\nu_p(D_1), \nu_p(d_1) + n_1\}}, \dots, p^{\max\{\nu_p(D_4), \nu_p(d_4) + n_4\}})}.$$

We claim that

$$c_p = \omega_{\boldsymbol{\lambda}, \boldsymbol{\mu}}(p), \tag{2.6}$$

for each $p > 2$, where $\omega_{\boldsymbol{\lambda}, \boldsymbol{\nu}}(p)$ is given by (1.17) and the values of $\boldsymbol{\lambda}, \boldsymbol{\nu}$ are as in the statement of Theorem 4. The proof of this claim will be in two steps: the case $p \equiv 1 \bmod 4$ and the case $p \equiv 3 \bmod 4$.

Lemma 1. *Let $p \equiv 1 \bmod 4$ be a prime. Then (2.6) holds.*

Proof. Let $A \in \mathbb{Z}$, and let $p \equiv 1 \bmod 4$ be a prime. On combining (2.3) with (2.2) it follows that

$$S_\alpha(A; p^n) = (1 + \nu_p(A) - \alpha)p^{n+\alpha}(1 - 1/p),$$

provided that $\alpha \leqslant \nu_p(A) < n$. Our plan will be to fix p-adic valuations ν_i of $L_i(\mathbf{x})$, and then to use this formula to count the resulting number of $\mathbf{s}, \mathbf{t} \in (\mathbb{Z}/p^n\mathbb{Z})^4$ in $N_{\boldsymbol{\lambda}, \boldsymbol{\mu}}(p^n)$. Note that we must have

$$\nu_i \geqslant M_i := \max\{\lambda_i, \mu_i\}.$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

It follows that

$$N_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p^n) = p^{4n+\lambda_1+\cdots+\lambda_4}\left(1-\frac{1}{p}\right)^4 \sum_{\nu_i \geqslant M_i} M_{\boldsymbol{\nu}}(p^n) \prod_{1\leqslant i\leqslant 4}(1+\nu_i-\lambda_i) + O(n^4p^{5n}),$$

where $M_{\boldsymbol{\nu}}(p^n)$ counts the number of $\mathbf{x}$ mod p^n such that $p^{\mu_i} \mid L_i(\mathbf{x})$ and $\nu_p(L_i(\mathbf{x})) = \nu_i$. But then

$$\begin{aligned} M_{\boldsymbol{\nu}}(p^n) &= \sum_{\mathbf{e}\in\{0,1\}^4} (-1)^{e_1+\cdots+e_4} \#\{\mathbf{x} \bmod p^n : p^{\max\{\nu_i+e_i,\mu_i\}} \mid L_i(\mathbf{x})\} \\ &= \sum_{\mathbf{e}\in\{0,1\}^4} (-1)^{e_1+\cdots+e_4} \#\{\mathbf{x} \bmod p^n : p^{\nu_i+e_i} \mid L_i(\mathbf{x})\} \\ &= p^{2n} \sum_{\mathbf{e}\in\{0,1\}^4} \frac{(-1)^{e_1+\cdots+e_4}}{\rho_*(p^{\nu_1+e_1},\dots,p^{\nu_4+e_4})}. \end{aligned}$$

Making the change of variables $n_i = \nu_i + e_i - \lambda_i$, and noting that $\nu_i + e_i \geqslant M_i + e_i \geqslant M_i$, we therefore deduce that

$$\begin{aligned} \omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) = \left(1-\frac{1}{p}\right)^4 &\sum_{n_i \geqslant M_i-\lambda_i} \rho_*(p^{\lambda_1+n_1},\dots,p^{\lambda_4+n_4})^{-1} \\ &\times \sum_{0\leqslant e_i\leqslant \min\{1,\lambda_i+n_i-M_i\}} (-1)^{e_1+\cdots+e_4} \prod_{1\leqslant i\leqslant 4}(1+n_i-e_i). \end{aligned}$$

Now it is clear that

$$\sum_{0\leqslant e\leqslant \min\{1,\lambda+n-M\}} (-1)^e(1+n-e) = \begin{cases} 1, & \text{if } \lambda+n-M \geqslant 1, \\ 1+M-\lambda, & \text{if } \lambda+n-M = 0. \end{cases}$$

Since $1+M-\lambda = \#\mathbb{Z}\cap[0,M-\lambda]$, a little thought reveals that

$$\begin{aligned} \omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) &= \left(1-\frac{1}{p}\right)^4 \sum_{n_i\geqslant 0} \rho_*(p^{\max\{M_1,\lambda_1+n_1\}},\dots,p^{\max\{M_4,\lambda_4+n_4\}})^{-1} \\ &= \left(1-\frac{1}{p}\right)^4 \sum_{n_i\geqslant 0} \rho_*(p^{\max\{\mu_1,\lambda_1+n_1\}},\dots,p^{\max\{\mu_4,\lambda_4+n_4\}})^{-1}. \end{aligned}$$

This completes the proof of the lemma. □

Lemma 2. *Let $p \equiv 3 \bmod 4$ be a prime. Then (2.6) holds.*

Proof. Let $\alpha \in \mathbb{Z}_{\geqslant 0}$ and $A \in \mathbb{Z}$, and recall the definition (2.1) of $S_\alpha(A;p^n)$. Combining (2.4) with (2.2), and arguing precisely as in the proof of Lemma 1, we conclude that

$$N_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p^n) = p^{6n+\lambda_1+\cdots+\lambda_4}\left(1+\frac{1}{p}\right)^4 \sum_{\substack{\nu_i\geqslant M_i \\ 2\mid \nu_i-\lambda_i}} \sum_{\mathbf{e}\in\{0,1\}^4} \frac{(-1)^{e_1+\cdots+e_4}}{\rho_*(p^{\nu_1+e_1},\dots,p^{\nu_4+e_4})} + O(n^4p^{5n}).$$

Making the change of variables $n_i = \nu_i + e_i - \lambda_i$, it follows that

$$\omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) = \left(1+\frac{1}{p}\right)^4 \sum_{n_i\geqslant M_i-\lambda_i} \rho_*(p^{\lambda_1+n_1},\dots,p^{\lambda_4+n_4})^{-1} \sum_{\substack{0\leqslant e_i\leqslant \min\{1,\lambda_i+n_i-M_i\} \\ e_i\equiv n_i \bmod 2}} (-1)^{e_1+\cdots+e_4}.$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

This time we find that the summand can be expressed in terms of

$$\sum_{\substack{0\leqslant e\leqslant \min\{1,\lambda+n-M\}\\ e\equiv n \bmod 2}} (-1)^e = \begin{cases} (-1)^n, & \text{if } \lambda+n-M \geqslant 1,\\ 1, & \text{if } \lambda+n-M=0 \text{ and } 2 \mid M-\lambda,\\ 0, & \text{if } \lambda+n-M=0 \text{ and } 2 \nmid M-\lambda. \end{cases}$$

Since $\sum_{0\leqslant n\leqslant M-\lambda}(-1)^n$ is equal to 1 if $M-\lambda$ is even, and 0 otherwise, we conclude that

$$\omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) = \left(1+\frac{1}{p}\right)^4 \sum_{n_i\geqslant 0} \frac{(-1)^{n_1+\cdots+n_4}}{\rho_*(p^{\max\{\mu_1,\lambda_1+n_1\}},\dots,p^{\max\{\mu_4,\lambda_4+n_4\}})}.$$

This completes the proof of the lemma. □

We now turn to the 2-adic density, for which we claim that

$$\delta_{j,k}(\mathbf{A}) = \omega_{j,k,\mathbf{d}}(2), \tag{2.7}$$

where $\delta_{j,k}(\mathbf{A})$ is given by (1.15) and $\omega_{j,k,\mathbf{d}}(2)$ is given by (1.18). On recalling the definition (1.14) of E_n, it follows from (2.5) that

$$N_{j,k,\mathbf{d}}(2^n) = 2^{4n+4}\#\left\{\mathbf{x}\in\mathbb{Z}/2^n\mathbb{Z} : \begin{array}{l} L_i(\mathbf{x})\in d_iE_n\\ x_1\equiv 1 \bmod 4,\ x_2\equiv j \bmod 2\end{array}\right\}.$$

But then

$$\omega_{j,k,\mathbf{d}}(2) = \lim_{n\to\infty}\frac{1}{2^{2n-4}}\#\left\{\mathbf{x}\in\mathbb{Z}/2^n\mathbb{Z} : \begin{array}{l} L_i(\mathbf{x})\in d_iE_n\\ x_1\equiv 1 \bmod 4,\ x_2\equiv j \bmod 2\end{array}\right\},$$

which is just $\delta_{j,k}(\mathbf{A})$. This completes the proof of (2.7).

Finally we turn to the archimedean density $\omega_{\mathcal{R}}(\infty)$ of points on the variety (1.16) for which $\mathbf{x}\in\mathcal{R}$. We claim that

$$\omega_{\mathcal{R}}(\infty) = \pi^4 \operatorname{meas}(\mathcal{R}). \tag{2.8}$$

Our assumptions on $L_1,\dots,L_4,\mathcal{R}$ imply that $L_i(\mathbf{x})>0$ for all $\mathbf{x}\in\mathcal{R}$. To begin with, it is clear that

$$\omega_{\mathcal{R}}(\infty) = 2^8\omega^+_{\mathcal{R}}(\infty),$$

where $\omega^+_{\mathcal{R}}(\infty)$ is defined as for $\omega_{\mathcal{R}}(\infty)$, but with the additional constraint that $s_i,t_i>0$. We will calculate $\omega^+_{\mathcal{R}}(\infty)$ by parametrising the points via the t_i, using the Leray form. In this setting the Leray form is given by

$$(2^4t_1t_2t_3t_4)^{-1}\,\mathrm{d}s_1\cdots\mathrm{d}s_4\,\mathrm{d}x_1\,\mathrm{d}x_2.$$

On making the substitution $t_i=\sqrt{d_i^{-1}L_i(\mathbf{x})-s_i^2}$, and noting that

$$\int_0^{\sqrt{A}}\frac{\mathrm{d}s}{\sqrt{A-s^2}} = \frac{\pi}{2},$$

we therefore conclude that

$$\begin{aligned}\omega_{\mathcal{R}}(\infty) &= 2^4\int_{\mathbf{x}\in\mathcal{R}}\left(\prod_{1\leqslant i\leqslant 4}\int_0^{\sqrt{d_i^{-1}L_i(\mathbf{x})}}\frac{\mathrm{d}s}{\sqrt{d_i^{-1}L_i(\mathbf{x})-s^2}}\right)\mathrm{d}x_1\,\mathrm{d}x_2\\ &= \pi^4\operatorname{meas}(\mathcal{R}),\end{aligned}$$

as required for (2.8).

Bringing together (2.6), (2.7) and (2.8), we easily deduce the statement of Theorem 4.

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

3. The 2-adic densities

In this section we explicitly calculate the value of the 2-adic densities $\delta_{j,k}(\mathbf{A}) = \delta_{j,k}(\mathbf{A}, \mathbf{d})$ in (1.15). In effect this will simplify the process of deducing Theorem 3. Let $L_1, \dots, L_4 \in \mathbb{Z}[x_1, x_2]$ be arbitrary linear forms that satisfy any of the normalisation conditions from the introduction, with L_3, L_4 given by (1.13). In particular, it is clear that there exist integers $k_3, k_4 \geqslant 0$ such that

$$2^{-k_3} L_3(\mathbf{x}) = 2^{\mu_3} a_3' x_1 + 2^{\nu_3} b_3' x_2, \quad 2^{-k_4} L_4(\mathbf{x}) = 2^{\mu_4} a_4' x_1 + 2^{\nu_4} b_4' x_2, \tag{3.1}$$

for integers a_i', b_i' such that

$$a_3' a_4' b_3' b_4' (a_3' b_4' - a_4' b_3') \neq 0, \quad 2 \nmid a_3' a_4' b_3' b_4', \tag{3.2}$$

and integers $\mu_i, \nu_i \geqslant 0$ such that

$$\mu_3 \nu_3 = \mu_4 \nu_4 = 0. \tag{3.3}$$

We are now ready to proceed with the calculation of $\delta_{j,k}(\mathbf{A})$, whose value will depend intimately on j, k, $\mathbf{d}$ and the values of the coefficients in (3.1). The calculations in this section are routine and so we will be brief. In fact we will meet these calculations again in § 7 under a slightly different guise.

Recall the definition (1.14) of E_n for any $n \in \mathbb{N}$, and the definition (1.15) of $\delta_{j,k}(\mathbf{A})$, for $L_1, \dots, L_4, \mathcal{R}$ satisfying $\mathsf{NH}_k(\mathbf{d})$. When $k = 0$, it easily follows from our normalisation conditions that $L_i(\mathbf{x}) \in d_i E_n$ for any integer vector $\mathbf{x}$ such that $x_1 \equiv 1 \bmod 4$. Hence

$$\delta_{j,0}(\mathbf{A}) = \delta_j, \tag{3.4}$$

in the notation of (1.12).

Let us now suppose that $j = k = 1$. Then clearly

$$\delta_{1,1}(\mathbf{A}) = \lim_{n \to \infty} \frac{1}{2^{2n-4}} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 : \begin{array}{l} x_1 \equiv 1 \bmod 4, \ 2 \nmid x_2 \\ d_3 L_3(\mathbf{x}), d_4 L_4(\mathbf{x}) \in E_n \end{array} \right\}. \tag{3.5}$$

It follows from (3.3) that at most two of $\mu_3, \mu_4, \nu_3, \nu_4$ can be non-zero. An easy calculation shows that

$$\delta_{1,1}(\mathbf{A}) = \begin{cases} 1, & \text{if } b_3' d_3 - 2^{\mu_3} \equiv b_4' d_4 - 2^{\mu_4} \bmod 4, \\ 0, & \text{otherwise,} \end{cases} \tag{3.6}$$

when $\nu_3 = \nu_4 = 0$ and $\mu_3, \mu_4 \geqslant 1$. Similarly, we deduce that

$$\delta_{1,1}(\mathbf{A}) = \begin{cases} 2, & \text{if } a_j' \equiv d_j - 2^{\nu_j} \bmod 4 \text{ for } j = 3, 4, \\ 0, & \text{otherwise,} \end{cases} \tag{3.7}$$

when $\mu_3 = \mu_4 = 0$ and $\nu_3, \nu_4 \geqslant 1$. Let j_1, j_2 denote distinct elements from the set $\{3, 4\}$. Then it follows from (3.5) that

$$\delta_{1,1}(\mathbf{A}) = \begin{cases} 1, & \text{if } a_{j_1}' \equiv d_{j_1} - 2^{\nu_{j_1}} \bmod 4, \\ 0, & \text{otherwise,} \end{cases} \tag{3.8}$$

when $\mu_{j_1} = \nu_{j_2} = 0$ and $\mu_{j_2}, \nu_{j_1} \geqslant 1$. Still with the notation $\{j_1, j_2\} = \{3, 4\}$, a simple calculation reveals that

$$\delta_{1,1}(\mathbf{A}) = \begin{cases} 1, & \text{if } a_{j_2}' \equiv d_{j_2} - 2^{\nu_{j_2}} \bmod 4, \\ 0, & \text{otherwise,} \end{cases} \tag{3.9}$$

when $\mu_3 = \mu_4 = \nu_{j_1} = 0$ and $\nu_{j_2} \geqslant 1$. In performing this calculation it is necessary to calculate the contribution to the right-hand side of (3.5) for fixed values of n and fixed 2-adic valuation ξ of $a_3' x_1 + b_3' x_2$, before then summing over all possible values of $\xi \geqslant 1$. In a similar fashion, one finds

$$\delta_{1,1}(\mathbf{A}) = 1/2, \tag{3.10}$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

when $\nu_3 = \nu_4 = \mu_{j_1} = 0$ and $\mu_{j_2} \geqslant 1$. It remains to handle the case in which all the μ_j, ν_j are zero. For this we set

$$v := \nu_2(a_3'b_4' - a_4'b_3'), \tag{3.11}$$

which must be a positive integer, since a_j', b_j' are all odd. Thus we have

$$\delta_{1,1}(\mathbf{A}) = \begin{cases} 1/2, & \text{if } v = 1, \\ 1 - 3/2^v, & \text{if } v \geqslant 2 \text{ and } b_3'd_3 \equiv b_4'd_4 \bmod 4, \\ 3/2^v, & \text{if } v \geqslant 2 \text{ and } b_3'd_3 \equiv -b_4'd_4 \bmod 4, \end{cases} \tag{3.12}$$

when $\mu_3 = \mu_4 = \nu_3 = \nu_4 = 0$.

When $j \neq 1$ and $k \neq 0$, we will find it convenient to phrase our formulae for $\delta_{j,k}(\mathbf{A})$ in terms of $\delta_{1,k}(\mathbf{A})$. We claim that

$$\delta_{0,k}(\mathbf{A}) = \sum_{\xi=1}^{\infty} \frac{\delta_{1,k}(\mathbf{A}\mathbf{M}_\xi)}{2^\xi}, \quad \delta_{*,k}(\mathbf{A}) = \sum_{\xi=0}^{\infty} \frac{\delta_{1,k}(\mathbf{A}\mathbf{M}_\xi)}{2^\xi}, \tag{3.13}$$

when $k = 1$ or 2, where

$$\mathbf{M}_\xi := \begin{pmatrix} 1 & 0 \\ 0 & 2^\xi \end{pmatrix}. \tag{3.14}$$

Here the formula for $\delta_{0,k}(\mathbf{A})$ is not hard to establish, and follows on extracting the 2-adic valuation of x_2 in (1.15). The formula for $\delta_{*,k}(\mathbf{A})$ follows on noting that $\delta_{*,k}(\mathbf{A}) = \delta_{0,k}(\mathbf{A}) + \delta_{1,k}(\mathbf{A})$. Finally, we express $\delta_{1,2}(\mathbf{A})$ in terms of $\delta_{*,1}(\mathbf{A})$ via the transformation

$$\mathbf{M}_{c,d_2} := \begin{pmatrix} 1 & 0 \\ \kappa + 4c & 4 \end{pmatrix}, \tag{3.15}$$

where $\kappa = \pm 1$ denotes the residue modulo 4 of d_2, and $c \in \{0, 1, 2\}$ is any parameter we care to choose. It is not hard to see that

$$\delta_{1,2}(\mathbf{A}) = \frac{\delta_{*,1}(\mathbf{A}\mathbf{M}_{c,d_2})}{4}, \tag{3.16}$$

using the fact that $x_1 \equiv 1 \bmod 4$ and $x_2 \equiv d_2 \bmod 4$.

4. Proof of Theorem 1

Our proof follows that given by Heath-Brown for [HB03, Theorem 1], but with extra care taken to keep track of the error term's dependence on $L_1, \dots, L_4$ and $\mathcal{R}$. Our improvement in the exponent of $\log X$ will emerge through a modification of the final stages of the argument.

Let $X\mathcal{R}_4 := \{\mathbf{x} \in \mathbb{Z}^2 \cap X\mathcal{R} : x_1 \equiv 1 \bmod 4\}$, and for given $\mathbf{d} \in \mathbb{N}^4$ let $\mathcal{R}(\mathbf{d}) \subseteq \mathcal{R}$ denote a convex region depending on $\mathbf{d}$. We write $X\mathcal{R}_4(\mathbf{d})$ for the set $\{\mathbf{x} \in \mathbb{Z}^2 \cap X\mathcal{R}(\mathbf{d}) : x_1 \equiv 1 \bmod 4\}$. The first step of the argument involves modifying the 'level of distribution' result that is employed by Heath-Brown [HB03, Lemma 2.1].

Lemma 3. *Let $X \geqslant 1$ and $Q_1, Q_2, Q_3, Q_4 \geqslant 2$. Write $Q = \max_i Q_i$ and $V = Q_1Q_2Q_3Q_4$. Then there is an absolute constant $A > 0$ such that*

$$\sum_{\substack{\mathbf{d} \in \mathbb{N}^4 \\ d_i \leqslant Q_i \\ 2 \nmid d_i}} \left| \#(\Gamma_{\mathbf{d}} \cap X\mathcal{R}_4(\mathbf{d})) - \frac{\operatorname{meas}(\mathcal{R}(\mathbf{d}))X^2}{4 \det \Gamma_{\mathbf{d}}} \right| \ll L_\infty^\varepsilon r_\infty X(V^{1/2}(\log Q)^A + Q) + V.$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Proof. We appeal to work of Daniel [Dan99, Lemma 3.2]. This gives

$$\left|\#(\Gamma_{\mathbf{d}} \cap X\mathcal{R}_4(\mathbf{d})) - \frac{\mathrm{meas}(\mathcal{R}(\mathbf{d}))X^2}{4\det \Gamma_{\mathbf{d}}}\right| \ll r_\infty \frac{X}{|\mathbf{v}|} + 1, \tag{4.1}$$

for some vector $\mathbf{v} \in \Gamma_{\mathbf{d}}$ with coprime coordinates, such that

$$|\mathbf{v}| \ll (\det \Gamma_{\mathbf{d}})^{1/2} \leqslant (d_1d_2d_3d_4)^{1/2} \leqslant V^{1/2}.$$

The contribution from the second term in (4.1) is clearly $O(V)$. To complete the proof of the lemma it will suffice to show that

$$\sum_{\substack{\mathbf{d}\in\mathbb{N}^4\\ d_i\leqslant Q_i}} \frac{1}{|\mathbf{v}|} \ll L_\infty^\varepsilon (V^{1/2}(\log Q)^A + Q), \tag{4.2}$$

for some absolute constant $A > 0$.

Let σ_1 denote the contribution from the case in which $L_1(\mathbf{v}) \cdots L_4(\mathbf{v}) \neq 0$, and let σ_2 denote the remaining contribution. We then have

$$\sigma_1 \leqslant \sum_{\substack{|\mathbf{v}|\ll V^{1/2}\\ L_i(\mathbf{v})\neq 0}} \frac{1}{|\mathbf{v}|} \sum_{\substack{\mathbf{d}\in\mathbb{N}^4\\ d_i\leqslant Q_i\\ d_i\mid L_i(\mathbf{v})}} 1 \ll L_\infty^\varepsilon \tau(F(\mathbf{v})),$$

where τ is the divisor function and F is a primitive binary form that is proportional to $L_1 \cdots L_4$. A simple application of [BB06, Corollary 1] now reveals that there exists a constant $A > 0$ such that

$$\sum_{|\mathbf{v}|\leqslant x} \tau(F(\mathbf{v})) \ll L_\infty^\varepsilon x^2 (\log x)^A.$$

We therefore obtain the estimate $\sigma_1 \ll L_\infty^\varepsilon V^{1/2}(\log Q)^A$, on carrying out a dyadic summation for the range of $\mathbf{v}$, which is satisfactory for (4.2).

Turning to a bound for σ_2, we suppose that $i_0 \in \{1, 2, 3, 4\}$ is an index for which $L_{i_0}(\mathbf{v}) = a_{i_0}v_1 + b_{i_0}v_2 = 0$. Since $\gcd(v_1, v_2) = 1$, we have $v_1 \mid b_{i_0}$ and $v_2 \mid a_{i_0}$. If $j \neq i_0$, then $L_j(\mathbf{v}) \neq 0$ because L_{i_0} and L_j are not proportional. Moreover, we have $|L_j(\mathbf{v})| \leqslant 2L_\infty^2$ and the number of possible values of $L_j(\mathbf{v})$ is bounded by $O(L_\infty^\varepsilon)$. Since $d_j \mid L_j(\mathbf{v})$, the number of available d_j is $O(L_\infty^\varepsilon)$, whereas the number of d_{i_0} is bounded by $Q_{i_0} \leqslant Q$. Thus it follows that $\sigma_2 \ll L_\infty^\varepsilon Q$, which therefore completes the proof of (4.2). □

Recall the definition (1.3) of $r' = r'(L_1, \dots, L_4, \mathcal{R})$. It will be convenient to set

$$X' := r'X$$

in what follows, and to assume that $r'X^{1-\varepsilon} \geqslant 1$. In particular this ensures that $\log X' \gg \log X$.

Our next task is to establish a uniform version of [HB03, Lemma 3.1]. The reader is recommended to consult [HB03] for full details of the ensuing argument, since we will only stress those parts where modification is needed. When $0 < m \leqslant X'$ and $m \equiv 1 \bmod 4$, we may write

$$r(m) = 4 \sum_{\substack{d\mid m\\ d\leqslant X'^{1/2}}} \chi(d) + 4 \sum_{\substack{e\mid m\\ m>eX'^{1/2}}} \chi(e) = 4A_+(m) + 4A_-(m),$$

say, as in [HB03]. This will be employed with $m = L_i(\mathbf{x})$ for $1 \leqslant i \leqslant 3$. The conditions $L_i(\mathbf{x}) \equiv v_1 \bmod 4$ and $v_1 \equiv 1 \bmod 4$ yield $m \equiv 1 \bmod 4$. In a similar fashion, we may write

$$r(m) = 4B_+(m) + 4C(m) + 4B_-(m),$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

under the same hypotheses on m, with

$$B_+(m) := \sum_{\substack{d|m\\ d\leqslant Y}} \chi(d), \quad C(m) := \sum_{\substack{d|m\\ Y<d\leqslant X'/Y}} \chi(d), \quad B_-(m) := \sum_{\substack{e|m\\ m>eX'/Y}} \chi(e).$$

Here $1 \leqslant Y \leqslant X'^{1/2}$ is a parameter to be chosen in due course. This formula will be used with $m = L_4(\mathbf{x})$. The variable e in $A_-(L_i(\mathbf{x}))$ and $B_-(L_4(\mathbf{x}))$ will satisfy $e \leqslant X'^{1/2}$ and $e \leqslant Y$, respectively.

On writing

$$S_{\pm,\pm,\pm,\pm} := \sum_{\mathbf{x}\in X\mathcal{R}_4} A_\pm(L_1(\mathbf{x}))A_\pm(L_2(\mathbf{x}))A_\pm(L_3(\mathbf{x}))B_\pm(L_4(\mathbf{x})),$$

we obtain

$$S_*(X) = 4S_0 + 4^4 \sum S_{\pm,\pm,\pm,\pm},$$

which is the analogue of [HB03, Equation (3.4)]. Let us consider the sum $S_{+,+,-,-}$, the other 15 sums being handled similarly. Write $Q_1 = Q_2 = Q_3 = X'^{1/2}$ and $Q_4 = Y$. Then

$$S_{+,+,-,-} = \sum_{\substack{\mathbf{d}\in\mathbb{N}^4\\ d_i\leqslant Q_i}} \chi(d_1d_2d_3d_4)\#(\Gamma_{\mathbf{d}} \cap X\mathcal{R}_4(\mathbf{d})),$$

where $\mathcal{R}(\mathbf{d}) := \{\mathbf{x} \in \mathcal{R} : L_3(\mathbf{x}) > d_3X'^{1/2},\ L_4(\mathbf{x}) > d_4X'/Y\}$. An application of Lemma 3 therefore implies that

$$S_{+,+,-,-} = \sum_{\substack{\mathbf{d}\in\mathbb{N}^4\\ d_i\leqslant Q_i}} \chi(d_1d_2d_3d_4)\frac{\operatorname{meas}(\mathcal{R}(\mathbf{d}))X^2}{4\det\Gamma_{\mathbf{d}}} + O(T), \tag{4.3}$$

with

$$T := L_\infty^\varepsilon r_\infty X X'^{3/4}Y^{1/2}(\log X')^A + X'^{3/2}Y$$

and $A \geqslant 2$. Choosing $Y = X'^{1/2}/(\log X')^{2A+2}$, we obtain

$$T \ll \frac{L_\infty^\varepsilon r_\infty r' X^2}{\log X'} + \frac{r'^2X^2}{(\log X')^{2A+2}}.$$

We claim that it is possible to take

$$T \ll \frac{L_\infty^\varepsilon r_\infty r' X^2}{\log X} \tag{4.4}$$

in (4.3). When $r' \leqslant r_\infty(\log X')^{2A+1}$ this is trivial, since the assumption $r'X^{1-\varepsilon} \geqslant 1$ yields $\log X' \gg \log X$. Suppose now that $r' > r_\infty(\log X')^{2A+1} \gg r_\infty(\log X)^{2A+1}$. Then on returning to the original definition of $S_{\pm,\pm,\pm,\pm}$, it follows from an easy application of [BB06, Corollary 1] that

$$S_{+,+,-,-} \ll \sum_{\mathbf{x}\in X\mathcal{R}_4} \tau(L_1(\mathbf{x})L_2(\mathbf{x})L_3(\mathbf{x})L_4(\mathbf{x})) \ll L_\infty^\varepsilon r_\infty^2 X^2(\log X)^4 \ll L_\infty^\varepsilon r_\infty r' X^2(\log X)^{3-2A}.$$

Thus we may certainly take (4.4) in (4.3) in this case too.

Although we will omit the details here, it is easy to modify the argument of [HB03] to deduce that the main term in (4.3) is

$$\frac{\pi^4\operatorname{meas}(\mathcal{R})X^2}{4^5}\prod_{p>2}\sigma_p^* + O(L_\infty^\varepsilon r_\infty r' X^{79/40+\varepsilon}),$$

and similarly for all the $S_{\pm,\pm,\pm,\pm}$. Bringing all of this together we have therefore established the following result.

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Lemma 4. *Assume that $r'X^{1-\varepsilon} \geqslant 1$. Then we have*

$$S_*(X) = 4\pi^4 \operatorname{meas}(\mathcal{R})X^2 \prod_{p>2} \sigma_p^* + 4S_0 + O\bigg(\frac{L_\infty^\varepsilon r_\infty r' X^2}{\log X}\bigg),$$

where

$$S_0 := \sum_{\mathbf{x} \in X\mathcal{R}_4} r(L_1(\mathbf{x}))r(L_2(\mathbf{x}))r(L_3(\mathbf{x}))C(L_4(\mathbf{x})).$$

To conclude our treatment of $S_*(X)$ we must estimate S_0. Let

$$\mathcal{B} := \{m \in \mathbb{Z} : \exists\, d \mid m, Y < d \leqslant X'/Y\} \cap \{m \in \mathbb{Z} : \exists\, \mathbf{x} \in X\mathcal{R}_4, L_4(\mathbf{x}) = m\}.$$

Then as in [HB03], we write

$$S_0 \ll \sum_{m \in \mathcal{B}} S_0(m)|C(m)|, \tag{4.5}$$

where

$$S_0(m) := \sum_{\mathbf{x} \in \mathcal{A}(m)} r(L_1(\mathbf{x}))r(L_2(\mathbf{x}))r(L_3(\mathbf{x}))$$

and $\mathcal{A}(m) := \{\mathbf{x} \in X\mathcal{R}_4 : L_4(\mathbf{x}) = m\}$. We proceed to establish the following estimate.

Lemma 5. *There exists an absolute constant $c_0 > 0$ such that*

$$S_0(m) \ll L_\infty^\varepsilon r_\infty X(\log\log X')^{c_0}.$$

Proof. We begin by recalling the notation used in [HB03], with only very minor modifications. Suppose that $L_i(\mathbf{x}) = a_i x_1 + b_i x_2$ with $a_i \equiv 1 \bmod 4$ and $b_i \equiv 0 \bmod 4$. Then we have $x_1 = (m - b_4 x_2)/a_4$ and

$$L_i(\mathbf{x}) = \frac{A_i m + B_i n}{a_4} = L_i'(m, n),$$

with $A_i = a_i$, $n = x_2$ and $B_i = a_4 b_i - a_i b_4$. It is crucial to observe that $B_1B_2B_3 \neq 0$ since none of L_1, L_2, L_3 are proportional to L_4. We will use the inequality $r(L_i'(m,n)) \leqslant r(a_4(A_i m + B_i n))$. Note that

$$a_4(A_i m + B_i n) = a_4 \gcd(A_i m, B_i)(A_i'(m) + B_i' n)$$

with $B_i' := B_i/\gcd(A_i m, B_i)$ and $A_i'(m) = A_i m/\gcd(A_i m, B_i)$. In particular these coefficients are coprime. Write

$$H = a_4^3 B_1 B_2 B_3 \prod_{1 \leqslant i \neq j \leqslant 3} |a_i b_j - a_j b_i|,$$

and introduce the multiplicative function r_1, given by

$$r_1(p^\nu) = \begin{cases} \nu + 1, & \text{if } p \mid H, \\ r(p^\nu), & \text{otherwise.} \end{cases}$$

Then we have

$$\begin{aligned} r(L_1(\mathbf{x}))r(L_2(\mathbf{x}))r(L_3(\mathbf{x})) &\leqslant r(a_4^3)r(B_1B_2B_3)\prod_{i=1}^3 r_1(A_i'(m) + B_i' n) \\ &\ll L_\infty^\varepsilon r_1\big(G_m(n)\big), \end{aligned}$$

where $G_m(X) := \prod_{i=1}^3 (A_i'(m) + B_i' X)$ is a primitive cubic polynomial with coefficients bounded in size by $O(L_\infty^6)$.

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Bringing all of this together we have so far shown that

$$S_0(m) \ll L_\infty^\varepsilon \sum_{n \leqslant r_\infty X} r_1(G_m(n)).$$

Arguing as in [HB03, § 4] to handle the possible fixed prime divisors of G_m, it now follows from [BB06, Theorem 2] that there exists an absolute constant $c_0 > 0$ such that

$$S_0(m) \ll L_\infty^\varepsilon r_\infty X (\log\log m)^{c_0} \ll L_\infty^\varepsilon r_\infty X (\log\log X')^{c_0},$$

since visibly $S_0(m) = 0$ unless $m \leqslant r'X = X'$. This completes the proof of the lemma. □

It remains to consider the sum $\sum_{m\in\mathcal{B}} |C(m)|$ in (4.5). It is precisely at this point that our argument diverges from the proof of Heath-Brown. Define the function

$$Q(\lambda) := \lambda \log \lambda - \lambda + 1. \tag{4.6}$$

Then we have

$$\max_{\lambda\in(1,2)} \min\{Q(\lambda), 2Q(\lambda/2)\} = Q(1/\log 2) = 2Q(1/(2\log 2)) = \eta,$$

where η is given by (1.4). With this in mind, we have the following result.

Lemma 6. *We have*

$$\sum_{m\in\mathcal{B}} |C(m)| \ll \frac{r'X(\log\log X')^{9/4}}{(\log X')^\eta}.$$

In view of the fact that $|C(m)| \geqslant 1$ for any m such that $C(m) \neq 0$, we deduce from [HT98, Theorem 21(ii)] that one cannot hope to do much better than this estimate, since up to multiplication by powers of $\log\log X'$ it is the true order of magnitude of the set $\mathcal{B}$.

Proof of Lemma 6. Define the sum

$$\sigma(X'; v) := \sum_{1\leqslant m\leqslant X'} |C(m)|^2 v^{\Omega(m)},$$

for any real number $v \in [0, 1]$, where $\Omega(m)$ denotes the total number of prime factors of m. A crucial ingredient in the proof of Lemma 6 will be the estimate

$$\sigma(X'; v) \ll X'(\log\log X')^3 (\log Y)^{2v-2}. \tag{4.7}$$

This coincides with the estimate obtained by Heath-Brown in [HB03, § 5] when $v = 1$. To establish (4.7) we begin by expanding $|C(m)|^2$ and drawing out the highest common factor of the variables involved. This gives

$$|C(m)|^2 = \sum_{h|m} \chi(h^2) \sum_{\substack{k_1|m/h \\ Y<hk_1\leqslant X'/Y}} \chi(k_1) \sum_{\substack{k_2|m/hk_1 \\ Y<hk_2\leqslant X'/Y \\ \gcd(k_1,k_2)=1}} \chi(k_2).$$

Once substituted into $\sigma(X'; v)$, let us write σ_1 for the overall contribution from $h \leqslant Y$ and σ_2 for the contribution from the remaining h. Note that we must have $Y < h \leqslant X'/Y$ in σ_2, since $h \leqslant hk_1 \leqslant X'/Y$. Write $Z := X'/Y$. Then we have

$$\sigma_1 = \sum_{h\leqslant Y} \chi(h^2) v^{\Omega(h)} \sum_{Y/h<k_1\leqslant Z/h} \chi(k_1) v^{\Omega(k_1)} \sum_{n<Z/k_1} v^{\Omega(n)} \sum_{k_2} \chi(k_2) v^{\Omega(k_2)},$$

where the final summation is over integers k_2 such that $\gcd(k_1, k_2) = 1$ and $Y/h < k_2 \leqslant \min\{Z/h, X'/hk_1n\}$. Here the inequality $n < Z/k_1$ follows from the two inequalities $n \leqslant X'/hk_1k_2$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

and $hk_2 > Y$. We will need the basic estimates

$$\sum_{n\leqslant x} v^{\Omega(n)} \ll x(\log 2x)^{v-1} \tag{4.8}$$

and

$$\sum_{\substack{k_2\leqslant x\\ \gcd(k_1,k_2)=1}} \chi(k_2)v^{\Omega(k_2)} \ll \tau(k_1)x\exp\{-3\sqrt{\log 2x}\}, \tag{4.9}$$

for any $v \in [0,1]$. When $k_1 = 1$ the latter bound follows from the fact that the corresponding Dirichlet series can be embedded holomorphically into a zero-free region for $L(s,\chi)$. The general case then follows from an application of Möbius inversion.

For fixed values of h and k_1, (4.9) and (4.8) imply that the overall contribution to σ_1 from $n \leqslant X'/Zk_1$ is

$$\begin{aligned}&\ll \frac{\tau(k_1)Z}{h}\exp\{-3\sqrt{\log 2Y/h}\}\sum_{n\leqslant X'/Zk_1} v^{\Omega(n)}\\ &\ll \frac{\tau(k_1)X'}{hk_1}(\log(2\max\{1,hY^2/X'\}))^{v-1}\exp\{-3\sqrt{\log 2Y/h}\}.\end{aligned}$$

Here we have used the fact that $X'/Zk_1 \geqslant hX'/Z^2 = hY^2/X'$, since $k_1 \leqslant Z/h$. Next, on breaking the interval into dyadic intervals we deduce from (4.8) that

$$\begin{aligned}\sum_{Y/k_1<n\leqslant Z/k_1}\frac{v^{\Omega(n)}}{n} &\ll \log(X'/Y^2)\max_{H>hY/Z}\sum_{H<n\leqslant 2H}\frac{v^{\Omega(n)}}{n}\\ &\ll \log(X'/Y^2)(\log(2\max\{1,hY^2/X'\}))^{v-1},\end{aligned}$$

for $v \in [0,1]$. For fixed values of h and k_1, it therefore follows from (4.9) that the contribution from $n > X'/Zk_1$ is

$$\begin{aligned}&\ll \frac{\tau(k_1)X'}{hk_1}\exp\{-3\sqrt{\log 2Y/h}\}\sum_{Y/k_1<n\leqslant Z/k_1}\frac{v^{\Omega(n)}}{n}\\ &\ll \frac{\tau(k_1)X'}{hk_1}\log(X'/Y^2)(\log(2\max\{1,hY^2/X'\}))^{v-1}\exp\{-3\sqrt{\log 2Y/h}\}.\end{aligned}$$

Combining these estimates with partial summation, we therefore deduce that

$$\begin{aligned}\sigma_1 &\ll X'(\log\log X')\sum_{h\leqslant Y}\Bigg(\frac{v^{\Omega(h)}}{h}(\log(Z/h))^2(\log(2\max\{1,hY^2/X'\}))^{v-1}\\ &\qquad\qquad\times\exp\{-3\sqrt{\log 2Y/h}\}\Bigg)\\ &\ll X'(\log\log X')^3(\log Y)^{2v-2},\end{aligned}$$

which is satisfactory for (4.7).

To bound σ_2, we estimate trivially the sum over k_2 as $\min\{Z/h, X'/hk_1n\}$. Arguing as above, it follows that

$$\begin{aligned}\sigma_2 &\ll X'\log(X'/Y^2)\sum_{Y<h\leqslant Z}\frac{v^{\Omega(h)}}{h}\sum_{k_1\leqslant Z/h}\frac{(\log Y)^{v-1}}{k_1}\\ &\ll X'(\log\log X')^3(\log Y)^{2v-2}.\end{aligned}$$

This therefore completes the proof of (4.7).

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

The rest of the argument is inspired by the proof of [HT98, Theorem 21(ii)]. We define the set of primes $E := \{p \text{ prime} : 2 < p \leqslant Y\}$, and introduce the quantities

$$\Omega(m, E) := \sum_{\substack{p^\nu \| m \\ p \in E}} \nu, \qquad E(x) := \sum_{\substack{p \leqslant x \\ p \in E}} \frac{1}{p},$$

for any $m \in \mathbb{N}$ and any $x > 0$. We will make use of the well-known bound (cf. [HT98, Exercise 04])

$$\#\{m \leqslant x : \Omega(m, E) \geqslant \lambda E(x)\} \ll \frac{x}{(\log x)^{Q(\lambda)} (\log\log x)^{1/2}}, \tag{4.10}$$

where Q is given by (4.6), and which is valid for any $\lambda \in [1, 2]$. We observe that

$$\sum_{m \in \mathcal{B}} |C(m)| \leqslant \sum_{1 \leqslant m \leqslant X'} \Big| \sum_{\substack{d \mid m \\ Y < d \leqslant Z}} \chi(d) \Big|, \tag{4.11}$$

where

$$Y = \frac{{X'}^{1/2}}{(\log X')^{2A+2}}, \quad Z = \frac{X'}{Y} = {X'}^{1/2} (\log X')^{2A+2}.$$

We will break the sum over m into three parts.

Let $\mathcal{B}_1$ denote the set of positive integers $m \leqslant X'$ such that

$$\Omega(m, E) \leqslant E(X')/\log 2,$$

let $\mathcal{B}_2$ denote the corresponding set for which

$$E(X')/\log 2 < \Omega(m, E) \leqslant 2E(X'),$$

and let $\mathcal{B}_3$ denote the remaining set of positive integers $m \leqslant X'$. We proceed by writing $S_j = \sum_{m \in \mathcal{B}_j} |\sum_d \chi(d)|$, for $1 \leqslant j \leqslant 3$, with the conditions on d as in (4.11). We then have

$$S_1 \leqslant \sum_{m \in \mathcal{B}_1} \sum_{\substack{d \mid m \\ Y < d \leqslant Z}} 1 = \sum_{h+k \leqslant E(X')/\log 2} \sum_{\substack{Y < d \leqslant Z \\ \Omega(d,E) = h}} \sum_{\substack{n \leqslant X'/d \\ \Omega(n,E) = k}} 1.$$

Since $E(X'/d) = E(X')$ for $d \leqslant Z$, an application of [HT98, Theorem 08] yields

$$\sum_{\substack{n \leqslant X'/d \\ \Omega(n,E) = k}} 1 \ll \frac{X'}{d} \exp\{-E(X')\} \frac{E(X')^k}{k!},$$

uniformly for $k \leqslant (3 - \varepsilon)E(X')$. Hence a repeated application of [HT98, Theorem 08] reveals that

$$\sum_{\substack{Y < d \leqslant Z \\ \Omega(d,E) = h}} \sum_{\substack{n \leqslant X'/d \\ \Omega(n,E) = k}} 1 \ll X' \log(Z/Y) \exp\{-2E(X')\} \frac{E(X')^h}{h!} \frac{E(X')^k}{k!},$$

uniformly for $h, k \leqslant (3 - \varepsilon)E(X')$. It is clear that $\log(Z/Y) \ll \log\log X'$ and

$$E(X') = E(Y) = \log\log Y + O(1) = \log\log X' + O(1). \tag{4.12}$$

Moreover, the binomial theorem implies that

$$\ell! \sum_{h+k=\ell} \frac{1}{h!k!} = \sum_{0 \leqslant h \leqslant \ell} \frac{\ell!}{h!(\ell - h)!} = 2^\ell,$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

for fixed ℓ. We therefore deduce from [HT98, Theorem 09] that

$$\begin{aligned} S_1 &\ll X' \log\log X' \sum_{\ell \leqslant E(X')/\log 2} \exp\{-2E(X')\}\frac{(2E(X'))^\ell}{\ell!} \\ &\ll X'(\log\log X')^{1/2}\exp\{-2Q(1/(2\log 2))E(X')\} \\ &\ll X'(\log\log X')^{1/2}(\log X')^{-\eta}, \end{aligned}$$

which is satisfactory for the lemma.

We now turn to S_2. Let $S_2(\ell)$ denote the overall contribution to S_2 from m such that $\Omega(m,E)=\ell$. There are clearly $O(\log\log X')$ possible values for ℓ. Write $\ell=\lambda E(X')$, for some $\lambda \in (1/\log 2, 2]$. Then on combining the Cauchy–Schwarz inequality with (4.7) and (4.10), we obtain

$$\begin{aligned} S_2(\ell)^2 &\ll \frac{X'}{(\log X')^{Q(\lambda)}(\log\log X')^{1/2}}((\lambda/2)^{-\lambda E(X')}\sigma(X',\lambda/2)) \\ &\ll \frac{X'^2(\log\log X')^{5/2}}{(\log X')^{Q(\lambda)+\lambda(\log(\lambda/2)-1)+2}}, \end{aligned}$$

since $E(X')=\log\log X'+O(1)$ by (4.12). Hence it follows that

$$S_2=\sum_{\ell \ll \log\log X'} S_2(\ell) \ll \frac{X'(\log\log X')^{9/4}}{(\log X')^{Q(\lambda)/2+\lambda(\log(\lambda/2)-1)/2+1}}.$$

This is satisfactory for the statement of the lemma, since

$$Q(\lambda)/2+\lambda(\log(\lambda/2)-1)/2+1 \geqslant Q(1/\log 2),$$

for $\lambda \geqslant 1/\log 2$.

It remains to deal with the sum S_3, which corresponds to a summation over positive integers $m \leqslant X'$ for which $\Omega(m,E) > 2E(X')$. For this we will combine the Cauchy–Schwarz inequality with (4.7) for $v=1$ and the bound (4.10), to deduce that

$$S_3 \ll \left(\frac{X'\sigma(X',1)}{(\log X')^{Q(2)}(\log\log X')^{1/2}}\right)^{1/2} \ll \frac{X'(\log\log X')^{5/4}}{(\log X')^{Q(2)/2}}.$$

This too is satisfactory for the statement of the lemma, since $Q(2)/2 > \eta$, and so completes its proof. □

Combining Lemmas 5 and 6 in (4.5), we may now conclude that there exists an absolute constant $c_1>0$ such that

$$S_0 \ll \frac{L_\infty^\varepsilon r_\infty r' X^2(\log\log X')^{c_1}}{(\log X')^\eta} \ll \frac{L_\infty^\varepsilon r_\infty r' X^2}{(\log X')^{\eta-\varepsilon}} \ll \frac{L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}},$$

since we have assumed that $r'X^{1-\varepsilon} \geqslant 1$ in the statement of Theorem 1. Once inserted into Lemma 4, this therefore completes the proof of the theorem.

5. Linear transformations

Our proof of Theorems 2 and 3 will involve first establishing the relevant estimate for a specific choice of $j \in \{*,0,1\}$. The corresponding estimate for the remaining values of j will be obtained via simple changes of variables. Thus it will be important to consider the effect of linear transformations on the sums (1.9), and that is the purpose of the present section.

We begin by recording a preliminary result from group theory. For any group G and any subgroup $H \subseteq G$, write $[G:H]$ for the index of H in G.

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

LEMMA 7. *Let A, B be subgroups of finite index in a group G, such that $[G : A]$ and $[G : B]$ are coprime. Then we have*

$$[G : A \cap B] = [G : A][G : B].$$

Proof. For any $x, y \in G$ we claim that either $xA \cap yB$ is empty, or else it is a left coset of $A \cap B$ in G. Indeed, supposing that $xA \cap yB$ is non-empty, we let $c \in xA \cap yB$. Note that $xA = cA$ and $yB = cB$. But then it follows that

$$xA \cap yB = cA \cap cB = c(A \cap B)$$

as required. Thus it follows that the total number of left cosets of $A \cap B$ in G is

$$[G : A \cap B] \leqslant [G : A][G : B].$$

However, by Lagrange's theorem we have $[G : A \cap B] = [G : A][A : A \cap B]$, whence $[G : A]$ divides $[G : A \cap B]$. Similarly, $[G : B]$ divides $[G : A \cap B]$. Thus it follows that

$$[G : A][G : B] \leqslant [G : A \cap B],$$

since $\gcd([G : A], [G : B]) = 1$. Once coupled with our upper bound for $[G : A \cap B]$, this completes the proof of the lemma. □

It will be useful to have a convenient way of referring back to the statements of our main results. Let us say that 'Hypothesis-(j, k)' holds if $S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}})$ satisfies the asymptotic formula described in Theorem 3 for all $L_1, \dots, L_4, \mathcal{R}$ that satisfy $\mathsf{NH}_k(\mathbf{d})$. Thus Hypothesis-$(j, k)$ amounts to the established existence of an asymptotic formula

$$S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}}) = \delta_{j,k}(\mathbf{A})C_0X^2 + O\left(\frac{D^{\varepsilon}L_{\infty}^{\varepsilon}r_{\infty}r'X^2}{(\log X)^{\eta-\varepsilon}}\right),$$

for $r'X^{1-\varepsilon} \geqslant 1$, under the assumption that $\mathsf{NH}_k(\mathbf{d})$ holds. Here

$$C_0 = C_0(L_1, \dots, L_4; \mathbf{d}, \Gamma_{\mathbf{D}}, \mathcal{R}) := \frac{\pi^4 \operatorname{meas}(\mathcal{R})}{\det \Gamma_{\mathbf{D}}} \prod_{p>2} \sigma_p, \tag{5.1}$$

and σ_p is given by (1.10) and (1.11).

Let $L_1, \dots, L_4 \in \mathbb{Z}[x_1, x_2]$ be binary linear forms, and let $\mathcal{R} \subset \mathbb{R}^2$. Let $(\mathbf{d}, \mathbf{D}) \in \mathcal{D}$, where $\mathcal{D}$ is given by (1.8), and set

$$\mathcal{X} := \Gamma_{\mathbf{D}} \cap X\mathcal{R}. \tag{5.2}$$

Then for a given matrix $\mathbf{M} \in \mathrm{GL}_2(\mathbb{Z})$, we define the sum

$$S_{\mathbf{M}} := \sum_{\substack{\mathbf{y} \in \mathbb{Z}^2,\ \mathbf{M}\mathbf{y} \in \mathcal{X} \\ 2 \nmid y_1,\ y_2 \equiv j \bmod 2}} r\left(\frac{L_1(\mathbf{M}\mathbf{y})}{d_1}\right) r\left(\frac{L_2(\mathbf{M}\mathbf{y})}{d_2}\right) r\left(\frac{L_3(\mathbf{M}\mathbf{y})}{d_3}\right) r\left(\frac{L_4(\mathbf{M}\mathbf{y})}{d_4}\right).$$

Here, as throughout this paper, we let $\mathrm{GL}_2(\mathbb{Z})$ denote the set of non-singular 2×2 integer-valued matrices with non-zero determinant. Note that $S_{\mathbf{M}}$ depends on $X, \mathbf{d}, \mathbf{D}, L_1, \dots, L_4$ and j, in addition to $\mathbf{M}$. In particular we have $S_{\mathbf{M}} = S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}})$, when $\mathbf{M}$ is the identity matrix. In general let us write $\|\mathbf{M}\|$ to denote the maximum modulus of the coefficients of $\mathbf{M}$. Bearing all this notation in mind, the following elementary result will prove useful.

LEMMA 8. *Let $(j, k) \in \{*, 0, 1\} \times \{0, 1, 2\}$ and suppose that Hypothesis-(j, k) holds. Let $\mathbf{M} \in \mathrm{GL}_2(\mathbb{Z})$ such that $\det \mathbf{M} = 2^m$ for some $m \in \mathbb{Z}_{\geqslant 0}$, and define $M_i(\mathbf{y}) := L_i(\mathbf{M}\mathbf{y})$. Let $\varepsilon > 0$ and suppose that $r'(L_1, \dots, L_4, \mathcal{R})X^{1-\varepsilon} \geqslant 1$. Assume that $M_1, \dots, M_4, \mathcal{R}_{\mathbf{M}}$ satisfy $\mathsf{NH}_k(\mathbf{d})$, where*

$$\mathcal{R}_{\mathbf{M}} := \{\mathbf{M}^{-1}\mathbf{z} : \mathbf{z} \in \mathcal{R}\}. \tag{5.3}$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Then we have

$$S_{\mathbf{M}} = \frac{\delta_{j,k}(\mathbf{AM})C_0}{\det \mathbf{M}} X^2 + O\bigg(\frac{D^{\varepsilon} L_{\infty}^{\varepsilon} \|\mathbf{M}\|^{\varepsilon} r_{\infty}(\mathcal{R}_{\mathbf{M}}) r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg),$$

where $D = D_1 \cdots D_4$, $L_{\infty} = L_{\infty}(L_1, \dots, L_4)$, $r' = r'(L_1, \dots, L_4, \mathcal{R})$.

It is important to note that the definition of σ_p that appears in (5.1) is precisely as in (1.11). Thus it involves lattices that depend on $L_1, \dots, L_4$, rather than $M_1, \dots, M_4$. The net outcome of Lemma 8 is that, for linear transformations that preserve the relevant normalisation conditions and have determinant 2^m for some $m \geqslant 0$, the main term of the corresponding asymptotic formula should be multiplied by $\delta_{j,k}(\mathbf{AM})(\delta_{j,k}(\mathbf{A}) \det \mathbf{M})^{-1}$.

Proof of Lemma 8. Recall the definition (5.2) of $\mathcal{X}$, and the notation introduced in (1.7). We begin by noting that $\mathbf{y} \in \mathbb{Z}^2$ and $\mathbf{My} \in \mathcal{X}$ if and only if $\mathbf{y} \in \Lambda_{\mathbf{M}} \cap \mathcal{R}_{\mathbf{M}}$, where

$$\Lambda_{\mathbf{M}} := \{\mathbf{y} \in \mathbb{Z}^2 : D_i \mid L_i(\mathbf{My})\} = \Gamma(\mathbf{D}; M_1, \dots, M_4),$$

and $\mathcal{R}_{\mathbf{M}}$ is given by (5.3). We claim that

$$\det \Lambda_{\mathbf{M}} = \det \Gamma(\mathbf{D}; M_1, \dots, M_4) = \det \Gamma(\mathbf{D}; L_1, \dots, L_4), \tag{5.4}$$

for any matrix $\mathbf{M} \in \mathrm{GL}_2(\mathbb{Z})$ such that $\gcd(\det \mathbf{M}, D) = 1$. In particular, since $\mathbf{M}$ has determinant 2^m for some $m \in \mathbb{Z}_{\geqslant 0}$, this holds for any $\mathbf{D} \in \mathbb{N}^4$ such that $2 \nmid D$. Assume (5.4) to be true for the moment, and note that

$$\mathrm{meas}(\mathcal{R}_{\mathbf{M}}) = \frac{\mathrm{meas}(\mathcal{R})}{\det \mathbf{M}}, \qquad r'(M_1, \dots, M_4, \mathcal{R}_{\mathbf{M}}) = r'(L_1, \dots, L_4, \mathcal{R}) = r',$$

in the notation of (1.3). Recalling the definitions in (1.1) and (1.2), we therefore deduce from Hypothesis-(j,k) that

$$\begin{aligned} S_{\mathbf{M}} &= \frac{\delta_{j,k}(\mathbf{AM})\pi^4 \,\mathrm{meas}(\mathcal{R}_{\mathbf{M}})}{\det \Gamma(\mathbf{D}; M_1, \dots, M_4)} X^2 \prod_{p>2} \sigma_p' + O\bigg(D^{\varepsilon} L_{\infty}(M_1, \dots, M_4)^{\varepsilon} r_{\infty}(\mathcal{R}_{\mathbf{M}}) r' \frac{X^2}{(\log X)^{\eta-\varepsilon}} \bigg) \\ &= \frac{\delta_{j,k}(\mathbf{AM})\pi^4 \,\mathrm{meas}(\mathcal{R})}{(\det \mathbf{M})(\det \Gamma(\mathbf{D}; L_1, \dots, L_4))} X^2 \prod_{p>2} \sigma_p' + O\bigg(D^{\varepsilon} L_{\infty}(M_1, \dots, M_4)^{\varepsilon} r_{\infty}(\mathcal{R}_{\mathbf{M}}) r' \frac{X^2}{(\log X)^{\eta-\varepsilon}} \bigg), \end{aligned}$$

where

$$\sigma_p' = \bigg(1 - \frac{\chi(p)}{p}\bigg)^4 \sum_{a,b,c,d=0}^{\infty} \chi(p)^{a+b+c+d} \rho_0(p^a, p^b, p^c, p^d; \mathbf{D}; M_1, \dots, M_4)^{-1}.$$

On noting that $L_{\infty}(M_1, \dots, M_4) \leqslant L_{\infty}(L_1, \dots, L_4)\|\mathbf{M}\|$, we see that the error term in this estimate for $S_{\mathbf{M}}$ is as claimed in the statement of the lemma. Moreover, (1.10) and (5.4) give

$$\begin{aligned} \rho_0(\mathbf{h}; \mathbf{D}; M_1, \dots, M_4) &= \frac{\det \Gamma\big(([D_1, d_1 h_1], \dots, [D_4, d_4 h_4]); M_1, \dots, M_4\big)}{\det \Gamma(\mathbf{D}; M_1, \dots, M_4)} \\ &= \rho_0(\mathbf{h}; \mathbf{D}; L_1, \dots, L_4), \end{aligned}$$

for any $\mathbf{h} \in \mathbb{N}^4$ such that $2 \nmid h_1 \cdots h_4$. Hence $\sigma_p' = \sigma_p$.

In order to complete the proof of Lemma 8 it remains to establish (5.4). For any matrix $\mathbf{N} \in \mathrm{GL}_2(\mathbb{Z})$ and any lattice $\Lambda \subseteq \mathbb{Z}^2$, it is easily checked that

$$\det(\mathbf{N}\Lambda) = \det \mathbf{N} \det \Lambda,$$

where $\mathbf{N}\Lambda := \{\mathbf{Nx} : \mathbf{x} \in \Lambda\}$. It therefore follows that

$$\det \Lambda_{\mathbf{M}} = \frac{\det(\mathbf{M}\Lambda_{\mathbf{M}})}{\det \mathbf{M}}.$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Note that $\mathbf{M}\Lambda_{\mathbf{M}} = \mathsf{M} \cap \Gamma(\mathbf{D}; L_1, \dots, L_4)$, where $\mathsf{M} = \{\mathbf{My} : \mathbf{y} \in \mathbb{Z}^2\}$. In particular we have $\det \mathsf{M} = \det \mathbf{M}$. To establish (5.4), it therefore suffices to show that

$$\det(\mathsf{L} \cap \Gamma(\mathbf{D}; L_1, \dots, L_4)) = (\det \mathsf{L})(\det \Gamma(\mathbf{D}; L_1, \dots, L_4))$$

for any lattice $\mathsf{L} \subseteq \mathbb{Z}^2$ such that $\gcd(\det \mathsf{L}, D_1D_2D_3D_4) = 1$. But this follows immediately from Lemma 7, since the determinant of a sublattice of $\mathbb{Z}^2$ is equal to its index in $\mathbb{Z}^2$. □

6. Proof of Theorem 2

We are now ready to establish the statement of Theorem 2. The proof will be in two stages: first we will establish the result for $j = *$, and then we will proceed to handle the cases $j \in \{0, 1\}$. Our proof of the estimate for $j = *$ is actually a straightforward generalisation of an argument already present in Heath-Brown's work [HB03, § 7], but we will include full details here for the sake of completeness.

Assume that $(\mathbf{d}, \mathbf{D}) \in \mathcal{D}$, where $\mathcal{D}$ is given by (1.8). In particular it follows that there exists $\mathbf{x} \in \Gamma_{\mathbf{D}}$ such that $x_1 \equiv 1 \bmod 4$, where $\Gamma_{\mathbf{D}}$ is given by (1.7). Indeed, the vector $\mathbf{x} = D_1^2D_2^2D_3^2D_4^2(1, 1)$ is clearly satisfactory. In estimating $S_*(X; \mathbf{d}, \Gamma_{\mathbf{D}})$, our goal is to replace the summation over lattice points $\mathbf{x} \in \Gamma_{\mathbf{D}}$ by a summation over all integer points restricted to a certain region. Given any basis $\mathbf{e}_1, \mathbf{e}_2$ for $\Gamma_{\mathbf{D}}$, let $M_i(\mathbf{v})$ be the linear form obtained from $d_i^{-1}L_i(\mathbf{x})$ via the change of variables $\mathbf{x} \mapsto v_1\mathbf{e}_1 + v_2\mathbf{e}_2$. We claim that there is a choice of basis such that

$$M_i(\mathbf{v}) \equiv v_1 (\bmod\ 4), \tag{6.1}$$

for each i, and also

$$\|\mathbf{M}\| \ll \det \Gamma_{\mathbf{D}}, \tag{6.2}$$

where $\mathbf{M}$ denotes the matrix formed from the basis vectors $\mathbf{e}_1, \mathbf{e}_2$. To check the claim we let $\mathbf{e}_1, \mathbf{e}_2$ be a minimal basis for $\Gamma_{\mathbf{D}}$. Thus we may assume that

$$|\mathbf{e}_1||\mathbf{e}_2| \ll \det \Gamma_{\mathbf{D}}. \tag{6.3}$$

Now there must exist integers w_1, w_2 such that $w_1e_{11} + w_2e_{21} \equiv 1 \bmod 4$, since we have seen that there exists $\mathbf{x} \in \Gamma_{\mathbf{D}}$ such that $x_1 \equiv 1 \bmod 4$. In particular we may assume without loss of generality that e_{11} is odd, and after multiplying $\mathbf{e}_1$ by ± 1, we may as well assume that $e_{11} \equiv 1 \bmod 4$. Next, on replacing $\mathbf{e}_2$ by $\mathbf{e}_2 - k\mathbf{e}_1$ for a suitable integer $k \in \{0, 1, 2, 3\}$, we may further assume that $4 \mid e_{21}$. In view of (6.3), this basis certainly satisfies (6.2). Moreover, the normalisation conditions on $L_1, \dots, L_4$ imply that

$$d_iM_i(\mathbf{v}) = L_i(v_1\mathbf{e}_1 + v_2\mathbf{e}_2) \equiv d_i(v_1e_{11} + v_2e_{21}) \equiv d_iv_1 \pmod 4,$$

which therefore establishes (6.1) since each d_i is odd.

Note that we must sum only over odd values of v_1, since we have been summing over odd x_1 in $S_*(X; \mathbf{d}, \Gamma_{\mathbf{D}})$. On recalling the definition (5.3) of $\mathcal{R}_{\mathbf{M}}$, we may therefore deduce that

$$S_*(X; \mathbf{d}, \Gamma_{\mathbf{D}}) = \sum_{\substack{\mathbf{v} \in \mathbb{Z}^2 \cap X\mathcal{R}_{\mathbf{M}} \\ 2 \nmid v_1}} r(M_1(\mathbf{v})) \cdots r(M_4(\mathbf{v})).$$

Note that (6.1) holds by construction, and also $M_i(\mathbf{v}) > 0$ for every $\mathbf{v}$ in the summations. We are therefore in a position to apply Theorem 1 to estimate this quantity. In view of (6.2) and the fact that $\det \Gamma_{\mathbf{D}} \mid D = D_1 \cdots D_4$, we may deduce that

$$L_\infty(M_1, \dots, M_4) \leqslant \|\mathbf{M}\| L_\infty(L_1, \dots, L_4) \ll DL_\infty,$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

where $L_\infty = L_\infty(L_1, \dots, L_4)$, as usual. Next we deduce from (6.2) that

$$r_\infty(\mathcal{R}_{\mathbf{M}}) \leqslant \frac{\|\mathbf{M}\|}{|\det \mathbf{M}|} r_\infty(\mathcal{R}) \ll r_\infty(\mathcal{R}) = r_\infty,$$

since $|\det \mathbf{M}| = \det \Gamma_{\mathbf{D}}$, and furthermore

$$r'(M_1, \dots, M_4, \mathcal{R}_{\mathbf{M}}) = r'(L_1, \dots, L_4, \mathcal{R}) = r'.$$

Moreover, it is clear that $\mathrm{meas}(\mathcal{R}_{\mathbf{M}}) = \mathrm{meas}(\mathcal{R})/|\det \mathbf{M}|$. It therefore follows from Theorem 1 that

$$S_*(X; \mathbf{d}, \Gamma_{\mathbf{D}}) = \frac{4\pi^4 \,\mathrm{meas}(\mathcal{R})}{\det \Gamma_{\mathbf{D}}} X^2 \prod_{p>2} \sigma_p^* + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg),$$

where σ_p^* is given by (1.5), but with $\rho_*(\mathbf{h}) = \det \Gamma(\mathbf{h}; M_1, \dots, M_4)$. To calculate this quantity we note that it is just the index of

$$\Lambda_1 = \{\mathbf{x} = v_1 \mathbf{e}_1 + v_2 \mathbf{e} : \mathbf{v} \in \mathbb{Z}^2, h_i \mid M_i(\mathbf{v})\}$$

in $\Lambda_2 = \{\mathbf{x} = v_1 \mathbf{e}_1 + v_2 \mathbf{e} : \mathbf{v} \in \mathbb{Z}^2\}$, whence

$$\begin{aligned} \rho_*(\mathbf{h}) = [\Lambda_1 : \Lambda_2] = \frac{\det \Lambda_1}{\det \Lambda_2} &= \frac{\det\{\mathbf{x} \in \Gamma(\mathbf{D}; L_1 \dots, L_4) : d_i h_i \mid L_i(\mathbf{x})\}}{\det \Gamma(\mathbf{D}; L_1, \dots, L_4)} \\ &= \rho_0(\mathbf{h}; \mathbf{D}; L_1, \dots, L_4), \end{aligned}$$

in the notation of (1.10). This therefore establishes the estimate in Theorem 2 when $j = *$.

In order to complete the proof of Theorem 2 it remains to handle the cases $j = 0, 1$. For this we carry out the change of variables $\mathbf{x} = \mathbf{M}\mathbf{y}$, with

$$\mathbf{M} = \begin{pmatrix} 1 & 0 \\ j & 2 \end{pmatrix}.$$

This has the effect of transforming the sum into one over integers $\mathbf{y}$ such that y_1 is odd, without any restriction on y_2. Moreover, it is clear that $L_i(\mathbf{M}\mathbf{y}) = L_i(y_1, jy_1 + 2y_2) \equiv d_i y_1 \bmod 4$, so that together with $\mathcal{R}_{\mathbf{M}}$, the new linear forms satisfy $\mathsf{NH}_0(\mathbf{d})$. Since we have already seen that Hypothesis-$(*, 0)$ holds, we may deduce from Lemma 8 that

$$S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}}) = \frac{\delta_{*,0}(\mathbf{A}\mathbf{M}) C_0}{2} X^2 + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg),$$

for $j = 0, 1$, where C_0 is given by (5.1). The statement of Theorem 2 follows since $\delta_{*,0}(\mathbf{A}\mathbf{M}) = \delta_* = 4$, by (3.4).

7. Proof of Theorem 3

We are now ready to establish Theorem 3. Let $(j, k) \in \{*, 1, 2\} \times \{1, 2\}$ and let $(\mathbf{d}, \mathbf{D}) \in \mathcal{D}$. It will ease notation if we write $S_{j,k}(X)$ to denote the sum $S_j(X; \mathbf{d}, \Gamma_{\mathbf{D}})$, when $L_1, \dots, L_4, \mathcal{R}$ are assumed to satisfy $\mathsf{NH}_k(\mathbf{d})$. Furthermore, let us write

$$\mathcal{S}_\alpha := \{\mathbf{y} \in \mathbb{Z}^2 : \ y_1 \equiv 1 \bmod 4, \ y_2 \equiv \alpha \bmod 2\}, \tag{7.1}$$

for $\alpha \in \{*, 0, 1\}$. We begin by showing how an estimate for $k = 1$ can be used to deduce a corresponding estimate for the case $k = 2$.

Suppose that $k = 2$ and $j = 1$. We may clearly assume that the summation in $S_{1,2}(X)$ is only over values of $x_1 \equiv 1 \bmod 4$ and $x_2 \equiv d_2 \bmod 4$, since the summand vanishes unless

$$d_1 x_1 \equiv 2^{-k_1} L_1(\mathbf{x}) \equiv d_1 (\mathrm{mod} 4), \quad x_2 \equiv 2^{-k_2} L_2(\mathbf{x}) \equiv d_2 (\mathrm{mod} 4).$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Write $\kappa = \pm 1$ for the residue modulo 4 of d_2, and choose an integer c such that

$$a_j + b_j(\kappa + 4c) \neq 0,$$

for $j = 3, 4$, where a_j, b_j are as in (1.13). This is plainly always possible with $c \in \{0, 1, 2\}$. We will carry out the transformation $\mathbf{x} = \mathbf{M}_{c,d_2}\mathbf{y}$, with $\mathbf{M}_{c,d_2}$ given by (3.15). Such a transformation is valid if and only if there exists an integer y_2 such that $x_2 - (\kappa + 4c)x_1 = 4y_2$ where $\kappa \equiv d_2 \bmod 4$. Thus the transformation is certainly valid for $x_1 \equiv 1 \bmod 4$ and $x_2 \equiv d_2 \bmod 4$, bringing the linear forms into new forms $M_i(\mathbf{y}) = L_i(\mathbf{M}_{c,d_2}\mathbf{y})$, say. It is not hard to see that $M_1, \dots, M_4, \mathcal{R}_{\mathbf{M}_{c,d_2}}$ will satisfy $\mathsf{NH}_1(\mathbf{d})$. There is now no 2-adic restriction on y_2, so that the summation is over $\mathbf{y} \in \mathcal{S}_*$, in the notation of (7.1). We clearly have $r_\infty(\mathcal{R}_{\mathbf{M}_{c,d_2}}) \ll r_\infty(\mathcal{R})$. By combining Lemma 8 with the assumption that Hypothesis-$(*, 1)$ holds, we therefore obtain

$$S_{1,2}(X) = \frac{\delta_{*,1}(\mathbf{A}\mathbf{M}_{c,d_2})C_0}{4}X^2 + O\left(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}}\right),$$

where C_0 is given by (5.1). This is clearly satisfactory for the statement of Theorem 3, since (3.16) yields $\delta_{1,2}(\mathbf{A}) = \delta_{*,1}(\mathbf{A}\mathbf{M}_{c,d_2})/4$.

To handle $S_{0,2}(X)$ we will need to extract 2-adic powers from the variable x_2. Accordingly, we write $x_1 = y_1$ and $x_2 = 2^\xi y_2$, for $\xi \geqslant 1$ and $y_2 \equiv 1 \bmod 2$. This corresponds to the transformation $\mathbf{x} = \mathbf{M}_\xi\mathbf{y}$ with $\mathbf{M}_\xi$ given by (3.14). The resulting linear forms $M_i(\mathbf{y}) = L_i(\mathbf{M}_\xi\mathbf{y})$ will continue to satisfy $\mathsf{NH}_2(\mathbf{d})$, and the summation will be over $\mathbf{y} \in \mathcal{S}_1$. Moreover, the restriction $\mathbf{x} \in X\mathcal{R}$ in the definition of $S_{0,2}(X)$ forces the upper bound $\xi \leqslant \log(r_\infty X)$. It turns that this is too crude for our purposes and we must work a little harder to control the contribution from large values of ξ. Recall the definitions (1.1) and (1.2) of L_∞ and r_∞. We will show that

$$\sum_{\substack{\mathbf{y}\in\mathbb{Z}^2\\ \mathbf{M}_\xi\mathbf{y}\in\mathcal{X}}} r\left(\frac{L_1(\mathbf{M}_\xi\mathbf{y})}{d_1}\right)\cdots r\left(\frac{L_4(\mathbf{M}_\xi\mathbf{y})}{d_4}\right) \ll (D2^\xi L_\infty)^\varepsilon\left(r_\infty^2\frac{X^2}{2^\xi} + r_\infty^{1+\varepsilon}X^{1+\varepsilon}\right). \tag{7.2}$$

Define the multiplicative function r_1 via

$$r_1(p^\nu) = \begin{cases} 1+\nu, & \text{if } p \mid d_1d_2d_3d_4,\\ r(p^\nu), & \text{if } p \nmid d_1d_2d_3d_4,\end{cases}$$

for any prime power p^ν. Then we have

$$r\left(\frac{L_1(\mathbf{M}_\xi\mathbf{y})}{d_1}\right)\cdots r\left(\frac{L_4(\mathbf{M}_\xi\mathbf{y})}{d_4}\right) \leqslant r_1(F(\mathbf{y})),$$

where $F(\mathbf{y}) = L_1(\mathbf{M}_\xi\mathbf{y})\cdots L_4(\mathbf{M}_\xi\mathbf{y})$. The maximum modulus of the coefficients of this binary form is $O(L_\infty^4 2^{4\xi})$. Hence (7.2) follows easily on taking $X_1 = r_\infty X$ and $X_2 = 2^{-\xi}r_\infty X$ in [BB06, Corollary 1]. Note that it would not be sufficient to work instead with the trivial upper bound $O(L_\infty^\varepsilon r_\infty^{2+\varepsilon}2^{-\xi}X^{2+\varepsilon})$.

To complete our estimate for $S_{0,2}(X)$ we will combine Lemma 8 with Hypothesis-$(1, 2)$ to handle the contribution from $\xi \leqslant \xi_1$, and we will use (7.2) to handle the contribution from $\xi_1 < \xi \leqslant \log(r_\infty X)$, for a value of ξ_1 to be determined. We claim that

$$r_\infty \leqslant 2L_\infty r'. \tag{7.3}$$

To see this, suppose that $\mathbf{z} \in \mathcal{R}$ is such that $r_\infty = |z_1|$, say. Then it follows that

$$r_\infty \leqslant |a_3b_4 - a_4b_3||z_1| = |b_4L_3(\mathbf{z}) - b_3L_4(\mathbf{z})| \leqslant 2L_\infty r',$$

in the notation of (1.13). Write

$$E_1 = \frac{2^{\varepsilon\xi}X^2}{(\log X)^{\eta-\varepsilon}}, \quad E_2 = L_\infty 2^{-\xi+\varepsilon\xi}X^2 + r'^\varepsilon 2^{\varepsilon\xi}X^{1+\varepsilon},$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

and choose $\xi_1 \in \mathbb{N}$ such that $2^{\xi_1-1} < L_\infty(\log X)^\eta \leqslant 2^{\xi_1}$. Next we note that

$$C_0 \ll L_\infty^\varepsilon D^\varepsilon \frac{r_\infty^2}{\det \mathsf{\Gamma_D}} \ll D^\varepsilon L_\infty^{1+\varepsilon} r_\infty r'$$

in (5.1). Hence we deduce from (3.13) and (7.3) that

$$S_{0,2}(X) = \sum_{\xi=1}^{\xi_1} \frac{\delta_{1,2}(\mathbf{AM}_\xi)C_0}{2^\xi} X^2 + O\bigg(D^\varepsilon L_\infty^\varepsilon r_\infty r' \bigg(\sum_{\xi=1}^{\xi_1} E_1 + \sum_{\xi=\xi_1+1}^{\log(r_\infty X)} E_2 \bigg) \bigg)$$

$$= \sum_{\xi=1}^{\infty} \frac{\delta_{1,2}(\mathbf{AM}_\xi)C_0}{2^\xi} X^2 + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg)$$

$$= \delta_{0,2}(\mathbf{A})C_0 X^2 + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg).$$

This completes the treatment of $S_{0,2}(X)$.

The estimate for $S_{*,2}(X) = S_{0,2}(X) + S_{1,2}(X)$ is now an immediate consequence of our estimates for $S_{0,2}(X)$ and $S_{1,2}(X)$. Indeed we plainly have

$$\delta_{*,2}(\mathbf{A}) = \delta_{0,2}(\mathbf{A}) + \delta_{1,2}(\mathbf{A}) = \sum_{\xi=0}^{\infty} \frac{\delta_{1,2}(\mathbf{AM}_\xi)}{2^\xi}.$$

The argument that we have presented here makes crucial use of our previous work [BB06] to control the contribution from large values of ξ that feature in the change of variables. This basic technique will recur at several points in the proof of Theorem 3. Rather than repeating exactly the same details each time, however, we will merely refer the reader back to (7.2) in order to draw attention to this basic chain of reasoning.

Let $j \in \{*, 0, 1\}$. It remains to estimate $S_{j,1}(X)$. In fact it will suffice to deal only with the case $j = 1$. Indeed, the remaining cases are handled just as above, leading to (3.13) in the case $k = 1$. Assume that $L_1, \dots, L_4, \mathcal{R}$ satisfy $\mathsf{NH}_1(\mathbf{d})$. We have

$$S_{1,1}(X) = \sum_{\mathbf{x} \in \mathcal{S}_1 \cap \mathcal{X}} r\bigg(\frac{L_1(\mathbf{x})}{d_1}\bigg) r\bigg(\frac{L_2(\mathbf{x})}{d_2}\bigg) r\bigg(\frac{L_3(\mathbf{x})}{d_3}\bigg) r\bigg(\frac{L_4(\mathbf{x})}{d_4}\bigg),$$

where $\mathcal{S}_1$ is given by (7.1) and $\mathcal{X} = \mathsf{\Gamma_D} \cap X\mathcal{R}$. Let us write $S(X) = S_{1,1}(X)$ for short. Our aim is to find a linear change of variables $\mathbf{x} = \mathbf{My}$, for some $\mathbf{M} \in \mathrm{GL}_2(\mathbb{Z})$, taking the linear forms L_i into forms $M_i(\mathbf{y}) = L_i(\mathbf{My})$ such that

$$2^{-\ell_i} M_i(\mathbf{y}) \equiv d_i y_1 (\mathrm{mod}\ 4), \tag{7.4}$$

for certain $\ell_i \in \mathbb{Z}_{\geqslant 0}$. On setting $M_i' = 2^{-\ell_i} M_i$, so that $M_1', \dots, M_4'$ satisfy $\mathsf{NH}_0(\mathbf{d})$, we will then be in a position to apply Lemma 8 under the assumption that Hypothesis-$(j, 0)$ holds for $j \in \{*, 0, 1\}$. Indeed, we have already seen that Theorem 2 holds in the previous section.

Let $\mathbf{x} \in \mathcal{S}_1 \cap \mathcal{X}$, so that $x_1 \equiv 1 \bmod 4$ and $2 \nmid x_2$. Recall the assumption that (3.1) holds for appropriate $k_j, a_j', b_j', \mu_j, \nu_j$. At certain points of the argument we will find it convenient to extract 2-adic factors from the terms $2^{-k_j} L_j(\mathbf{x})$. Let us write

$$\xi_j = \nu_2(2^{-k_j} L_j(\mathbf{x})), \tag{7.5}$$

for $j = 3, 4$. This will allow certain linear transformations to take place, and it turns out that the matrices needed to bring L_i in line with (7.4) will all take the shape

$$\mathbf{M} = \begin{pmatrix} 1 & 0 \\ A & 2^{\xi+2} \end{pmatrix}, \tag{7.6}$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

for appropriate non-negative integers $A \in [0, 2^{\xi+2})$ and ξ. Here ξ will be a simple function of ξ_3 and ξ_4. Assuming that we are now in a position to combine Lemma 8 with Hypothesis-$(j,0)$, we will then obtain a contribution

$$\begin{aligned} &= \frac{\delta_{j,0}(\mathbf{AM})C_0}{2^{\xi+2}}X^2 + O\left(\frac{D^{\varepsilon}L_{\infty}^{\varepsilon}r_{\infty}r'2^{\xi\varepsilon}X^2}{(\log X)^{\eta-\varepsilon}}\right) \\ &= \frac{\delta_j C_0}{2^{\xi+2}}X^2 + O\left(\frac{D^{\varepsilon}L_{\infty}^{\varepsilon}r_{\infty}r'2^{\xi\varepsilon}X^2}{(\log X)^{\eta-\varepsilon}}\right), \end{aligned} \tag{7.7}$$

since (3.4) implies that $\delta_{j,0}(\mathbf{B}) = \delta_j$, and furthermore,

$$r_{\infty}(\mathcal{R}_{\mathbf{M}}) \leqslant \frac{\|\mathbf{M}\|}{\det \mathbf{M}} r_{\infty}(\mathcal{R}) = r_{\infty}(\mathcal{R}) = r_{\infty}.$$

Finally, we will need to sum this quantity over all available ξ_3 and ξ_4. It is here that we must return to (7.2) and repeat the sort of argument used there to handle the large values of ξ_3 and ξ_4.

Under any transformation $\mathbf{x} = \mathbf{My}$, with $\mathbf{M}$ taking the shape (7.6), it follows from condition $(\mathrm{iv}')_{\mathbf{d}}$ in the introduction that

$$2^{-k_j}L_j(\mathbf{My}) \equiv d_j y_1 (\mathrm{mod}\, 4)$$

for $j = 1, 2$. As long as our transformations have this general shape therefore, we will be able to focus our attention on the effect that the transformation has on the linear forms L_3 and L_4. Unfortunately, bringing these forms into the required shape is not entirely straightforward, and the permissible choice of $\mathbf{M}$ depends intimately upon the values of a_j', b_j', μ_j, ν_j in (3.1). We may assume that these constants satisfy (3.2) and (3.3), and we proceed to consider a number of distinct subcases separately.

7.1 The case $\max\{\mu_3, \nu_3\} \geqslant 1$ and $\max\{\mu_4, \nu_4\} \geqslant 1$

This case is equivalent to the case in which precisely two of the exponents $\mu_3, \mu_4, \nu_3, \nu_4$ are non-zero, which in turn is equivalent to the statement that $\mu_j + \nu_j \geqslant 1$ for $j = 3, 4$, since $\mu_3\nu_3 = \mu_4\nu_4 = 0$. In particular it follows that $2^{-k_j}L_j(\mathbf{x})$ is odd for any odd values of x_1, x_2. Recall that the summation is over $x_1 \equiv 1 \bmod 4$ and x_2 odd in $S(X)$. Let us write g for the number of values of $\gamma \in \{-1, 1\}$ such that

$$2^{-k_j}L_j(1, \gamma) = 2^{\mu_j}a_j' + 2^{\nu_j}b_j'\gamma \equiv d_j (\mathrm{mod}\, 4) \tag{7.8}$$

for $j = 3$ and 4. Our aim is to show that

$$\delta_{1,1}(\mathbf{A}) = g, \tag{7.9}$$

which we claim is satisfactory for (3.6)–(3.8). To see this, we suppose first that $\nu_3, \nu_4 \geqslant 1$. Then it is clear that $g = 2$ if a_j' is congruent to $d_j - 2^{\nu_j}$ modulo 4 for $j = 3, 4$, and $g = 0$ otherwise. When $\mu_3, \mu_4 \geqslant 1$, we have $g = 1$ if $b_3'd_3 - 2^{\mu_3} \equiv b_4'd_4 - 2^{\mu_4} \bmod 4$, and $g = 0$ otherwise. When $\mu_4, \nu_3 \geqslant 1$ we have $g = 1$ when $a_3' \equiv d_3 - 2^{\nu_3} \bmod 4$, the value of γ being given by the residue of $b_4'd_4 - 2^{\mu_4}$ modulo 4, and $g = 0$ otherwise. Finally, the case $\mu_3, \nu_4 \geqslant 1$ is symmetric.

It remains to establish (7.9). We may clearly proceed under the assumption that $g \geqslant 1$. Let us write $S(X) = \sum_{\gamma} S(X; \gamma)$, where $S(X; \gamma)$ is the overall contribution to $S(X)$ from vectors such that $x_2 \equiv \gamma \bmod 4$, and the summation is over the g values of γ for which (7.8) holds. We will carry out the transformation

$$\mathbf{M} = \begin{pmatrix} 1 & 0 \\ \gamma & 4 \end{pmatrix}.$$

This transformation is valid if and only if there exists an integer y_2 such that $x_2 = \gamma y_1 + 4y_2$, for each $\mathbf{x}$ in $S(X)$. This is clearly true for $x_1 = y_1 \equiv 1 \bmod 4$ and $x_2 \equiv \gamma \bmod 4$. Next we observe that (7.4) holds for the new linear forms $M_i(\mathbf{y}) = L_i(\mathbf{My})$, since (7.8) holds for $j = 3, 4$.

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

The summation over $\mathbf{y}$ is now over $\mathbf{y} \in \mathcal{S}_*$, since as usual the condition $y_1 \equiv 1 \bmod 4$ is automatic for odd values of y_1 such that $r(M_1(\mathbf{y})/d_1) \neq 0$. In line with (7.7), we therefore deduce from Lemma 8 and Hypothesis-$(*,0)$ that

$$S(X;\gamma) = \frac{\delta_* C_0}{4} X^2 + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg) = C_0 X^2 + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg),$$

when γ is admissible. We complete the proof of (7.9) by summing over the g admissible choices for γ.

7.2 The case $\mu_3 = \mu_4 = 0$ and $\max\{\nu_3, \nu_4\} \geqslant 1 > \min\{\nu_3, \nu_4\} = 0$

For reasons of symmetry we may restrict ourselves to the case $\nu_3 \geqslant 1$ and $\nu_4 = 0$. For $\mathbf{x} \in \mathcal{S}_1 \cap \mathcal{X}$ the term $2^{-k_3} L_3(\mathbf{x})$ is odd, whereas $2^{-k_4} L_4(\mathbf{x})$ is always even. We note that $r(L_3(\mathbf{x})/d_3)$ is non-zero if and only if $a_3' \equiv d_3 - 2^{\nu_3} \bmod 4$. We must show that (3.9) holds with $(j_1, j_2) = (4, 3)$.

Let us write $\xi_4 = \nu_2(2^{-k_4} L_4(\mathbf{x}))$, as in (7.5). Then necessarily $\xi_4 \geqslant 1$, since $\mathbf{x} \in \mathcal{S}_1$. We now see that, in order for $r(2^{-k_4-\xi_4} L_4(\mathbf{x})/d_4)$ to be non-zero, it is necessary and sufficient that

$$x_2 \equiv (d_4 2^{\xi_4} - a_4' x_1)\overline{b_4'} \equiv (d_4 2^{\xi_4} - a_4')\overline{b_4'} x_1 \pmod{2^{\xi_4+2}}, \tag{7.10}$$

where $\overline{b_4'}$ is the multiplicative inverse of b_4' modulo 2^{ξ_4+2}. Here, we have used the fact that $x_1 \equiv 1 \bmod 4$ in the summation over $\mathbf{x}$. For each $\xi_4 \geqslant 1$ we make the transformation

$$\mathbf{M} = \begin{pmatrix} 1 & 0 \\ A & 2^{\xi_4+2} \end{pmatrix}, \tag{7.11}$$

where $A \in [0, 2^{\xi_4+2})$ denotes the residue of $(d_4 2^{\xi_4} - a_4')\overline{b_4'}$ modulo 2^{ξ_4+2}. This brings L_3 and L_4 into a satisfactory shape for $\mathsf{NH}_0(\mathbf{d})$, by which we mean that $2^{-k_3} L_3(\mathbf{My}) \equiv d_3 y_1 \bmod 4$ and $2^{-k_4-\xi_4} L_4(\mathbf{My}) \equiv d_4 y_1 \bmod 4$. Moreover, the summation is now over $\mathbf{y} \in \mathcal{S}_*$. In line with (7.7), and using the estimate (7.2) to handle large values of ξ_4, we therefore deduce from Lemma 8 and Hypothesis-$(*,0)$ that

$$S(X) = \sum_{\xi_4=1}^{\infty} \frac{\delta_* C_0}{2^{\xi_4+2}} X^2 + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg) = C_0 X^2 + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg).$$

Thus $\delta_{1,1}(\mathbf{A}) = 1$ when $a_3' \equiv d_3 - 2^{\mu_3} \bmod 4$, as claimed in (3.9).

7.3 The case $\nu_3 = \nu_4 = 0$ and $\max\{\mu_3, \mu_4\} \geqslant 1 > \min\{\mu_3, \mu_4\} = 0$

The treatment of this case runs parallel to the previous section. For reasons of symmetry we may restrict ourselves to the case $\mu_3 \geqslant 1$ and $\mu_4 = 0$. For $\mathbf{x} \in \mathcal{S}_1 \cap \mathcal{X}$ the term $2^{-k_3} L_3(\mathbf{x})$ is odd, whereas $2^{-k_4} L_4(\mathbf{x})$ is always even. We now observe that $r(L_3(\mathbf{x})/d_3)$ is non-zero if and only if $x_2 \equiv b_3' d_3 - 2^{\mu_3} \bmod 4$. Our task is to show that (3.10) holds.

Let us write $\xi_4 = \nu_2(2^{-k_4} L_4(\mathbf{x})) \geqslant 1$. Arguing as above we see that in order for $r(2^{-k_4-\xi_4} L_4(\mathbf{x})/d_4)$ to be non-zero, it is necessary and sufficient that (7.10) holds. In particular we must take care to sum only over those ξ_4 for which

$$a_4' + b_3' b_4' d_3 \equiv 2^{\mu_3} + 2^{\xi_4} (\mathrm{mod} 4). \tag{7.12}$$

For each such ξ_4 we make the transformation (7.11) as above, which again brings L_3 and L_4 into a satisfactory shape for $\mathsf{NH}_0(\mathbf{d})$, and the summation is over $\mathbf{y} \in \mathcal{S}_*$. We may now deduce from Lemma 8 and Hypothesis-$(*,0)$, together with the argument involving (7.2), that

$$S(X) = \sum_{\xi_4} \frac{\delta_* C_0}{2^{\xi_4+2}} X^2 + O\bigg(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}} \bigg),$$

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

where the sum is over $\xi_4 \geqslant 1$ such that (7.12) holds. If $a_4' + b_3'b_4'd_3 - 2^{\mu_3} \equiv 2 \bmod 4$, then we must restrict attention to the single value $\xi_4 = 1$, which gives $\delta_{1,1}(\mathbf{A}) = 1/2$. If however $a_4' + b_3'b_4'd_3 - 2^{\mu_3} \equiv 0 \bmod 4$, then we must restrict attention to $\xi_4 \geqslant 2$, giving $\delta_{1,1}(\mathbf{A}) = \sum_{\xi_4=2}^{\infty} 2^{-\xi_4} = 1/2$. This therefore confirms (3.10).

7.4 The case $\mu_3 = \nu_3 = \mu_4 = \nu_4 = 0$

We reason in an analogous manner to the previous sections. Our valuation of $\delta_{1,1}(\mathbf{A})$ will depend on the 2-adic valuation v of $a_3'b_4' - a_4'b_3'$, as defined in (3.11). Our aim is to show that (3.12) holds.

Let $\mathbf{x} \in \mathcal{S}_1 \cap \mathcal{X}$, and introduce parameters $\xi_3, \xi_4 \geqslant 1$ such that (7.5) holds for $j = 3, 4$. Let us deal with the case $\xi_4 \geqslant \xi_3$. The system

$$a_3'x_1 + b_3'x_2 \equiv 0 (\mathrm{mod} 2^{\xi_3}), \quad a_4'x_1 + b_4'x_2 \equiv 0 (\mathrm{mod} 2^{\xi_4})$$

is equivalent to

$$(a_3'b_4' - a_4'b_3')x_1 \equiv 0 (\mathrm{mod} 2^{\xi_3}), \quad a_4'x_1 + b_4'x_2 \equiv 0 (\mathrm{mod} 2^{\xi_4}).$$

Let us write $a_3'b_4' - a_4'b_3' = 2^v c_{34}$, with c_{34} odd. We clearly have $\xi_3 \leqslant v$. Moreover, the term $r(2^{-k_4-\xi_4}L_4(\mathbf{x})/d_4)$ is non-zero if and only if (7.10) holds. Assuming this to be the case, we must therefore have

$$a_3'x_1 + b_3'x_2 \equiv (a_3' + b_3'\overline{b_4'}(d_4 2^{\xi_4} - a_4'))x_1 \equiv \overline{b_4'}c_{34}2^v + b_3'\overline{b_4'}d_4 2^{\xi_4} (\mathrm{mod} 2^{\xi_3+2}).$$

Provided that

$$\overline{b_4'}c_{34}2^v + b_3'\overline{b_4'}d_4 2^{\xi_4} \equiv 2^{\xi_3} d_3 (\mathrm{mod} 2^{\xi_3+2}), \tag{7.13}$$

therefore, it follows that we may again carry out the transformation (7.11) to bring L_3 and L_4 into a satisfactory shape for $\mathsf{NH}_0(\mathbf{d})$. The summation is now over $\mathbf{y} \in \mathcal{S}_*$. We easily deduce from Lemma 8 and Hypothesis-$(*, 0)$ that there is the contribution

$$\frac{\delta_* C_0}{2^{\xi_4+2}} X^2 + O\Big(\frac{D^\varepsilon L_\infty^\varepsilon r_\infty r' 2^{\varepsilon\xi_4} X^2}{(\log X)^{\eta-\varepsilon}} \Big),$$

for fixed $1 \leqslant \xi_3 \leqslant \xi_4$ such that (7.13) holds. Using an estimate of the type (7.2), it is an easy matter to deduce that the overall contribution to the error in summing over the available ξ_3, ξ_4 is $O\big(D^\varepsilon L_\infty^\varepsilon r_\infty r' X^2 (\log X)^{-\eta+\varepsilon}\big)$. Moreover, we deduce that

$$\delta_{1,1}(\mathbf{A}) = \sum_{\xi_3=\xi_4} \frac{1}{2^{\xi_4}} + 2 \sum_{\xi_3<\xi_4} \frac{1}{2^{\xi_4}},$$

for a summation over $\xi_3, \xi_4 \geqslant 1$ such that (7.13) holds. To evaluate this quantity we consider a number of subcases, beginning with the contribution from $\xi_3 = \xi_4$. Then we must have $1 \leqslant \xi_3 \leqslant v-1$ and $b_3'\overline{b_4'}d_4 + 2^{v-\xi_3} \equiv d_3 \bmod 4$. Let us write W_1 for the set of all such positive integers ξ_3. Then we obtain the overall contribution

$$\sum_{\xi \in W_1} \frac{1}{2^\xi} = \begin{cases} 0, & \text{if } v = 1, \\ 1 - 1/2^{v-2}, & \text{if } v \geqslant 2 \text{ and } b_3'd_3 \equiv b_4'd_4 \bmod 4, \\ 1/2^{v-1}, & \text{if } v \geqslant 2 \text{ and } b_3'd_3 \equiv -b_4'd_4 \bmod 4. \end{cases} \tag{7.14}$$

Turning to the contribution from $\xi_3 < \xi_4$, it follows from (7.13) that $\xi_3 = v$ and $\overline{b_4'}c_{34} + 2^{\xi_4 - v} \equiv d_3 \bmod 4$. Write W_2 for the set of all such vectors $(\xi_3, \xi_4) \in \mathbb{N}^2$. Then a little thought reveals that we obtain a contribution

$$2 \sum_{(\xi_3,\xi_4) \in W_2} \frac{1}{2^{\xi_4}} = \frac{1}{2^v}$$

from this case. Combining this with (7.14), we therefore conclude the proof of (3.12).

https://doi.org/10.1112/S0010437X08003692 Published online by Cambridge University Press

Acknowledgements

The authors are grateful to Gérald Tenenbaum for discussions that have led to the overall improvement in the error term of Theorem 1, and to Emmanuel Peyre for conversations relating to the interpretation of the constant in Theorem 4. Part of this work was undertaken while the second author was visiting the first author at the Université Paris VII, the hospitality and financial support of which is gratefully acknowledged. While working on this paper the second author was supported by EPSRC grant number EP/E053262/1. It is a pleasure to thank the referee for his careful reading of the manuscript.

References

BB06 R. de la Bretèche and T. D. Browning, *Sums of arithmetic functions over values of binary forms*, Acta Arith. **125** (2006), 291–304.

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

FMT89 J. Franke, Y. I. Manin and Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), 421–435.

HT98 R. R. Hall and G. Tenenbaum. *Divisors*, Cambridge Tracts in Mathematics, vol. 90 (Cambridge University Press, Cambridge, 1998).

HB03 D. R. Heath-Brown, *Linear relations amongst sums of two squares*, in *Number theory and algebraic geometry*, London Mathematical Society Lecture Note Series, vol. 303 (Cambridge University Press, Cambridge, 2003), 133–176.

R. de la Bretèche breteche@math.jussieu.fr
Institut de Mathématiques de Jussieu, Université Paris 7 Denis Diderot, Case Postale 7012, 2 Place Jussieu, F-75251 Paris cedex 05, France

T. D. Browning t.d.browning@bristol.ac.uk
School of Mathematics, University of Bristol, Bristol BS8 1TW, UK