Canad. J. Math. Vol. 70 (6), 2018 pp. 1390–1415
http://dx.doi.org/10.4153/CJM-2017-060-4

Square-free Values of Decomposable Forms

Stanley Yao Xiao

Abstract. In this paper we prove that decomposable forms, or homogeneous polynomials $F(x_1, \ldots, x_n)$ with integer coefficients that split completely into linear factors over $\mathbb{C}$, take on infinitely many square-free values subject to simple necessary conditions, and they have $\deg f \leq 2n + 2$ for all irreducible factors f of F. This work generalizes a theorem of Greaves.

1 Introduction

In this paper, we consider the density of integer tuples $(x_1, \ldots, x_n)$ satisfying $|x_i| \leq B$ and for which $F(x_1, \ldots, x_n)$ is square-free, where F is an n-ary decomposable form of degree $d > n$. A homogeneous polynomial F is said to be a *decomposable form* if it splits into linear factors over the algebraic closure of its field of definition. If F has rational coefficients and is irreducible over $\mathbb{Q}$, we say that F is an *incomplete norm form*. Before stating our result, we give a brief summary of work done on square-free values of polynomials to date.

For a polynomial $g(x)$ with integer coefficients, define the counting function

$$N_g(B) = \#\{x \in \mathbb{Z} : |x| \leq B, g(x) \text{ is square-free}\}.$$

Estermann [6] showed that when $g(x) = x^2 + 1$, there exists a positive number c_g such that the asymptotic formula

$$N_g(B) = c_g B + O(B^{2/3} \log B) \tag{1.1}$$

holds. We will say that a polynomial g has *no fixed square divisor* if for all primes p there exists $n_p \in \mathbb{Z}$ such that $p^2 \nmid g(n_p)$. Ricci [19] generalized Estermann's work and showed that for any irreducible quadratic polynomial with no fixed square divisor, there exists a positive number c_g such that (1.1) holds. Erdős [5] showed that

$$\lim_{B \to \infty} N_g(B) = \infty$$

for cubic polynomials with no fixed square divisor. Hooley [11] refined the work of Estermann, Ricci, and Erdős and showed that for all cubic polynomials g with no fixed square divisor, there exists a positive number c_g such that (1.1) holds with a worse error term. Helfgott further refined Hooley's work in [10] by showing that an analogous asymptotic formula to (1.1) holds when we replace integer inputs with prime inputs. To date, it is not known whether (1.1) holds unconditionally for any polynomial g with no fixed square divisor with $\deg g \geq 4$.

Received by the editors June 27, 2017; revised November 15, 2017.
Published electronically February 14, 2018.
This work was supported by the Government of Ontario, the University of Waterloo, and the Natural Sciences and Engineering Research Council of Canada.
AMS subject classification: **11B05**.
Keywords: square-free value, decomposable form, Selberg sieve.

Assuming the abc-conjecture, Granville [7] and Poonen [17] proved that polynomials in a single variable and polynomials in multiple variables take on infinitely many square-free values. We note that Poonen's result does not allow one to deduce an asymptotic formula analogous to (1.1). Bhargava, Shankar, and Wang recently showed the existence of an asymptotic formula for square-free values of *discriminant polynomials*, which does not use the abc-conjecture in [2].

A natural generalization from the case of single-variable polynomials is to binary forms. Greaves made a breakthrough in [8] on the problem of square-free values of binary forms for suitable binary forms $F(x, y)$ with integer coefficients with no fixed square divisor. He showed that the density of integer pairs (x, y) such that $F(x, y)$ is square-free is exactly as expected provided that $d' \le 6$, where d' is the largest degree of an irreducible factor of F. One observes that the requirement $d' \le 6$ can be compared to $d \le 3$ in the single variable case. Hooley, in [12, 13], extended Greaves's results to the case when F is a polynomial in two variables that splits into linear factors over $\mathbb{C}$.

Schmidt [21] introduced an invariant that he called the discriminant for (incomplete) *norm forms*, which we define below. Write

$$F(\mathbf{x}) = \prod_{j=1}^{d} L_j(\mathbf{x}),$$

where the L_j's are conjugates of the linear form

$$L_1(\mathbf{x}) = \omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n$$

with algebraic integer coefficients in a number field K. We then put

$$\Delta(F) = \prod_{\{i_1,\ldots,i_n\} \subset \{1,\ldots,d\}} |\det(L_{i_1}, \ldots, L_{i_n})|, \tag{1.2}$$

where the determinant of n linear forms in $x_1, \ldots, x_n$ refers to the determinant of its coefficients. It is easy to check that $\Delta(F)$ is invariant under any action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and since each term that appears in the product is an algebraic integer, it follows that $\Delta(F)$ is a rational integer. We say that F has *bad reduction* at a prime p if F has a repeated linear factor over $\mathbb{F}_p$. One notes that bad reduction can only occur if $p \mid \Delta(F)$. Therefore, if $\Delta(F)$ is non-zero, then bad reduction can only occur at finitely many primes.

In this paper, we extend Greaves's work in [8] and Hooley's work in [12, 13] by generalizing Greaves's geometry of numbers method for n-ary decomposable forms and adapting Hooley's sieve arguments.

For an integer k and an integer m, we say that m is k-free if for all primes p dividing m, we have $p^k \nmid m$. For a set S, we write $\#S$ for the cardinality of S. Let us write, for an n-ary form F with integer coefficients,

$$\rho_F(m) = \#\{(a_1, \ldots, a_n) \in (\mathbb{Z}/m\mathbb{Z})^n : F(a_1, \ldots, a_n) \equiv 0 \pmod{m}\} \tag{1.3}$$

and for a positive number B and an integer $k \ge 2$,

$$N_{F,k}(B) = \#\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : |x_i| \le B, F(x_1, \ldots, x_n) \text{ is } k\text{-free}\}. \tag{1.4}$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

We will prove the following theorem.

Theorem 1.1 *Write* $\mathbf{x} = (x_1, \dots, x_n)$ *and let* $F(\mathbf{x}) = L_1(\mathbf{x}) \cdots L_r(\mathbf{x})$ *be a* decomposable *form with integer coefficients and non-zero discriminant* $\Delta(F)$ *as given in* (1.2), *where* $L_1, \dots, L_r$ *are linear forms with algebraic integral coefficients in some finite extension* $K/\mathbb{Q}$. *Let* d *be the maximal degree of a* $\mathbb{Q}$*-irreducible factor of* F. *Let* $k \geq 2$ *be an integer with the property that for all primes* p, *there exists a vector* $\mathbf{x}^{(p)} = (x_1^{(p)}, \dots, x_n^{(p)}) \in \mathbb{Z}^n$ *such that* $p^k \nmid F(\mathbf{x}^{(p)})$. *Then the asymptotic relation*

$$N_{F,k}(B) \sim B^n \prod_p \Big(1 - \frac{\rho_F(p^k)}{p^{nk}}\Big)$$

holds whenever

$$k \geq \frac{d-2}{n}. \tag{1.5}$$

In particular, if $k = 2$, then F takes on infinitely many square-free values as long as $d \leq 2n + 2$. This recovers the theorem of Greaves in [8]. We further remark that Maynard [16] used methods from geometry of numbers related to the methods in Section 3 to prove an analogous theorem to Theorem 1.1 for primes represented by incomplete norm forms.

The outline of our paper is as follows. In Section 2 we will use an elementary sieve argument to partition the relevant main terms and error terms to be estimated in order to prove Theorem 1.1. In Section 3, we will generalize Greaves's geometry of numbers argument in [8] to the case of decomposable forms over $\mathbb{Z}$. In Sections 4 and 5, we adapt the Ekedahl sieve as described in [1, 4] and the Selberg sieve, as expressed by Hooley in [12], to establish an estimate for the remaining error terms relevant to condition (1.5) of Theorem 1.1.

2 Preliminaries

We will show that $N_{F,k}(B)$ (recall (1.4)) satisfies an inequality of the form

$$N_1(B) - N_2(B) - N_3(B) \leq N_{F,k}(B) \leq N_1(B).$$

Our goal will be to demonstrate, for any $\varepsilon > 0$, that

$$N_1(B) = B^n \prod_{p \leq \xi_1} \Big(1 - \frac{\rho_F(p^k)}{p^{nk}}\Big) + O_{F,\varepsilon}(B^{n-1+\varepsilon}).$$

Next we will show that for some $\delta_n > 0$ and some slowly growing function $\xi_1 = \xi_1(B)$ tending to infinity as the parameter B tends to infinity,

$$N_2(B) = O_F\big(B^n(\xi_1^{-1} + (\log B)^{-\delta_n})\big)$$

and that $N_3(B) = o_F(B^n)$. Put $\log_1(B) = \max\{1, \log B\}$ and $\log_s B = \log_1 \log_{s-1} B$ for $s \geq 2$. We now let

$$\xi_1 = \xi_1(B) \tag{2.1}$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

be an eventually increasing real-valued function tending to infinity that we will define later. For now, it suffices to suppose that $\xi_1(B) = O(\log_2 B/\log_3 B)$. Next, put

$$\xi_2 = B^n(\log B)^{2/3}. \tag{2.2}$$

Now define

$$N_1(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : |x_i| \le B, \text{ and if } p^k \mid F(\mathbf{x}), \text{ then } p > \xi_1\},$$
$$N_2(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : |x_i| \le B, \text{ and there exists } p \in (\xi_1, \xi_2] \text{ such that } p^2 \mid F(\mathbf{x}) \text{ and if } p^k \mid F(\mathbf{x}), \text{ then } p > \xi_1\},$$

and

$$N_3(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : |x_i| \le B, \text{ and there exists } p > \xi_2 \text{ such that } p^k \mid F(\mathbf{x}), F(\mathbf{x}) \text{ is indivisible by } p^2 \text{ for } \xi_1 < p \le \xi_2 \text{ and if } p^k \mid F(\mathbf{x}), \text{ then } p > \xi_1\}. \tag{2.3}$$

Before we proceed with estimating $N_1(B)$, let us establish some facts about the function ρ_F as defined in (1.3). For a positive integer m and a real number α, let us write

$$\sigma_\alpha(m) = \sum_{s \mid m} s^\alpha.$$

Furthermore, for each prime p, we define

$$\tau_F(p) = \# \text{ geometrically irreducible components of } F \text{ defined over } \mathbb{F}_p,$$

and for square-free integers, we define

$$\tau_F(m) = \prod_{p \mid m} \tau_F(p).$$

We remark that in our case, the only geometrically irreducible components are hyperplanes that are defined over $\mathbb{F}_p$.

We will establish the following lemma.

Lemma 2.1 *Let ρ_F be defined as in (1.3). Then ρ_F is multiplicative, and for all primes p, we have*

$$\rho_F(p^k) = O_{d,n}(p^{k(n-1)} + p^{n(k-1)}).$$

If m is a square-free integer, then

$$\rho_F(m) = O_F\big(m^{n-1}\tau_F(m)\sigma_{-1/4}(m)\big).$$

Proof The fact that ρ_F is multiplicative follows from the Chinese Remainder Theorem. For the upper bound, let us first suppose that there exists an index, say $i = 1$, such that $p \nmid x_1$. Then there are at most p^k many choices for $x_2, \dots, x_n$. Having fixed these, there are then at most d choices for x_1. Hence, there are at most $ndp^{(n-1)k}$ choices for $(x_1, \dots, x_n)$. Otherwise, suppose that $p \mid x_i$ for $i = 1, \dots, n$. Write $x_i = px_i'$ for $i = 1, \dots, n$. Then there are at most p^{k-1} choices for each $i = 1, \dots, n$, whence there are $p^{n(k-1)}$ choices altogether. Combining these, we obtain the claimed upper bound.

For the second part, we use a result of Lang and Weil in [15], which asserts that for any algebraic variety V defined over $\mathbb{Q}$ and any prime p, we have

$$\#V(\mathbb{F}_p) = C_V(p)p^{\dim V} + O_V(p^{\dim V - 1/2}),$$

where $C_V(p)$ is the number of geometrically irreducible, top-dimensional components of V that are defined over $\mathbb{F}_p$. We then have

$$\rho_F(p) = \tau_F(p)p^{n-1} + O_F(p^{n-3/2}).$$

Multiplicativity of ρ_F then yields

$$\begin{aligned}\rho_F(m) &= \prod_{p|m}\big(\tau_F(p)p^{n-1} + O_F(p^{n-3/2})\big)\\ &= m^{n-1}\prod_{p|m}\big(\tau_F(p) + O_F(p^{-1/2})\big)\\ &= O_F\big(m^{n-1}\tau_F(m)\sigma_{-1/4}(m)\big).\end{aligned}$$

■

We remark that Lemma 2.1 implies that the infinite product

$$\prod_p\Big(1 - \frac{\rho_F(p^k)}{p^{nk}}\Big)$$

converges. This is because

$$\frac{\rho_F(p^k)}{p^{nk}} = O\Big(\frac{1}{p^k} + \frac{1}{p^n}\Big) = O\Big(\frac{1}{p^2}\Big),$$

since $k, n \geq 2$, by assumption.

We give an estimate for $N_1(B)$. For a positive integer b, define the quantity

$$N(b, B) = \#\big\{\mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n : b^k \mid F(\mathbf{x})\big\}.$$

Then from the familiar property of the Mobius function μ, we have

$$\begin{aligned}N_1(B) &= \sum_{\substack{b\in\mathbb{N}\\ p|b\Rightarrow p\leq\xi_1}} \mu(b)N(b,B)\\ &= \sum_{\substack{b\in\mathbb{N}\\ p|b\Rightarrow p\leq\xi_1}} \mu(b)\rho_F(b^k)\Bigg(\frac{B^n}{b^{nk}} + O\Big(\frac{B^{n-1}}{b^{(n-1)k}} + 1\Big)\Bigg)\\ &= B^n\prod_{p\leq\xi_1}\Big(1 - \frac{\rho_F(p^k)}{p^{nk}}\Big) + O\Bigg(\sum_{\substack{b\in\mathbb{N}\\ p|b\Rightarrow p\leq\xi_1}} \rho_F(b^k)\Big(\frac{B^{n-1}}{b^{(n-1)k}} + 1\Big)\Bigg).\end{aligned}$$

By a theorem of Rosser and Schoenfeld [20], it follows that for all $\varepsilon > 0$ and some $C' > 0$, we have

$$\prod_{p\leq\xi_1} p \leq e^{2\xi_1} = O\Big((\log B)^{\frac{C'}{\log_3 B}}\Big) = O_\varepsilon(B^\varepsilon),$$

by (2.1). Hence, we obtain via Lemma 2.1 that, for any $\varepsilon > 0$,

$$N_1(B) = B^n\prod_{p\leq\xi_1}\Big(1 - \frac{\rho_F(p^k)}{p^{nk}}\Big) + O\Big(\sum_{b\ll_\varepsilon B^\varepsilon} B^{n-1+\varepsilon} + b^{n(k-1)+\varepsilon} + b^{k(n-1)+\varepsilon}\Big).$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

We then see that

$$N_1(B) = B^n \prod_{p \le \xi_1} \Big(1 - \frac{\rho_F(p^k)}{p^{nk}}\Big) + O_\varepsilon(B^{n-1+\varepsilon}). \tag{2.4}$$

As $B \to \infty$, the partial product in (2.4) tends to the convergent product in Theorem 1.1; thus it suffices to show that $N_2(B), N_3(B)$ are error terms.

In the next section we will see that we can obtain good estimates for $N_2(B)$ even when ξ_2 is as large as $B^n(\log B)^{2/3}$. Let

$$F(x_1, \dots, x_n) = \mathcal{F}_1(\mathbf{x}) \cdots \mathcal{F}_r(\mathbf{x}),$$

where each $\mathcal{F}_i$ is irreducible over $\mathbb{Q}$ for $i = 1, \dots, r$. Here $d = \max_{1 \le j \le r} \deg \mathcal{F}_j$. Let us write

$$N_2^{(j)}(B) = \#\big\{\mathbf{x} \in \mathbb{Z}^n : |x_i| \le B, \text{and there exists } p \in (\xi_1, \xi_2] \text{ such that } p^k \mid \mathcal{F}_j(\mathbf{x}) \\ \text{and if } p^k \mid \mathcal{F}_j(\mathbf{x}), \text{then } p > \xi_1\big\},$$

and

$$N_3^{(j)}(B) = \#\big\{\mathbf{x} \in \mathbb{Z}^n : |x_i| \le B, \text{and there exists } p > \xi_2 \text{ such that } p^k \mid \mathcal{F}_j(\mathbf{x}), \\ p^2 \nmid F_j(\mathbf{x}) \text{ for } \xi_1 < p \le \xi_2, \text{ and if } p^k \mid \mathcal{F}_j(\mathbf{x}), \text{then } p > \xi_2\big\}.$$

If $\mathbf{x}$ is counted by $N_2(B)$ (resp. $N_3(B)$) but not by $N_2^{(j)}(B)$ (resp. $N_3^{(j)}(B)$) for $j = 1, \dots, r$, then there must exist $j_1 < j_2$ and a positive integer $k' < k$ such that

$$\mathcal{F}_{j_1}(\mathbf{x}) \equiv 0 \pmod{p^{k'}} \text{ and } \mathcal{F}_{j_2}(\mathbf{x}) \equiv 0 \pmod{p^{k-k'}}.$$

However, this can only happen if $p \mid \Delta(F)$, so this situation can be avoided if B is chosen sufficiently large. Hence, we have

$$N_2(B) \le \sum_{j=1}^{r} N_2^{(j)}(B) \quad \text{and} \quad N_3(B) \le \sum_{j=1}^{r} N_3^{(j)}(B).$$

It therefore suffices to deal with the case when F is irreducible over $\mathbb{Q}$ and $d = \deg F$.

3 Geometry of Numbers

In this section, we shall give an estimate for $N_2(B)$. To do so, we show that for each modulus m we can reduce the problem to counting integer points of bounded height in a finite number $\mathcal{N}_F$ of lattices, the important feature being that $\mathcal{N}_F$ is dependent only on F.

Lemma 3.1 *Let $F \in \mathbb{Z}[x_1, \dots, x_n]$ be an incomplete norm form of degree $d > n$. Let $p \nmid \Delta(F)$ be a prime, and let $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$ be a solution to the congruence*

$$F(\mathbf{x}) \equiv 0 \pmod{p^2}.$$

Then $\mathbf{a}$ lies on a finite number $\mathcal{N}_F$ of lattices $\Lambda \subset \mathbb{Z}^n$. Moreover, for each such lattice Λ, we have $\det \Lambda \ge p^2$.

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

Proof By the same argument as that in [13, Section 5], we can factor F into

$$F(\mathbf{x}) = F^*(\mathbf{x}) \prod_{i=1}^{\tau_F(p)} \mathcal{L}_i(\mathbf{x}),$$

where $\mathcal{L}_i(\mathbf{x}) = v_1^{(i)} x_1 + v_2^{(i)} x_2 + \cdots + v_n^{(i)} x_n$ are defined over $\mathbb{Z}_p$, while $F^*(\mathbf{x})$ is a form defined over $\mathbb{Z}_p$. Suppose that $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ is a solution to the congruence

$$F(\mathbf{a}) \equiv 0 \pmod{p^2}.$$

Then $\mathbf{a}$ is of one of the following types:

(a) There exists exactly one $i, 1 \le i \le \tau_F(p)$ such that $\mathcal{L}_i(\mathbf{a}) \equiv 0 \pmod{p^2}$, while $\mathcal{L}_j(\mathbf{a}) \not\equiv 0 \pmod{p}$ for $j \ne i$, and $F^*(\mathbf{a}) \not\equiv 0 \pmod{p}$.
(b) There exist $1 \le i_1 < i_2 \le \tau_F(p)$ such that $\mathcal{L}_{i_1}(\mathbf{a}) \equiv \mathcal{L}_{i_2}(\mathbf{a}) \equiv 0 \pmod{p}$.
(c) $F^*(\mathbf{a}) \equiv 0 \pmod{p}$.

If $\mathbf{a}$ is of type (a), then $\mathbf{a}$ lies in the union of at most $\tau_F(p) \le d$ lattices of determinant p^2. If $\mathbf{a}$ is of type (b), then there are two further sub-cases. First, and more simply, there exist two indices $i_1 < i_2$ and an integer t such that

$$\mathcal{L}_{i_1}(\mathbf{x}) \equiv t\mathcal{L}_{i_2}(\mathbf{x}) \pmod{p}. \tag{3.1}$$

If (3.1) holds, then it follows that $\Delta(F) \equiv 0 \pmod{p}$, hence p divides the discriminant $\Delta(F)$ of F. Thus, there are only finitely many primes for which this could happen. Otherwise, $\mathbf{a}$ lies on the intersection of two distinct lattices Λ_1, Λ_2 of determinant p, defined by

$$\Lambda_1 = \left\{ \mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \cdot \mathbf{a}_1 \equiv 0 \pmod{p} \right\} \quad \text{and} \quad \Lambda_2 = \left\{ \mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \cdot \mathbf{a}_2 \equiv 0 \pmod{p} \right\},$$

where $\mathbf{a}_1, \mathbf{a}_2$ are two non-proportional non-zero vectors modulo p. Now let ϕ_1, ϕ_2 be homomorphisms from $\mathbb{Z}^n$ to $\mathbb{F}_p$ defined by

$$\phi_1(\mathbf{x}) = \mathbf{a}_1 \cdot \mathbf{x} \pmod{p} \quad \text{and} \quad \phi_2(\mathbf{x}) = \mathbf{a}_2 \cdot \mathbf{x} \pmod{p}.$$

Then Λ_1, Λ_2 are the kernels of ϕ_1, ϕ_2, respectively. Now let ϕ be defined by $\phi\colon \mathbb{Z}^n \to (\mathbb{Z}/p\mathbb{Z})^2, \phi(\mathbf{x}) = (\phi_1(\mathbf{x}), \phi_2(\mathbf{x}))$. The image of ϕ is the full set $(\mathbb{Z}/p\mathbb{Z})^2$ whenever $\mathbf{a}_1, \mathbf{a}_2$ are not proportional modulo p. Hence, $\mathbf{a}$ lies in a lattice of determinant at least p^2. Further, there are at most $\tau_F(p)^2 \le d^2$ such lattices.

If $\mathbf{a}$ is of type (c), then modulo p there exists a linear factor $\mathcal{L}_j$ of F^* that is not defined over $\mathbb{F}_p$ such that $\mathcal{L}_j(\mathbf{a}) \equiv 0 \pmod{p}$. Let s be the degree of the field of definition of $\mathcal{L}_j$ over $\mathbb{F}_p$. By assumption, we have $s \ge 2$. Then $\mathcal{L}_j$ can be written as

$$\mathcal{L}_j = \alpha_1 \mathcal{L}_{j,1} + \cdots + \alpha_s \mathcal{L}_{j,s},$$

where $\mathcal{L}_{j,i}$ are linear forms with coefficients in $\mathbb{F}_p$ and $\alpha_1, \ldots, \alpha_s$ is a basis of $\mathbb{F}_{p^s}$ over $\mathbb{F}_p$. In particular, $\alpha_1, \ldots, \alpha_s$ are linearly independent over $\mathbb{F}_p$. Therefore, $\mathcal{L}_j(\mathbf{a}) \equiv 0 \pmod{p}$ implies that $\mathcal{L}_{j,i}(\mathbf{a}) \equiv 0 \pmod{p}$ for $i = 1, \ldots, s$. It thus follows that $\mathbf{a}$ lies in the intersection of the lattice in $\mathbb{Z}^n$ given by the linear forms $\mathcal{L}_{j,1}, \mathcal{L}_{j,2}$; hence, it follows by the same argument that $\mathbf{a}$ lies in a lattice of determinant at least p^2. Moreover, the number of such lattices is at most d^2. ∎

Now we generalize [8, Lemma 1] (see also [9]) for norm forms in $n \ge 2$ variables. Indeed, we will prove the following lemma.

Lemma 3.2 *Let $\Lambda \subset \mathbb{Z}^n$ be a lattice of determinant m. For $\mathbf{x} \in \mathbb{Z}^n$, denote the sup norm of $\mathbf{x}$ by $H(\mathbf{x})$. Put*

$$N_\Lambda(B) = \{\mathbf{x} \in \mathbb{Z}^n : H(\mathbf{x}) \leq B\}$$

and put M_Λ for the sup norm of the shortest vector in Λ. Then

$$N_\Lambda(B) \ll_n \frac{B^n}{m} + O\Big(\frac{B^{n-1}}{M_\Lambda^{n-1}} + 1\Big).$$

Proof Let $\mathbf{x}_1 = (x_1^{(1)}, \ldots, x_n^{(1)})$ be one of the shortest vectors with respect to sup norm. Without loss of generality, we can assume that $|x_1^{(0)}| = M_\Lambda$. Observe that $M_\Lambda \leq m^{1/n}$. To see this, let $l = l(m)$ denote the smallest positive integer such that $(l+1)^n > m$. Then there exist two distinct vectors $\mathbf{a}_1, \mathbf{a}_2$ such that the coordinates of both vectors are at most $l/2$ in absolute value and

$$\mathbf{a}_1 \equiv \mathbf{a}_2 \pmod{m},$$

whence their difference $\mathbf{a}_1 - \mathbf{a}_2$ lies in $\mathcal{L}$ and $H(\mathbf{a}_1 - \mathbf{a}_2) \leq m^{1/n}$.

By [3, Lemma 4.3], there exist vectors $\mathbf{x}_2, \ldots, \mathbf{x}_n \in \mathcal{L}$ such that

$$m \leq \prod_{j=1}^{n} H(\mathbf{x}_j) \ll_n m,$$

and for all vectors $\mathbf{x} \in \mathcal{L}$, if we write

$$\mathbf{x} = \sum_{j=1}^{n} \lambda_j \mathbf{x}_j,$$

we have

$$|\lambda_j| \ll_n \frac{H(\mathbf{x})}{H(\mathbf{x}_j)}.$$

In particular, for a vector $\mathbf{x}$ counted by $N_\Lambda(B)$, we have

$$|\lambda_j| \ll_n \frac{B}{H(\mathbf{x}_j)}.$$

By observing that $H(\mathbf{x}_j) \geq M_\Lambda$ for $j = 1, \ldots, n$, we obtain the bound

$$N_\Lambda(B) \ll_n \prod_{j=1}^{n} \Big(1 + \frac{B}{H(\mathbf{x}_j)}\Big) \ll_n \frac{B^n}{m} + \frac{B^{n-1}}{M_\Lambda^{n-1}} + \cdots + 1.$$

Hence we obtain the consequence of the lemma. ∎

For each prime p, we denote by $\mathcal{U}_p$ the set of lattices containing the solutions to the congruence $F(\mathbf{x}) \equiv 0 \pmod{p^2}$. For each $\Lambda \in \mathcal{U}_p$, we say that Λ is of type (a), (b), or (c) if Λ arises from a solution $\mathbf{a}$ to $F(\mathbf{x}) \equiv 0 \pmod{p^2}$ of type (a), (b), or (c) in the proof of Lemma 3.1. Then write F_Λ to be equal to:

(a) $L_i(\mathbf{x})$, if Λ is of type (a) and $\mathcal{L}_i$ is the unique linear form associated to Λ;
(b) $\mathcal{L}_{i_1} \cdots \mathcal{L}_{i_s}$, where $\mathcal{L}_{i_1}, \ldots, \mathcal{L}_{i_s}$ are the linear factors of F defined over $\mathbb{F}_p$ that vanish on Λ modulo p when Λ is of type (b); and
(c) F^* if Λ is of type (c).

We now estimate $N_2(B)$ via the following lemma.

Lemma 3.3 *The error term $N_2(B)$ satisfies*

$$N_2(B) = O_n\big(B^n\big(\xi_1^{-1} + (\log B)^{-1/3n}\big)\big).$$

Proof Let $\mathcal{U}_p$ denote the set of at most $\mathcal{N}_F$ many lattices Λ, each with determinant at least p^2 by Lemma 3.1, which contains all of the solutions to $F(\mathbf{x}) \equiv 0 \pmod{p^2}$. Then

$$N_2(B) \ll_n \sum_{\xi_1 < p \leq B^n (\log B)^{2/3}} \sum_{\Lambda \in \mathcal{U}_p} N_\Lambda(B).$$

By Lemma 3.2, it follows that

$$N_2(B) \ll_n \sum_{\xi_1 < p \leq B^n (\log B)^{2/3}} \sum_{\Lambda \in \mathcal{U}_p} \Big(\frac{B^n}{p^2} + \frac{B^{n-1}}{M_\Lambda^{n-1}} + 1 \Big).$$

We first consider consider the term

$$\sum_{\xi_1 < p \leq \xi_2} \sum_{\Lambda \in \mathcal{U}_p} \frac{B^n}{p^2}.$$

The sum

$$\sum_{p > \xi_1} \sum_{1 \leq j \leq \mathcal{N}_F} \frac{1}{p^2}$$

converges and is bounded by $O_F(\xi_1^{-1})$. Now we look at the sum

$$\sum_{\xi_1 < p \leq \xi_2} \sum_{\Lambda \in \mathcal{U}_p} \frac{B^{n-1}}{M_\Lambda^{n-1}}.$$

We break this sum into three sub-sums S_1, S_2, and S_3. S_1 will consist of the contribution from those primes $\xi_1 < p \leq B$. In this case, we have

$$S_1 = \sum_{\xi_1 < p \leq B} \sum_{\Lambda \in \mathcal{U}_p} \frac{B^{n-1}}{M_\Lambda^{n-1}} \ll B^{n-1} \sum_{1 \leq j \leq \mathcal{N}_F} \sum_{p \leq B} 1 \ll \frac{B^n}{\log B},$$

where we used the trivial estimate that $M_\Lambda \geq 1$.

S_2 will be the sub-sum consisting of those $M_\Lambda \geq B(\log B)^{-1/3n}$. In this case, we have

$$\begin{aligned} S_2 &\ll_d \sum_{\xi_1 < p \leq B^n (\log B)^{2/3}} \sum_{\Lambda \in \mathcal{U}_p} \frac{B^{n-1}(\log B)^{(n-1)/3n}}{B^{n-1}} \\ &\ll_d (\log B)^{\frac{(n-1)}{3n}} \frac{B^n (\log B)^{2/3}}{\log B} \ll_d B^n (\log B)^{-1/3n}. \end{aligned}$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

Finally, S_3 will denote the sub-sum consisting of those primes $p > B$ and $M_\Lambda \le B(\log B)^{-1/3n}$. We then have

$$\begin{aligned} S_3 &\ll \sum_{0<|x_1^{(1)}|,\dots,|x_n^{(1)}|\le B(\log B)^{-1/3n}} \sum_{M_\Lambda \in \mathcal{U}_p} \sum_{\substack{p^2 | F_\Lambda(\mathbf{x}_1) \\ p>B}} \frac{B^{n-1}}{M_\Lambda^{n-1}} \\ &\ll B^{n-1} \sum_{0<|x_1^{(1)}|\le B(\log B)^{-1/3n}} \frac{1}{|x_1^{(1)}|^{n-1}} \sum_{0\le |x_2^{(1)}|,\dots,|x_n^{(1)}|\le |x_1^{(1)}|} \sum_{\substack{p^2|F(\mathbf{x}_1)\\ p>B}} 1 \\ &\ll B^{n-1}B(\log B)^{-1/3n}, \end{aligned}$$

the last inequality following from the fact that, since $\|\mathbf{x}_1\| \le B$, at most $\lfloor d/2 \rfloor + 1$ many primes with $p > B$ can satisfy $p^2 \mid F(\mathbf{x}_1)$.

Finally, the last term needing to be estimated is

$$\sum_{\xi_1 < p \le B^n(\log B)^{2/3}} \sum_{\Lambda \in \mathcal{U}_p} 1.$$

This is bounded by the number of primes in the interval $[\xi_1, B^n(\log B)^{2/3}]$, which by the prime number theorem is $O(B^n(\log B)^{2/3}/\log B) = O(B^n(\log B)^{-1/3})$, and so constitutes a negligible error term. ∎

4 The Ekedahl Sieve

In this section, we use the following result of Ekedahl [4] to handle certain contributions to $N_3(B)$. The version below was formulated by Bhargava and Shankar [1].

Proposition 4.1 (Ekedahl sieve) *Let $\mathcal{B}$ be a compact region in $\mathbb{R}^n$ having finite measure, and let Y be any closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$ of co-dimension $s \ge 2$. Let r and M be positive real numbers. Then we have*

$$\#\{\mathbf{x} \in r\mathcal{B} \cap \mathbb{Z}^n : \mathbf{x} \pmod p \in Y(\mathbb{F}_p) \textit{ for some prime } p > M\} = O\Big(\frac{r^n}{M^{s-1}\log M} + r^{n-s+1}\Big).$$

We factor F into linear factors over $\overline{\mathbb{Q}}$, where

$$F(\mathbf{x}) = \prod_{j=1}^{d}(\psi_1^{(j)}x_1 + \dots + \psi_n^{(j)}x_n) = \prod_{i=1}^{d} L_i(\mathbf{x}). \tag{4.1}$$

Let $Y_{i,j}$ denote the variety defined by $L_i(\mathbf{x}) = L_j(\mathbf{x}) = 0$, and let $Y = \bigcup_{1\le i<j\le n} Y_{i,j}$. Since Y is invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, it is defined over $\mathbb{Q}$. Moreover, it has co-dimension at least two in $\mathbb{A}^n_{\mathbb{Z}}$. Let p be a prime. Over $\mathbb{Z}_p$, we have the factorization (see [12]) of F into

$$F(\mathbf{x}) = F^*(\mathbf{x}) \prod_{i=1}^{\tau_F(p)} \mathcal{L}_i(\mathbf{x}),$$

where $F^*, \mathcal{L}_i$ have $\mathbb{Z}_p$-coefficients and F^* does not have linear factors over $\mathbb{Q}_p$. Let $\mathcal{S}_p$ be those congruence classes $\mathbf{x}$ in $(\mathbb{Z}/p\mathbb{Z})^n = \mathbb{F}_p^n$ such that either

(a) there exist $1 \le i < j \le \tau_F(p)$ such that $\mathcal{L}_i(\mathbf{x}) \equiv \mathcal{L}_j(\mathbf{x}) \equiv 0 \pmod{p}$, or
(b) $F^*(\mathbf{x}) \equiv 0 \pmod{p}$.

Since linear factors of F^* are not defined over $\mathbb{F}_p$ and hence have a non-trivial conjugate, it follows that, whenever $\mathbf{a} \in \mathcal{S}_p$, $\mathbf{a} \in Y(\mathbb{F}_p)$. We then have the following consequence of Ekedahl's sieve.

Lemma 4.2 *Let $N_3^*(B)$ denote the number of elements $\mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n$ for which $\mathbf{x} \pmod{p} \in \mathcal{S}_p$ for some $p > \xi_1$. Then*

$$N_3^*(B) = O\Big(\frac{B^n}{\xi_1 \log \xi_1} + B^{n-1}\Big).$$

Note that Lemma 4.2 completes the proof of Lemma 3.3.

5 The Selberg Sieve

In this section we use a variant of the Selberg sieve to give an upper bound for $N_3(B)$. Our main goal in this section is to establish the following proposition.

Proposition 5.1 *Let $N_3(B)$ be as given in (2.3). Then $N_3(B) = o(B^n)$.*

Proposition 5.1 will follow from Lemmas 5.4, 5.6, 5.7, 5.10, and 5.12 as well as Lemma 4.2. Consider the set

(5.1)

$$\mathcal{N}_3^\dagger(B) = \left\{ \mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n \;\middle|\; \begin{array}{l} F(\mathbf{x}) = uq^k, u \text{ is indivisible by } p^k \text{ for } p \le \xi_1 \text{ and} \\ \text{indivisible by } p^2 \text{ for } \xi_1 < p \le \xi_2,\ q \text{ is a prime} \\ \text{exceeding } \xi_2, \text{ and } \mathbf{x} \notin \mathcal{S}_p \text{ for all } p \mid u. \end{array} \right\},$$

and put $N_3^\dagger(B) = \#\mathcal{N}_3^\dagger(B)$. Observe that

$$N_3(B) = N_3^\dagger(B) + N_3^*(B).$$

We shall establish the following preliminary result.

Lemma 5.2 *Let $\mathbf{x} \in \mathcal{N}_3^\dagger(B)$ and u, q be as in (5.1). Then we have*

$$u = O\big(B^2 (\log B)^{-2k/3}\big).$$

Furthermore, u can be written as $u = u_1 u_2$, where u_1 divides

$$C(\xi_1) = \prod_{p \le \xi_1} p^{k-1},$$

and u_2 is square-free with each prime divisor p of u_2 satisfying $\xi_1 < p \le \xi_2$.

Proof Observe that from $F(\mathbf{x}) = uq^k$ and our assumptions on q, we have

$$u = O(B^d \xi_2^{-k}).$$

By (1.5) and (2.2), there exists an absolute positive constant C_1 such that

$$|u| < C_1 B^{d-kn} (\log B)^{-2k/3} \le C_1 B^{d-d+2} (\log B)^{-2k/3} = C_1 B^2 (\log B)^{-2k/3}.$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

We now factor u into two factors u_1 and u_2, where u_1 consists of only prime factors less than ξ_1. We observe that since we have accounted for small prime powers via our treatment of $N_1(B)$, we have that u_1 divides $\prod_{p \le \xi_1} p^{k-1}$. Then the factor u_2 will be composed of prime factors larger than ξ_1. Further, it must be *square-free*. This is because, by definition, the prime factors of u between ξ_1 and ξ_2 divide u exactly once, and u cannot have a prime factor exceeding ξ_2, since otherwise

$$uq^k \gg B^{n(k+1)} \log B \gg B^d \log B,$$

which contradicts $\mathbf{x} \in [-B, B]^n$ for B sufficiently large. ∎

For each square-free integer u_2 such that each prime divisor p of u_2 satisfies $\xi_1 < p \le \xi_2$, put

$$\mathcal{D}(u_2) = \prod_{\substack{\xi_1 < p \le \frac{1}{12}\log(B^2 u_2^{-1}) \\ p \nmid u_2 \\ p \equiv 1 \pmod{k}}} p. \tag{5.2}$$

We then have the following lemma.

Lemma 5.3 *Let u_2 be a square-free integer such that all of its prime divisors are between ξ_1 and ξ_2. Let $\omega(m)$ denote the number of distinct prime divisors of m. Let $\mathcal{D}(u_2)$ be as in (5.2). If $q > \xi_2$ is a prime, then there exists exactly $k^{\omega(\mathcal{D})}$ residue classes $\{\mathfrak{d}_1, \dots, \mathfrak{d}_{k^{\omega(\mathcal{D})}}\}$ such that $\mathfrak{d}_j^k \equiv q^k \pmod{\mathcal{D}}$ for $j = 1, \dots, k^{\omega(\mathcal{D})}$.*

Proof Since all prime divisors of $\mathcal{D}$ are $O(\log B)$, it follows that q^k is a proper k-th power residue modulo $\mathcal{D}$. Now consider the family of all k-th power residues modulo $\mathcal{D}$. By our choice of $\mathcal{D}$, we have that $k \mid \varphi(\mathcal{D})$, so that the family of k-th power residues is not the set of all residues modulo $\mathcal{D}$. For each $p \mid \mathcal{D}$, q^k has k pre-images modulo p, meaning there exist k distinct elements $\mathfrak{q}_1, \dots, \mathfrak{q}_k$ in $\{0, 1, \dots, p-1\}$ such that $\mathfrak{q}_j^k \equiv q^k \pmod{\mathcal{Q}}$. For a positive integer l, let us write $\omega(l)$ for the number of distinct prime divisors of l. Then it follows from the Chinese Remainder Theorem that there exist $k^{\omega(\mathcal{D})}$ residue classes $\{\mathfrak{d}_1, \dots, \mathfrak{d}_{k^{\omega(\mathcal{D})}}\}$ modulo $\mathcal{D}$ such that $\mathfrak{d}_j^k \equiv q^k \pmod{\mathcal{D}}$. ∎

Let C_1 be as in Lemma 5.2, and put $\xi_3 = C_1 B^2 (\log B)^{-2k/3}$. Lemmas 5.2 and 5.3 have the following consequence, which is crucial for our estimation of $N_3(B)$.

Lemma 5.4 *Let u_1 be a divisor of $C(\xi_1)$ and let u_2 a square-free integer whose prime divisors p satisfy $\xi_1 < p \le \xi_3$. Let $H_{u_1,u_2}(B)$ be the number of solutions $(m_1, \dots, m_n) \in \mathbb{Z}^n \cap [-B, B]^n$ to the two congruences*

$$F(m_1, \dots, m_n) \equiv 0 \pmod{u_1}, \tag{5.3}$$

$$F(m_1, \dots, m_n) \equiv 0 \pmod{u_2}, \tag{5.4}$$

and solutions to the congruences

$$F(m_1, \dots, m_n) \equiv u_1 u_2 s^k \pmod{\mathcal{D}} \tag{5.5}$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

for $0 \le s < \mathcal{D}$*, such that* $(m_1, \ldots, m_n) \pmod p \notin \mathcal{S}_p$ *for* $p \mid u_1 u_2$*. Then we have*

$$N_3(B) \le \sum_{\substack{u_1 | C(\xi_1) \\ u_2 \le \xi_3}} \frac{H_{u_1,u_2}(B)}{k^{\omega(\mathcal{D})}} + N_3^*(B). \tag{5.6}$$

Proof Equation (5.6) follows from the fact that the solutions to (5.5) can be partitioned into sets of cardinality $k^{\omega(\mathcal{D})}$ by Lemma 5.3. ∎

In view of Lemma 4.2, we shall be primarily concerned with the term

$$N_3^\dagger(B) = \sum_{\substack{u_1 | C(\xi_1) \\ u_2 \le \xi_3}} \frac{H_{u_1,u_2}(B)}{k^{\omega(\mathcal{D})}}.$$

5.1 Selberg Sieve Weights

We now introduce the relevant Selberg sieve weights. Selberg devised an ingenious method to establish an upper bound for counting integer points in a box. To state this precisely, suppose that we wanted to count the set of points inside the box $[-B, B]^n$ satisfying a set of congruence conditions $\mathcal{R}_l$ modulo a positive integer l. Selberg introduced smooth functions γ that satisfy the inequality

$$\sum_{\substack{(m_1,\ldots,m_n) \in \mathbb{Z}^n \cap [-B,B]^n \\ (m_1,\ldots,m_n) \in \mathcal{R}_l}} 1 \le \sum_{\substack{(m_1,\ldots,m_n) \in \mathbb{Z}^n \\ (m_1,\ldots,m_n) \in \mathcal{R}_l}} \gamma(m_1) \cdots \gamma(m_n), \tag{5.7}$$

where γ is an upper bound for the characteristic function $\chi_B(z)$ of the interval $[-B, B]$, tends to zero rapidly outside of this interval, and is sufficiently smooth to be conducive to Fourier analysis and the Poisson summation formula. This reduces various counting problems into a question about exponential sums, from which one can draw results from a vast literature, including the seminal works of Weil and Deligne.

Our choice of γ is identical to that of Hooley's in [12]. Namely, we start with the following function, first given by Beurling and later utilized by Selberg to establish the optimal general bound for the large sieve inequality:

$$\mathrm{Beu}(z) = \Big(\frac{\sin \pi z}{\pi}\Big)^2 \Big(\sum_{n=0} \frac{1}{(z-n)^2} - \sum_{n=-\infty}^{-1} \frac{1}{(z-n)^2} + \frac{1}{2z} \Big).$$

For the interval $[-U, U]$ we construct the function

$$g_U(z) = \frac{1}{2}\big(\mathrm{Beu}(U - z) + \mathrm{Beu}(U + z)\big)$$

which has the property that it is non-negative and majorizes the characteristic function of $[-U, U]$ (see [22]). Further, it satisfies the important property that its Fourier transform $\widehat{g}_U(t)$ satisfies

$$\widehat{g}_U(t) = \begin{cases} 2U + 1 & \text{if } t = 0, \\ 0 & \text{if } |t| > U, \end{cases}$$

$$|\widehat{g}_U(t)| \le 2U + 1.$$

We now define the function γ as

$$\gamma(z) = g_1\Big(\frac{z}{B}\Big), \tag{5.8}$$

whence it follows that $\widehat{\gamma}(t) = B\widehat{g_1}(Bt)$. It is clear that $\gamma(z) \geq \chi_B(z)$ for all real numbers z. Because of the smoothness of γ, we can evaluate the sum

$$\sum_{\substack{(m_1,\dots,m_n)\in\mathbb{Z}^n \\ (m_1,\dots,m_n)\in\mathcal{R}_l}} \gamma(m_1)\cdots\gamma(m_n)$$

via Poisson summation. We have the following lemma, which is standard.

Lemma 5.5 *Let l be a positive integer, and let $\mathcal{R}_l$ be a subset of $(\mathbb{Z}/l\mathbb{Z})^n$. Let γ be as in (5.8), and put*

$$M_{\mathcal{R}_l}(B) = \sum_{\substack{(m_1,\dots,m_n)\in\mathbb{Z}^n \\ (m_1,\dots,m_n)\in\mathcal{R}_l}} \gamma(m_1)\cdots\gamma(m_n).$$

Let

$$E_{\mathcal{R}_l}(t_1,\dots,t_n;l) = \sum_{(a_1,\dots,a_n)\in\mathcal{R}_l} e^{-2\pi i(a_1t_1+\cdots+a_nt_n)/l}. \tag{5.9}$$

Then

$$M_{\mathcal{R}_l}(B) = \frac{1}{l^n}\sum_{(t_1,\dots,t_n)\in\mathbb{Z}^n} \widehat{\gamma}\Big(\frac{t_1}{l}\Big)\cdots\widehat{\gamma}\Big(\frac{t_n}{l}\Big)E_{\mathcal{R}_l}(t_1,\dots,t_n;l).$$

Proof See [13]. ∎

We decompose $M_{\mathcal{R}_l}(B)$ into two terms, given by

$$M_{\mathcal{R}_l}(B) = M^{+}_{\mathcal{R}_l}(B) + O\big(M^{++}_{\mathcal{R}_l}(B)\big), \tag{5.10}$$

where

$$M^{+}_{\mathcal{R}_l}(B) = \frac{1}{l^n}\big(\widehat{\gamma}(0)\big)^n E_{\mathcal{R}_l}(0,\dots,0;l) = \frac{(3B)^n\#\mathcal{R}_l}{l^n},$$

$$M^{++}_{\mathcal{R}_l}(B) = \frac{B^n}{l^n}\sum_{|t_i|\leq l/B}{}' |E_{\mathcal{R}_l}(t_1,\dots,t_n;l)|,$$

where the symbol $\sum'$ denotes that the tuple $(0,\dots,0)$ was omitted. We then have the following lemma.

Lemma 5.6 *Let $l = u_1u_2\mathcal{D}$, where $u_1, u_2, \mathcal{D}$ are as in Lemma 5.4. Put $l = u_1u_2\mathcal{D}$, and let $\mathcal{R}_l = \mathcal{R}_{u_1u_2\mathcal{D}}$ denote the set of congruence classes modulo l satisfying (5.3), (5.4), and (5.5). Then*

$$N_3^{\dagger}(B) \leq \sum_{\substack{u_1|C(\xi_1) \\ u_2\leq\xi_3}} \frac{M^{+}_{\mathcal{R}_l}(B)}{k^{\omega(\mathcal{D})}} + O\bigg(\sum_{\substack{u_1|C(\xi_1) \\ u_2\leq\xi_3}} \frac{M^{++}_{\mathcal{R}_l}(B)}{k^{\omega(\mathcal{D})}}\bigg).$$

Proof This follows from (5.6), (5.7), and (5.10). ∎

We put

$$N_4(B) = \sum_{\substack{u_1 | C(\xi_1) \\ u_2 \le \xi_3}} \frac{M^+_{\mathcal{R}_l}(B)}{k^{\omega(\mathcal{D})}}. \tag{5.11}$$

Our next lemma gives us an estimate for $N_4(B)$.

Lemma 5.7 *Let $u_1, u_2, \mathcal{D}, l, \mathcal{R}_l$ be as in Lemma 5.6 and $N_4(B)$ as in (5.11). Then there exists a positive number C_4 such that*

$$N_4(B) = O\Big(\frac{B^n \exp(2(n+1)(k-1)\xi_1)}{(\log B)^{C_4/\log_3 B}}\Big).$$

Proof Let $\mathcal{R}_{u_1}, \mathcal{R}_{u_2}, \mathcal{R}_{\mathcal{D}}$ denote the congruence classes corresponding to (5.3), (5.4), and (5.5), respectively. By the Chinese Remainder Theorem, it follows that $\#\mathcal{R}_l = \#\mathcal{R}_{u_1}\#\mathcal{R}_{u_2}\#\mathcal{R}_{\mathcal{D}}$. Since $u_1 \,|\, C(\xi_1)$, it follows that $u_1 \le C(\xi_1)$. From its definition and the result of Rosser and Schoenfeld [20], we see that

$$C(\xi_1) \le \exp(2(k-1)\xi_1).$$

For $\mathcal{R}_{u_1}$, we use the trivial bound $\#\mathcal{R}_{u_1} = O(u_1^n) = O(\exp(2n(k-1)\xi_1))$. We have $\#\mathcal{R}_{u_2} = O(u_2^{n-1}\tau_F(u_2)\sigma_{-1/4}(u_2))$ by Lemma 2.1, since u_2 is square-free. Observe that $\gcd(u_1u_2, \mathcal{D}) = 1$. By a theorem of Lang and Weil [15], which states that for a prime $p \,|\, \mathcal{D}$, the number of points over $\mathbb{F}_p$, on the variety defined by the congruence

$$F(x_1, \dots, x_n) - u_1u_2q^k \equiv 0 \pmod{p},$$

is $p^n + O(p^{n-1/2})$. Then

$$\#\mathcal{R}_{\mathcal{D}} = \prod_{p|\mathcal{D}} \big(p^n + O(p^{n-1/2})\big), \tag{5.12}$$

whence

$$\#\mathcal{R}_{\mathcal{D}} = \mathcal{D}^n \prod_{p|\mathcal{D}} \big(1 + O(p^{-1/2})\big) = O\big(\mathcal{D}^n \sigma_{-1/4}(\mathcal{D})\big).$$

Thus, by (5.10), (5.12), and Lemma 2.1, we see that

$$\begin{aligned} N_4(B) &= O\Bigg(\exp(2n(k-1)\xi_1) \sum_{\substack{u_1 | C(\xi_1) \\ u_2 \le \xi_3}} \frac{(3B)^n u_2^{n-1}\tau_F(u_2)\sigma_{-1/4}(u_2)\mathcal{D}^n\sigma_{-1/4}(\mathcal{D})}{(u_2\mathcal{D})^n k^{\omega(\mathcal{D})}}\Bigg) \\ &= O\Bigg(\exp(2n(k-1)\xi_1) \sum_{\substack{u_1 | C(\xi_1) \\ u_2 \le \xi_3}} \frac{B^n \sigma_{-1/4}(u_2)\tau_F(u_2)\sigma_{-1/4}(\mathcal{D})}{u_2 k^{\omega(D)}}\Bigg). \end{aligned}$$

Observe that

$$\sigma_{-1/4}(\mathcal{D}) = \prod_{p|\mathcal{D}} (1 + p^{-1/4}) = O\Big(\Big(\frac{2k}{3}\Big)^{\omega(\mathcal{D})}\Big).$$

It follows that

$$N_4(B) = O\Bigg((\exp(2n(k-1)\xi_1) \sum_{\substack{u_1 | C(\xi_1) \\ u_2 \le \xi_3}} \frac{B^n \tau_F(u_2)\sigma_{-1/4}(u_2)}{u_2(3/2)^{\omega(D)}}\Bigg).$$

Let us write

$$\xi_4 = \xi_4(u_2) = \frac{1}{12}\log(B^2 u_2^{-1}) \quad \text{and} \quad \mathcal{D}' = \mathcal{D}'(u_2) = \prod_{p \le \xi_4} p.$$

Observe that as $B^2\xi_3^{-1} \to \infty$ as B tends to infinity and $u_2^{-1} \gg \xi_3^{-1}$, we have

$$\log \mathcal{D}' = \sum_{p \le \xi_4} \log p < \frac{12}{11}\xi_4$$

for B sufficiently large, say by Rosser and Schoenfeld [20]. From (5.2), we see that

$$\mathcal{D} \le \mathcal{D}' < \exp(12\xi_4/11) = \Big(\frac{B^2}{u_2}\Big)^{1/11}.$$

Next, we have

$$\omega(\mathcal{D}') = \pi(\xi_4; k, 1) \sim \frac{\xi_4}{\varphi(k)\log \xi_4},$$

where $\pi(B; q, a)$ is the counting function of primes p satisfying $p \equiv a \pmod q$ up to B, and the above asymptotic follows from Dirichlet's theorem on primes in arithmetic progressions. Therefore, we can find a constant C_2 such that

$$\omega(\mathcal{D}') > \frac{C_2\xi_4}{\log \xi_4}$$

for all B sufficiently large. Observe that for a square-free number l, we have

$$\sigma_0(l) = \prod_{p \mid l}(1+1) = 2^{\omega(l)}.$$

From the definition of $\mathcal{D}$ and $\mathcal{D}'$, it follows that

$$(3/2)^{\omega(\mathcal{D}')} < (3/2)^{\omega(D')}C(\xi_1)(3/2)^{\gcd(\mathcal{D}',u_2)} < (3/2)^{\omega(\mathcal{D})}C(\xi_1)\sigma_0(\gcd(\mathcal{D}',u_2)).$$

Hence, there exists a positive number C_3 such that

$$\frac{1}{(3/2)^{\omega(\mathcal{D})}} < \frac{C_3}{(3/2)^{\omega(\mathcal{D}')}}\sigma_0\big(\gcd(\mathcal{D}',u_2)\big)\exp\big(2(k-1)\xi_1\big).$$

From here we obtain the estimate

(5.13)
$$N_4(B) = O\bigg(\exp(2(n+1)(k-1)\xi_1)\sum_{u_2 \le \xi_3}\frac{B^n\tau_F(u_2)\sigma_{-1/4}(u_2)\sigma_0(\gcd(\mathcal{D}',u_2))}{(3/2)^{\omega(\mathcal{D}')}u_2}\bigg).$$

We now estimate the sum

$$S(t) = \sum_{u_2 \le t}\tau_F(u_2)\sigma_{-1/4}(u_2)\sigma_0\big(\gcd(\mathcal{D},u_2)\big).$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

We proceed, as with Hooley, by invoking his [12, Lemma 6.2]. We then have

$$\begin{aligned}
S(t) &\le \sum_{h\mid\mathcal{D}} \mu^2(h)\sigma_0(h) \sum_{\substack{u_2\le t\\ u_2\equiv 0 \pmod h}} \tau_F(u_2)\sigma_{-1/4}(u_2)\\
&= \sum_{h\mid\mathcal{D}} \mu^2(h)\sigma_0(h) \sum_{\substack{u_2' h\le t\\ \gcd(u_2',h)=1}} \tau_F(hu_2')\sigma_{-1/4}(hu_2')\\
&\le \sum_{h\mid\mathcal{D}} \mu^2(h)\sigma_0(h)\tau_F(h)\sigma_{-1/4}(h) \sum_{u_2'\le t/h} \tau_F(u_2')\sigma_{-1/4}(u_2')\\
&= O\Big(t\sum_{h\mid\mathcal{D}} \frac{\mu^2(h)\sigma_0(h)\tau_F(h)\sigma_{-1/4}(h)}{h}\Big)\\
&= O\Big(t\prod_{w\le\xi_4} \Big(1+\frac{2d+1}{w}\Big)\Big)\\
&= O\big(t(\log\xi_4)^{2d+1}\big) = O\big(t(\log\log B)^{2d+1}\big).
\end{aligned}$$

By following Hooley's treatment of the term $N^{(6)}(X)$ in [12, Section 8] and cutting the range of the summation in (5.13) into dyadic parts, we see that, for some positive number C_4, we have

$$N_4(B) = O\Big(\frac{B^n\exp(2(n+1)(k-1)\xi_1)}{(\log B)^{C_4/\log_3 B}}\Big). \qquad \blacksquare$$

We now put

$$\xi_1(B) = \max\Big\{1, \frac{C_4\log\log B}{4(n+1)(k-1)\log_3 B}\Big\},$$

so that

$$\frac{\exp(2(n+1)(k-1)g(B))}{\exp(C_4\log_2 B/\log_3 B)} = \exp\Big(\frac{-C_4\log_2 B}{2\log_3 B}\Big),$$

whence

$$N_4(B) = O\Big(B^n\exp\Big(\frac{-C_4\log_2 B}{2\log_3 B}\Big)\Big) = o(B^n).$$

Next we turn our attention to the much more difficult component

$$N_5(B) = \sum_{\substack{u_1\mid C(\xi_1)\\ u_2\le\xi_3}} \frac{M^{++}_{\mathcal{R}_l}(B)}{k^{\omega(\mathcal{D})}}. \tag{5.14}$$

Recall from (5.9) that

$$E_{\mathcal{R}_l}(t_1,\dots,t_n;l) = E_{\mathcal{R}_{u_1}}E_{\mathcal{R}_{u_2}}E_{\mathcal{R}_{\mathcal{D}}}.$$

The term $E_{\mathcal{R}_{u_1}}(t_1,\dots,t_n;u_1)$ can be trivially estimated by u_1^n, which is of size

$$O(\exp(\frac{C_4\log_2 B}{4(k-1)\log_3 B})).$$

We now consider the term $E_{\mathcal{R}_{u_2}}$. For each prime p dividing u_2, we write

$$F(\mathbf{x}) = F^*(\mathbf{x}) \prod_{j=1}^{\tau(p)} \mathcal{L}_i(\mathbf{x}),$$

where F^* and $\mathcal{L}_i$ have coefficients in $\mathbb{Z}_p$. We then write $E_{\mathcal{R}_{u_2}}$ as

$$\begin{aligned} E_{\mathcal{R}_{u_2}}(t_1,\dots,t_n;u_2) &= \prod_{p|u_2}\Bigg(\sum_{1\le i\le \tau_F(p)} \sum_{\substack{(a_1,\dots,a_n)\in\mathbb{F}_p^n \\ \mathcal{L}_i(a_1,\dots,a_n)\equiv 0 \pmod p}} e^{2\pi i(a_1t_1+\cdots+a_nt_n)/p}\Bigg) \\ &= \prod_{p|u_2} S(t_1,\dots,t_n;p). \end{aligned}$$

We will obtain the following estimate for $S(t_1,\dots,t_n;p)$.

Lemma 5.8 *Let p be a prime, and put*

$$S(t_1,\dots,t_n;p) = \sum_{1\le i\le \tau_F(p)} \sum_{\substack{(a_1,\dots,a_n)\in\mathbb{F}_p^n \\ \mathcal{L}_i(a_1,\dots,a_n)\equiv 0 \pmod p}} e^{2\pi i(a_1t_1+\cdots+a_nt_n)/p}.$$

Then we have

$$S(t_1,\dots,t_n;p)\begin{cases} \le \tau_F(p)p^{n-1} & \text{if } t_1x_1+\cdots+t_nx_n \text{ divides } F(\mathbf{x}) \text{ over } \mathbb{F}_p, \\ = 0 & \text{otherwise.} \end{cases}$$

Proof We consider two scenarios. Suppose that

$$\mathcal{L}_s(x_1,\dots,x_n) = v_1^{(s)}x_1+\cdots+v_n^{(s)}x_n,\ v_j^{(s)}\in\mathbb{Z}_p \text{ for } 1\le j\le n.$$

If $(t_1,\dots,t_n)\equiv\lambda(v_1^{(s)},v_2^{(s)},\dots,v_n^{(s)}) \pmod p$ for some $\lambda\in\mathbb{F}_p^*$, then

$$\sum_{\substack{(a_1,\dots,a_n)\in\mathbb{F}_p^n \\ \mathcal{L}_s(a_1,\dots,a_n)\equiv 0 \pmod p}} e^{2\pi i(a_1t_1+\cdots+a_nt_n)/p} = p^{n-1}.$$

Observe that since $p\nmid\Delta(F)$, there does not exist $1\le s\le\tau_F(p)$ such that $p\,|\,v_j^{(s)}$ for all $j=1,\dots,n$. We can suppose, without loss of generality, that $v_1^{(s)}\not\equiv 0 \pmod p$. Suppose that $\mathbf{a}\in\mathbb{F}_p^n$ is such that $\mathcal{L}_s(\mathbf{a})\equiv 0 \pmod p$. It then follows that

$$a_1\equiv -(v_1^{(s)})^{-1}(v_2^{(s)}a_2+\cdots+v_n^{(s)}a_n).$$

This implies

$$\sum_{\substack{(a_1,\dots,a_n)\in\mathbb{F}_p^n \\ \mathcal{L}_s(a_1,\dots,a_n)\equiv 0 \pmod p}} e^{2\pi i(a_1t_1+\cdots+a_nt_n)/p} = \sum_{(a_2,\dots,a_n)\in\mathbb{F}_p^n} e^{2\pi i(a_2(t_2-t_1(v_1^{(s)})^{-1}v_2^{(s)})+\cdots+a_n(t_n-t_1(v_1^{(s)})^{-1}v_n^{(s)}))/p}. \tag{5.15}$$

The right-hand side can be written as

$$\prod_{j=2}^{n} \sum_{a_j \in \mathbb{F}_p} e^{2\pi i a_j (v_1^{(s)} t_j - t_1 v_j^{(s)})/p}.$$

For each j, the sum

$$\sum_{a_j \in \mathbb{F}_p} e^{2\pi i a_j (v_1^{(s)} t_j - t_1 v_j^{(s)})/p}$$

is zero unless the exponent is identically zero. This shows that (5.15) is non-zero if and only if $v_1^{(s)} t_j \equiv t_1 v_j^{(s)} \pmod p$ for $j = 2, \dots, n$. This implies that

$$\begin{aligned}(t_1, \dots, t_n) &\equiv t_1 (v_1^{(s)})^{-1} (v_1^{(s)}, v_1^{(s)} t_2 t_1^{-1}, \dots, v_1^{(s)} t_n t_1^{-1}) \pmod p\\ &\equiv t_1 (v_1^{(s)})^{-1} (v_1^{(s)}, v_2^{(s)}, \dots, v_n^{(j)}) \pmod p,\end{aligned}$$

hence the first situation is the only case where the sum

$$\sum_{\substack{(a_1,\dots,a_n)\in\mathbb{F}_p^n \\ \mathcal{L}_s(a_1,\dots,a_n)\equiv 0 \pmod p}} e^{2\pi i (a_1 t_1 + \cdots + a_n t_n)/p}$$

is non-zero. In other words, we have

$$S(t_1, \dots, t_n; p) \begin{cases} \le \tau_F(p) p^{n-1} & \text{if } t_1 x_1 + \cdots + t_n x_n \text{ divides } F(\mathbf{x}) \text{ over } \mathbb{F}_p, \\ = 0 & \text{otherwise,} \end{cases}$$

as desired. ∎

For square-free l, let us write

$$S(t_1, \dots, t_n; l) = \prod_{p \mid l} S(t_1, \dots, t_n; p).$$

We have the following lemma.

Lemma 5.9 *Let $u_1, u_2, \mathcal{D}$ be as in Lemma 5.6. Then*

$$\sum_{\substack{u_1 \mid C(\xi_1) \\ u_2 \le \xi_3}} \frac{M_l^{++}(B)}{k^{\omega(\mathcal{D})}} = O\Big(\exp(2(n+1)(k-1)\xi_1) \sum_{u_2 \le \xi_3} \frac{B^n}{u_2^n} \sideset{}{'}\sum_{|t_1|,\dots,|t_n| \le l/B} S(t_1, \dots, t_n; u_2) \Big). \tag{5.16}$$

Proof Recall that

$$M_l^{++}(B) = \frac{B^n}{u_1^n u_2^n \mathcal{D}^n} \sideset{}{'}\sum_{|t_i| \le l/B} |E_{\mathcal{R}_l}(t_1, \dots, t_n; l)|.$$

Note that

$$|E_{\mathcal{R}_l}(t_1, \dots, t_n; \mathcal{D})| = O\big(\mathcal{D}^n \sigma_{-1/4}(\mathcal{D}) \big),$$

and the multiplicativity of $E_{\mathcal{R}_l}$ implies that

$$\big| E_{\mathcal{R}_l}(t_1, \dots, t_n; l) \big| = O\big(u_1^n \mathcal{D}^n \sigma_{-1/4}(\mathcal{D}) S(t_1, \dots, t_n; u_2) \big).$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

Next note that $\sigma_{-1/4}(\mathcal{D}) = O(k^{\omega(\mathcal{D})})$, since $k \geq 2$. This then implies (5.16), since the number of divisors of $C(\xi_1)$ does not exceed $C(\xi_1)$. ■

We now assess $S(t_1, \ldots, t_n; u_2)$ for an n-tuple $(t_1, \ldots, t_n) \in \mathbb{Z}^n$. By Lemma 5.8, this is zero unless for each prime $p \mid u_2$ there exists $\lambda_p \in \mathbb{F}_p$ and $1 \leq s_p \leq \tau_F(p)$ such that $(t_1, \ldots, t_n) \equiv \lambda_p(v_1^{(s_p)}, v_2^{(s_p)}, \ldots, v_n^{(s_p)}) \pmod p$. One checks at once that for a fixed vector $\boldsymbol{v} = (v_1, \ldots, v_n)$, the set

$$\left\{ (x_1, \ldots, x_n) \in \mathbb{Z}^n : (x_1, \ldots, x_n) \equiv \lambda(v_1, \ldots, v_n) \pmod p \text{ for some } \lambda \in \mathbb{F}_p \right\}$$

is a lattice. For each prime p dividing u_2, there are $\tau_F(p) \leq d$ such lattices to consider. If $(t_1, \ldots, t_n) \in \mathbb{Z}^n$ is such that $S(t_1, \ldots, t_n; u_2)$ is non-zero, then it must lie on one such lattice for each prime divisor of u_2. Therefore, $(t_1, \ldots, t_n)$ lies on one of at most $d^{\omega(u_2)}$ lattices, each with determinant u_2^{n-1}. Let $\mathfrak{L}(u_2)$ denote the set of lattices to which the n-tuples $(t_1, \ldots, t_n)$ such that $S(t_1, \ldots, t_n; u_2) \neq 0$ are restricted.

We now replace the bound l/B for the variables t_i in Lemma 5.16 by something that is easier to work with. Observe that

$$u_1 \mathcal{D} = O\Big(\exp(2(k-1)\xi_1) \Big(\frac{B^2}{u_2} \Big)^{1/11} \Big).$$

Therefore, it follows that

$$\frac{l}{B} = \frac{u_1 u_2 \mathcal{D}}{B} = O\Big(\exp(2(k-1)\xi_1) \frac{B^{2/11}}{u_2^{1/11}} \frac{u_2}{B} \Big) = O\Big(\exp(2(k-1)\xi_1) \Big(\frac{u_2^{10/11}}{B^{9/11}} \Big) \Big).$$

Moreover, we have

$$\exp(2(k-1)\xi_1) \frac{u_2^{10/11}}{B^{9/11}} = O\Big(\frac{u_2^{9/10}}{B^{4/5}} \Big),$$

since

$$\frac{u_2^{9/10}}{B^{4/5}} \cdot \frac{B^{9/11}}{u_2^{10/11}} = \Big(\frac{B^2}{u_2} \Big)^{1/55} \gg (\log B)^{\frac{2k}{165}} \gg (\log B)^{\frac{C_4}{2(n+1)\log_3 B}}.$$

Put

$$Q(B) = \sum_{u_2 \leq \xi_3} \frac{1}{u_2^n} \sideset{}{'}\sum_{|t_1|, \ldots, |t_n| \leq u_2^{9/10}/B^{4/5}} S(t_1, \ldots, t_n; u_2). \tag{5.17}$$

Then it is clear that

$$\sum_{\substack{u_1 \mid C(\xi_1) \\ u_2 \leq \xi_3}} \frac{M_l^{++}(B)}{k^{\omega(\mathcal{D})}} = O\big(B^n g(B)^{k-1} Q(B) \big). \tag{5.18}$$

We will assess $Q(B)$ by restricting the range of u_2 to a dyadic interval of the form $(U/2, U]$, with $U \leq \xi_3$. Denote this contribution to $Q(B)$ by $Q_U(B)$. We have the following lemma.

Lemma 5.10 *Let $Q(B)$ be as in (5.17). Then there exists a positive number C_5 such that for all $U > 1$, we have*

$$Q_U(B) = O\Big(\frac{U^{9/10} (\log B)^{C_5}}{B^{8/5}} \Big).$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

Proof Let us write $F_s(x_1, x_s)$ for the product

$$F_s(x_1, x_s) = \prod_{j=1}^{d} (\psi_1^{(j)} x_1 + \psi_s^{(j)} x_s),$$

where $\psi_s^{(j)}$ are as in (4.1). Note that each F_s has integer coefficients. Moreover, since F is irreducible over $\mathbb{Q}$ it follows that each F_s is a perfect power of a binary form with integer coefficients. Further, F_s is not identically zero for $s = 2, \dots, n$. If we fix a vector $(t_1, \dots, t_n) \in \mathbb{Z}^n$, then there are at most $\sigma_0(F_2(t_2, -t_1))$ many u_2 such that $(t_1, \dots, t_n) \in \Lambda$ for some $\Lambda \in \mathfrak{L}(u_2)$. To see this, if $(t_1, \dots, t_n) \in \Lambda$ for $\Lambda \in \mathfrak{L}(u_2)$, then for each prime $p \mid u_2$, we have $(t_1, \dots, t_n) \equiv \lambda_p(1, v_2^{(s)}, \dots, v_n^{(s)}) \pmod{p}$ for some $\lambda_p \in \mathbb{F}_p$ and $1 \le s \le \tau_F(p)$. Then it follows that $t_2 \equiv t_1 v_2^{(s)} \pmod{p}$, hence it follows that

$$F_2(t_2, -t_1) \equiv 0 \pmod{p}.$$

This implies that $u_2 \mid F_2(t_2, -t_1)$, as claimed. Further, by the same argument, we get that $u_2 \mid F_s(t_s, -t_1)$ for all $2 \le s \le n$.

Now we can estimate $Q_U(B)$ when U is suitably small as follows:

$$\begin{aligned} Q_U(B) &\le \frac{2^n}{U^n} \sum_{U/2 < u_2 \le U} \sideset{}{'}\sum_{|t_1|, \dots, |t_n| \le U^{9/10}/B^{4/5}} S(t_1, \dots, t_n; u_2) \\ &\le \frac{2^n}{U} \sum_{U/2 < u_2 \le U} d^{\omega(u_2)} \sideset{}{'}\sum_{\substack{|t_1|, \dots, |t_n| \le U^{9/10}/B^{4/5} \\ u_2 \mid \gcd(F_2(t_2, -t_1), \dots, F_n(t_n, -t_1))}} 1. \end{aligned}$$

Observe that for fixed t_1, t_2, the condition $u_2 \mid F_j(t_j, -t_1)$ constrains each $t_j, j = 3, \dots, n$, to at most $d^{\omega(u_2)}$ congruence classes modulo u_2, and for each congruence class, at most $(2U^{9/10}B^{-4/5})/u_2 + 1$ choices in the range $[-U^{9/10}/B^{4/5}, U^{9/10}/B^{4/5}]$. Since $U/2 < u_2 \le U$, there is at most one choice when B is sufficiently large. By the binomial theorem, for a number A and a square-free positive integer m, we have

$$\sum_{r \mid m} A^{\omega(r)} = (A + 1)^{\omega(m)}.$$

By permuting the variables if necessary, we can assume that $t_1 \ne 0$, at the cost of a factor of n. Hence,

$$\begin{aligned} Q_U(B) &\le \frac{n2^n}{U} \sum_{\substack{|t_1|, |t_2| \le U^{9/10}/B^{4/5} \\ t_1 \ne 0}} \sum_{u_2 \mid F_2(t_2, -t_1)} d^{(n-1)\omega(u_2)} \\ &= \frac{n2^n}{U} \sideset{}{'}\sum_{\substack{|t_1|, |t_2| \le U^{9/10}/B^{4/5} \\ t_1 \ne 0}} (d^{n-1} + 1)^{\omega(F_2(t_2, -t_1))}, \end{aligned} \tag{5.19}$$

so by [12, Lemma 10.1], there exists a positive number C_5 such that

$$Q_U(B) = O\Big(\frac{U^{9/10} (\log B)^{C_5}}{B^{8/5}} \Big). \qquad \blacksquare$$

If U is relatively small, say $U < B^{5/3}$, then this is a satisfactory bound. Otherwise, we use [12, Lemma 10.2], which we state as follows.

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

Lemma 5.11 (Hooley, 2009) *Set $\Xi(B) = B^{\frac{1}{6(\log\log B)^2}}$. Fix $u_2 \le \xi_3$. Let $\omega^\dagger(m)$ denote the number of distinct prime factors of m that exceed Ξ and let*

$$l^* = \prod_{\substack{p\le\Xi\\ p\mid u_2}} p \quad \text{and} \quad l^\dagger = \prod_{\substack{p>\Xi\\ p\mid u_2}} p.$$

Suppose that $l^* \le B^{1/6}$. Then, for any positive constant C_6 and for $B^{1/2} < Y < B$, there exists a positive number C_7, depending only on C_6, such that

$$\sideset{}{'}\sum_{\substack{(u_1,u_2)\equiv(t_1,t_2) \pmod{l^*}\\ |u_1|,|u_2|\le Y}} C_6^{\omega^\dagger(F(u_1,u_2))} = O\Big(\frac{Y^2(\log\log B)^{C_7}}{(l^*)^2}\Big).$$

When $U > B^{5/3}$ we employ the divisors $l^*, l^\dagger$ of u_2 as in Lemma 5.11. Suppose first that $l^* > B^{1/6}$. This means that $B^{1/6} < \Xi^{\omega(l^*)} \le \Xi^{\omega(u_2)}$, which shows that $\omega(u_2) > (\log_2 B)^2$. Hence, either $\omega(u_2) > (\log_2 B)^2$ or $l^* \le B^{1/6}$. Put

$$Q_U^{(1)}(B) = \sum_{\substack{U/2<u_2\le U\\ \omega(u_2)>(\log_2 B)^2}} \frac{1}{u_2^n} \sideset{}{'}\sum_{|t_1|,\dots,|t_n|\le u_2^{9/10}/B^{4/5}} S(t_1,\dots,t_n;u_2), \tag{5.20}$$

$$Q_U^{(2)}(B) = \sum_{\substack{U/2<u_2\le U\\ l^*\le B^{1/6}}} \frac{1}{u_2^n} \sideset{}{'}\sum_{|t_1|,\dots,|t_n|\le u_2^{9/10}/B^{4/5}} S(t_1,\dots,t_n;u_2). \tag{5.21}$$

We have the following estimates for $Q_U^{(1)}(B)$ and $Q_U^{(2)}(B)$.

Lemma 5.12 *Let $Q_U^{(1)}(B), Q_U^{(2)}(B)$ be as in (5.20) and (5.21), respectively. Then there exists a positive number C_6 depending only on d, n such that*

$$Q_U^{(1)}(B) = O_d\Big(\frac{U^{4/5}(\log B)^{C_6}}{B^{8/5}(\log B)^{\log_2 B}}\Big) \quad \text{and} \quad Q_U^{(2)}(B) = O_d\Big(\frac{U^{4/5}\log B(\log_2 B)^{C_7}}{B^{8/5}}\Big).$$

Proof To estimate $Q_U^{(1)}(B)$, by (5.19) we have

$$\begin{aligned} Q_U^{(1)}(B) &\le \frac{n2^n}{U} \sum_{\substack{u_2\le U\\ \omega(u_2)>(\log\log B)^2}} \sideset{}{'}\sum_{|t_1|,|t_2|\le u_2^{9/10}/B^{4/5}} d^{(n-1)\omega(F(t_2,-t_1))} \\ &\ll_n \frac{1}{U} \sideset{}{'}\sum_{|t_1|,|t_2|\le U^{9/10}/B^{4/5}} \sum_{\substack{u_2\mid F_2(t_2,-t_1)\\ \omega(u_2)>(\log_2 B)^2}} d^{(n-1)\omega(u_2)}. \end{aligned}$$

Observe that since $u_2 \mid F_2(t_2,-t_1)$, we have

$$d^{(n-1)\omega(u_2)} = \frac{d^{(n-1)\omega(u_2)}e^{(\log_2 B)^2}}{(\log B)^{\log_2 B}} < \frac{(3d^{n-1})^{\omega(u_2)}}{(\log B)^{\log_2 B}}.$$

https://doi.org/10.4153/CJM-2017-060-4 Published online by Cambridge University Press

By the binomial theorem and the fact that u_2 is square-free, it follows that

$$\sum_{\substack{u_2 \mid F_2(t_2,-t_1) \\ \omega(u_2) > (\log_2 B)^2}} d^{(n-1)\omega(u_2)} \le \sum_{\substack{u_2 \mid F_2(t_2,-t_1) \\ \omega(u_2) > (\log_2 B)^2}} \frac{(3d^{n-1})^{\omega(u_2)}}{(\log B)^{\log_2 B}} = \frac{(3d^{n-1}+1)^{\omega(F_2(t_2,-t_1))}}{(\log B)^{\log_2 B}}.$$

Hence, we see that for some positive C_6,

$$\begin{aligned} Q_U^{(1)}(B) &\ll_n \frac{1}{U(\log B)^{\log_2 B}} \sideset{}{'}\sum_{|t_1|,|t_2| \le U^{9/10}/B^{4/5}} (3d^{n-1}+1)^{\omega(F_2(t_2,-t_1))} \\ &= O\Big(\frac{U^{4/5}(\log B)^{C_6}}{B^{8/5}(\log B)^{\log_2 B}} \Big) \end{aligned}$$

by [12, Lemma 10.1]. This completes the estimation of $Q_U^{(1)}(B)$.

Observe that

$$\frac{U^{4/5}}{B^{8/5}} = O(\xi_3^{4/5} B^{-8/5}) = O((\log B)^{-8k/15}),$$

and thus the desired conclusion for $Q_U^{(1)}(B)$ holds.

The sum $Q_U^{(2)}(B)$ is more difficult. The key tool will be Lemma 5.11. Recall that $Q_U^{(2)}(B)$ consists of the contribution from those tuples for which $l^* \le B^{1/6}$ and $U > B^{5/3}$. By the multiplicativity of $S(t_1,\dots,t_n,\cdot)$, it follows that

$$Q_U^{(2)}(B) \le \frac{2^n}{U^n} \sideset{}{'}\sum_{|t_1|,\dots,|t_n| \le U^{9/10}/B^{4/5}} \sum_{\substack{l^* l^\dagger \le U \\ l^* \le B^{1/6}}} S(t_1,\dots,t_n; l^*) S(t_1,\dots,t_n; l^\dagger).$$

We rearrange the summation to obtain

$$\frac{2^n}{U^n} \sum_{\substack{l^* l^\dagger \le U \\ l^* \le B^{1/6}}} \sum_{b_1,\dots,b_n \pmod{l^*}} S(b_1,\dots,b_n; l^*) \sideset{}{'}\sum_{\substack{|t_1|,\dots,|t_n| \le U^{9/10}/B^{4/5} \\ t_i \equiv b_i \pmod{l^*}}} S(t_1,\dots,t_n; l^\dagger).$$

We estimate $S(t_1,\dots,t_n; l^\dagger)$ by $d^{\omega(l^\dagger)}(l^\dagger)^{n-1}$ when it is non-zero. Next we observe that from the proof of Lemma 5.10, $S(t_1,\dots,t_n; l^\dagger)$ is non-zero only if $l^\dagger$ divides $F_s(t_s,-t_1)$ for $s = 2,\dots,n$. Since $U > B^{5/3}$ and $l^* \le B^{1/6}$, it follows that $l^\dagger > B^{3/2}$. Therefore, $(U^{9/10}B^{-4/5})/l^\dagger \ll B^{-1/2}(\log B)^{-2k/3}$. In other words, for sufficiently large B and for fixed t_1, t_2, the congruence condition imposed by $l^\dagger$ leads to at most $d^{\omega(l^\dagger)}$

choices for $t_3, \ldots, t_n$ as before. It then follows that

$$
\begin{aligned}
Q_U^{(2)}(B) & \\
&\leq \frac{n2^n}{U^n} \sum_{\substack{l^* \leq B^{1/6} \\ b_1,\ldots,b_n \pmod{l^*}}} S(b_1,\ldots,b_n; l^*) \sideset{}{'}\sum_{\substack{|t_1|,|t_2| \leq U^{9/10}/B^{4/5} \\ t_i \equiv b_i \pmod{l^*}}} \sum_{l^\dagger | F_2(t_2,-t_1)} d^{\omega(l^\dagger)} (l^\dagger)^{n-1} \\
&\leq \frac{n2^n}{U} \sum_{\substack{l^* \leq B^{1/6} \\ b_1,\ldots,b_n \pmod{l^*}}} \frac{S(t_1,\ldots,t_n; l^*)}{(l^*)^{n-1}} \sideset{}{'}\sum_{\substack{|t_1|,|t_2| \leq U^{9/10}/B^{4/5} \\ t_i \equiv b_i \pmod{l^*}}} \sum_{l^\dagger | F_2(t_2,-t_1)} d^{\omega(l^\dagger)} \\
&\ll \frac{n2^n}{U} \sum_{\substack{l^* \leq B^{1/6} \\ b_1,\ldots,b_n \pmod{l^*}}} \frac{S(b_1,\ldots,b_n; l^*)}{(l^*)^{n-1}} \sideset{}{'}\sum_{\substack{|t_1|,|t_2| \leq U^{9/10}/B^{4/5} \\ t_i \equiv b_i \pmod{l^*}}} (d^{n-1}+1)^{\omega^\dagger(F_2(t_2,-t_1))} \\
&\ll \frac{n2^n}{U} \sum_{\substack{l^* \leq B^{1/6} \\ b_1,\ldots,b_n \pmod{l^*}}} \frac{S(b_1,\ldots,b_n; l^*)}{(l^*)^{n-1}} \sideset{}{'}\sum_{\substack{|t_1|,|t_2| \leq U^{9/10}/B^{4/5} \\ t_1 \equiv b_1 \pmod{l^*} \\ t_2 \equiv b_2 \pmod{l^*}}} (d^{n-1}+1)^{\omega^\dagger(F(t_2,-t_1))}.
\end{aligned}
$$

Note that $U < \xi_3 = C_1 B^2 (\log B)^{-2k/3}$, whence $U^{9/10}/B^{4/5} < B$. Further, our assumption of $U > B^{5/3}$ shows that $U^{9/10}/B^{4/5} > B^{7/10}$. Hence, the innermost sum is treatable by Lemma 5.11. We then have

$$
Q_U^{(2)}(B) = O_d\Big(\frac{U^{4/5} (\log_2 B)^{C_7}}{B^{8/5}} \sum_{l^* \leq B^{1/6}} \frac{1}{(l^*)^{n+1}} \sum_{b_1,\ldots,b_n \pmod{l^*}} S(b_1,\ldots,b_n; l^*) \Big).
$$

By the proof of Lemma 5.8, we see that for each prime p, we have

$$
\sum_{b_1,\ldots,b_n \pmod{p}} S(b_1,\ldots,b_n; p) = p \cdot \tau_F(p) p^{n-1} = \tau_F(p) p^n.
$$

It thus follows from multiplicativity that for any squarefree l, we have

$$
\sum_{b_1,\ldots,b_n \pmod{l}} S(b_1,\ldots,b_n; l) = \tau_F(l) l^n.
$$

We then deduce that

$$
\sum_{l^* \leq B^{1/6}} \frac{1}{(l^*)^{n+1}} \sum_{b_1,\ldots,b_n \pmod{l^*}} S(b_1,\ldots,b_n; l^*) \leq \frac{\tau_F(l^*)}{l^*}.
$$

By [12, Lemma 6.1], we then see that

$$
\begin{aligned}
Q_U^{(2)}(B) &= O_d\Big(\frac{U^{4/5} (\log_2 B)^{C_7}}{B^{8/5}} \sum_{l^* \leq B^{1/6}} \frac{\tau_F(l^*)}{l^*} \Big) \\
&= O_d\Big(\frac{U^{4/5} (\log_2 B)^{C_7}}{B^{8/5}} \prod_{p \leq B^{1/6}} \Big(1 + \frac{\tau_F(p)}{p}\Big) \Big) \\
&= O_d\Big(\frac{U^{4/5} \log B (\log_2 B)^{C_7}}{B^{8/5}} \Big),
\end{aligned}
$$

as desired. ∎

By summing $Q_U(B), Q_U^{(1)}(B), Q_U^{(2)}(B)$ over dyadic ranges of U up to ξ_2, we then see that

$$\sum_{1\le k\ll \log B} O_d\Big(\frac{(B^{5/3}/2^k)^{9/10}(\log B)^{C_5}}{B^{8/5}}\Big) = O\Big(\frac{(\log B)^{C_5}}{B^{1/10}}\Big),$$

$$\sum_{1\le k\ll \log B} O_d\Big(\frac{(\xi_3/2^k)^{4/5}(\log B)^{C_6}}{B^{8/5}(\log B)^{\log_2 B}}\Big) = O\Big((\log B)^{C_6-8k/15-\log_2 B}\Big),$$

$$\sum_{1\le k\ll \log B} O_d\Big(\frac{(\xi_3/2^k)^{4/5}\log B(\log_2 B)^{C_7}}{B^{8/5}}\Big) = O_d\Big(\frac{(\log_2 B)^{C_7}}{(\log B)^{(2k-3)/3}}\Big).$$

This shows that

$$Q(B) = O_F\Big(\frac{(\log_2 B)^{C_7}}{(\log B)^{(2k-3)/3}}\Big) = o(1),$$

and by (5.18), (5.14), and Lemmas 4.2 and 5.6 we see that $N_3(B) = o(B^n)$, and this completes the proof of Theorem 1.1. ∎

Acknowledgments The author would like to thank C. L. Stewart and D. Tweedle for their discussions and comments, as well as the anonymous referee, whose feedback has been invaluable in improving the paper.

References

[1] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*. Ann. of Math. **181**(2015), 191–242. http://dx.doi.org/10.4007/annals.2015.181.1.3
[2] M. Bhargava, A. Shankar, and X. Wang, *Squarefree values of polynomial discriminants I*. arxiv:1611.09806
[3] T. D. Browning, *Quantitative arithmetic on projective varieties*. Progress in Mathematics, 277, Birkhäuser Verlag, Basel, 2009.
[4] T. Ekedahl, *An infinite version of the Chinese remainder theorem*. Comment. Math. Univ. St. Paul. **40**(1991), 53–59.
[5] P. Erdős, *Arithmetical properties of polynomials*. J. London Math. Soc. **28**(1953), 416–425. http://dx.doi.org/10.1112/jlms/s1-28.4.416
[6] T. Estermann, *Einige Satze uber quadratfeie Zahlen*. Math. Ann. **105**(1931), 653–662. http://dx.doi.org/10.1007/BF01455836
[7] A. Granville, *ABC allows us to count squarefrees*. Internat. Math. Res. Notices **9**(1998), 991–1009.
[8] G. Greaves, *Power-free values of binary forms*. Quart. J. Math Oxford Ser. (2) **43**(1992), 45–65. http://dx.doi.org/10.1093/qmath/43.1.45
[9] D. R. Heath-Brown, *Diophantine approximation with square free numbers*. Math. Z. **187**(1984), 335–344. http://dx.doi.org/10.1007/BF01161951
[10] H. A. Helfgott, *Power-free values, large deviations, and integer points on irrational curves*. J. Théor. Nombres Bordeaux **19**(2007), 433–472. http://dx.doi.org/10.5802/jtnb.596
[11] C. Hooley, *On the power free values of polynomials*. Mathematika **14**(1967), 21–26. http://dx.doi.org/10.1112/S002557930000797X
[12] ———, *On the power-free values of polynomials in two variables*. In: Analytic number theory, Cambridge University Press, Cambridge, 2009, pp. 235–266.
[13] ———, *On the power-free values of polynomials in two variables. II*. J. Number Theory **129**(2009), 1443–1455. http://dx.doi.org/10.1016/j.jnt.2008.12.006
[14] M. N. Huxley and M. Nair, *Power free values of polynomials. III*. Proc. London Math. Soc. **41**(1980), 66–82. http://dx.doi.org/10.1112/plms/s3-41.1.66
[15] S. Lang and A. Weil, *Number of points of varieties over finite fields*. Amer. J. Math. **76**(1954), 819–827. http://dx.doi.org/10.2307/2372655

[16] J. Maynard, *Primes represented by incomplete norm forms*. arxiv:1507.05080
[17] B. Poonen, *Squarefree values of multivariate polynomials*. Duke Math. J. **118**(2003), 353–373. http://dx.doi.org/10.1215/S0012-7094-03-11826-8
[18] T. Reuss, *Power-free values of polynomials*. Bull. London Math. Soc. **47**(2015), no. 2, 270–284. http://dx.doi.org/10.1112/blms/bdu116
[19] G. Ricci, *Riecenche aritmetiche sui polynomials*. Rend. Circ. Mat. Palermo **57**(1933), 433–475.
[20] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois J. Math. **6**(1962), 64–94.
[21] W. M. Schmidt, *The number of solutions of norm form equations*. Trans. Amer. Math. Soc. **317**(1990), 197–227. http://dx.doi.org/10.1090/S0002-9947-1990-0961596-2
[22] J. D. Vaaler, *Some extremal functions in Fourier analysis*. Bull. Amer. Math. Soc. **12**(1985), 183–216. http://dx.doi.org/10.1090/S0273-0979-1985-15349-2

Mathematical Institute, University of Oxford, Oxford, UK
e-mail: stanley.xiao@maths.ox.ac.uk