Journal of Number Theory 132 (2012) 1741–1757

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Counting rational points on smooth cyclic covers

D.R. Heath-Brown, Lillian B. Pierce *

Mathematical Institute, 24-29 St. Giles', Oxford, OX1 3LB, United Kingdom

ARTICLE INFO

Article history:
Received 8 September 2011
Accepted 21 February 2012
Available online 4 April 2012
Communicated by K. Soundararajan

MSC:
14G05
11D45
11L40

Keywords:
Rational points
Cyclic covers
Power sieve
Character sums

ABSTRACT

A conjecture of Serre concerns the number of rational points of bounded height on a finite cover of projective space $\mathbb{P}^{n-1}$. In this paper, we achieve Serre's conjecture in the special case of smooth cyclic covers of any degree when $n \geqslant 10$, and surpass it for covers of degree $r \geqslant 3$ when $n > 10$. This is achieved by a new bound for the number of perfect r-th power values of a polynomial with nonsingular leading form, obtained via a combination of an r-th power sieve and the q-analogue of van der Corput's method.

1. Introduction

Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_n]$ be an irreducible form of degree mr with $r \geqslant 2$, $m \geqslant 1$, such that the projective hypersurface defined by $F(\mathbf{x}) = 0$ is smooth. In this paper we will investigate the number of integer solutions to

$$y^r = F(x_1, \dots, x_n) \tag{1}$$

with $|x_i| \leqslant B$. Our interest stems from the fact that an upper bound for the number of such points provides an upper bound for the number of rational points on cyclic covers of $\mathbb{P}^{n-1}$.

* Corresponding author.
E-mail addresses: rhb@maths.ox.ac.uk (D.R. Heath-Brown), lillian.pierce@maths.ox.ac.uk (L.B. Pierce).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.02.010

The density of rational points on covers of projective space is the subject of a well-known conjecture of Serre. Precisely, given a finite cover $\phi : X \to \mathbb{P}^{n-1}$ over $\mathbb{Q}$, where $n \geqslant 2$, define the counting function

$$N_B(\phi) = \#\{P \in X(\mathbb{Q}):\ H(\phi(P)) \leqslant B\}.$$

Here H is the usual multiplicative height function on $\mathbb{P}^{n-1}$. Using a sieve method, Serre [13] proved that there exists $\gamma < 1$ such that

$$N_B(\phi) \ll B^{(n-1)+\frac{1}{2}} (\log B)^{\gamma}, \tag{2}$$

as long as the degree of ϕ is at least two. In fact, however, Serre conjectures that

$$N_B(\phi) \ll B^{n-1} (\log B)^{c}, \tag{3}$$

for some c, for covers of any degree $r \geqslant 2$ (see Theorems 3, 4 of Chapter 13 in [13]).

Several results are known in this direction. Broberg [1] has applied Heath-Brown's determinant method [7] to prove results for covers of $\mathbb{P}^1$ and $\mathbb{P}^2$. In the case of $\mathbb{P}^1$, Broberg proves that for $\phi : X \to \mathbb{P}^1$ of degree $r \geqslant 2$,

$$N_B(\phi) \ll_{\phi,\epsilon} B^{2/r+\epsilon}.$$

For $\phi : X \to \mathbb{P}^2$ of degree $r \geqslant 3$, Broberg proves that

$$N_B(\phi) \ll_{\phi,\epsilon} B^{2+\epsilon},$$

and if ϕ is of degree 2, then

$$N_B(\phi) \ll_{\phi,\epsilon} B^{9/4+\epsilon}.$$

These results nearly prove Serre's conjecture (3) for $n = 2, 3$.

Recently, Munshi [11] considered the case in which ϕ is a *smooth cyclic* cover of $\mathbb{P}^{n-1}$, given by an equation of the type (1) with F a nonsingular form. In this situation he proves that for all $n \geqslant 2$, one has

$$N_B(\phi) \ll_{\phi} B^{n-\frac{n}{n+1}} (\log B)^{\frac{n}{n+1}}. \tag{4}$$

Note that if $n \geqslant 2$, this improves on (2), and even approaches Serre's conjecture in the limit as $n \to \infty$.

Unpublished results of Salberger on the dimension growth conjecture [7, Conjecture 2] imply the truth of Serre's conjecture with $(\log B)^c$ replaced by B^{ϵ} for covers ϕ given by (1) with F a form of precisely degree r, for any $r \geqslant 2$. But note that while (3) is as good as one can hope for in complete generality, one might expect an estimate of the shape

$$N_B(\phi) \ll B^{n-m(r-1)} (\log B)^{c}$$

for covers of Munshi's type, under favorable circumstances. Thus Serre's conjecture probably does not reflect the whole truth in this area.

In this paper, we again start from the foundation of Munshi's approach: given a form F as above, Eq. (1) defines a variety X in weighted projective space $\mathbb{P}(m, 1, \dots, 1)$, where the first coordinate y has weight m and the coordinates $x_1, \dots, x_n$ have weight 1. The variety X can now be regarded as a cyclic r-sheeted cover of $\mathbb{P}^{n-1}$, given explicitly by the map $\phi : X \to \mathbb{P}^{n-1}$ that takes the point $(y, x_1, \dots, x_n)$ to $(x_1, \dots, x_n)$. Thus our attention turns to counting perfect r-th power values of the form $F(x_1, \dots, x_n)$ with $|x_i| \leqslant B$.

For convenience, we employ a smooth non-negative weight $w:\mathbb{R}^n \to \mathbb{R}$ such that $w \geqslant 1$ on the unit cube $[-1/2, 1/2]^n$, is supported in $[-1, 1]^n$, and satisfies the differential inequality

$$\left|\frac{\partial^\alpha}{\partial \mathbf{x}^\alpha} w(\mathbf{x})\right| \ll_\alpha 1,$$

for all multi-indices $\alpha = (\alpha_1, \dots, \alpha_n)$. Define the normalized weight function

$$w_B(\mathbf{x}) = w(\mathbf{x}/B), \tag{5}$$

so that w_B is supported in the box $\mathcal{B} = [-B, B]^n$ and satisfies the differential inequalities

$$\left|\frac{\partial^\alpha}{\partial \mathbf{x}^\alpha} w_B(\mathbf{x})\right| \ll_\alpha B^{-|\alpha|},$$

where $|\alpha| = \alpha_1 + \cdots + \alpha_n$. We then define the counting function

$$N_{w,B}(F) = \sum_{y \in \mathbb{Z}} \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ F(\mathbf{x}) = y^r}} w_B(\mathbf{x}), \tag{6}$$

with the aim of proving upper bounds of the form

$$N_{w,B}(F) \ll B^{n-\delta},$$

for some $\delta > 0$ independent of the degree of F.

The counting function $N_B(\phi)$ associated to the cyclic cover $\phi : X \to \mathbb{P}^{n-1}$, where X is defined by (1), satisfies the relation

$$N_B(\phi) \leqslant N_{w,2B}(F).$$

Munshi employed the square sieve, adapted to count perfect r-th powers, in order to count solutions to (1). This method ultimately requires one to estimate mixed character sums, for which bounds Munshi employed bounds of Deligne [3] and Katz [9,10]. We also use a version of the power sieve, but we sieve over certain almost-primes, instead of primes, and this allows us to apply the q-analogue of van der Corput's method; a similar combination has been used previously in [12,8].

With no extra effort we can handle equations of the form (1) in which F is a general polynomial f, not necessarily homogeneous, whose leading form is nonsingular. Ultimately, we prove the following theorem for the counting function $N_{w,B}(f)$ defined as in (6) for solutions to the equation

$$y^r = f(x_1, \dots, x_n). \tag{7}$$

Theorem 1. *Let $f(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_n]$ be a polynomial of degree $d \geqslant 3$, and assume that its leading form is nonsingular. Then for any $r \geqslant 2$, the counting function $N_{w,B}(f)$ for the number of solutions to* (7) *satisfies*

$$N_{w,B}(f) \ll \begin{cases} B^{n-3n/(2n+10)}(\log B)^2, & n \geqslant 8, \\ B^{n-n(n-2)/(6n+4)}(\log B)^2, & 2 \leqslant n \leqslant 8, \end{cases}$$

where the implied constant depends on f, d, n.

The reader should recall that if f is a polynomial of degree d then its leading form is defined to be the form composed of all those terms in f with degree exactly d.

This theorem fails to hold for $d=2$. That the method of proof fails to hold is visible from the inapplicability of Proposition 2, which requires $\deg f \geqslant 3$. But in fact the statement of the theorem is also false for $d=2$ and $n>10$, since it is well known that there are $\gg B^{n-1}$ values $\mathbf{x} \in [-B,B]^n$ for which $x_1^2+\cdots+x_n^2$ is a square. (This follows from Theorems 5, 6 and 8 of Heath-Brown [6], for example.)

As an immediate corollary, we have:

Theorem 2. *Let $\phi : X \to \mathbb{P}^{n-1}$ be a smooth finite cyclic cover given by Eq.* (1) *with F a nonsingular form of degree mr. Suppose either that ϕ has degree $r \geqslant 3$, or that $r=2$ and $m \geqslant 2$. Then*

$$N_B(\phi) \ll \begin{cases} B^{n-3n/(2n+10)}(\log B)^2, & n \geqslant 8, \\ B^{n-n(n-2)/(6n+4)}(\log B)^2, & 2 \leqslant n \leqslant 8. \end{cases}$$

In the case $r=2$, $m=1$, Theorem 1 no longer applies directly, but in this case the function F in (1) is a quadratic form, and it is well known that $N_{w,B}(F) \ll_F B^{n-1}\log B$. (See Theorems 5–8 of Heath-Brown [6], for example.) Assembling this with the relevant result of Theorem 2 for $r=2$, we therefore have the following result for all smooth finite covers of degree 2 given by (1):

Theorem 3. *Let $\phi : X \to \mathbb{P}^{n-1}$ be a smooth finite cover of degree 2, given by Eq.* (1) *with F nonsingular. Then*

$$N_B(\phi) \ll \begin{cases} B^{n-1}(\log B)^2, & n \geqslant 10, \\ B^{9-27/28}(\log B)^2, & n=9, \\ B^{n-n(n-2)/(6n+4)}(\log B)^2, & 2 \leqslant n \leqslant 8. \end{cases}$$

We therefore see that, for cyclic covers of any degree with F nonsingular, we can achieve Serre's conjecture (3) for $n \geqslant 10$, and indeed surpass it for $n>10$ and degree $r \geqslant 3$. Moreover we improve on Munshi's bound (4) for $n \geqslant 8$.

There is some prospect of a better result if one could treat the sum $T(\mathbf{h})$ in (24) without splitting into residue classes $k \pmod{q_1}$. If this were possible we would expect a gain of $q_1^{1/2}$ at this stage. What would be required is an estimate of the shape

$$\sum_{\mathbf{x} \pmod p} \chi_1\big(f(\mathbf{x})+g(\mathbf{x})\big)\chi_2\big(f(\mathbf{x})\big)e_p(\mathbf{c}\cdot\mathbf{x}) \ll p^{n/2}$$

in which $f(\mathbf{x})$ and $g(\mathbf{x})$ are polynomials in n variables, having smooth leading forms, and in which $\deg(f) > \deg(g) \geqslant 2$. Katz [10] proves related results, but his theorems appear not to cover the case required here.

2. The power sieve

We begin by formulating the sieve inequality we will use to count integer solutions to (7). The method has its origins in the "square sieve" of Heath-Brown [4]. Following the presentation of Munshi, we define a character that detects perfect r-th powers, in analogy to the Legendre symbol used to detect perfect squares. For any prime p, since $\mathbb{F}_p^*$ is a cyclic group, there is a non-canonical isomorphism

$$\theta_p : \mathbb{F}_p^* \to \mu_{p-1}$$

onto the set μ_{p-1} of $(p-1)$-th roots of unity in $\mathbb{C}^*$. For each $p \equiv 1 \pmod r$, fix such a θ_p. On the other hand, for such p, for every element $a \in \mathbb{F}_p^*$, the quantity $a^{\frac{p-1}{r}}$ is a well-defined r-th root of unity. Thus we can define a primitive Dirichlet character modulo p by setting

$$\chi_p(n) = \theta_p\big(\bar{n}^{\frac{p-1}{r}}\big)$$

for $(n,p)=1$ and $\chi_p(n)=0$ for $p \mid n$. Note that if n is such that $(n,p)=1$ and $n=m^r$ for some m, then

$$\chi_p(n) = \chi_p\big(\big(\bar{m}^r\big)^{\frac{p-1}{r}}\big) = 1,$$

so that χ_p detects r-th powers, as desired (with the possibility of over-counting). We will require characters to composite moduli, so for $q = p_1 \cdots p_k$ with primes $p_1, p_2, \ldots, p_k \equiv 1 \pmod r$, we define

$$\chi_q(n) = \chi_{p_1}(n)\chi_{p_2}(n)\cdots\chi_{p_k}(n).$$

Then it still remains true that for $(n,q)=1$ such that $n=m^r$ we have $\chi_q(n)=1$, although now we may be over-counting r-th powers even more significantly.

We now describe an r-th power sieve using the characters χ_q; we have specialized the statement of the following lemma to suit our particular needs, but a more flexible formulation may be found in [12] (stated there for the case $r=2$, but easily generalized to $r \geqslant 2$).

Lemma 1. *Let χ_q be the multiplicative character modulo q defined as above. Let $\mathcal{A} = \{uv\colon\ u \in \mathcal{U},\ v \in \mathcal{V}\}$ where $\mathcal{U}$ and $\mathcal{V}$ are disjoint sets of primes satisfying $p \equiv 1 \pmod r$. Let $A = \#\mathcal{A}$, $U = \#\mathcal{U}$, and $V = \#\mathcal{V}$, so that $A = UV$. Furthermore, assume that $V^3 \ll A$. Let ω be a non-negative weight such that $\omega(n)=0$ for $|n| \geqslant \exp(\min(U,V))$. Then*

$$\sum_{n\neq 0} \omega\big(n^r\big) \ll A^{-1}\sum_n \omega(n) + A^{-2}\sum_{v,v'\in\mathcal{V}}\ \sum_{u\neq u'\in\mathcal{U}}\left|\sum_n \omega(n)\chi_{uv}(n)\overline{\chi_{u'v'}(n)}\right|$$
$$+ UA^{-2}\sum_{v\neq v'\in\mathcal{V}}\left|\sum_n \omega(n)\chi_v(n)\overline{\chi_{v'}(n)}\right|. \tag{8}$$

We will refer to the terms on the right hand side of the r-th power sieve (8) respectively as the trivial leading term, the main sieve, and the prime sieve. To prove the lemma, consider

$$\Sigma = \sum_n \omega(n)\left|\sum_{q\in\mathcal{A}} \chi_q(n)\right|^2.$$

Each n is summed with non-negative weight, and in particular, if $n = m^r \neq 0$ and $\omega(n) \neq 0$, then

$$\sum_{q\in\mathcal{A}} \chi_q(n) = \sum_{q\in\mathcal{A}} \chi_q\big(m^r\big) = \sum_{\substack{q\in\mathcal{A}\\(q,m)=1}} 1 \geqslant A - \sum_{\substack{q\in\mathcal{A}\\(q,m)\neq 1}} 1 \gg A.$$

The last step follows since $\omega(n)$ is non-zero only if $|n| < \exp(\min(U,V))$, so that $p(m) \ll \min(U,V) = o(A)$, where $p(m)$ denotes the number of distinct prime divisors of m. Thus

$$\Sigma \gg A^2 \sum_{n\neq 0} \omega\big(n^r\big). \tag{9}$$

But also

$$\begin{aligned}\Sigma &= \sum_{q,q'\in\mathcal{A}}\sum_n \omega(n)\chi_q(n)\overline{\chi_{q'}(n)}\\ &= \sum_{q\in\mathcal{A}}\sum_n \omega(n)\chi_q(n)\overline{\chi_q(n)} + \sum_{\substack{q\neq q'\in\mathcal{A}\\ (q,q')=1}}\sum_n \omega(n)\chi_q(n)\overline{\chi_{q'}(n)}\\ &\quad + \sum_{\substack{q\neq q'\in\mathcal{A}\\ (q,q')\neq 1}}\sum_n \omega(n)\chi_q(n)\overline{\chi_{q'}(n)}. \end{aligned} \tag{10}$$

The first term in (10) is bounded above by $A\sum_n \omega(n)$. The second term in (10) will belong to the main term in the sieve. The last term in (10) may be broken into two subsums $S(\mathcal{U})+S(\mathcal{V})$, where

$$S(\mathcal{U}) = \sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_n \omega(n)\chi_{uv}(n)\overline{\chi_{u'v}(n)}$$

and

$$S(\mathcal{V}) = \sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_n \omega(n)\chi_{uv}(n)\overline{\chi_{uv'}(n)}.$$

The sum $S(\mathcal{U})$ is simply included in the main sieve term, but $S(\mathcal{V})$ requires a different approach. We split it into two further pieces, writing:

$$\begin{aligned} S(\mathcal{V}) &= \sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_{\substack{n\\ u\nmid n}} \omega(n)\chi_v(n)\overline{\chi_{v'}(n)}\\ &= U\sum_{v\neq v'\in\mathcal{V}}\sum_n \omega(n)\chi_v(n)\overline{\chi_{v'}(n)} - \sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_{\substack{n\\ u\mid n}} \omega(n)\chi_v(n)\overline{\chi_{v'}(n)}\\ &= M(\mathcal{V}) - E(\mathcal{V}), \end{aligned}$$

say. The term $M(\mathcal{V})$ now gives rise to the third term in (8), the prime sieve. The error term $E(\mathcal{V})$ can be bounded above in absolute value to give

$$\left|E(\mathcal{V})\right| \leqslant \sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_{\substack{n\neq 0\\ u\mid n}} \omega(n) \leqslant V^2\sum_{n\neq 0}\omega(n)p(n),$$

where as usual $p(n)$ denotes the number of distinct prime divisors of n. By assumption, if $\omega(n)\neq 0$ for some $n\neq 0$, then $p(n)\ll \min(U,V)$. Thus

$$\left|E(\mathcal{V})\right| \ll V^3\sum_n \omega(n),$$

which is dominated by the trivial leading term as long as $V^3 \ll A$. Thus, under this assumption, we have shown that

$$|\Sigma| \ll A \sum_n \omega(n) + \sum_{v,v' \in \mathcal{V}} \sum_{u \neq u' \in \mathcal{U}} \left| \sum_n \omega(n) \chi_{uv}(n) \overline{\chi_{u'v'}(n)} \right| + U \sum_{v \neq v' \in \mathcal{V}} \left| \sum_n \omega(n) \chi_v(n) \overline{\chi_{v'}(n)} \right|.$$

The result of the lemma then follows by comparison with (9).

We will apply the r-th power sieve using the sets

$$\mathcal{U} = \{\text{primes } u \equiv 1 \ (\mathrm{mod}\ r){:}\ Q^{\alpha} < u \leqslant 2Q^{\alpha}\}, \tag{11}$$

$$\mathcal{V} = \{\text{primes } v \equiv 1 \ (\mathrm{mod}\ r){:}\ Q^{1-\alpha} < v \leqslant 2Q^{1-\alpha}\}, \tag{12}$$

where $Q = B^{\delta}$ for some $\delta > 0$, and the exponent α is a real parameter satisfying $2/3 \leqslant \alpha < 1$; these parameters will be chosen later. Note in particular that under these conditions, $V^3 \leqslant A$, and we may assume that the sieving primes u and v do not divide r.

Recall the smooth weight function $w_B(\mathbf{x}) = w(\mathbf{x}/B)$ given in (5). We will define the sieve weight by

$$\omega(n) = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ f(\mathbf{x}) = n}} w_B(\mathbf{x}).$$

Then

$$N_{w,B}(f) \ll \omega(0) + \sum_{n \neq 0} \omega(n^r). \tag{13}$$

We need to handle separately the contribution to $N_{w,B}(f)$ arising from terms with $f(\mathbf{x}) = 0$. There are many estimates in the literature covering this situation. For example Heath-Brown [5, Theorem 2] gives a bound $O(B^{n-3+15/(n+5)})$, which is adequate for Theorem 1.

For the remainder of (13), the leading term in the sieve has upper bound

$$A^{-1} \sum_n \omega(n) \ll Q^{-1} (\log Q)^2 \sum_{\mathbf{x}} w_B(\mathbf{x}) \ll B^n Q^{-1} (\log Q)^2. \tag{14}$$

If we take $Q = B^{\delta}$, we therefore see that this contributes $O(B^{n-\delta}(\log B)^2)$ to $N_{w,B}(f)$.

Our principal task is to estimate the main sieve term, namely

$$\begin{aligned} \sum_n \omega(n) \chi_{uv}(n) \overline{\chi_{u'v'}(n)} &= \sum_{\mathbf{x} \in \mathbb{Z}^n} w_B(\mathbf{x}) \chi_{uv}\big(f(\mathbf{x})\big) \overline{\chi_{u'v'}\big(f(\mathbf{x})\big)} \\ &= \sum_{\mathbf{x} \in \mathbb{Z}^n} w_B(\mathbf{x}) \chi^*_{q_1}\big(f(\mathbf{x})\big) \chi^*_{q_2}\big(f(\mathbf{x})\big), \end{aligned} \tag{15}$$

where for convenience we have defined $q_1 = uu'$ to be the product of the "large" primes u, u', and $q_2 = vv'$ to be the product of the "small" primes. Moreover we have set

$$\chi^*_{q_1}(n) = \chi_u(n) \overline{\chi_{u'}(n)} \quad \text{and} \quad \chi^*_{q_2}(n) = \chi_v(n) \overline{\chi_{v'}(n)}. \tag{16}$$

In fact, for the prime sieve term we shall need to consider a similar sum with q_1 being prime. We therefore prove the following more general result for weighted character sums of the form (15).

Proposition 1. *Let q_1 and q_2 be coprime integers and suppose that q_1 is either prime or a product p_1p_2 of primes satisfying $p_1 < p_2 < 2p_1$. Write $p = q_1$ if q_1 is prime, or $p = p_1$ if $q_1 = p_1p_2$. Let χ_{q_1} and χ_{q_2} be multiplicative characters modulo q_1 and q_2 respectively, and suppose that χ_{q_1} is non-principal. Define*

$$T(q_1, q_2) = \sum_{\mathbf{x}\in\mathbb{Z}^n} w_B(\mathbf{x})\chi_{q_1}\big(f(\mathbf{x})\big)\chi_{q_2}\big(f(\mathbf{x})\big), \tag{17}$$

where $B \geqslant q_2$. Then

$$T(q_1, q_2) \ll_f B^{n/2}q_1^{1/2}q_2^{n/2} + B^{n/2}q_1^{(n+2)/4} + B^n p^{-(n-2)/4}. \tag{18}$$

We will apply this result to the main sieve with q_1, q_2 each being a product of two primes (not necessarily distinct in the case of q_2), and to the prime sieve with q_1, q_2 being distinct primes. Theorem 1 will then follow, as we will show in Section 4.

3. The *q*-analogue of van der Corput's method

We begin our proof of Proposition 1 by applying the q-analogue of van der Corput's method. The sum $T(q_1, q_2)$ involves a character to modulus q_1q_2, and the effect of our version of van der Corput's method is to produce a sum involving a character with a smaller modulus, namely q_1. To do this we take $H = [B/q_2]$ and let $\mathcal{H}$ denote the set of integer n-tuples in $[1, H]^n$, so that $\#\mathcal{H} = H^n$. Then

$$\begin{aligned} H^n T(q_1, q_2) &= \sum_{\mathbf{h}\in\mathcal{H}}\sum_{\mathbf{x}} w_B(\mathbf{x}+q_2\mathbf{h})\chi_{q_1}\big(f(\mathbf{x}+q_2\mathbf{h})\big)\chi_{q_2}\big(f(\mathbf{x}+q_2\mathbf{h})\big) \\ &= \sum_{\mathbf{x}\in[-B-Hq_2, B-q_2]^n} \chi_{q_2}\big(f(\mathbf{x})\big)\sum_{\mathbf{h}\in\mathcal{H}} w_B(\mathbf{x}+q_2\mathbf{h})\chi_{q_1}\big(f(\mathbf{x}+q_2\mathbf{h})\big). \end{aligned}$$

Applying Cauchy–Schwarz,

$$H^{2n}\big|T(q_1, q_2)\big|^2 \leqslant \Sigma_1\Sigma_2, \tag{19}$$

where

$$\begin{aligned} \Sigma_1 &= \sum_{\mathbf{x}\in[-B-Hq_2, B-q_2]^n} \big|\chi_{q_2}\big(f(\mathbf{x})\big)\big|^2, \\ \Sigma_2 &= \sum_{\substack{\mathbf{x} \\ (f(\mathbf{x}), q_2)=1}} \bigg|\sum_{\mathbf{h}\in\mathcal{H}} w_B(\mathbf{x}+q_2\mathbf{h})\chi_{q_1}\big(f(\mathbf{x}+q_2\mathbf{h})\big)\bigg|^2. \end{aligned}$$

It will be convenient to drop the condition that $(f(\mathbf{x}), q_2) = 1$ in Σ_2; by positivity this will still produce an upper bound. Then, expanding the resulting sums in Σ_2, we have

$$\Sigma_2 \leqslant \sum_{\mathbf{x}}\bigg|\sum_{\mathbf{h}\in\mathcal{H}} w_B(\mathbf{x}+q_2\mathbf{h})\chi_{q_1}\big(f(\mathbf{x}+q_2\mathbf{h})\big)\bigg|^2 = \sum_{\mathbf{h}_1\in\mathcal{H}}\sum_{\mathbf{h}_2\in\mathcal{H}} S(\mathbf{h}_1, \mathbf{h}_2)$$

where

$$S(\mathbf{h}_1, \mathbf{h}_2) = \sum_{\mathbf{x}} \chi_{q_1}\big(f(\mathbf{x}+q_2\mathbf{h}_1)\big)\overline{\chi_{q_1}\big(f(\mathbf{x}+q_2\mathbf{h}_2)\big)}w_B(\mathbf{x}+q_2\mathbf{h}_1)w_B(\mathbf{x}+q_2\mathbf{h}_2).$$

We then see that $S(\mathbf{h}_1,\mathbf{h}_2)=S(\mathbf{h}_1-\mathbf{h}_2,\mathbf{0})$, and hence that

$$\begin{aligned}\Sigma_2 &\leqslant \sum_{\mathbf{h}_1\in\mathcal{H}}\sum_{\mathbf{h}_2\in\mathcal{H}} S(\mathbf{h}_1-\mathbf{h}_2,\mathbf{0})\\ &= \sum_{\mathbf{h}\in\mathcal{H}_0}\prod_{j=1}^{n}\big(H-|h_j|\big)S(\mathbf{h},\mathbf{0})\\ &\leqslant H^n\sum_{\mathbf{h}\in\mathcal{H}_0}\left|\sum_{\mathbf{x}}\chi_{q_1}\big(f(\mathbf{x}+q_2\mathbf{h})\big)\overline{\chi_{q_1}\big(f(\mathbf{x})\big)}w_B(\mathbf{x}+q_2\mathbf{h})w_B(\mathbf{x})\right|,\end{aligned}$$

where $\mathcal{H}_0=[-H,H]^n$. We now further split Σ_2 into the single term with $\mathbf{h}=(0,\dots,0)$, which we will call Σ_{2A}, and the remainder of the sum over $\mathbf{h}\in\mathcal{H}_0$, $\mathbf{h}\neq 0$, which we will call Σ_{2B}.

Our goal is to give upper bounds for Σ_1 and Σ_2. The first admits a trivial bound: clearly,

$$\Sigma_1 \ll B^n. \tag{20}$$

Note that as we apply a trivial bound to this term, which is the only sum whose modulus is q_2, we do not need to assume that q_2 is square-free. (This is what enables us to treat $S(\mathcal{U})$ as part of the main sieve in Lemma 1, but not $S(\mathcal{V})$.)

Similarly, we bound Σ_{2A} trivially as

$$\Sigma_{2A} \leqslant H^n\sum_{\mathbf{x}\in\mathbb{Z}^n}\big(w_B(\mathbf{x})\big)^2 \ll H^nB^n. \tag{21}$$

Combining (20) and (21) in (19), we have now shown that

$$T(q_1,q_2)\ll H^{-n}\Sigma_1^{1/2}(\Sigma_{2A}+\Sigma_{2B})^{1/2}\ll H^{-n}B^{n/2}\big(H^nB^n+\Sigma_{2B}\big)^{1/2},$$

whence

$$T(q_1,q_2)\ll B^{n/2}q_2^{n/2}+B^{-n/2}q_2^n\Sigma_{2B}^{1/2}. \tag{22}$$

We now require a nontrivial upper bound for Σ_{2B}. We may write

$$\Sigma_{2B}\ll H^n\sum_{\substack{\mathbf{h}\in\mathcal{H}_0\\ \mathbf{h}\neq 0}}\big|T(\mathbf{h})\big|, \tag{23}$$

where

$$T(\mathbf{h})=\sum_{k \pmod{q_1}}\chi_{q_1}(k)\sum_{\substack{\mathbf{x}\in\mathbb{Z}^n\\ f(\mathbf{x}+q_2\mathbf{h})-kf(\mathbf{x})\equiv 0 \pmod{q_1}\\ (f(\mathbf{x}),q_1)=1}} w_{B,\mathbf{h}}(x). \tag{24}$$

Here we have set $w_{B,\mathbf{h}}(\mathbf{x})=w_B(\mathbf{x}+q_2\mathbf{h})w_B(\mathbf{x})$.

In order to bound $T(\mathbf{h})$, we shall consider a general sum of the form

$$S=\sum_{\substack{\mathbf{x}\in\mathbb{Z}^n\\ q\mid h(\mathbf{x}),\ (g(\mathbf{x}),q)=1}} W(\mathbf{x}/L)$$

in which q is either prime or a product p_1p_2 of primes satisfying $p_1 < p_2 < 2p_1$. We suppose that $h(\mathbf{x})$ and $g(\mathbf{x})$ are integral polynomials in $\mathbf{x} = (x_1, \ldots, x_n)$, with $\deg(h) \leqslant \deg(g) = d$, where $d \geqslant 3$. We shall take the weight function $W(\mathbf{x})$ to be smooth and supported on $[-1, 1]^n$, and we shall write Δ for the maximum of the moduli of all partial derivatives of W with order at most $n + 1$.

Under these assumptions we shall estimate S, using information on the behavior of $h(\mathbf{x})$ and $g(\mathbf{x})$ modulo the prime factors of q. Let $G(\mathbf{x})$ be the leading form for $g(\mathbf{x})$, so that $G(\mathbf{x})$ has degree d. We will require $G(\mathbf{x})$ to be nonsingular modulo every prime factor p of q. We shall assume further that either the leading form for $h(\mathbf{x})$ is a constant multiple of $G(\mathbf{x})$ or that the degree of $h(\mathbf{x})$ is strictly less than d. It follows that there is exactly one value γ modulo p for which $h(\mathbf{x}) - \gamma g(\mathbf{x})$ has degree less than d, when considered over $\mathbb{F}_p$. If $H(\mathbf{x}) \in \mathbb{F}_p[\mathbf{x}]$ is the leading form for $h(\mathbf{x}) - \gamma g(\mathbf{x})$ we shall require H to have degree at least 2, and we write $s(h, g; p)$ for the dimension of the singular locus of the variety $H(\mathbf{x}) = 0$ in $\mathbb{A}^n(\mathbb{F}_p)$.

In the situation above, the leading form of $ah(\mathbf{x}) + bg(\mathbf{x})$ will have a singular locus of dimension at most $s(h, g; p)$, for any $(a, b) \in \mathbb{F}_p^2 - \{(0, 0)\}$. In particular, if $s(h, g; p) = 0$ it follows from the fundamental theorem of Deligne [3] that

$$\sum_{\mathbf{x} \pmod p} e_p\big(ah(\mathbf{x}) + bg(\mathbf{x}) + \mathbf{v} \cdot \mathbf{x}\big) \ll_{n,d} p^{n/2}. \tag{25}$$

Using this bound we shall ultimately establish in Section 5 the following result.

Proposition 2. *Adopt the assumptions above, and let $p = q$ if q is prime, or $p = p_1$ if $q = p_1p_2$. Then if $L \geqslant 1$ and $n \geqslant 2$ we have*

$$S = q^{-2}\phi(q) \sum_{\mathbf{x} \in \mathbb{Z}^n} W(\mathbf{x}/L) + O_{n,d}\big(\Delta L^s q^{(n-s)/2}\big) + O_{n,d}\big(\Delta L^n p^{(s-n+2)/2} q^{-1}\big). \tag{26}$$

Here we have set $s = s(h, g; q)$ if q is prime, or

$$s = \min\big(s(h, g; p_1), s(h, g; p_2)\big)$$

if $q = p_1p_2$.

In our application Δ will be $O_{n,d}(1)$. However since our proof of Proposition 2 uses an induction in which the weight W varies, we have found it clearer to include Δ in the error estimates above.

We apply Proposition 2 to the innermost sum in (24) with $q = q_1$,

$$h(\mathbf{x}) = f(\mathbf{x} + q_2\mathbf{h}) - kf(\mathbf{x}), \qquad g(\mathbf{x}) = f(\mathbf{x}),$$

$W(\mathbf{x}) = w(\mathbf{x} + q_2\mathbf{h})w(\mathbf{x})$, and $L = B$. Note that $W(\mathbf{x})$ is then supported on a cube of side 2, and so $\Delta \ll_{n,d} 1$. Note also that the condition that the leading form $G(\mathbf{x})$ of $g(\mathbf{x})$ is nonsingular modulo every prime factor of q_1 is satisfied, provided that $B \gg 1$. Conveniently, since the main term in (26) is independent of k, its total contribution to (24) when summed over k is zero. In order to estimate Σ_{2B} via (23) we need to understand how

$$s = s(h, g; p) = s\big(f(\mathbf{x} + q_2\mathbf{h}) - kf(\mathbf{x}), f(\mathbf{x}); p\big)$$

varies as we change $\mathbf{h}$. The leading form of $f(\mathbf{x} + q_2\mathbf{h}) - kf(\mathbf{x}) - \gamma f(\mathbf{x})$, taken over $\mathbb{F}_p$, can only have degree less than d in the case $k + \gamma = 1$, in which case the terms of degree $d - 1$ are $q_2\mathbf{h} \cdot \nabla F(\mathbf{x})$, where $F(\mathbf{x})$ is the leading form of f. Thus we may interpret $s(h, g; p)$ as the dimension of the singular locus of the variety $\mathbf{h} \cdot \nabla F(\mathbf{x}) = 0$ in $\mathbb{A}^n(\mathbb{F}_p)$. Our next lemma provides the necessary information about this.

Lemma 2. *Suppose that $F(\mathbf{x}) \in \mathbb{F}_p[x_1, \dots, x_n]$ is a nonsingular form of degree d, and let H be a positive integer. Then if $0 \leqslant s \leqslant n$, the number of non-zero $\mathbf{h} \in [-H, H]^n$ for which the variety $\mathbf{h} \cdot \nabla F(\mathbf{x}) = 0$ has singular locus of affine dimension s is $O_{n,d}(H^{n-s} + H^n p^{-s})$.*

We will prove this in Section 6. It follows immediately from Lemma 2 that the number of non-zero $\mathbf{h} \in \mathcal{H}_0$ for which $s(h, g; q_1) = s$ will be $O_{n,d}(H^{n-s} + H^n q_1^{-s})$ if q_1 is a prime. On the other hand, if $q_1 = p_1 p_2$ with $p_1 < p_2 < 2p_1$ then the number of $\mathbf{h}$ with $\min(s(h, g; p_1), s(h, g; p_2)) = s$ will be $O_{n,d}(H^{n-s} + H^n p^{-s})$ where $p = p_1$ or p_2. Thus in either case we may write the bound as $O_{n,d}(H^{n-s} + H^n p^{-s})$, in the notation of Proposition 2. The error terms in (26) therefore contribute to (23) a total of

$$\ll_{n,d} q_1 H^n \sum_{0 \leqslant s \leqslant n} \left(H^{n-s} + H^n p^{-s}\right)\left(B^s q_1^{(n-s)/2} + B^n p^{(s-n+2)/2} q_1^{-1}\right).$$

Each summand takes the form XY^s as a function of s and is therefore maximal either at $s = 0$ or $s = n$. From $s = 0$ we get a contribution

$$\begin{aligned} &\ll_{n,d} q_1 H^n \left(H^n + H^n\right)\left(q_1^{n/2} + B^n p^{-(n-2)/2} q_1^{-1}\right) \\ &\ll_{n,d} H^{2n} q_1^{(n+2)/2} + H^{2n} B^n p^{-(n-2)/2}, \end{aligned}$$

while for $s = n$ we obtain

$$\begin{aligned} &\ll_{n,d} q_1 H^n \left(1 + H^n p^{-n}\right)\left(B^n + B^n p q_1^{-1}\right) \\ &\ll_{n,d} H^n B^n q_1 + H^{2n} B^n p^{-n} q_1. \end{aligned}$$

We therefore conclude that an overall bound for Σ_{2B} in (23) is

$$\Sigma_{2B} \ll_{n,d} H^{2n} q_1^{(n+2)/2} + H^{2n} B^n p^{-(n-2)/2} + H^n B^n q_1.$$

Proposition 1 now follows from (22) on recalling that $H = [B/q_2]$.

4. Bounding the sieve terms

We are now ready to apply Proposition 1 to bound the main sieve and the prime sieve in (13) and prove Theorem 1. The main sieve is bounded above by

$$A^{-2} \sum_{v, v' \in \mathcal{V}} \sum_{u \neq u' \in \mathcal{U}} \left| \sum_n \omega(n) \chi_{uv}(n) \overline{\chi_{u'v'}(n)} \right| \ll \sup_{v, v' \in \mathcal{V}} \sup_{u \neq u' \in \mathcal{U}} \left| T\left(uu', vv'\right)\right|,$$

where $T(uu', vv')$ is defined as in (17) with $q_1 = uu'$, $q_2 = vv'$, and the characters $\chi_{q_1}^*$, $\chi_{q_2}^*$ as defined in (16). According to the definitions (11) and (12) for the sieving sets U and V, Proposition 1 shows that the above is

$$\ll_f B^{n/2} Q^{\,n-(n-1)\alpha} + B^{n/2} Q^{\,(n+2)\alpha/2} + B^n Q^{\,-(n-2)\alpha/4}.$$

We choose $\alpha = 2/3$ so as to match the first two terms above, giving a bound

$$\ll_f B^{n/2} Q^{\,(n+2)/3} + B^n Q^{\,-(n-2)/6} \tag{27}$$

for the main sieve term. This is subject to the condition $q_2 \leqslant B$, for which it suffices to have $4Q^{2/3} \leqslant B$.

We now turn to the prime sieve, given in (8) as

$$UA^{-2} \sum_{v \neq v' \in \mathcal{V}} \left| \sum_n \omega(n) \chi_v(n) \overline{\chi_{v'}(n)} \right| \ll UV^2 A^{-2} \sup_{v \neq v' \in \mathcal{V}} \left| T\left(v, v'\right) \right|$$
$$\ll U^{-1} \sup_{v \neq v' \in \mathcal{V}} \left| T\left(v, v'\right) \right|,$$

where $T(v, v')$ is again defined as in (17) but with respect to characters χ_v, $\overline{\chi_{v'}}$ with prime moduli. Since v and v' are each of order $Q^{1-\alpha} = Q^{1/3}$ we get the immediate bound

$$\ll_{n,d} U^{-1} \left\{ B^{n/2} Q^{(n+1)/6} + B^{n/2} Q^{(n+2)/12} + B^n Q^{-(n-2)/12} \right\}$$
$$\ll_{n,d} Q^{-2/3} (\log Q) \left\{ B^{n/2} Q^{(n+1)/6} + B^n Q^{-(n-2)/12} \right\}.$$

On combining this bound with (14) and (27) and inserting the result into Lemma 1, we find that

$$\sum_{n \neq 0} \omega\left(n^r\right) \ll_f B^n Q^{-1} (\log Q)^2 + B^{n/2} Q^{(n+2)/3} + B^n Q^{-(n-2)/6}$$
$$+ Q^{-2/3} (\log Q) \left\{ B^{n/2} Q^{(n+1)/6} + B^n Q^{-(n-2)/12} \right\}$$
$$\ll_f (\log Q)^2 \left\{ B^n \left(Q^{-1} + Q^{-(n-2)/6} + Q^{-2/3-(n-2)/12} \right) + B^{n/2} Q^{(n+2)/3} \right\}.$$

The optimal choice of Q will be

$$Q = \begin{cases} B^{3n/(2n+10)}, & n \geqslant 8, \\ B^{3n/(3n+2)}, & 2 \leqslant n \leqslant 8, \end{cases}$$

yielding bounds

$$\ll_f B^{n-3n/(2n+10)} (\log B)^2$$

and

$$\ll_f B^{n-n(n-2)/(6n+4)} (\log B)^2,$$

respectively. Theorem 1 then follows.

5. Proof of Proposition 2

Our treatment of Proposition 2, which is essentially a version of Poisson summation, is motivated by the argument used by Heath-Brown [5, Theorem 3], and employs induction on s. We therefore begin by establishing the base case for the induction, in which $s = 0$. We split the values of $\mathbf{x}$ into residue classes modulo q and use the Poisson Summation Formula to obtain

$$S = \sum_{\substack{\mathbf{z} \ (\mathrm{mod}\ q) \\ q \mid h(\mathbf{z}),\, (g(\mathbf{z}), q) = 1}} \sum_{\mathbf{u} \in \mathbb{Z}^n} W\left(\frac{\mathbf{z} + q\mathbf{u}}{L} \right)$$
$$= \left(\frac{L}{q} \right)^n \sum_{\mathbf{v} \in \mathbb{Z}^n} \widehat{W}\left(\frac{L\mathbf{v}}{q} \right) S_q(\mathbf{v}), \tag{28}$$

where

$$S_q(\mathbf{v}) = \sum_{\substack{\mathbf{z} \ (\mathrm{mod}\ q) \\ q|h(\mathbf{z}),\ (g(\mathbf{z}),q)=1}} e_q(\mathbf{v}\cdot\mathbf{z}).$$

We may estimate

$$\widehat{W}(\mathbf{x}) = \int_{\mathbb{R}^n} W(\mathbf{y}) e(-\mathbf{x}\cdot\mathbf{y})\, d\mathbf{y}$$

by integrating by parts $n+1$ times with respect to y_j, say. This shows that $\widehat{W}(\mathbf{x}) \ll_n \Delta|x_j|^{-n-1}$, and since j is arbitrary we may conclude that

$$\widehat{W}(\mathbf{x}) \ll_n \Delta|\mathbf{x}|^{-n-1}, \quad \text{for } |x| \geqslant 1; \tag{29}$$

for $|x| \leqslant 1$, we will employ the trivial bound $\widehat{W}(\mathbf{x}) \ll_n \Delta$.

When $q = p_1 p_2$ the sum $S_q(\mathbf{v})$ satisfies a multiplicativity relation

$$S_q(\mathbf{v}) = S_{p_1}(\mathbf{v}) S_{p_2}(\mathbf{v}).$$

Moreover if p is prime then

$$\begin{aligned} S_p(\mathbf{v}) &= \sum_{p|h(\mathbf{z})} e_p(\mathbf{v}\cdot\mathbf{z}) - \sum_{p|h(\mathbf{z}),g(\mathbf{z})} e_p(\mathbf{v}\cdot\mathbf{z}) \\ &= p^{-1} \sum_{a \ (\mathrm{mod}\ p)} \sum_{\mathbf{z} \ (\mathrm{mod}\ p)} e_p\big(ah(\mathbf{z}) + \mathbf{v}\cdot\mathbf{z}\big) - p^{-2} \sum_{a,b \ (\mathrm{mod}\ p)} \sum_{\mathbf{z} \ (\mathrm{mod}\ p)} e_p\big(ah(\mathbf{z}) + bg(\mathbf{z}) + \mathbf{v}\cdot\mathbf{z}\big). \end{aligned}$$

Since we are assuming that $s = 0$, the Deligne estimate (25) applies when $a \neq 0$, for the first sum above, and for $(a,b) \neq (0,0)$ for the second. We therefore have

$$S_p(\mathbf{v}) = \big(p^{-1} - p^{-2}\big) \sum_{\mathbf{z} \ (\mathrm{mod}\ p)} e_p(\mathbf{v}\cdot\mathbf{z}) + O_{n,d}\big(p^{n/2}\big).$$

It follows that

$$S_p(\mathbf{0}) = \phi(p) p^{n-2} + O_{n,d}\big(p^{n/2}\big) \tag{30}$$

and that $S_p(\mathbf{v}) = O_{n,d}(p^{n/2})$ for $p \nmid \mathbf{v}$. Using the multiplicativity relation, we now see by (29) that terms in (28) with $\mathbf{v} \neq 0$, $\mathbf{v}$ coprime to q contribute

$$\begin{aligned} &\ll_{n,d} \left(\frac{L}{q}\right)^n q^{n/2} \sum_{\mathbf{v}\in\mathbb{Z}^n-\{\mathbf{0}\}} \left|\widehat{W}\left(\frac{L\mathbf{v}}{q}\right)\right| \\ &\ll_{n,d} L^n q^{-n/2} \sum_{\mathbf{v}\in\mathbb{Z}^n-\{\mathbf{0}\}} \Delta \min\left\{1, \left(\frac{q}{L|\mathbf{v}|}\right)^{n+1}\right\} \\ &\ll_{n,d} L^n q^{-n/2} \Delta \left(\frac{q}{L}\right)^n \\ &\ll_{n,d} \Delta q^{n/2}. \end{aligned}$$

If $q=p_1p_2$ then the terms with $p_1 \mid \mathbf{v}$ but $p_2 \nmid \mathbf{v}$ have $S_q(\mathbf{v}) \ll q^n$ and hence contribute

$$\begin{aligned}
&\ll_{n,d} \left(\frac{L}{q}\right)^n q^n \sum_{\substack{\mathbf{v}\in\mathbb{Z}^n-\{\mathbf{0}\}\\ p_1\mid\mathbf{v}}} \left|\widehat{W}\left(\frac{L\mathbf{v}}{q}\right)\right| \\
&\ll_{n,d} L^n \sum_{\mathbf{u}\in\mathbb{Z}^n-\{\mathbf{0}\}} \Delta \min\left\{1, \left(\frac{q}{Lp_1|\mathbf{u}|}\right)^{n+1}\right\} \\
&\ll_{n,d} L^n \Delta \left(\frac{q}{p_1 L}\right)^n \\
&\ll_{n,d} \Delta q^{n/2},
\end{aligned}$$

and similarly if $p_2 \mid \mathbf{v}$ but $p_1 \nmid \mathbf{v}$. We therefore deduce that

$$S = \left(\frac{L}{q}\right)^n S_q(\mathbf{0}) \sum_{\substack{\mathbf{v}\in\mathbb{Z}^n\\ q\mid\mathbf{v}}} \widehat{W}\left(\frac{L\mathbf{v}}{q}\right) + O_{n,d}\left(\Delta q^{n/2}\right).$$

However (30) yields $S_q(\mathbf{0}) = \phi(q^{n-1}) + O_{n,d}(q^{n/2})$ if q is prime and similarly $S_q(\mathbf{0}) = \phi(q^{n-1}) + O_{n,d}(q^{(3n-2)/4})$ if $q=p_1p_2$. Moreover

$$\sum_{\substack{\mathbf{v}\in\mathbb{Z}^n\\ q\mid\mathbf{v}}} \widehat{W}\left(\frac{L\mathbf{v}}{q}\right) = \sum_{\mathbf{u}\in\mathbb{Z}^n} \widehat{W}(L\mathbf{u}) = L^{-n} \sum_{\mathbf{u}\in\mathbb{Z}^n} W\left(L^{-1}\mathbf{u}\right) \ll \Delta.$$

The case $s=0$ of the proposition then follows.

When $n=2$ and $s=1$ or 2, the proposition is immediate. To see this we observe that the polynomial $h(\mathbf{x})$ cannot vanish identically modulo a prime divisor p of q, by our initial assumption that $h(\mathbf{x}) - \gamma g(\mathbf{x})$ has degree at least 2, but strictly less than d. We then estimate S via the following lemma.

Lemma 3. *Suppose that q is either prime or the product p_1p_2 of primes $p_1 < p_2 < 2p_1$. Suppose $k \leqslant n$ and that for $p=q$ (in the first case) or for $p=p_1$ and $p=p_2$ (in the second) we are given a variety $V_p \subseteq \mathbb{A}^n(\mathbb{F}_p)$ of dimension k and degree at most D. Then if τ_p is the natural map from $\mathbb{Z}$ to $\mathbb{F}_p$, we have*

$$\#\left\{\mathbf{x}\in\mathbb{Z}^n \cap [-R,R]^n\colon\ \tau_p(\mathbf{x}) \in V_p \text{ for } p \mid q\right\} \ll_{n,D} R^n q^{k-n} + R^k.$$

This is a special case of Lemma 4 of Browning and Heath-Brown's work [2], in which we take $W = \mathbb{A}^n(\mathbb{Q})$, $l=n$, and $k_i = k$ in their notation.

We apply the lemma with $n=2$ and $k=1$ to give $S \ll_{n,d} L^2q^{-1} + L$ in our situation. We also have

$$q^{-n}\phi\left(q^{n-1}\right) \sum_{\mathbf{x}\in\mathbb{Z}^n} W(\mathbf{x}/L) \ll L^2 q^{-1}.$$

We therefore see that these are dominated by the error terms in (26) if $n=2$ and $s=1$ or 2.

We turn now to the induction argument, for which we assume $n \geqslant 3$ and $s \geqslant 1$. The induction step will reduce both n and s by 1, giving us a case for which we already know that the proposition holds. The plan is to choose a suitable matrix $M \in \mathrm{SL}_n(\mathbb{Z})$, and to work with polynomials $h_{M,c}(\mathbf{y})$ and $g_{M,c}(\mathbf{y})$ in $n-1$ variables $\mathbf{y} = (y_1, \dots, y_{n-1})$ defined by setting

$$h_M(\mathbf{x}) = h(M\mathbf{x}) \quad \text{and} \quad h_{M,c}(\mathbf{y}) = h_M(\mathbf{y}, c),$$

and similarly for g. If we also set

$$W_M(\mathbf{x}) = W(M\mathbf{x}) \quad \text{and} \quad W_{M,c}(\mathbf{y}) = W_M(\mathbf{y}, c)$$

we then find that

$$S = \sum_{c \in \mathbb{Z}} \sum_{\substack{\mathbf{y} \in \mathbb{Z}^{n-1} \\ q \mid h_{M,c}(\mathbf{y}),\, (g_{M,c}(\mathbf{x}), q) = 1}} W_{M,c}(\mathbf{y}/L).$$

In order to apply the induction hypothesis we use the following lemma to provide a suitable matrix M.

Lemma 4. *Suppose that q and the polynomials h and g are as in the preamble to Proposition 2. Then there is a matrix $M \in \mathrm{SL}_n(\mathbb{Z})$ with entries bounded in modulus by $\|M\| \ll_{n,d} 1$, and having the following properties for every prime divisor p of q. Firstly, the leading form for $g_{M,c}$ will be nonsingular modulo p, and secondly, the leading form for $h_{M,c} - \gamma g_{M,c}$ will have degree at least 2 over $\mathbb{F}_p$, with singular locus of dimension at most* $\max(s(h, g; p) - 1, 0)$.

We will prove this in the next section, but we first show how we can then complete the induction step. We first note that $\|M^{-1}\| \ll_n \|M\|^{n-1} \ll_{n,d} 1$. Hence if $W_M(\mathbf{x}) \neq 0$ we have $M\mathbf{x} \ll_n 1$, and hence $\mathbf{x} \ll_{n,d} 1$. It follows that $W_{M,c}(\mathbf{y}/L)$ vanishes unless $c \ll_{n,d} L$ and that $W_{M,c}(\mathbf{t})$ has support $\mathbf{t} \in [-c_0, c_0]^{n-1}$ with $c_0 \ll_{n,d} 1$. We therefore write $W_0(\mathbf{t}) = W_{M,c}(c_0\mathbf{t})$ so that $W_0(\mathbf{t})$ is supported in $[-1, 1]^{n-1}$. We also observe that any j-th order partial derivative of W_0 is of size $O_{n,d}(\Delta)$. We may now apply Proposition 2 with s replaced by $s - 1$ to find that

$$\begin{aligned}
\sum_{\substack{\mathbf{y} \in \mathbb{Z}^{n-1} \\ q \mid h_{M,c}(\mathbf{y}),\, (g_{M,c}(\mathbf{x}), q) = 1}} W_{M,c}(\mathbf{y}/L) &= \sum_{\substack{\mathbf{y} \in \mathbb{Z}^{n-1} \\ q \mid h_{M,c}(\mathbf{y}),\, (g_{M,c}(\mathbf{x}), q) = 1}} W_0\big(c_0^{-1} L^{-1} \mathbf{y}\big) \\
&= q^{1-n} \phi\big(q^{n-2}\big) \sum_{\mathbf{y} \in \mathbb{Z}^{n-1}} W_0\big(c_0^{-1} L^{-1} \mathbf{y}\big) \\
&\quad + O_{n,d}\big(\Delta L^{s-1} q^{((n-1)-(s-1))/2}\big) \\
&\quad + O_{n,d}\big(\Delta L^{n-1} p^{((s-1)-(n-1)+2)/2} q^{-1}\big).
\end{aligned}$$

When we sum over all c such that $W_{M,c}(\mathbf{y}/L) \neq 0$, the error terms contribute

$$\begin{aligned}
&\ll_{n,d} L \Delta L^{s-1} q^{((n-1)-(s-1))/2} + L \Delta L^{n-1} p^{((s-1)-(n-1)+2)/2} q^{-1} \\
&\ll_{n,d} \Delta L^s q^{(n-s)/2} + \Delta L^n p^{(s-n+2)/2} q^{-1}.
\end{aligned}$$

Moreover we have

$$\begin{aligned}
\sum_{c \in \mathbb{Z}} \sum_{\mathbf{y} \in \mathbb{Z}^{n-1}} W_0\big(c_0^{-1} L^{-1} \mathbf{y}\big) &= \sum_{c \in \mathbb{Z}} \sum_{\mathbf{y} \in \mathbb{Z}^{n-1}} W_{M,c}(\mathbf{y}/L) \\
&= \sum_{\mathbf{x} \in \mathbb{Z}^n} W(\mathbf{x}/L).
\end{aligned}$$

It will then follow that

$$S = q^{1-n}\phi\bigl(q^{n-2}\bigr)\sum_{\mathbf{x}\in\mathbb{Z}^n} W(\mathbf{x}/L) + O_{n,d}\bigl(\Delta L^s q^{(n-s)/2}\bigr) + O_{n,d}\bigl(\Delta L^n p^{(s-n+2)/2} q^{-1}\bigr),$$

which suffices for our induction step.

6. Proof of Lemmas 2 and 4

Our proof of Lemma 2 is based on the following result of Heath-Brown [5, Lemma 2]:

Lemma 5. *Let $F(\mathbf{x}) \in \mathbb{F}_p[x_1, \ldots, x_n]$ be a smooth form of degree d. For each $\mathbf{h} \in \overline{\mathbb{F}_p}^n$, let $S_{\mathbf{h}}$ denote the affine variety*

$$S_{\mathbf{h}} = \bigl\{\mathbf{x}\colon\ \mathbf{h}\cdot\nabla^2 F(\mathbf{x}) = 0\bigr\},$$

and for every non-negative integer $s \leqslant n$, let

$$T_s = \bigl\{\mathbf{h}\colon\ \dim\bigl(S_{\mathbf{h}}(F)\bigr) \geqslant s\bigr\}.$$

Then T_s is an affine variety, and has dimension at most $n-s$. Moreover it may be defined by $O_{n,d}(1)$ equations, each of degree $O_{n,d}(1)$.

Clearly Lemma 2 follows from this estimate in conjunction with Lemma 3.

We turn now to the proof of Lemma 4. We recall that G is the leading form of g (and is assumed to be nonsingular modulo every prime divisor of q) and that H is the leading form of $h-\gamma g$. Thus the leading form of $g_{M,c}$ will be $G_{M,0}$, and similarly the leading form of $h_{M,c}-\gamma g_{M,c}$ will be $H_{M,0}$, providing that $G_{M,0}$ and $H_{M,0}$ do not vanish identically. We may view the variety in $\mathbb{A}^n(\mathbb{F}_p)$ defined by $G_{M,0}(\mathbf{y}) = 0$ as being the intersection of $G_M(\mathbf{x}) = 0$ with the hyperplane $x_n = 0$. This is isomorphic to the intersection of the variety

$$\mathcal{G}_p\colon\quad G(\mathbf{x}) = 0$$

with $(M^{-1}\mathbf{x})_n = 0$. Thus if $\mathbf{m}$ is the column vector whose transpose is the bottom row of M^{-1}, the variety in which we are interested will be

$$\mathcal{G}_p^{\mathbf{m}}\colon\quad G(\mathbf{x}) = \mathbf{m}\cdot\mathbf{x} = 0.$$

It will be convenient to use the notation $s(V)$ for the affine dimension of the singular locus of a variety V. Thus to confirm the first conclusion of Lemma 4, we are hoping to show that $s(\mathcal{G}_p^{\mathbf{m}}) = 0$, and hence $g_{M,c}$ is nonsingular modulo p, for a suitable matrix M.

We now recall Lemma 5 of Heath-Brown [5], which states that for any prime p and any form $R(\mathbf{x}) \in \mathbb{F}_p[x_1, \ldots, x_n]$ one has $s(\mathcal{R}_p^{\mathbf{m}}) \geqslant s(\mathcal{R}_p) - 1$ for all non-zero $\mathbf{m} \in \mathbb{F}_p^n$, where $\mathcal{R}_p$ and $\mathcal{R}_p^{\mathbf{m}}$ are defined analogously to the case for G above. Moreover there exists a non-zero form $\widehat{R}_p$ depending on p and R such that the degree of $\widehat{R}_p$ is bounded in terms of n and the degree of R alone, and such that

$$s\bigl(\mathcal{R}_p^{\mathbf{m}}\bigr) = \max\bigl(s(\mathcal{R}_p) - 1, 0\bigr)$$

whenever $p \nmid \widehat{R}_p(\mathbf{m})$.

Thus in our case, if $p \nmid \widehat{G}_p(\mathbf{m})$ then $\mathcal{G}_p^{\mathbf{m}}$ will be nonsingular, since $s(G) = 0$ and so $s(\mathcal{G}_p) \leqslant 1$. In exactly the same way we find that if $p \nmid \widehat{H}_p(\mathbf{m})$ then

$$s(\mathcal{H}_p^{\mathbf{m}}) = \max(s(\mathcal{H}_p) - 1, 0),$$

and in particular $H_{M,0}$ will not vanish identically.

We therefore wish to find a vector $\mathbf{m}$ such that $q \nmid \widehat{G}_q(\mathbf{m})\widehat{H}_q(\mathbf{m})$, if q is prime, or such that $p \nmid \widehat{G}_p(\mathbf{m})\widehat{H}_p(\mathbf{m})$ for $p = p_1$ and $p = p_2$ in the case $q = p_1 p_2$. However, according to Lemma 3, if one has a non-zero polynomial $f(\mathbf{x}) \in \mathbb{F}_p[x_1, \ldots, x_n]$ of degree D, then

$$\#\{\mathbf{x} \in (0, T]^n\colon\ f(\mathbf{x}) \equiv 0 \ (\mathrm{mod}\ p)\} \ll_{n,D} T^n p^{-1} + T^{n-1}.$$

In our case we deduce that, if $T \gg_{n,d} 1$ and $q, p_1, p_2 \gg_{n,d} 1$, then there will be a vector $\mathbf{m} \in (0, T]^n$, such that none of $q \mid \widehat{G}_q(\mathbf{m})\widehat{H}_q(\mathbf{m})$ or $p \mid \widehat{G}_p(\mathbf{m})\widehat{H}_p(\mathbf{m})$ holds. Clearly we may suppose that $\mathbf{m}$ is primitive, since we can divide out by any common factor without affecting the non-divisibility result. Proposition 2 is of course trivial if $q \ll_{n,d} 1$ and so we may therefore conclude that there is an admissible primitive $\mathbf{m} \ll_{n,d} 1$.

Finally, to finish the proof of Lemma 4 we observe that given such a vector $\mathbf{m}$ there is a matrix $M_1 \in \mathrm{SL}_n(\mathbb{Z})$ having the transpose of $\mathbf{m}$ as its last row, and such that $\|M_1\| \ll_{n,d}$. We then find that M defined by $M^{-1} = M_1$ is acceptable for Lemma 4. This completes the proof of Lemma 4.

Acknowledgments

Part of this work was carried out while Roger Heath-Brown was visiting the Mathematical Sciences Research Institute, Berkeley. The hospitality and financial support of the institute is gratefully acknowledged. Lillian Pierce was supported by a Marie Curie Fellowship funded by the European Commission for the duration of this work.

References

[1] N. Broberg, Rational points on finite covers of $\mathbb{P}^1$ and $\mathbb{P}^2$, J. Number Theory 101 (2009) 195–207.
[2] T.D. Browning, D.R. Heath-Brown, Rational points on quartic hypersurfaces, J. Reine Angew. Math. 629 (2009) 37–88.
[3] P. Deligne, La conjecture de Weil I, Inst. Hautes Études Sci. Publ. Math. 43 (1974) 273–307.
[4] D.R. Heath-Brown, The square sieve and consecutive square-free numbers, Math. Ann. 266 (1984) 251–259.
[5] D.R. Heath-Brown, The density of rational points on non-singular hypersurfaces, Proc. Indian Acad. Sci. Math. Sci. 104 (1994) 13–29.
[6] D.R. Heath-Brown, A new form of the circle method, and its application to quadratic forms, J. Reine Angew. Math. 481 (1996) 149–206.
[7] D.R. Heath-Brown, The density of points on curves and surfaces, Ann. of Math. 155 (2002) 553–595.
[8] D.R. Heath-Brown, Imaginary quadratic fields with class group exponent 5, Forum Math. 20 (2008) 275–283.
[9] N.M. Katz, Estimates for nonsingular multiplicative character sums, Int. Math. Res. Not. IMRN (2002) 333–349.
[10] N.M. Katz, Estimates for nonsingular mixed character sums, Int. Math. Res. Not. IMRN (2007).
[11] R. Munshi, Density of rational points on cyclic covers of $\mathbb{P}^n$, J. Théor. Nombres Bordeaux 21 (2009) 335–341.
[12] L.B. Pierce, A bound for the 3-part of class numbers of quadratic fields by means of the square sieve, Forum Math. 18 (2006) 677–698.
[13] J.-P. Serre, Lectures on the Mordell–Weil Theorem, Friedr. Vieweg and Sohn, Braunschweig, 1989.