

THE GEOMETRIC SIEVE FOR QUADRICS

T.D. BROWNING AND D.R. HEATH-BROWN

ABSTRACT. We develop a version of Ekedahl’s geometric sieve for integral quadratic forms of rank at least five. As one ranges over the zeros of such quadratic forms, we use the sieve to compute the density of coprime values of polynomials, and furthermore, to address a question about local solubility in families of varieties parameterised by the zeros.

CONTENTS

1. Introduction	1
2. The geometric sieve for affine space	6
3. The geometric sieve for quadrics: preliminaries	10
4. The geometric sieve for quadrics: lattices	13
5. Proof of Theorem 1.3	18
6. Proof of Corollary 1.4: coprime polynomials	21
7. Proof of Corollary 1.5: arithmetic purity	24
8. Proof of Corollary 1.6: local solubility	25
References	28

1. INTRODUCTION

The geometric sieve originates in pioneering work of Ekedahl [10]. It is usually taken to mean that for any codimension 2 subvariety $Z \subset \mathbb{A}_{\mathbb{Z}}^n$ that is defined over \mathbb{Z} , the asymptotic proportion of lattice points in a homogeneously expanding region in \mathbb{R}^n that reduce modulo p to an \mathbb{F}_p -point of Z , for some prime $p > M$, approaches zero as $M \rightarrow \infty$. Bhargava [1, Thm. 3.3] has established a precise quantitative version of Ekedahl’s result. This basic fact has yielded an impressive array of applications in arithmetic statistics.

The earliest application of the geometric sieve concerned relatively prime polynomials $f, g \in \mathbb{Z}[X_1, \dots, X_n]$. It was shown by Ekedahl [10] that the density of n -tuples of positive integers for which the values of f and g are

Date: September 14, 2020.

2010 Mathematics Subject Classification. 11D45 (11G35, 11G50, 11P55, 14G05, 14G25).

coprime is equal to $\prod_p (1 - c_p p^{-n})$, where

$$c_p = \#\{\mathbf{x} \in (\mathbb{Z}/p\mathbb{Z})^n : f(\mathbf{x}) \equiv g(\mathbf{x}) \equiv 0 \pmod{p}\}.$$

This result has since been generalised and extended to function fields of positive characteristic by Poonen [14, Thm. 3.1].

Next, when degree d hypersurfaces $X \subset \mathbb{P}^m$ with rational coefficients are ordered by height, a positive proportion are everywhere locally soluble, provided that $(d, m) \neq (2, 2)$. This application of the geometric sieve is due to Poonen and Voloch [16, Thm. 3.6], but has been extended to more general families of varieties $Y \rightarrow \mathbb{P}^n$ over arbitrary number fields by Bright, Browning and Loughran [5, Thm. 1.3].

The geometric sieve has also proved instrumental in questions about square-free values of polynomials. For example, using the geometric sieve, Bhargava, Shankar and Wang [2] have recently determined the precise density of monic integer polynomials of fixed degree that have square-free discriminant.

Very recently Cremona and Sadek [9] have used the geometric sieve to investigate the proportion of integral Weierstrass equations of elliptic curves (when ordered by height) which are, for example, globally minimal. They establish a form of the sieve which applies to boxes of unequal sides, somewhat in the spirit of Lemma 2.1 below, though less general.

The primary goal of this paper is to achieve a version of the geometric sieve which works for codimension 2 subvarieties of arbitrary smooth projective quadrics of rank at least 5.

Theorem 1.1. *Let $X \subset \mathbb{P}^m$ be a hypersurface defined over \mathbb{Q} by a quadratic form of rank at least 5. Let $Z \subset X$ be a codimension 2 subvariety defined over \mathbb{Q} , let \mathcal{Z} be its scheme-theoretic closure in $\mathbb{P}_{\mathbb{Z}}^m$, and let $Z_p = \mathcal{Z} \otimes_{\mathbb{Z}} \mathbb{F}_p$, for any prime p . Then for any $\varepsilon > 0$ there exists a constant $c_{\varepsilon, X, Z} > 0$ depending only on X, Z and ε , such that the number of $x \in X(\mathbb{Q})$ of height $H(x) \leq B$ which specialise to a point in $Z_p(\mathbb{F}_p)$, for some $p > M$, is at most*

$$c_{\varepsilon, X, Z} B^{\varepsilon} \left(\frac{B^{m-1}}{M \log M} + B^{m-1-1/m} \right).$$

The height function H in Theorem 1.1 is the naive exponential height on $\mathbb{P}^m(\mathbb{Q})$. For X as in the theorem, the Hardy–Littlewood circle method ensures that either $X(\mathbb{R}) = \emptyset$ or there is a constant $c_X > 0$ such that

$$\#\{x \in X(\mathbb{Q}) : H(x) \leq B\} \sim c_X B^{m-1},$$

as $B \rightarrow \infty$. This follows from work of Birch [3], for example. Theorem 1.1 therefore implies that it is rare for rational points on X to specialise to points on $Z_p(\mathbb{F}_p)$ for large primes p .

We shall prove Theorem 1.1 in the following more explicit form.

Theorem 1.2. *Let $Q(X_0, \dots, X_n)$ be a quadratic form defined over \mathbb{Z} with rank at least 5, and let $F_1(X_0, \dots, X_n), \dots, F_r(X_0, \dots, X_n)$ be forms defined over \mathbb{Z} . Assume that the variety $Z \subset \mathbb{P}^n$ given by*

$$Z : Q(X_0, \dots, X_n) = F_1(X_0, \dots, X_n) = \dots = F_r(X_0, \dots, X_n) = 0$$

has codimension at least 3 in \mathbb{P}^n . For $B, M \geq 1$ let $N(B, M)$ be the number of vectors $\mathbf{x} \in \mathbb{Z}^{n+1}$ such that

$$Q(x_0, \dots, x_n) = 0,$$

with $|\mathbf{x}| \leq B$, and for which $F_1(x_0, \dots, x_n), \dots, F_r(x_0, \dots, x_n)$ have a common prime divisor $p > M$. Then

$$N(B, M) \ll_{\varepsilon, Q, F_1, \dots, F_r} \frac{B^{n-1+\varepsilon}}{M \log M} + B^{n-1-1/n+\varepsilon},$$

for any fixed $\varepsilon > 0$.

Here we write $|\cdot|$ for the supremum norm $\|\cdot\|_\infty$ on \mathbb{R}^m for any $m \in \mathbb{N}$. These results could be false when the underlying quadratic form has rank less than 5. For example, if $n \geq 3$ and

$$Q(X_0, \dots, X_n) = X_0X_1 - X_2X_3,$$

or

$$Q(X_0, \dots, X_n) = X_0X_1 - X_3^2,$$

then we may take Z to be the linear space $X_1 = X_2 = X_3 = 0$. If M is in the range $B^{1/2} < M \leq B^{3/4}$, say, then we may consider points

$$(a, 0, bp, 0, x_4, \dots, x_n)$$

of height at most B , where p ranges over primes in the interval $M < p \leq B$, and $\gcd(a, bp) = 1$. There will be at least cB^{n-1} such points, for a suitable absolute constant $c > 0$. Moreover each of them lies on $Q = 0$, and each of them reduces to a point of Z modulo the relevant prime p .

A result similar in spirit to Theorem 1.1 has been proved simultaneously by Cao and Huang [7, Thm. 4.7], for affine quadrics defined by

$$Q(X_1, \dots, X_n) = m,$$

with m a non-zero integer. Their result is more delicate than ours, saving only a factor $\sqrt{\log B}$.

The case in which the quadric hypersurface has no non-singular rational point is uninteresting, but the examples above leave open the situation in which the quadratic form takes the shape

$$Q(X_0, \dots, X_n) = X_0X_1 - (X_2^2 - dX_4^2),$$

for some non-square $d \in \mathbb{Z}$. This is covered in the following theorem.

Theorem 1.3. *Let $Q(X_0, \dots, X_n)$ be a quadratic form defined over \mathbb{Z} , equivalent over \mathbb{Q} to a non-zero multiple of $X_0X_1 - (X_2^2 - dX_4^2)$ for some non-square $d \in \mathbb{Z}$. Let $F_1(X_0, \dots, X_n), \dots, F_r(X_0, \dots, X_n)$ be forms defined over \mathbb{Z} . Assume that the variety $Z \subset \mathbb{P}^n$ given by*

$$Z : Q(X_0, \dots, X_n) = F_1(X_0, \dots, X_n) = \dots = F_r(X_0, \dots, X_n) = 0$$

has codimension at least 3 in \mathbb{P}^n . Then

$$N(B, M) \ll_{\varepsilon, Q, F_1, \dots, F_r} \frac{B^{n-1+\varepsilon}}{M \log M} + B^{n-3/2+\varepsilon},$$

for any fixed $\varepsilon > 0$, where $N(B, M)$ is defined in Theorem 1.2 for $B, M \geq 1$.

Our proof of Theorem 1.3 will be a non-trivial variant of that for Theorem 1.2.

It is natural to ask what applications are available for our version of the geometric sieve for quadrics. We first demonstrate that the result of Ekedahl [10] and Poonen [14, Thm. 3.1] about coprime values of polynomials remains true when one restricts to the much thinner set of zeros of a given quadratic form. For any $\mathcal{S} \subset \mathbb{Z}^n$ and any non-singular quadratic form $Q \in \mathbb{Z}[X_1, \dots, X_n]$ we define

$$\mu_Q(\mathcal{S}) = \lim_{B \rightarrow \infty} \frac{\#\{\mathbf{x} \in \mathcal{S} \cap [-B, B]^n : Q(\mathbf{x}) = 0\}}{\#\{\mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n : Q(\mathbf{x}) = 0\}}, \quad (1.1)$$

if the limit exists. Given polynomials $f, g \in \mathbb{Z}[X_1, \dots, X_n]$, let

$$\mathcal{R}_{f,g} = \{\mathbf{x} \in \mathbb{Z}^n : \gcd(f(\mathbf{x}), g(\mathbf{x})) = 1\}.$$

We shall prove the following result in Section 6.

Corollary 1.4. *Assume that Q is indefinite and has rank at least 5. Let $f, g \in \mathbb{Z}[X_1, \dots, X_n]$ be homogenous, such that the variety $Q = f = g = 0$ has codimension 3 in \mathbb{P}^{n-1} . Then $\mu_Q(\mathcal{R}_{f,g})$ exists, and is equal to $\prod_p \mu_{Q,p}(\mathcal{R}_{f,g})$, where*

$$\mu_{Q,p}(\mathcal{R}_{f,g}) = \lim_{k \rightarrow \infty} \frac{\#\{\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n : Q(\mathbf{x}) \equiv 0 \pmod{p^k}, p \nmid \gcd(f(\mathbf{x}), g(\mathbf{x}))\}}{\#\{\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n : Q(\mathbf{x}) \equiv 0 \pmod{p^k}\}}.$$

Despite having Theorem 1.3 at our disposal, we prove the corollary only for the case of rank 5 or more, although it seems likely that it might be extended to cover the quadratic forms in Theorem 1.3.

A closely related consequence of the geometric sieve concerns “arithmetic purity” for projective quadrics. The implicit function theorem implies that weak approximation over \mathbb{Q} is birationally invariant among smooth varieties. Let V be a variety defined over \mathbb{Q} such that $V(\mathbb{Q}) \neq \emptyset$. Strong approximation off ∞ is said to hold for V if the diagonal image of the set $V(\mathbb{Q})$ of rational points is dense in the space of finite adeles $V(\mathbf{A}_{\mathbb{Q}}^f)$, equipped with the adelic

topology. Wittenberg [18, Question 2.11] has asked whether the property of strong approximation off ∞ is invariant among smooth varieties up to a closed subvariety of codimension at least 2. We say V satisfies “arithmetic purity” if strong approximation off ∞ holds for V and also for the open subset $V \setminus Z$, for any codimension 2 subvariety $Z \subset V$. This property has been observed to hold for $V = \mathbb{A}^m$ or $V = \mathbb{P}^m$, for example, by Cao and Xu [8, Prop. 3.6].

Smooth projective quadrics with a rational point are well-known to satisfy strong approximation. The following result establishes the arithmetic purity property for this class of varieties.

Corollary 1.5. *Let $m \geq 4$ and let $X \subset \mathbb{P}^m$ be a smooth quadric hypersurface defined over \mathbb{Q} such that $X(\mathbb{Q}) \neq \emptyset$. For any codimension two subvariety $Z \subset X$ the variety $X \setminus Z$ satisfies strong approximation off ∞ .*

The proof of this result is given in Section 7. In fact Corollary 1.5 follows rather easily by adapting the proof of Lemma 1.8 in work of Harpaz and Wittenberg [11]. (To be precise, one replaces \mathbb{A}^n by the quadric X and one replaces the line L passing through Q and Q' by a conic which arises from intersecting X with a plane passing through Q and Q' .) We have chosen to include Corollary 1.5 in order to illustrate the scope of the geometric sieve.

Our final application concerns local solubility for families of varieties. Recall that a scheme over a perfect field is said to be split if it contains a geometrically integral open subscheme. Suppose one has a family $Y \rightarrow X$ of varieties over \mathbb{Q} . A conjecture of Loughran [13, Conj. 1.7] states that under suitable hypotheses, when ordered by height, a positive proportion of the fibres have adelic points if and only if the morphism is split in codimension 1. This is established when $X = \mathbb{P}^m$ in [5, Thm. 1.3]. The following result confirms the conjecture when X is a quadric hypersurface of large enough rank.

Corollary 1.6. *Let $X \subset \mathbb{P}^m$ be a hypersurface defined over \mathbb{Q} by an indefinite quadratic form of rank at least 5. Let $\pi : Y \rightarrow X$ be a dominant quasi-projective \mathbb{Q} -morphism, with geometrically integral generic fibre. Assume that:*

- (1) *the fibre of π over each codimension-1 point of X is split;*
- (2) *$Y(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset$.*

Then the limit

$$\sigma(\pi) = \lim_{B \rightarrow \infty} \frac{\#\{x \in X(\mathbb{Q}) : H(x) \leq B, \pi^{-1}(x)(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset\}}{\#\{x \in X(\mathbb{Q}) : H(x) \leq B\}}$$

exists, and it is equal to a positive product of local densities.

This will be established in Section 8, where an explicit value for $\sigma(\pi)$ is also recorded.

Acknowledgements. The authors were inspired to work on this problem following discussions at the AIM workshop “Rational and integral points on higher-dimensional varieties” in May, 2014. They would particularly like to thank David Harari and Olivier Wittenberg for their patient explanations of the issues involved with the geometric sieve for quadrics. The authors are also grateful to Julian Lyczak and Olivier Wittenberg for further helpful remarks. A number of useful comments were also made by the anonymous referee, whose input is gratefully acknowledged. During the preparation of this article the first-named author was supported by EPSRC grant EP/P026710/1 and FWF grant P 32428-N35.

2. THE GEOMETRIC SIEVE FOR AFFINE SPACE

We shall reduce the proof of Theorem 1.1 to an application of the usual geometric sieve for affine space. However, it will be important to have a version of [1, Thm. 3.3] in which the dependence on the coefficients of all the polynomials is made explicit and, furthermore, the variables are allowed to run over a lopsided box.

Given $B_1, \dots, B_n \geq 1$, it will be convenient to set

$$V = \prod_{1 \leq i \leq n} B_i$$

and

$$B_{\min} = \min(B_1, \dots, B_n).$$

Let $H(f)$ denote the height of a polynomial f , which is defined as the maximum of the moduli of its coefficients. We shall adhere to this notation throughout this section, the main result of which is the following.

Lemma 2.1. *Let $B_1, \dots, B_n, H, M \geq 2$ and let $f_1, \dots, f_r \in \mathbb{Z}[X_1, \dots, X_n]$ be polynomials with no common factor in the ring $\mathbb{Z}[X_1, \dots, X_n]$, and having degrees at most d and heights at most H . Then*

$$\begin{aligned} \#\{\mathbf{x} \in \mathbb{Z}^n : |x_i| \leq B_i \text{ for } i \leq n, \exists p > M, p \mid f_j(\mathbf{x}) \text{ for } j \leq r\} \\ \ll \frac{V \log(VH)}{M \log M} + \frac{V \log(VH)}{B_{\min}}, \end{aligned}$$

where the implied constant is only allowed to depend on d and n (and is independent of r).

One recovers a version of [1, Thm. 3.3] by taking $B_1 = \dots = B_n$ and by absorbing H into the implied constant. The proof is a minor modification of the proof of [1, Thm. 3.3], but we shall give full details for the sake of completeness.

We begin the proof with an easy lemma.

Lemma 2.2. *Let $f \in \mathbb{Z}[X_1, \dots, X_n]$ be a non-zero polynomial of degree d , and let $B \geq 1$. Then*

$$\#\{\mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n : f(\mathbf{x}) = 0\} \leq nd(2B+1)^{n-1}.$$

Moreover, if p is a prime which does not divide f identically, then

$$\#\{\mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n : p \mid f(\mathbf{x})\} \leq nd(2B/p+1)(2B+1)^{n-1}$$

and

$$\#\{\mathbf{x} \in \mathbb{Z}^n \cap (0, p]^n : p \mid f(\mathbf{x})\} \leq ndp^{n-1}.$$

Proof. The first assertion may be proved by induction on n , there being at most d zeros when $n = 1$. For general n suppose that x_i is a variable that genuinely occurs in $f(\mathbf{x})$. With no loss of generality we may suppose that $i = n$ and that x_n^e occurs as $x_n^e f_0(x_1, \dots, x_{n-1})$ for some exponent $e \leq d$, with f_0 not vanishing identically. By our induction assumption there are at most

$$(n-1)d(2B+1)^{n-2}$$

vectors $(x_1, \dots, x_{n-1}) \in \mathbb{Z}^{n-1} \cap [-B, B]^{n-1}$ which are zeros of f_0 . For each of these, there are at most $2B+1$ choices for x_n . Next, there are at most $(2B+1)^{n-1}$ choices of (x_1, \dots, x_{n-1}) which are not zeros of f_0 , and for each of these there are at most d possible values for x_n . The total number of solutions is thus at most

$$(n-1)d(2B+1)^{n-1} + d(2B+1)^{n-1} = nd(2B+1)^{n-1}.$$

This completes the induction step.

For the second assertion we argue similarly, supposing that x_n^e occurs in f as $x_n^e f_0(x_1, \dots, x_{n-1})$ with f_0 not identically divisible by p . The argument then proceeds as before, except that now a non-trivial polynomial congruence in one variable x , of degree at most d , has at most $d(2B/p+1)$ solutions modulo p in the interval $[-B, B]$. The final claim is proved similarly, a one-variable congruence having at most d solutions. \square

We now start the proof of Lemma 2.1. When $r = 1$ the coprimality condition means that f_1 must be constant, equal to ± 1 . In this case there can never be a prime $p > M$ dividing f_1 . We may therefore assume from now on that r is at least 2, and our first move is to show that it suffices to take $r = 2$. Let us temporarily write $\mathcal{N}(f_1, \dots, f_r)$ for the counting function in Lemma 2.1. If f_1 factors into irreducibles as $g_1 \dots g_k$ over $\mathbb{Z}[X_1, \dots, X_n]$ one sees that $k \leq d$ and

$$\mathcal{N}(f_1, \dots, f_r) \leq \sum_{j=1}^k \mathcal{N}(g_j, f_2, \dots, f_r).$$

Each polynomial g_j will have degree at most d . Moreover, for any polynomials $u, v \in \mathbb{R}[X_1, \dots, X_n]$ with degree at most d one has

$$H(u)H(v) \ll_{n,d} H(uv),$$

by Prasolov [17, Section 4.2.4], for example. It follows that $H(g_j) \ll_{n,d} H$, and one then sees that it will suffice to prove the lemma in the case in which f_1 is irreducible. With this latter assumption the coprimality condition shows that not all of f_2, \dots, f_r can be divisible by f_1 . We suppose without loss of generality that $f_1 \nmid f_2$, and note that

$$\mathcal{N}(f_1, \dots, f_r) \leq \mathcal{N}(f_1, f_2),$$

with f_1 and f_2 coprime. Thus it suffices to prove the lemma in the case $r = 2$, as claimed.

We proceed to make a further simplification, reducing to the case in which $B_1 = \dots = B_n$. To achieve this, set $k = [B_{\min}]$. Then if $|x_i| \leq B_i$ we may write $x_i = y_i + kh_i$ with $0 \leq y_i < k$ and $|h_i| \leq 1 + B_i/k \ll B_i/B_{\min}$. We set $f_i(\mathbf{Y}; \mathbf{h}) = f_i(\mathbf{Y} + k\mathbf{h})$, and observe that these will be coprime as polynomials in \mathbf{Y} , for any fixed \mathbf{h} . Moreover they will have height at most $O_{d,n}(HV^d)$. Thus if we have proved Lemma 2.1 in the case $B_1 = \dots = B_n (= k)$, we may deduce that the number of acceptable vectors \mathbf{y} corresponding to a given choice of \mathbf{h} will be

$$\ll_{n,d} \frac{k^n \log(VH)}{M \log M} + \frac{k^n \log(VH)}{k}.$$

Since there are $O_{n,d}(VB_{\min}^{-n})$ choices for \mathbf{h} we then recover the required bound for general lopsided values of the B_i .

For the remainder of the proof we may now assume that $B_1 = \dots = B_n = B$, say, so that we need to prove that the number of suitable \mathbf{x} is

$$\ll_{n,d} \frac{B^n \log(BH)}{M \log M} + B^{n-1} \log(BH). \quad (2.1)$$

We have one further manoeuvre to perform before reaching the crux of the proof, and that is to show that we may assume that if $f_1 f_2$ has total degree $e (\leq 2d)$ then $f_1 f_2$ contains a non-zero term in X_1^e . (Hence both f_1 and f_2 will contain monomials in X_1 of the maximum possible degrees.) To show this, let $F(\mathbf{X})$ be the homogeneous part of $f_1(\mathbf{X})f_2(\mathbf{X})$ of degree e . According to Lemma 2.2, the form F has at most $ne(2K+1)^{n-1}$ zeros with $|\mathbf{x}| \leq K$. Taking $K = ne$ we deduce that there is a non-zero integer vector \mathbf{a} with $F(\mathbf{a}) \neq 0$, having size $|\mathbf{a}| \leq ne$. Without loss of generality we will suppose that $a_1 \neq 0$. We now define variables Y_i by setting $Y_1 = X_1$, and $Y_i = a_1 X_i - a_i X_1$ for $2 \leq i \leq n$. We then have $a_1 X_1 = a_1 Y_1$, and $a_1 X_i = a_i Y_1 + Y_i$ for $2 \leq i \leq n$. Then $a_1^d f_j(\mathbf{X})$ may be written as $g_j(\mathbf{Y})$ say, for $j = 1, 2$, with $H(g_j) \ll_{d,n} H$. Moreover the coefficient of Y_1^e in $g_1 g_2$ will be $a_1^{2d-e} F(\mathbf{a}) \neq 0$. We also see that

\mathbf{y} is an integer vector whenever \mathbf{x} is, and that $|\mathbf{y}| \ll_{n,d} B$ whenever $|\mathbf{x}| \leq B$. The linear transform connecting \mathbf{X} and \mathbf{Y} has determinant a_1^{n-1} , so that any constant factors of $g_1(\mathbf{Y})$ or $g_2(\mathbf{Y})$ must have prime factors dividing a_1 . These may safely be removed, since Lemma 2.1 is trivial when $M \ll_{n,d} 1$. We then see that it suffices to prove the lemma for the polynomials g_1 and g_2 .

We now proceed with the proof, under the assumption that

$$B_1 = \cdots = B_n = B,$$

and that $f_1 f_2$ has a non-zero term, cX_1^e say, where e is the total degree of $f_1 f_2$. We begin by considering the case in which there is a prime $p > M$ dividing both $f_1(\mathbf{x})$ and $f_2(\mathbf{x})$ and for which $p \mid c$. Since $c \ll_{n,d} H^2$, the number of such primes is $O_{n,d}(\log H / \log M)$. It is not possible for both $f_1(\mathbf{X})$ and $f_2(\mathbf{X})$ to vanish modulo p , since we have assumed that f_1 and f_2 have no constant factor. Assume without loss of generality that $f_1(\mathbf{X})$ does not vanish modulo p . We may therefore apply Lemma 2.2, which shows that the number of possible \mathbf{x} for which $p \mid f_1(\mathbf{x})$ will be

$$\ll_{n,d} (B/p + 1)B^{n-1} \ll B^n M^{-1} + B^{n-1}.$$

This is satisfactory for (2.1), since the number of available primes is

$$\ll_{n,d} \frac{\log H}{\log M}.$$

We next consider primes which do not divide c . Let $R(X_2, \dots, X_n)$ be the resultant $\text{Res}_{X_1}(f_1, f_2)$ of f_1 and f_2 with respect to X_1 . Since f_1 and f_2 are coprime over $\mathbb{Z}[X_1, \dots, X_n]$ this resultant cannot vanish identically. If f_1 and f_2 have degrees d_1 and d_2 with respect to X_1 this resultant is given by the determinant of a $(d_1 + d_2) \times (d_1 + d_2)$ matrix, whose entries are polynomials in X_2, \dots, X_n , of height $O_{n,d}(H)$ and degree at most d . Thus R has degree at most $2d^2$ and height $H(R) \ll_{n,d} H^{2d}$. Moreover, for any choice $(x_2, \dots, x_n) \in \mathbb{Z}^{n-1}$, the 1-variable polynomials $f_1(X_1, x_2, \dots, x_n)$ and $f_2(X_1, x_2, \dots, x_n)$ have a common factor modulo p if and only if $p \mid R(x_2, \dots, x_n)$. Note that for us to draw this conclusion we need to observe that the 1-variable polynomials $f_1(X_1, x_2, \dots, x_n)$ and $f_2(X_1, x_2, \dots, x_n)$ still have degrees d_1 and d_2 when considered modulo p , because $p \nmid c$. There are now two alternative situations to consider. Firstly, it could happen that $R(x_2, \dots, x_n) = 0$. According to Lemma 2.2 there are at most $O_{n,d}(B^{n-2})$ possible solutions $(x_2, \dots, x_n) \in \mathbb{Z}^{n-1}$ in the cube $[-B, B]^{n-1}$. For each of these there are at most $2B + 1$ possibilities for x_1 , making $O_{n,d}(B^{n-1})$ in total. This is acceptable for (2.1). In the alternative case we have $R(x_2, \dots, x_n) \neq 0$. If p divides both $f_1(x_1, x_2, \dots, x_n)$ and $f_2(x_1, x_2, \dots, x_n)$ then the 1-variable polynomials $f_1(X_1, x_2, \dots, x_n)$ and $f_2(X_1, x_2, \dots, x_n)$ have a common root modulo p , namely x_1 . We must therefore have $p \mid R(x_2, \dots, x_n)$. Since R has degree at most $2d^2$ and height

$O_{n,d}(H^{2d})$, we have

$$0 < |R(x_2, \dots, x_n)| \ll_{n,d} B^{2d^2} H^{2d}.$$

It follows that the number of primes $p > M$ which can divide $R(x_2, \dots, x_n)$ is $O_{n,d}((\log BH)/(\log M))$. Given x_2, \dots, x_n , and given a prime $p \mid R(x_2, \dots, x_n)$, there are at most $2B/p + 1 \leq 2B/M + 1$ integers $x_1 \in [-B, B]$ for which p divides $f_1(x_1, x_2, \dots, x_n)$, by Lemma 2.2. Here we note that the 1-variable polynomial $f_1(X_1, x_2, \dots, x_n)$ does not vanish modulo p , since $p \nmid c$. We now deduce that there are

$$\ll_{n,d} B^{n-1} \frac{\log(BH)}{\log M} \left(\frac{B}{M} + 1 \right)$$

vectors $(x_1, \dots, x_n) \in \mathbb{Z}^n \cap [-B, B]^n$ for which $R(x_2, \dots, x_n) \neq 0$ and such that $f_1(x_1, x_2, \dots, x_n)$ and $f_2(x_1, x_2, \dots, x_n)$ have a common factor $p > M$ which does not divide c . This bound is again acceptable, thereby completing our treatment of (2.1).

3. THE GEOMETRIC SIEVE FOR QUADRICS: PRELIMINARIES

We will deduce Theorem 1.2 from a result in which the quadric takes a specific shape.

Theorem 3.1. *Let $Q_0(X_2, \dots, X_n)$ be a quadratic form defined over \mathbb{Z} and let $F_1(X_0, \dots, X_n), \dots, F_r(X_0, \dots, X_n)$ be forms defined over \mathbb{Z} . Write*

$$Q(X_0, \dots, X_n) = X_0 X_1 - Q_0(X_2, \dots, X_n).$$

Assume that the rank of Q_0 is at least 3 and that the variety $Z \subset \mathbb{P}^n$ given by

$$Z : Q(X_0, \dots, X_n) = F_1(X_0, \dots, X_n) = \dots = F_r(X_0, \dots, X_n) = 0$$

has codimension at least 3 in \mathbb{P}^n . For $B, M \geq 1$ let $N(B, M)$ be the number of vectors $\mathbf{x} \in \mathbb{Z}^{n+1}$ such that

$$Q(x_0, \dots, x_n) = 0, \tag{3.1}$$

with $|\mathbf{x}| \leq B$, and for which $F_1(x_0, \dots, x_n), \dots, F_r(x_0, \dots, x_n)$ have a common prime divisor $p > M$. Then

$$N(B, M) \ll_{\varepsilon, Q, F_1, \dots, F_r} \frac{B^{n-1+\varepsilon}}{M \log M} + B^{n-1-1/n+\varepsilon},$$

for any fixed $\varepsilon > 0$.

Let us show how this result implies Theorem 1.2. We first note that if the quadric hypersurface has no non-singular rational points (i.e. if Q is not indefinite) the rational points will be restricted to a linear space of dimension $n - \text{rank}(Q)$. In this case there will only be $O_n(B^{n-4})$ rational points of height B or less. This is more than sufficient, and so we may assume that there is at

least one smooth rational point. In this case there is a linear transformation $\mathbf{T}_1 \in \mathrm{SL}_{n+1}(\mathbb{Q})$ such that

$$Q(\mathbf{T}_1^{-1}\mathbf{X}) = X_0X_1 - Q_1(X_2, \dots, X_n),$$

where Q_1 is a quadratic form with rational coefficients. Rescaling the variables X_2, \dots, X_n we obtain $\mathbf{T}_2 \in \mathrm{GL}_{n+1}(\mathbb{Q})$ such that $Q(\mathbf{T}_2^{-1}\mathbf{X}) = Q^*(\mathbf{X})$, where

$$Q^*(\mathbf{X}) = X_0X_1 - Q_0(X_2, \dots, X_n),$$

with $Q_0 \in \mathbb{Z}[X_2, \dots, X_n]$. We then have $Q^*(\mathbf{T}_2\mathbf{X}) = Q(\mathbf{X})$. We now choose N so that $N\mathbf{T}_2 = \mathbf{T}$ has integer entries, with the result that $\mathbf{T}\mathbf{x}$ is an integer zero of Q^* whenever \mathbf{x} is an integer zero of Q . We can choose \mathbf{T} to depend only on Q , so that $|\mathbf{T}\mathbf{x}| \ll_Q |\mathbf{x}|$. Finally, if the forms F_i have degrees at most d , and we set $G_i(\mathbf{X}) = \det(\mathbf{T})^d F_i(\mathbf{T}^{-1}\mathbf{X})$, then the forms G_i will have integer coefficients, and any common prime divisor of $F_1(\mathbf{x}), \dots, F_r(\mathbf{x})$ will also divide $G_1(\mathbf{T}\mathbf{x}), \dots, G_r(\mathbf{T}\mathbf{x})$. Since the variety $Q^* = G_1 = \dots = G_r = 0$ is produced from $Q = F_1 = \dots = F_r = 0$ by a non-singular linear transformation, it also has codimension at least 3 in \mathbb{P}^n . We therefore see that Theorem 3.1 applies to Q^* and G_1, \dots, G_r , and yields exactly the bound required for Theorem 1.2.

We now begin our treatment of Theorem 3.1. For the proof we shall allow all of our implied constants to depend on the polynomials Q, F_1, \dots, F_r , as well as on the small parameter $\varepsilon > 0$. We begin by disposing of points on the quadric (3.1) for which there is a prime $p > M$ dividing x_0 and x_1 as well as $F_1(x_0, \dots, x_n), \dots, F_r(x_0, \dots, x_n)$. In this case p^2 divides $Q_0(x_2, \dots, x_n)$, so that $Q_0(x_2, \dots, x_n) = p^2k$ for some integer $k \ll B^2p^{-2}$. The equation $Q_0(x_2, \dots, x_n) = h$ has $O(B^{n-3+\varepsilon})$ integer solutions in $[-B, B]^{n-1}$, uniformly in h . (This would be false for $h = 0$ if Q_0 had rank at most 2 and factored over \mathbb{Q} .) Moreover the equation $x_0x_1 = h$ has $O(B^\varepsilon)$ solutions when $h \neq 0$. The case $k \neq 0$ therefore produces a contribution

$$\ll \sum_{p>M} B^2p^{-2} \cdot B^{n-3+\varepsilon} \cdot B^\varepsilon \ll \frac{B^{n-1+2\varepsilon}}{M \log M}.$$

On the other hand, the equation $x_0x_1 = 0$ has $O(B)$ solutions of the correct size, so that the case $k = 0$ contributes $O(B^{n-3+\varepsilon} \cdot B)$ solutions. Hence, on re-defining ε we see that the number of points under consideration is

$$\ll \frac{B^{n-1+\varepsilon}}{M \log M} + B^{n-2+\varepsilon}.$$

This is satisfactory for the theorem.

We may now assume that the common prime factor of

$$F_1(x_0, \dots, x_n), \dots, F_r(x_0, \dots, x_n)$$

does not divide both x_0 and x_1 , and we proceed to estimate $N_i(B, M)$, defined for $i = 0, 1$ to be the number of vectors $\mathbf{x} \in \mathbb{Z}^{n+1}$ on the quadric (3.1) such that $|\mathbf{x}| \leq B$, and for which $F_1(x_0, \dots, x_n), \dots, F_r(x_0, \dots, x_n)$ have a common prime divisor $p > M$ which does not divide x_i . Clearly it will now suffice to estimate both $N_0(B, M)$ and $N_1(B, M)$. By symmetry, it will be enough to consider $N_1(B, M)$.

We may add suitable multiples of Q to any of the forms F_i , so as to suppose that F_i has no monomials divisible by X_0X_1 . This will not affect the hypotheses of Theorem 3.1. If all the F_i have degrees at most D we may then write

$$F_i(X_0, \dots, X_n) = G_i(X_1, \dots, X_n) + \sum_{j=1}^D X_0^j H_{i,j}(X_2, \dots, X_n),$$

say. Then if (x_0, \dots, x_n) lies on the quadric (3.1) we will have

$$x_1^D F_i(x_0, \dots, x_n) = K_i(x_1, \dots, x_n),$$

with

$$\begin{aligned} K_i(X_1, \dots, X_n) &= X_1^D G_i(X_1, \dots, X_n) \\ &\quad + \sum_{j=1}^D Q_0(X_2, \dots, X_n)^j X_1^{D-j} H_{i,j}(X_2, \dots, X_n). \end{aligned}$$

Thus if $p \mid F_i$ for all i , then $p \mid K_i$ for all i .

We now claim that the forms K_i can have no common factor of positive degree over $\overline{\mathbb{Q}}[X_1, \dots, X_n]$, except possibly a power of X_1 . Suppose for a contradiction that $R(X_1, \dots, X_n)$ is an irreducible form, different from X_1 , which divides all the forms K_i , so that $K_i = RS_i$, say. It is clear from our construction that we may write

$$K_i(X_1, \dots, X_n) = X_1^D F_i(X_0, \dots, X_n) + Q(X_0, \dots, X_n) T_i(X_0, \dots, X_n)$$

for suitable forms T_i , so that

$$RS_i = X_1^D F_i + QT_i.$$

We then see that any point on $Q = R = 0$ lies either on $Q = X_1 = 0$ or on $Q = F_1 = \dots = F_r = 0$. However every irreducible component of the intersection $Q = R = 0$ has codimension at most 2 in \mathbb{P}^n , while the variety $Q = F_1 = \dots = F_r = 0$ was assumed to have codimension at least 3. It follows that the intersection $Q = R = 0$ must be contained in the hyperplane $X_1 = 0$. This however is impossible. Indeed, since X_1 does not divide R there are points on $R = 0$ for which $x_1 \neq 0$, and since R does not involve X_0 we can choose x_0 so that $Q = 0$ as well. This gives a point of $Q = R = 0$ not lying on the hyperplane $X_1 = 0$. This contradiction proves our claim.

4. THE GEOMETRIC SIEVE FOR QUADRICS: LATTICES

We now wish to count points on $Q = 0$, such that the forms K_i have a common factor $p > M$ that does not divide x_1 . We have arranged that the K_i do not involve X_0 , and that they have no common factor of positive degree except possibly for powers of X_1 . We may remove any such factors, since they will not affect the divisibility by p . Indeed we may remove any constant factors, since Theorem 3.1 is trivial when $M \ll_{\varepsilon, Q, F_1, \dots, F_r} 1$, because the quadric (3.1) has $O(B^{n-1+\varepsilon})$ points.

Our plan is to apply the geometric sieve for \mathbb{A}^n to the K_i , but we need to account for the condition that $Q_0(x_2, \dots, x_n) = x_0 x_1$. We may eliminate any mention of the variable x_0 by weakening this last condition to say instead that $x_1 \mid Q_0(x_2, \dots, x_n)$. In effect we then need a geometric sieve for \mathbb{A}^n , with a divisibility side condition. We tackle this problem by fixing x_1 , and working with $(x_2, \dots, x_n) \in \mathbb{A}^{n-1}$, subject to a divisibility condition for a modulus x_1 , which is now fixed. The key idea is then to interpret this divisibility condition in terms of lattices.

It will be notationally convenient to work with a general quadratic form $R(X_1, \dots, X_m)$ of rank at least 3, in place of $Q_0(X_2, \dots, X_n)$. We shall say that a prime is “ R -good” if it is odd and the reduction of R modulo p has the same rank as R itself. Let q be a product of distinct R -good primes. We seek to cover all integer vector solutions of the congruence $R(x_1, \dots, x_m) \equiv 0 \pmod{q}$ by lattices of the shape

$$\Lambda(\mathbf{y}) := \{\mathbf{x} \in \mathbb{Z}^m : \exists \varrho \in \mathbb{Z}, \mathbf{x} \equiv \varrho \mathbf{y} \pmod{q}\}, \quad (4.1)$$

for suitable $\mathbf{y} \in \mathbb{Z}^m$ with $\gcd(\mathbf{y}, q) = 1$. We note that $\Lambda(\mathbf{y})$ has rank m and determinant q^{m-1} . We begin by asking how many such lattices will be required.

Lemma 4.1. *Suppose that $R \in \mathbb{Z}[X_1, \dots, X_m]$ is a quadratic form of rank at least 3, and let $q \in \mathbb{N}$ be a product of distinct R -good primes. Then*

$$\{\mathbf{x} \in \mathbb{Z}^m : R(\mathbf{x}) \equiv 0 \pmod{q}\} \subseteq \bigcup_{\mathbf{y} \in Y(q)} \Lambda(\mathbf{y}), \quad (4.2)$$

where $\Lambda(\mathbf{y})$ is given by (4.1) and

$$\#Y(q) \leq (3m)^{\omega(q)} q^{m-2}. \quad (4.3)$$

Moreover, each $\mathbf{y} \in Y(q)$ is an integer vector satisfying $Q(\mathbf{y}) \equiv 0 \pmod{q}$ and $\gcd(\mathbf{y}, q) = 1$.

Finally, for any $L > 0$, the number of these lattices for which the largest successive minimum is greater than L , is

$$\ll_m (3m)^{\omega(q)} q^{2m-3} L^{-m}. \quad (4.4)$$

Note that our successive minima are taken with respect to the Euclidean norm $\|\cdot\|_2$.

Proof. For the first part it is enough to consider the individual prime factors of q , and to combine the corresponding lattices using the Chinese Remainder Theorem. Assume that $q = p$ is an R -good prime. According to the final part of Lemma 2.2 the congruence $R(\mathbf{x}) \equiv 0 \pmod{p}$ has at most $2mp^{m-1}$ solutions. (This is a very poor bound, but sufficient for our purposes.) The solutions $\mathbf{x} \not\equiv \mathbf{0} \pmod{p}$ will then be covered by at most

$$2mp^{m-1}/(p-1) \leq 3mp^{m-2}$$

lattices $\Lambda(\mathbf{y})$ with $Q(\mathbf{y}) \equiv 0 \pmod{p}$ and $p \nmid \mathbf{y}$. Since $m \geq 3$ there is at least one such \mathbf{y} , and the corresponding lattice will cover the solution $\mathbf{0}$. It then follows that for general q we can cover all solutions using at most $(3m)^{\omega(q)}q^{m-2}$ lattices $\Lambda(\mathbf{y})$ with $R(\mathbf{y}) \equiv 0 \pmod{q}$ and $\gcd(\mathbf{y}, q) = 1$, as claimed in (4.2) and (4.3).

Associated to any rank m lattice $\Lambda \subset \mathbb{R}^m$ is the dual lattice

$$\Lambda^* = \{\mathbf{t} \in \mathbb{R}^m : \mathbf{t} \cdot \mathbf{x} \in \mathbb{Z}, \forall \mathbf{x} \in \Lambda\}.$$

If the successive minima of Λ are $\lambda_1 \leq \dots \leq \lambda_m$, and the successive minima of the dual lattice Λ^* are $\lambda_1^* \leq \dots \leq \lambda_m^*$, then it follows from Theorem VI on page 219 of Cassels [6] that

$$1 \leq \lambda_i \lambda_{m+1-i}^* \leq m!,$$

for $1 \leq i \leq m$. We shall apply this with $\Lambda = \Lambda(\mathbf{y})$. Assume that $\lambda_m > L$. Then it follows that $\lambda_1^* \leq m!L^{-1}$. Since $q\mathbb{Z}^m \subseteq \Lambda(\mathbf{y}) \subseteq \mathbb{Z}^m$, it follows that $\mathbb{Z}^m \subseteq \Lambda(\mathbf{y})^* \subseteq q^{-1}\mathbb{Z}^m$. Each element of $\Lambda(\mathbf{y})$ has the shape $\varrho\mathbf{y} + q\mathbf{k}$ for some $\mathbf{k} \in \mathbb{Z}^m$, so that $q^{-1}\mathbf{s}$ belongs to $\Lambda(\mathbf{y})^*$ if and only if \mathbf{s} is an integer vector for which $q^{-1}\varrho\mathbf{s} \cdot \mathbf{y} \in \mathbb{Z}$ for every $\varrho \in \mathbb{Z}$. But this is equivalent to \mathbf{s} being an integer vector for which $\mathbf{s} \cdot \mathbf{y} \equiv 0 \pmod{q}$. Thus $q\lambda_1^*$ will be the length of the shortest non-zero integer vector for which $\mathbf{s} \cdot \mathbf{y} \equiv 0 \pmod{q}$. It follows that if $\Lambda(\mathbf{y})$ has $\lambda_m > L$ then $\mathbf{s} \cdot \mathbf{y} \equiv 0 \pmod{q}$ for some non-zero integer vector \mathbf{s} with $|\mathbf{s}| \leq m!q/L$.

We now bound the number of lattices with $\lambda_m > L$. Here we should recall that the total number of lattices $\Lambda(\mathbf{y})$ under consideration is at most $(3m)^{\omega(q)}q^{m-2}$. For each choice of \mathbf{s} we count values of \mathbf{y} modulo q for which both $R(\mathbf{y}) \equiv 0 \pmod{q}$ and $\mathbf{s} \cdot \mathbf{y} \equiv 0 \pmod{q}$. This can be done by applying the Chinese Remainder Theorem to the case in which $q = p$ is a prime. The vector \mathbf{s} need not be primitive, and if $p \mid \mathbf{s}$ there will be at most $2mp^{m-1}$ values of \mathbf{y} , as above. On the other hand, when $p \nmid \mathbf{s}$ the conditions produce a non-trivial hyperplane slice of the quadric $R = 0$ over \mathbb{F}_p . Since the prime p is R -good the form R has rank at least 3 over \mathbb{F}_p . It follows that the hyperplane

cannot contain the quadric, whence Lemma 2.2 shows that there are at most $2(m-1)p^{m-2}$ solutions \mathbf{y} , corresponding to at most

$$\frac{2(m-1)p^{m-2}}{p-1} \leq 3mp^{m-3}$$

points in $\mathbb{P}^{m-1}(\mathbb{F}_p)$. It then follows from the Chinese Remainder Theorem that there are at most $(3m)^{\omega(q)}q^{m-3}\gcd(q, \mathbf{s})$ distinct lattices corresponding to \mathbf{s} . We may now sum over non-zero integer vectors \mathbf{s} with $|\mathbf{s}| \leq m!q/L$. When $\gcd(q, \mathbf{s}) = d$, say, there are no such \mathbf{s} unless $d \leq m!q/L$, in which case there will be at most $\ll_m q^m L^{-m} d^{-m}$ possible vectors \mathbf{s} . This gives a total contribution

$$\ll_m (3m)^{\omega(q)} q^{m-3} d \cdot q^m L^{-m} d^{-m},$$

for each divisor d of q . Since $m \geq 3$ we may then sum over $d \mid m$ to produce the bound (4.4) stated in the lemma. \square

We are now ready to put our plan into action. Recall that we are counting points $(x_1, \dots, x_n) \in \mathbb{Z}^n$ of size at most B , such that x_1 is non-zero and is a divisor of $Q_0(x_2, \dots, x_n)$, and for which $K_1(x_1, \dots, x_n), \dots, K_r(x_1, \dots, x_n)$ have a common prime factor $p > M$ which does not divide x_1 .

We take $q = q(x_1)$ to be the product of all Q_0 -good primes dividing x_1 , and we weaken the condition $x_1 \mid Q_0(x_2, \dots, x_n)$, requiring instead only that $q \mid Q_0(x_2, \dots, x_n)$. We apply Lemma 4.1 to the form $R = Q_0$, in $m = n - 1$ variables. The corresponding lattices $\Lambda(\mathbf{y})$ are therefore contained in \mathbb{Z}^{n-1} . The lemma then shows that

$$N_1(B, M) \leq \sum_{q \leq B} \sum_{\substack{a \neq 0 \\ q(a)=q}} \sum_{\mathbf{y} \in Y(q)} N(B, M, q, \mathbf{y}, a),$$

where $N(B, M, q, \mathbf{y}, a)$ is the number of $\mathbf{x} = (x_2, \dots, x_n) \in \Lambda(\mathbf{y})$ in the box $|\mathbf{x}| \leq B$ for which the polynomials $K_i(a, x_2, \dots, x_n)$ all have a common prime divisor $p > M$. Notice that we have written a in place of x_1 to emphasize the different role it plays in our argument.

We proceed to estimate how many values of a can correspond to a given q . Let Δ be the product of the (finitely many) primes which are not Q -good. Then q will divide a and every prime factor of $a/q = t$ will divide Δq . Since we will have $|t| \leq B$ we find using Rankin's trick that the number of available

t is at most

$$\begin{aligned}
2 \sum_{\substack{1 \leq t \leq B \\ t | (\Delta q)^\infty}} 1 &\leq 2 \sum_{t | (\Delta q)^\infty} \frac{B^\varepsilon}{t^\varepsilon} \\
&= 2B^\varepsilon \prod_{p | \Delta q} \frac{1}{1 - p^{-\varepsilon}} \\
&\ll B^\varepsilon \tau(\Delta q) \\
&\ll B^{2\varepsilon},
\end{aligned}$$

whenever $\varepsilon > 0$. Here we have used the fact that $q \leq B$ at the very last step. On re-defining ε , we therefore see that for every q there is a value $a^{(q)}$ which is divisible by q , such that

$$N_1(B, M) \ll B^\varepsilon \sum_{q \leq B} \sum_{\mathbf{y} \in Y(q)} N(B, M, q, \mathbf{y}, a^{(q)}). \quad (4.5)$$

Suppose now that we have a lattice $\Lambda = \Lambda(\mathbf{y})$ with $\mathbf{y} \in Y(q)$. As previously, suppose that $\lambda_1 \leq \dots \leq \lambda_m$ are the successive minima of Λ , which we recall has determinant q^{m-1} . (Here we continue to use the notation $m = n - 1$ for the dimension of $\Lambda(\mathbf{y})$.) It follows from Minkowski's second convex body theorem [6, Section VIII.2] that

$$q^{m-1} \leq \prod_{i=1}^m \lambda_i \ll_m q^{m-1}. \quad (4.6)$$

Moreover, it is clear that Λ has m independent vectors of length q , so that $\lambda_m \leq q$. According to the corollary to Theorem VII on page 222 of Cassels [6], the lattice Λ has a basis $\mathbf{e}_1, \dots, \mathbf{e}_m$ with $|\mathbf{e}_j| \leq \lambda_j$ for all j . We now define \mathbf{E} to be the $m \times m$ matrix formed by the column vectors $\mathbf{e}_1, \dots, \mathbf{e}_m$. Then the maximum modulus of the entries of \mathbf{E} is

$$||\mathbf{E}|| \ll \lambda_m \leq q \leq B.$$

Moreover, $|\det(\mathbf{E})| = \det(\Lambda) = q^{m-1}$. We then see that \mathbf{E}^{-1} is the transpose of the matrix formed from column vectors $\mathbf{e}_1^*, \dots, \mathbf{e}_m^*$, say, where

$$\begin{aligned}
|\mathbf{e}_j^*| &\ll |\det(\mathbf{E})|^{-1} \prod_{\substack{i=1 \\ i \neq j}}^m |\mathbf{e}_i| \\
&\ll |\det(\mathbf{E})|^{-1} \prod_{\substack{i=1 \\ i \neq j}}^m \lambda_i \\
&\ll \lambda_j^{-1},
\end{aligned}$$

by (4.6). Moreover, as described in [6, Section I.5], we have

$$\mathbf{e}_j^* \cdot \mathbf{e}_i = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Thus if $\mathbf{x} \in \Lambda$ is written as $\mathbf{x} = w_1 \mathbf{e}_1 + \cdots + w_m \mathbf{e}_m$, we will have $w_j = \mathbf{e}_j^* \cdot \mathbf{x}$, so that $w_j \ll |\mathbf{x}|/\lambda_j$ for each index j .

The next stage of the argument is to handle those $\mathbf{y} \in Y(q)$ for which one has $\lambda_m > L$. Since we automatically have $\lambda_m \leq q \leq B$, it follows from the above that the number of $\mathbf{x} = (x_2, \dots, x_n) \in \Lambda(\mathbf{y})$ in the box $|\mathbf{x}| \leq B$ will be

$$\ll \prod_{1 \leq j \leq m} (B/\lambda_j + 1) \ll B^m q^{1-m} = B^{n-1} q^{2-n}.$$

Thus we will trivially have $N(B, M, q, \mathbf{y}, a^{(q)}) \ll B^{n-1} q^{2-n}$. Combining this with the estimate (4.4) in Lemma 4.1 for the number of lattices with $\lambda_n > L$ we find that the contribution to $N_1(B, M)$ is

$$\ll B^\varepsilon \sum_{q \leq B} (3n)^{\omega(q)} q^{2n-5} L^{1-n} B^{n-1} q^{2-n} \ll B^{2n-3+2\varepsilon} L^{1-n}.$$

On re-defining ε , we therefore conclude that

$$N_1(B, M) \ll B^{2n-3+\varepsilon} L^{1-n} + B^\varepsilon \sum_{q \leq B} \sum_{\substack{\mathbf{y} \in Y(q) \\ \lambda_m \leq L}} N(B, M, q, \mathbf{y}, a^{(q)}). \quad (4.7)$$

Suppose now that $\Lambda = \Lambda(\mathbf{y})$ is a lattice with $\mathbf{y} \in Y(q)$, and for which $\lambda_m \leq L$. We define polynomials

$$f_i(W_1, \dots, W_m) = K_i(a^{(q)}, \mathbf{E}\mathbf{W}) \quad (1 \leq i \leq r),$$

where \mathbf{W} is the column vector (W_1, \dots, W_m) and \mathbf{E} is the matrix defined above, formed from the basis vectors for Λ . We are then left with estimating the number of integer vectors $\mathbf{w} \in \mathbb{Z}^m$, with $w_j \ll B/\lambda_j$ for $1 \leq j \leq m$, and for which all the $f_i(\mathbf{w})$ have a prime factor $p > M$ in common, for which $p \nmid a^{(q)}$. We already observed that the forms K_i can be taken to have no common factor, and we now claim that the polynomials f_i can have no common factors apart possibly for primes p that divide $a^{(q)}$. To see this, suppose firstly that $g(W_1, \dots, W_m)$ is a non-constant common factor of the f_i , with $f_i = gh_i$, say. We then set $W_i = U_i U_0^{-1}$ and multiply through by $U_0^{d_i}$, where d_i is the degree of f_i . This will produce relations

$$K_i(a^{(q)} U_0, \mathbf{E}\mathbf{U}) = G(U_0, \dots, U_m) H_i(U_0, \dots, U_m)$$

in which G and the H_i are homogeneous, and G is non-constant. After a non-singular linear change of variables one would then find a common factor of the forms $K_i(X_1, \dots, X_n)$, at least over $\mathbb{Q}[X_1, \dots, X_n]$. This contradiction shows

that the f_i cannot have a non-constant common factor. Suppose now that there is a prime common factor $p \nmid a^{(q)}$. It is then clear that p must divide the forms $K_i(W_0, \mathbf{E}\mathbf{W})$. However, since \mathbf{E} has determinant q^{m-1} , with $q \mid a^{(q)}$, it must be invertible modulo p . It would then follow that p divides each of the forms $K_i(X_1, \dots, X_n)$, which is impossible.

Since we are concerned with common prime factors $p > M$ which do not divide $a^{(q)}$ we may remove from the polynomials f_i any constant factors dividing $a^{(q)}$. The situation is then exactly right for an application of Lemma 2.1. We note that the polynomials f_i have height bounded by a power of B , so that the lemma yields

$$N(B, M, q, \mathbf{y}, a^{(q)}) \ll \frac{V \log B}{M \log M} + \frac{V \log B}{B_{\min}},$$

where

$$V = \prod_{i=1}^m (B/\lambda_i) \ll B^m q^{1-m}$$

by (4.6), and $B_{\min} = B/\lambda_m \geq B/L$. Here we have used the observation that $\lambda_i \leq q \leq B$ for each index i , so that $B/\lambda_i \gg 1$. Recalling that $m = n - 1$ it follows that

$$N(B, M, q, \mathbf{y}, a^{(q)}) \ll B^{n-2} q^{2-n} \left\{ \frac{B}{M \log M} + L \right\} \log B.$$

We proceed to insert this estimate into (4.7), using the bound (4.3) for $\#Y(q)$ given by Lemma 4.1. This produces

$$\begin{aligned} N(B, M) &\ll B^{2n-3+\varepsilon} L^{1-n} \\ &\quad + B^\varepsilon \sum_{q \leq B} (3n)^{\omega(q)} q^{n-3} \cdot B^{n-2} q^{2-n} \left\{ \frac{B}{M \log M} + L \right\} \log B \\ &\ll B^{2n-3+\varepsilon} L^{1-n} + B^{n-2+2\varepsilon} \left\{ \frac{B}{M \log M} + L \right\}. \end{aligned}$$

We therefore choose $L = B^{1-1/n}$, and Theorem 3.1 follows, on re-defining ε .

5. PROOF OF THEOREM 1.3

Our argument starts in the same way as for Theorem 1.2 in Section 3. As before we may assume that $Q(\mathbf{X}) = X_0 X_1 - Q_0(X_2, \dots, X_n)$ with

$$Q_0(X_2, \dots, X_n) = X_2^2 - dX_3^2,$$

for $d \in \mathbb{Z}$ a non-square. Similarly, points where there is a prime $p > M$ which divides x_0 and x_1 as well as $F_1(\mathbf{x}), \dots, F_r(\mathbf{x})$ contribute

$$\ll B^{n-1+\varepsilon} M^{-1} + B^{n-2+\varepsilon}.$$

We should note though that in order to assert that $Q_0(x_2, \dots, x_n) = 0$ has $O(B^{n-3+\varepsilon})$ integral solutions in $[-B, B]^{n-1}$ we need to use the fact that d is not a square. We then have to estimate $N_1(B, M)$, and we may take $F_i(\mathbf{X}) = K_i(X_1, \dots, X_n)$ to be independent of X_0 .

As before we change notation, replacing $Q_0(X_2, \dots, X_n)$ by $R(X_1, \dots, X_m)$ with $m = n - 1$, and $R(X_1, \dots, X_m) = X_1^2 - dX_2^2$. However, instead of using “ R -good” primes we will employ a different classification. We will say that a prime p is ramified if $p \mid 2d$, and otherwise is split if d is a square modulo p , and inert if d is a non-square modulo p . Suppose that q_1 is a product of distinct split primes, and q_2 a product of distinct inert primes. We define the lattices

$$\Lambda(\varrho; q_1, q_2) = \{\mathbf{x} \in \mathbb{Z}^m : x_1 \equiv \varrho x_2 \pmod{q_1}, x_1 \equiv x_2 \equiv 0 \pmod{q_2}\},$$

for integers ϱ in the set

$$Z(q_1) = \{\varrho \pmod{q_1} : \varrho^2 \equiv d \pmod{q_1}\}.$$

These lattices have $\det(\Lambda(\varrho; q_1, q_2)) = q_1 q_2^2$ for each $\varrho \in Z(q_1)$. Moreover it is clear that $\#Z(q_1) = 2^{\omega(q_1)}$. We then have the following result, which will replace Lemma 4.1.

Lemma 5.1. *Suppose that $R(X_1, \dots, X_m) = X_1^2 - dX_2^2$, where $d \in \mathbb{Z}$ is a non-square. Let q_1 be a product of distinct split primes, and q_2 a product of distinct inert primes. Then*

$$\{\mathbf{x} \in \mathbb{Z}^m : R(\mathbf{x}) \equiv 0 \pmod{q_1 q_2}\} \subseteq \bigcup_{\varrho \in Z(q_1)} \Lambda(\varrho; q_1, q_2).$$

Moreover, for each of the lattices $\Lambda(\varrho; q_1, q_2)$ the largest successive minimum is $O(q_1^{1/2} q_2)$, with an implied constant depending only on d .

Proof. For any split prime p , and any $x_1, x_2 \in \mathbb{Z}$ satisfying $x_1^2 \equiv dx_2^2 \pmod{p}$, there is an integer ϱ for which $\varrho^2 \equiv d \pmod{p}$ and $x_1 \equiv \varrho x_2 \pmod{p}$. Moreover, for any inert prime p we have $x_1 \equiv x_2 \equiv 0 \pmod{p}$ whenever $x_1^2 \equiv dx_2^2 \pmod{p}$. It follows via the Chinese Remainder Theorem that the lattices $\Lambda(\varrho; q_1, q_2)$ with $\varrho \in Z(q_1)$ cover all solutions of $R(\mathbf{x}) \equiv 0 \pmod{q_1 q_2}$. Finally, $\Lambda(\varrho; q_1, q_2)$ has a basis consisting of the $m - 2$ unit coordinate vectors $\mathbf{e}_3, \dots, \mathbf{e}_m$, together with two further vectors $(q_2 \mathbf{a}, 0, \dots, 0)$ and $(q_2 \mathbf{b}, 0, \dots, 0)$, where \mathbf{a} and \mathbf{b} are 2-dimensional vectors forming a basis for the lattice

$$\Lambda_0(\varrho) = \{\mathbf{x} \in \mathbb{Z}^2 : x_1 \equiv \varrho x_2 \pmod{q_1}\}.$$

This lattice has determinant q_1 , and successive minima satisfying $\lambda_1 \lambda_2 \ll q_1$. However, for any non-zero vector $\mathbf{x} \in \Lambda_0(\varrho)$ one has

$$x_1^2 - dx_2^2 \equiv \varrho^2 x_2^2 - \varrho^2 x_2^2 \equiv 0 \pmod{q_1}.$$

Moreover $x_1^2 - dx_2^2$ cannot vanish, since d is not a square. We therefore deduce that

$$q_1 \leq |x_1^2 - dx_2^2| \leq |d| \cdot \|\mathbf{x}\|_2^2.$$

Thus we must have $\lambda_1 \gg q_1^{1/2}$, and hence $\lambda_2 \ll q_1^{1/2}$. It follows that the vectors \mathbf{a} and \mathbf{b} above may be chosen both to have length $O(q_1^{1/2})$, so that the largest successive minimum of $\Lambda(\varrho; q_1, q_2)$ is $O(q_1^{1/2} q_2)$, as required. \square

Now, following the argument in Section 4 we take $q_1 = q_1(x_1)$ to be the product of split primes dividing x_1 , and similarly $q_2 = q_2(x_1)$ to be the product of inert primes dividing x_1 . We write $q = q_1 q_2$. As before, we weaken the condition $x_1 \mid Q_0(x_2, \dots, x_n)$, requiring only that $q \mid Q_0(x_2, \dots, x_n)$. In analogy to (4.5) there exists $a^{(q)}$ such that

$$N_1(B, M) \ll B^\varepsilon \sum_{q=q_1 q_2 \leq B} \sum_{\varrho \in Z(q_1)} N(B, M, q, \varrho, a^{(q)}), \quad (5.1)$$

where $N(B, M, q, \varrho, a)$ is the number of $\mathbf{x} = (x_2, \dots, x_n) \in \Lambda(\varrho; q_1, q_2)$ in the box $|\mathbf{x}| \leq B$ for which the polynomials $K_i(a, x_2, \dots, x_n)$ all have a common prime divisor $p > M$.

The argument then proceeds as before, but without the need to handle separately lattices where the largest successive minimum is big. If the successive minima of $\Lambda(\varrho; q_1, q_2)$ are $\lambda_1 \leq \dots \leq \lambda_m$ (with $m = n - 1$) we apply Lemma 2.1 to vectors \mathbf{w} with $w_i \ll B/\lambda_i$ to show that

$$N(B, M, q, \varrho, a^{(q)}) \ll \frac{V \log B}{M \log M} + \frac{V \log B}{B_{\min}},$$

with $V = \prod_{i=1}^m (B/\lambda_i)$. Since

$$\prod_{i=1}^m \lambda_i \geq \det(\Lambda(\varrho; q_1, q_2)) = q_1 q_2^2$$

we find that

$$N(B, M, q, \varrho, a^{(q)}) \ll \frac{B^m \log B}{q_1 q_2^2 M \log M} + \frac{B^{m-1} \lambda_m \log B}{q_1 q_2^2}.$$

According to Lemma 5.1 we have $\lambda_m \ll q_1^{1/2} q_2$. Since $\#Z(q_1) \ll B^\varepsilon$ we then deduce from (5.1) that

$$\begin{aligned} N_1(B, M) &\ll B^{2\varepsilon} \sum_{q_1 q_2 \leq B} \left\{ \frac{B^m \log B}{q_1 q_2^2 M \log M} + \frac{B^{m-1} \log B}{q_1^{1/2} q_2} \right\} \\ &\ll B^{3\varepsilon} \left\{ \frac{B^m}{M \log M} + B^{m-1/2} \right\}. \end{aligned}$$

On recalling that $m = n - 1$ we see that this is sufficient for Theorem 1.3, after re-defining ε .

6. PROOF OF COROLLARY 1.4: COPRIME POLYNOMIALS

The implied constants in this section are allowed to depend on Q, f and g . Assume that Q is an indefinite quadratic form of rank at least 5. For any square-free $q \in \mathbb{N}$ and any vector $\mathbf{a} \in (\mathbb{Z}/q\mathbb{Z})^n$, we shall require an asymptotic formula for

$$N(B; q, \mathbf{a}) = \#\{\mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n : Q(\mathbf{x}) = 0, \mathbf{x} \equiv \mathbf{a} \pmod{q}\}, \quad (6.1)$$

as $B \rightarrow \infty$, in which the error term depends explicitly on q . In fact there exist constants $\delta, \Delta > 0$ such that

$$N(B; q, \mathbf{a}) = c(q, \mathbf{a})B^{n-2} + O(q^\Delta B^{n-2-\delta}), \quad (6.2)$$

where the implied constant depends on Q but not on \mathbf{a} or q . Assuming that q is square-free and that $Q(\mathbf{a}) \equiv 0 \pmod{q}$, the leading constant is positive and takes the shape

$$c(q, \mathbf{a}) = \sigma_\infty \prod_{p \nmid q} \sigma_p \prod_{p|q} \sigma_p(\mathbf{a}).$$

Here σ_∞ is the density of real zeros of Q , which is independent of q and \mathbf{a} . Moreover

$$\sigma_p = \lim_{k \rightarrow \infty} p^{-k(n-1)} \nu(p^k) \quad \text{and} \quad \sigma_p(\mathbf{a}) = \lim_{k \rightarrow \infty} p^{-k(n-1)} \nu(p^k; p, \mathbf{a}),$$

with

$$\nu(p^k) = \#\{\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n : Q(\mathbf{x}) \equiv 0 \pmod{p^k}\}$$

and

$$\nu(p^k; p, \mathbf{a}) = \#\left\{\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n : \begin{array}{l} Q(\mathbf{x}) \equiv 0 \pmod{p^k} \\ \mathbf{x} \equiv \mathbf{a} \pmod{p} \end{array}\right\},$$

for every prime p . As part of the circle method analysis one shows that all the limits involved exist. We shall write $c = c(1, \mathbf{0})$ for brevity. The proof of (6.2) is a standard application of the Hardy–Littlewood circle method and will not be repeated here. (A more refined treatment of the analogous smoothly weighted counting function is found in [4, Thm. 4.1], in which any values $\Delta > n/2$ and $\delta < n/2 - 2$ are shown to be admissible.)

We remark that the analogous statement for quadratic forms of rank 4 is false in general, even for the forms $X_0X_1 - (X_2^2 - dX_3^2)$ with non-square d that are considered in Theorem 1.3. We refer the reader to Lindqvist [12] for further details on this phenomenon.

Let $M > \xi > 1$ and let $P_\xi = \prod_{p \leq \xi} p$. We shall tackle Corollary 1.4 by observing that

$$\#S_1 - \#S_2 - \#S_3 \leq \#\{\mathbf{x} \in \mathcal{R}_{f,g} \cap [-B, B]^n : Q(\mathbf{x}) = 0\} \leq \#S_1, \quad (6.3)$$

where

$$S_1 = \{\mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n : Q(\mathbf{x}) = 0, \gcd(f(\mathbf{x}), g(\mathbf{x}), P_\xi) = 1\},$$

S_2 is the set of $\mathbf{x} \in S_1$ for which $p \mid \gcd(f(\mathbf{x}), g(\mathbf{x}))$ for some $p \in (\xi, M]$, and finally S_3 is the set of $\mathbf{x} \in S_1$ for which $p \mid \gcd(f(\mathbf{x}), g(\mathbf{x}))$ for some $p > M$. Noting that $f = g = 0$ cuts out a codimension 2 subvariety in the hypersurface $Q = 0$, it follows from Theorem 1.2 that

$$\#S_3 \ll B^{n-2+\varepsilon} M^{-1} + B^{n-2-1/(n-1)+\varepsilon}, \quad (6.4)$$

for any $\varepsilon > 0$.

Turning to the size of S_1 we use inclusion–exclusion to deduce that

$$\begin{aligned} \#S_1 &= \sum_{q|P_\xi} \mu(q) \# \left\{ \mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n : \begin{array}{l} Q(\mathbf{x}) = 0 \\ f(\mathbf{x}) \equiv g(\mathbf{x}) \equiv 0 \pmod{q} \end{array} \right\} \\ &= \sum_{q|P_\xi} \mu(q) \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/q\mathbb{Z})^n \\ Q(\mathbf{a}) \equiv f(\mathbf{a}) \equiv g(\mathbf{a}) \equiv 0 \pmod{q}}} N(B; q, \mathbf{a}). \end{aligned}$$

Note that there are at most q^n vectors \mathbf{a} which contribute to the final sum. Invoking (6.2), and recalling that $c = c(1, \mathbf{0})$, it follows that

$$\#S_1 = cB^{n-2} \sum_{q|P_\xi} \mu(q) g(q) + O \left(B^{n-2-\delta} \sum_{q|P_\xi} q^{n+\Delta} \right), \quad (6.5)$$

with

$$g(q) = \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/q\mathbb{Z})^n \\ Q(\mathbf{a}) \equiv f(\mathbf{a}) \equiv g(\mathbf{a}) \equiv 0 \pmod{q}}} \prod_{p|q} \lim_{k \rightarrow \infty} \frac{\nu(p^k; p, \mathbf{a})}{\nu(p^k)}.$$

The error term here is found to be

$$\ll B^{n-2-\delta} \prod_{p \leq \xi} p^{n+\Delta} = B^{n-2-\delta} \exp \left((n + \Delta) \sum_{p \leq \xi} \log p \right) \leq B^{n-2-\delta} e^{2(n+\Delta)\xi},$$

if $\xi \gg 1$, by the prime number theorem.

For the main term in (6.5) we wish to extend the product to run over all primes. The function $g(q)$ is multiplicative and for any prime p we have

$$g(p) = \lim_{k \rightarrow \infty} \frac{\nu_0(p^k)}{\nu(p^k)},$$

where

$$\nu_0(p^k) = \# \left\{ \mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n : \begin{array}{l} Q(\mathbf{x}) \equiv 0 \pmod{p^k} \\ f(\mathbf{x}) \equiv g(\mathbf{x}) \equiv 0 \pmod{p} \end{array} \right\}.$$

It is clear that $g(p) \leq 1$ for every prime, but we will need a better bound for large p . Suppose that Q has rank $r \geq 5$. If p is odd, we may diagonalize Q modulo p^k as $\text{Diag}(d_1, \dots, d_r, 0, \dots, 0)$ with respect to a suitable basis, and if p is large enough we will have $p \nmid d_i$ for $1 \leq i \leq r$. Using this new basis we see that $\nu(p^k; p, \mathbf{a})$ counts $\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n$ with $\mathbf{x} \equiv \mathbf{a} \pmod{p}$ and

$$\sum_{i=1}^r d_i x_i^2 \equiv 0 \pmod{p^k}. \quad (6.6)$$

If we write $\mathbf{b} = (a_1, \dots, a_r)$ it follows that $\nu(p^k; p, \mathbf{a}) = p^{(k-1)(n-r)} \xi(p^k; p, \mathbf{b})$, where $\xi(p^k; p, \mathbf{b})$ counts $\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^r$ with $\mathbf{x} \equiv \mathbf{b} \pmod{p}$, such that (6.6) holds. When $\mathbf{b} \not\equiv \mathbf{0} \pmod{p}$ we find that $\xi(p^k; p, \mathbf{b}) = p^{(k-1)(r-1)}$, by Hensel's Lemma, so that $\nu(p^k; p, \mathbf{a}) = p^{(k-1)(n-1)}$. For large p the number of $\mathbf{a} \pmod{p}$ for which $Q(\mathbf{a}) \equiv f(\mathbf{a}) \equiv g(\mathbf{a}) \equiv 0 \pmod{p}$ will be $O(p^{n-3})$, so that vectors \mathbf{a} for which $\mathbf{b} \not\equiv \mathbf{0} \pmod{p}$ contribute $O(p^{k(n-1)-2})$ to $\nu_0(p^k)$. On the other hand, a standard calculation gives $\xi(p^k; p, \mathbf{0}) \ll p^{r+(k-2)(r-1)}$, so that $\nu(p^k; p, \mathbf{a}) \ll p^{(k-1)(n-1)+1}$ for those \mathbf{a} for which $\mathbf{b} \equiv \mathbf{0} \pmod{p}$. The number of such \mathbf{a} is $p^{n-r} \leq p^{n-5}$, whence this case contributes $O(p^{k(n-1)-3})$ to $\nu_0(p^k)$. However a standard analysis shows that $\nu(p^k) \gg p^{k(n-1)}$, so that

$$g(p) \ll \lim_{k \rightarrow \infty} \frac{p^{k(n-1)-2} + p^{k(n-1)-3}}{p^{k(n-1)}} \ll p^{-2}.$$

Since $g(q)$ is multiplicative we then have $g(q) = O(q^{-3/2})$ for any square-free $q \in \mathbb{N}$. Hence it follows that

$$\sum_{q|P_\xi} \mu(q)g(q) - \sum_{q=1}^{\infty} \mu(q)g(q) \ll \sum_{q>\xi} \frac{1}{q^{3/2}} \ll \xi^{-1/2}.$$

Our work so far has therefore shown that

$$\#S_1 = cB^{n-2} \prod_p \mu_{Q,p}(\mathcal{R}_{f,g}) + O(\xi^{-1/2} B^{n-2}) + O(e^{2(n+\Delta)\xi} B^{n-2-\delta}), \quad (6.7)$$

where $\mu_{Q,p}(\mathcal{R}_{f,g})$ is as in the statement of Corollary 1.4.

To handle S_2 , we note that

$$\#S_2 \leq \sum_{p \in (\xi, M]} \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/p\mathbb{Z})^n \\ Q(\mathbf{a}) \equiv f(\mathbf{a}) \equiv g(\mathbf{a}) \equiv 0 \pmod{p}}} N(B; p, \mathbf{a}).$$

But (6.2) allows us to conclude that

$$\sum_{\substack{\mathbf{a} \in (\mathbb{Z}/p\mathbb{Z})^n \\ Q(\mathbf{a}) \equiv f(\mathbf{a}) \equiv g(\mathbf{a}) \equiv 0 \pmod{p}}} N(B; p, \mathbf{a}) \ll \frac{B^{n-2}}{p^2} + p^{n+\Delta} B^{n-2-\delta}, \quad (6.8)$$

since $g(p) = O(p^{-2})$. Summing over $p \in (\xi, M]$ it follows that

$$\#S_2 \ll \frac{B^{n-2}}{\xi \log \xi} + M^{n+1+\Delta} B^{n-2-\delta}. \quad (6.9)$$

We now return to (6.3), taking $\xi = \sqrt{\log B}$ and $M = B^{\delta/(2(n+1+\Delta))}$. Making the choice $\varepsilon = \delta/(4(n+1+\Delta))$ in (6.4), and combining it with (6.7) and (6.9), it follows that

$$\#\{\mathbf{x} \in \mathcal{R}_{f,g} \cap [-B, B]^n : Q(\mathbf{x}) = 0\} = cB^{n-2} \prod_p \mu_{Q,p}(\mathcal{R}_{f,g}) + O\left(\frac{B^{n-2}}{(\log B)^{1/4}}\right).$$

Finally, we divide both sides by $N(B; 1, \mathbf{0})$ and reapply (6.2), before taking a limit $B \rightarrow \infty$ in order to complete the proof of Corollary 1.4.

7. PROOF OF COROLLARY 1.5: ARITHMETIC PURITY

Let $m \geq 4$ and let $X \subset \mathbb{P}^m$ be a smooth hypersurface defined by a non-singular indefinite quadratic form $Q \in \mathbb{Z}[X_0, \dots, X_m]$. Let $Z \subset X$ be a codimension 2 subvariety and put $U = X \setminus Z$. To establish strong approximation off ∞ on U we must show that for any point $(P_p)_p$ in the set of finite adelic points $U(\mathbf{A}_{\mathbb{Q}}^f)$ and for any finite set S of primes, there exists a point $P \in U(\mathbb{Q})$ which is arbitrarily close to P_p for all $p \in S$.

There exists an integral model \mathcal{U} for U over \mathbb{Z} . It will suffice to show that there exists a point $P \in U(\mathbb{Q})$ with $P \in \mathcal{U}(\mathbb{Z}_p)$ for all $p \notin S$, such that P is arbitrarily close to P_p for all $p \in S$.

Let \mathcal{Z} be the scheme-theoretic closure of Z in $\mathbb{P}_{\mathbb{Z}}^m$. We may suppose that \mathcal{Z} is cut out by equations

$$F_1(X_0, \dots, X_m) = \dots = F_r(X_0, \dots, X_m) = 0,$$

for $F_1, \dots, F_r \in \mathbb{Z}[X_0, \dots, X_m]$ such that the intersection with $Q = 0$ has codimension 3 in \mathbb{P}^m . For any prime p , elements of $\mathcal{U}(\mathbb{Z}_p)$ correspond to vectors $\mathbf{x} \in \mathbb{Z}_p^{m+1}$ for which $Q(\mathbf{x}) = 0$ and

$$\min\{\text{val}_p(F_1(\mathbf{x})), \dots, \text{val}_p(F_r(\mathbf{x}))\} = 0.$$

Let $C \in \mathbb{Z}$ be a product of primes in S , chosen so that $P'_p = CP_p \in \mathbb{Z}_p^{m+1}$ for all $p \in S$. By the Chinese Remainder Theorem we can find a vector $\mathbf{a} \in \mathbb{Z}^{m+1}$ which is arbitrarily close to P'_p for all $p \in S$. A vector $\mathbf{x} \in \mathbb{Z}^{m+1}$ representing a point in $U(\mathbb{Q})$ is then close to \mathbf{a} in the p -adic topology for all $p \in S$ if and only if $\mathbf{x} \equiv \mathbf{a} \pmod{M}$, for a suitable positive integer M built from the primes in S . In order to establish Corollary 1.5, it will suffice to prove the existence of a vector $\mathbf{x} \in \mathbb{Z}^{m+1}$, satisfying $Q(\mathbf{x}) = 0$ and

$$\gcd(p, F_1(\mathbf{x}), \dots, F_r(\mathbf{x})) = 1 \text{ for all } p \notin S,$$

and for which $\mathbf{x} \equiv \mathbf{a} \pmod{M}$. Indeed, once this is achieved the vector $C^{-1}\mathbf{x}$ will represent a point $P \in U(\mathbb{Q})$ which is p -adically close to P_p for all $p \in S$ and which belongs to $\mathcal{U}(\mathbb{Z}_p)$ for all $p \notin S$.

Finally, to deduce the existence of the vector \mathbf{x} we count the number of such vectors in the box $[-B, B]^{m+1}$, as $B \rightarrow \infty$. But then we are once more in the situation considered in Section 6, where we dealt with exactly this question when $S = \emptyset$ and $r = 2$. Extending the argument to general S and r is routine and will not be repeated here.

8. PROOF OF COROLLARY 1.6: LOCAL SOLUBILITY

The aim of this section is to prove Corollary 1.6, the main tool for which is Theorem 1.2. The strategy for our argument closely follows the proof of Lemma 20 in work of Poonen and Stoll [15], as further developed by Bright, Browning and Loughran [5, Section 3]. We shall write $m = n - 1$ in order to simplify notation. Let $X \subset \mathbb{P}^{n-1}$ be a hypersurface defined by an indefinite quadratic form $Q \in \mathbb{Z}[X_1, \dots, X_n]$ of rank at least 5. Let $\pi : Y \rightarrow X$ be a morphism as in the statement of the theorem. Thus the fibre of π over every point of codimension 1 is split and the generic fibre of π is geometrically integral. Appealing to Corollary 3.7 of [5], it then follows that there exist a finite set S of places of \mathbb{Q} , together with models \mathcal{Y} and \mathcal{X} of Y and X over $\text{Spec}(\mathbb{Z}_S)$ and a closed subset $\mathcal{Z} \subset \mathcal{X}$ of codimension at least 2, such that the map

$$(\mathcal{Y} \setminus \pi^{-1}(\mathcal{Z}))(\mathbb{Z}_p) \rightarrow (\mathcal{X} \setminus \mathcal{Z})(\mathbb{Z}_p)$$

is surjective for all primes $p \notin S$. We may assume without loss of generality that S contains the infinite place. It follows that

$$\{x \in X(\mathbb{Z}_p) : x \bmod p \notin \mathcal{Z}(\mathbb{F}_p)\} \subset \pi(Y(\mathbb{Q}_p)), \quad (8.1)$$

for all sufficiently large primes p . We proceed under the assumption that \mathcal{Z} is cut out from \mathcal{X} by a system of forms $F_1, \dots, F_r \in \mathbb{Z}[X_1, \dots, X_n]$. We henceforth allow all of the implied constants in this section to depend on F_1, \dots, F_r and on X .

For any field k and any subset $\Omega \subset \mathbb{P}^{n-1}(k)$, we shall denote by Ω^{aff} the affine cone of Ω . For each prime p we let $\Omega_p = \pi(Y(\mathbb{Q}_p))^{\text{aff}} \cap \mathbb{Z}_p^n$. At the infinite place we put $\Omega_\infty = \{\mathbf{x} \in \pi(Y(\mathbb{R}))^{\text{aff}} : |\mathbf{x}| \leq 1\} \cap \mathbb{R}^n$. Let μ_∞ and μ_p be the Haar measures on \mathbb{R}^n and \mathbb{Z}_p^n , respectively. It follows from Lemma 3.9 of [5] that Ω_ν is measurable with respect to μ_ν , with $\mu_\nu(\partial\Omega_\nu) = 0$ and $\mu_\nu(\Omega_\nu) > 0$. The proof of this result is based on the Tarski–Seidenberg–Macintyre theorem, as applied here to the affine cone of the map obtained by composing π with the \mathbb{Q} -birational map to \mathbb{P}^{n-2} admitted by X . If $x = (x_1 : \dots : x_n)$ denotes the

projective point in \mathbb{P}^{n-1} associated to a vector $\mathbf{x} = (x_1, \dots, x_n)$, then we have

$$\mu_p(\Omega_p) = \lim_{k \rightarrow \infty} \frac{\#\{\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n : Q(\mathbf{x}) \equiv 0 \pmod{p^k}, \pi^{-1}(x)(\mathbb{Q}_p) \neq \emptyset\}}{p^{k(n-1)}}$$

and

$$\mu_\infty(\Omega_\infty) = \lim_{\delta \rightarrow 0} \frac{1}{2\delta} \text{meas} \{\mathbf{x} \in [-1, 1]^n : |Q(\mathbf{x})| < \delta, \pi^{-1}(x)(\mathbb{R}) \neq \emptyset\}.$$

Recall the notation $\mu_Q(\mathcal{S})$ that was introduced in (1.1), for any subset $\mathcal{S} \subset \mathbb{Z}^n$. In order to prove Corollary 1.6, it will suffice to study

$$\mu_Q(\mathcal{R}_{\text{loc}}) = \lim_{B \rightarrow \infty} \frac{\#\{\mathbf{x} \in \mathcal{R}_{\text{loc}} \cap [-B, B]^n : Q(\mathbf{x}) = 0\}}{\#\{\mathbf{x} \in \mathbb{Z}^n \cap [-B, B]^n : Q(\mathbf{x}) = 0\}},$$

where

$$\mathcal{R}_{\text{loc}} = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \in \Omega_\nu \text{ for all places } \nu\}.$$

Suppose first that there exists $M \in \mathbb{N}$ such that $\Omega_p = \mathbb{Z}_p^n$ for all primes $p > M$. We let $P = \prod_{p \leq M} \Omega_p$ and $Q = \prod_{p \leq M} (\mathbb{Z}_p^n \setminus \Omega_p)$. The sets Ω_p and $\mathbb{Z}_p^n \setminus \Omega_p$ have boundary of measure zero. Hence by compactness we can cover the closure \overline{P} of P by a finite number of boxes $\prod_{p \leq M} I_p$, the sum of whose measures is arbitrarily close to the measure $\prod_p \mu_p(\Omega_p)$ of \overline{P} , where each $I_p \subset \mathbb{Z}_p^n$ is a cartesian product of closed balls of the shape $\{x \in \mathbb{Z}_p : |x - a|_p \leq b\}$, for $a \in \mathbb{Z}_p$ and $b \in \mathbb{R}$. Similarly, the closure \overline{Q} of Q is covered by a finite number of boxes $\prod_{p \leq M} J_p$, say, the sum of whose measures approximates the measure $1 - \prod_p \mu_p(\Omega_p)$ of \overline{Q} to arbitrary precision.

It follows from the Chinese Remainder Theorem that there exist a vector $\mathbf{a}_M \in \mathbb{Z}^n$ and a modulus $q_M \in \mathbb{N}$, depending on M , such that for any $\mathbf{x} \in \mathbb{Z}^n$ we have $\mathbf{x} \in \prod_{p \leq M} I_p$ if and only if $\mathbf{x} \equiv \mathbf{a}_M \pmod{q_M}$. Let

$$N_{\mathfrak{R}}(B; q, \mathbf{a}) = \#\{\mathbf{x} \in \mathbb{Z}^n \cap B\mathfrak{R} : Q(\mathbf{x}) = 0, \mathbf{x} \equiv \mathbf{a} \pmod{q}\},$$

for any $\mathfrak{R} \subset \mathbb{R}^n$ of finite measure, any $q \in \mathbb{N}$ and any $\mathbf{a} \in (\mathbb{Z}/q\mathbb{Z})^n$. When $\mathfrak{R} = [-1, 1]^n$ we simply write $N(B; q, \mathbf{a})$ and thereby recover the counting function that was introduced in (6.1). It now follows from (6.2) that

$$\begin{aligned} \mu_Q \left(\prod_{p \leq M} I_p \right) &= \lim_{B \rightarrow \infty} \frac{N_{\Omega_\infty}(B; q_M, \mathbf{a}_M)}{N(B; 1, \mathbf{0})} \\ &= \frac{\mu_\infty(\Omega_\infty)}{\sigma_\infty} \prod_p \frac{\mu_p(I_p)}{\sigma_p}. \end{aligned}$$

Similarly,

$$\mu_Q \left(\prod_{p \leq M} J_p \right) = \frac{\mu_\infty(\Omega_\infty)}{\sigma_\infty} \prod_p \frac{\mu_p(J_p)}{\sigma_p}.$$

Combining these facts, we are therefore done when there exists M such that $\Omega_p = \mathbb{Z}_p^n$ for all primes $p > M$.

We now turn to the general case. For $M \leq M' \leq \infty$ and $B > 0$, let

$$f_{M,M'}(B) = \frac{\#\{\mathbf{x} \in \mathbb{Z}^n \cap B\Omega_\infty : Q(\mathbf{x}) = 0, \mathbf{x} \in \Omega_p \text{ for all } p \in [M, M']\}}{N(B; 1, \mathbf{0})}.$$

Put $f_M(B) = f_{1,M}(B)$ and note that this is a non-increasing function of M . According to (8.1), there are forms $F_1, \dots, F_r \in \mathbb{Z}[X_1, \dots, X_n]$ whose common zero locus meets X in a codimension 3 subset of \mathbb{P}^{n-1} , for which

$$\begin{aligned} f_M(B) - f_\infty(B) &= \frac{\#\{\mathbf{x} \in \mathbb{Z}^n \cap B\Omega_\infty : Q(\mathbf{x}) = 0, \exists p > M, \mathbf{x} \notin \Omega_p\}}{N(B; 1, \mathbf{0})} \\ &\leq \frac{E(B, M)}{N(B; 1, \mathbf{0})}, \end{aligned}$$

where $E(B, M)$ is the number of $\mathbf{x} \in \mathbb{Z}^n$ such that $Q(\mathbf{x}) = 0$ and $|\mathbf{x}| \leq B$, and for which $F_1(\mathbf{x}), \dots, F_r(\mathbf{x})$ have a common prime divisor $p > M$. We have $N(B; 1, \mathbf{0}) \gg B^{n-2}$ by (6.2). We may sort $E(B, M)$ into two contributions. Let $\eta > 0$ be a parameter at our disposal.

The contribution from \mathbf{x} for which $F_1(\mathbf{x}), \dots, F_r(\mathbf{x})$ have a common prime divisor $p > B^\eta$ is seen to be

$$\ll B^{n-2+\varepsilon-\eta} + \frac{B^{n-2+\varepsilon}}{B^{1/(n-1)}},$$

by Theorem 1.2. (The reader will note that we are concerned with quadratic forms in n variables, rather than $n+1$ variables, as in the statement of the theorem.) Next, the contribution from \mathbf{x} for which $F_1(\mathbf{x}), \dots, F_r(\mathbf{x})$ have a common prime divisor $p \in (M, B^\eta]$ is at most

$$\sum_{M < p \leq B^\eta} \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/p\mathbb{Z})^n \\ Q(\mathbf{a}) \equiv F_1(\mathbf{a}) \equiv \dots \equiv F_r(\mathbf{a}) \pmod{p}}} N(B; p, \mathbf{a}) \ll \frac{B^{n-2}}{M \log M} + B^{n-2-\delta+\eta(n+1+\Delta)},$$

by (6.8).

It now follows that

$$f_M(B) - f_\infty(B) \ll B^{\varepsilon-\eta} + \frac{B^\varepsilon}{B^{1/(n-1)}} + \frac{1}{M \log M} + \frac{B^{\eta(n+1+\Delta)}}{B^\delta},$$

for any $\varepsilon > 0$. On taking $\eta = \delta/(n+2+\Delta)$ and choosing ε sufficiently small, we obtain

$$\lim_{M \rightarrow \infty} \limsup_{B \rightarrow \infty} (f_M(B) - f_\infty(B)) = 0. \quad (8.2)$$

Moreover, our work so far shows that

$$\lim_{B \rightarrow \infty} f_{M,M'}(B) = \frac{\mu_\infty(\Omega_\infty)}{\sigma_\infty} \prod_{M \leq p < M'} \frac{\mu_p(\Omega_p)}{\mu_p(X(\mathbb{Q}_p)^{\text{aff}} \cap \mathbb{Z}_p^n)}, \quad (8.3)$$

for all $M < M' < \infty$. Combining (8.2) and (8.3), we conclude that

$$\begin{aligned} \lim_{B \rightarrow \infty} f_\infty(B) &= \lim_{M \rightarrow \infty} \lim_{B \rightarrow \infty} f_M(B) \\ &= \frac{\mu_\infty(\Omega_\infty)}{\sigma_\infty} \lim_{M \rightarrow \infty} \prod_{p < M} \frac{\mu_p(\Omega_p)}{\sigma_p} \end{aligned}$$

To complete the proof, it suffices to show the convergence of the above infinite product. In order to apply Cauchy's criterion we need to check that

$$\lim_{M \rightarrow \infty} \sup_{M' \in \mathbb{N}} \left| 1 - \prod_{M \leq p < M+M'} \frac{\mu_p(\Omega_p)}{\sigma_p} \right| = 0.$$

But (8.3) implies that the left hand side is

$$\frac{\sigma_\infty}{\mu_\infty(\Omega_\infty)} \lim_{M \rightarrow \infty} \sup_{M' \in \mathbb{N}} \lim_{B \rightarrow \infty} |f_1(B) - f_{M,M+M'}(B)|,$$

which vanishes by a further application of (8.2). Combining our argument, we have therefore shown that

$$\mu_Q(\mathcal{R}_{\text{loc}}) = \frac{\mu_\infty(\Omega_\infty)}{\sigma_\infty} \prod_p \frac{\mu_p(\Omega_p)}{\sigma_p},$$

which thereby completes the proof of Corollary 1.6.

REFERENCES

- [1] M. Bhargava, The geometric sieve and the density of squarefree values of invariant polynomials. ([arXiv:1402.0031](#))
- [2] M. Bhargava, A. Shankar, X. Wang, Squarefree values of polynomial discriminants I. ([arXiv:1611.09806](#))
- [3] B.J. Birch, Forms in many variables. *Proc. Roy. Soc. Ser. A* **265** (1961/62), 245–263.
- [4] T.D. Browning and D. Loughran, Sieving rational points on varieties. *Trans. Amer. Math. Soc.* **371** (2019), 5757–5785.
- [5] T.D. Browning, M. Bright and D. Loughran, Failures of weak approximation in families. *Compositio Math.* **152** (2016), 1435–1475.
- [6] J.W.S. Cassels, *Introduction to the geometry of numbers*. Springer-Verlag, 1971.
- [7] Y. Cao and Z. Huang, Arithmetic purity, geometric sieve, and counting integral points on affine quadrics. ([arXiv:2003.07287](#))
- [8] Y. Cao and F. Xu, Strong approximation with Brauer–Manin obstruction for toric varieties. *Ann. Inst. Fourier* **68** (2018), 1879–1908.
- [9] J.E. Cremona and M. Sadek, Local and global densities for Weierstrass models of elliptic curves. ([arXiv:2003.08454](#))

- [10] T. Ekedahl, An infinite version of the Chinese remainder theorem. *Comment. Math. Univ. St. Paul.* **40** (1991), 53–59.
- [11] Y. Harpaz and O. Wittenberg, On the fibration method for zero-cycles and rational points. *Annals of Math.* **183** (2016), 229–295.
- [12] S. Lindqvist, Weak approximation results for quadratic forms in four variables. ([arXiv:1704.00502](#)).
- [13] D. Loughran, The number of varieties in a family which contain a rational point. *J. Eur. Math. Soc.* **20** (2018), 2539–2588.
- [14] B. Poonen, Squarefree values of multivariable polynomials. *Duke Math. J.* **118** (2003), 189–373.
- [15] B. Poonen and M. Stoll, The Cassels–Tate pairing on polarized abelian varieties. *Annals of Math.* **150** (1999), 1109–1149.
- [16] B. Poonen and J. F. Voloch, Random Diophantine equations. *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, 175–184, Progr. Math. **226**, Birkhäuser, 2004.
- [17] V.V. Prasolov, *Polynomials. Algorithms and Computation in Mathematics* **11**, Springer-Verlag, 2004.
- [18] O. Wittenberg, Rational points and zero-cycles on rationally connected varieties over number fields. *Algebraic Geometry: Salt Lake City 2015*, Part 2, 597–635, Proceedings of Symposia in Pure Mathematics **97**, American Mathematical Society, 2018.

IST AUSTRIA, AM CAMPUS 1, 3400 KLOSTERNEUBURG, AUSTRIA
Email address: `tdb@ist.ac.at`

MATHEMATICAL INSTITUTE, RADCLIFFE OBSERVATORY QUARTER, WOODSTOCK ROAD,
 OXFORD, OX2 6GG, UNITED KINGDOM
Email address: `rhb@maths.ox.ac.uk`