Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Tim SANTENS

Integral points on affine quadric surfaces

Tome 34, n° 1 (2022), p. 141-161.

https://doi.org/10.5802/jtnb.1196

Journal de Théorie des Nombres de Bordeaux **34** (2022), 141–161

Integral points on affine quadric surfaces

par Tim SANTENS

Résumé. Il est bien connu que le principe de Hasse est valable pour les hypersurfaces quadratiques. Le principe de Hasse échoue pour les points entiers sur les hypersurfaces quadratiques lisses de dimension 2, mais cet échec peut être complètement expliqué par l'obstruction de Brauer–Manin. Nous étudions à quelle fréquence la famille d'hypersurfaces quadratiques $ax^2 + by^2 + cz^2 = n$ a une obstruction de Brauer–Manin, où a, b, c, n sont des entiers. Nous améliorons les éstimations précédentes de Mitankin [7].

Abstract. It is well-known that the Hasse principle holds for quadric hypersurfaces. The Hasse principle fails for integral points on smooth quadric hypersurfaces of dimension 2 but the failure can be completely accounted for by the Brauer–Manin obstruction. We investigate how often the family of quadric hypersurfaces $ax^2 + by^2 + cz^2 = n$ has a Brauer–Manin obstruction where a, b, c, n are integers. We improve previous bounds of Mitankin [7].

1. Introduction

One of the oldest questions in number theory is whether a particular polynomial equation has a solution in the integers or in the rational numbers. The general problem of finding an algorithm which can decide for every polynomial $f \in \mathbb{Z}[X_1, \dots, X_n]$ whether it has an integral zero is known as Hilbert's 10th problem. It was shown to be impossible in the second half of the twentieth century by Matiyasevich [6], building upon work of Robinson, Davis and Putnam. The analogous question for rational zeros is still open but is also expected to be unsolvable. A slight generalization in which we allow systems of polynomial equations can be restated in a more modern terminology as follows. Given a $\mathbb{Q}$-variety X and an integral model $\mathcal{X}$, the question is whether $X(\mathbb{Q}) = \mathcal{X}(\mathbb{Q}) \neq \emptyset$? Respectively whether $\mathcal{X}(\mathbb{Z}) \neq \emptyset$? Note that the second question is only interesting if $\mathcal{X}$ is not proper (and thus not projective) since if it were proper, then because of the valuative criterion of properness $\mathcal{X}(\mathbb{Z}) = \mathcal{X}(\mathbb{Q})$. Necessary conditions for the existence of rational or integral points are that $X(\mathbb{Q}_p) \neq \emptyset$ for all prime numbers p and $X(\mathbb{R}) \neq \emptyset$, respectively that $\mathcal{X}(\mathbb{Z}_p) \neq \emptyset$ for all prime numbers p and

Manuscrit reçu le 9 septembre 2020, révisé le 22 avril 2021, accepté le 5 juin 2021.
2020 *Mathematics Subject Classification.* 14G05, 14G12.
Mots-clefs. Brauer–Manin obstruction, integral point, quadric surface.

$\mathcal{X}(\mathbb{R}) \neq 0$. Here $\mathbb{Q}_p$ are the p-adic numbers and $\mathbb{Z}_p$ are the p-adic integers. If these conditions are also sufficient we say that X satisfies the Hasse principle, respectively that $\mathcal{X}$ satisfies the integral Hasse principle.

The simplest example of varieties, those defined by a system of linear equations, satisfy the Hasse principle and the integral Hasse principle by linear algebra and Euclid's algorithm. The first non-trivial examples are quadrics. Both projective and affine quadrics satisfy the Hasse principle [9, §4: Theorem 8], this was proved by Minkowski. Sadly, this does not generalize to their integral models. The situation depends on the dimension of the variety. We may assume that the associated quadratic form is non-degenerate, equivalently that the corresponding variety is smooth. If its dimension is greater or equal to 3 and the set of real points is unbounded, then they satisfy the integral Hasse principle, [1, Theorem 6.1]. This was originally proved by Kneser [5]. Note that the unboundedness assumption is necessary due to counterexamples like $4x^2 + 4y^2 + 4z^2 + 9t^2 = 1$. On the other hand if the real points are bounded then whether there are integral points can checked with a finite computation. This theorem fails when the rank of the quadratic form is less than 4. In the case when the rank is 3 the failure of the integral Hasse principle can be completely explained by the Brauer–Manin obstruction [1, Theorem 6.3] which was proved by Colliot-Thélène and Xu. The dimension 1 case is the rich subject of integers represented by binary quadratic forms which lies outside the scope of this article.

A natural question is then: what is the amount of surfaces that actually have a Brauer–Manin obstruction? This question was investigated in work by Mitankin [7]. To be precise, for a fixed non-zero integer n consider the family $\mathcal{F}_n$ of surfaces $X_{a,b,c} : ax^2 + by^2 + cz^2 = n$ where $a, b, c \in \mathbb{Z}$ such that $ax^2 + by^2 + cz^2$ is indefinite and non-degenerate. The first question is how often this family has integral solutions everywhere locally. To study this one introduces the height function $H(a, b, c) = \max(|a|, |b|, |c|)$ and considers the following quantity as $B > 0$ varies:

$$N_{\mathrm{loc}}(B) = |\{X_{a,b,c} \in \mathcal{F}_n : H(a, b, c) \leq B, X_{a,b,c}(\mathbb{A}_{\mathbb{Z}}) \neq \emptyset\}|.$$

Here $\mathbb{A}_{\mathbb{Z}}$ are the integral adeles. Then Mitankin proves [7, Theorem 1.1] that there exist a non-zero constant c_n such that $N_{\mathrm{loc}}(B) \sim c_n B^3$. So a positive proportion of such surfaces have integral solutions everywhere locally. The second quantity they consider is

$$N_{\mathrm{Br}}(B) = |\{X_{a,b,c} \in \mathcal{F}_n : H(a, b, c) \leq B, X_{a,b,c}(\mathbb{A}_{\mathbb{Z}}) \neq \emptyset, X_{a,b,c}(\mathbb{Z}) = \emptyset\}|.$$

For this quantity it is proven that [7, Theorem 1.2, Corollary 1.4]:

$$B^{\frac{3}{2}}(\log B)^{-\frac{1}{2}} \ll_n N_{\mathrm{Br}}(B) \ll_n B^{\frac{3}{2}}(\log B)^3.$$

So in particular 0% of these surfaces have a Brauer–Manin obstruction. In this paper we improve both of these bounds.

Theorem 1.1. *The following bounds hold*

$$B^{\frac{3}{2}}(\log B)^{\frac{1}{2}} \ll_n N_{\mathrm{Br}}(B) \ll_n B^{\frac{3}{2}}(\log B)^{\frac{3}{2}}.$$

Acknowledgements. I would like to thank my thesis advisor Vladimir Mitankin for providing the topic of this paper, answering questions related to it and the helpful comments provided while writing it. I am also thankful of Valentin Blomer for his feedback on the thesis this paper is based on. This paper is a result of the author's Master's thesis completed in the context of the Master of mathematics at the university of Bonn.

Structure. This paper is organized as follows, in the first section we give an introduction to the integral Brauer–Manin obstruction and in particular describe the case of integral affine quadrics. In the second section we give a proof of Theorem 1.1, first of the lower and then the upper bound.

2. Brauer–Manin obstruction

2.1. The general Brauer–Manin obstruction. We will first give an overview of the (integral) Brauer–Manin obstruction. For more details on the Brauer–Manin obstruction we refer the reader to [10, §5.2] and for the integral Brauer–Manin obstruction [1, §1].

For an arbitrary scheme X its Brauer group is $\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m)$. We refer the reader to [4] for an introduction to the Brauer group. Let K be a number field, Ω_K the set of equivalence classes of places of K and for $v \in \Omega_K$ we let K_v be the completion of K with respect to the place v. From local class theory we know that for every place v there exists an injective map $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$. Let X be a K-variety, $\mathbb{A}_K$ be the ring of adeles of K and $X(\mathbb{A}_K)$ the set of adelic points of X. There is then a pairing

$$\begin{aligned} X(\mathbb{A}_K) \times \mathrm{Br}(X) &\longrightarrow \mathbb{Q}/\mathbb{Z} : \\ ((x_v)_v, \alpha) &\longmapsto \sum_{v \in \Omega_v} \mathrm{inv}_v(\alpha(x_v)). \end{aligned} \tag{2.1}$$

The left kernel of this pairing is called the Brauer–Manin set $X(\mathbb{A}_K)^{\mathrm{Br}}$ and the set of rational points $X(K)$ injects into it. The right kernel of this pairing contains $\mathrm{Br}(K)$. We remark that the quotient $\mathrm{Br}(X)/\mathrm{Br}(K)$ is often finite. If $X(\mathbb{A}_K) \neq \emptyset$ but $X(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$, then $X(K)$ has to be empty, thus X fails the Hasse principle. We say that X has a Brauer–Manin obstruction to the Hasse principle.

Let now $\mathcal{X}$ be an integral model of X, it is separated so we can identify $\mathcal{X}(\mathcal{O}_{K_v})$ with a subset of $\mathcal{X}(K_v) = X(K_v)$ and thus form a similar obstruction for integral points by considering the pairing

$$\begin{aligned} \mathcal{X}(\mathbb{A}_{\mathcal{O}_K}) \times \operatorname{Br}(X) &\longrightarrow \mathbb{Q}/\mathbb{Z} : \\ ((x_v)_v, \alpha) &\longmapsto \sum_{v \in \Omega_v} \operatorname{inv}_v(\alpha(x_v)). \end{aligned} \tag{2.2}$$

Here $\mathbb{A}_{\mathcal{O}_K}$ is the ring of integral adeles and $\mathcal{X}(\mathbb{A}_{\mathcal{O}_K})$ is the set of integral adelic points. The left kernel of this pairing is called the Brauer–Manin set $\mathcal{X}(\mathbb{A}_{\mathcal{O}_K})^{\mathrm{Br}}$ and the set of integral points $\mathcal{X}(\mathcal{O}_K)$ injects into it. It is clear from the definitions that $\mathcal{X}(\mathbb{A}_{\mathcal{O}_K})^{\mathrm{Br}} = \mathcal{X}(\mathbb{A}_{\mathcal{O}_K}) \cap X(\mathbb{A}_K)^{\mathrm{Br}}$. If $\mathcal{X}(\mathbb{A}_{\mathcal{O}_K}) \neq \emptyset$ but $\mathcal{X}(\mathbb{A}_{\mathcal{O}_K})^{\mathrm{Br}} = \emptyset$ we say that $\mathcal{X}$ has a Brauer–Manin obstruction to the integral Hasse principle.

2.2. The case of affine integral quadric surfaces. We now come to the case of interest for this paper. Let q be a non-degenerate indefinite integral quadratic form of rank 3 and n a non-zero integer. The question we want to answer is whether there exist integers $x, y, z \in \mathbb{Z}$ such that $q(x, y, z) = n$. Let X be the affine surface defined over $\mathbb{Q}$ by this equation and let $\mathcal{X}$ be the obvious integral model of it. It is then shown by Colliot-Thélène and Xu in [1, Theorem 6.3] that the Brauer–Manin obstruction is the only obstruction to the integral Hasse principle, i.e. if $\mathcal{X}(\mathbb{A}_{\mathbb{Z}})^{\mathrm{Br}} \neq \emptyset$ then $\mathcal{X}(\mathbb{Z}) \neq 0$. It is also shown that if $X(\mathbb{Q}) \neq \emptyset$ and $d = -\operatorname{disc}(q)n$ is not a square, then $\operatorname{Br}(X)/\operatorname{Br}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ and if d is a square then $\operatorname{Br}(X)/\operatorname{Br}(\mathbb{Q}) = 0$. An explicit algorithm to find a generator of this group is given in Section 5.8 of [1]. We now give a description of this algorithm.

Consider first the projectivization $\overline{X}$ of X, concretely $\overline{X} \subseteq \mathbb{P}^3$ is the projective surface defined by $q(x, y, z) = nt^2$ for $[x : y : z : t] \in \mathbb{P}^3$. Then choose a $\mathbb{Q}$-point M on $\overline{X}$. Let $\ell_1 = \ell_1(x, y, z, t)$ be the linear form defining the tangent plane of $\overline{X}$ at M. Then by [9, §IV: Proposition 3'] there exist linearly independent linear forms ℓ_2, ℓ_3, ℓ_4 and $c \in \mathbb{Q}^*$ such that

$$q(x, y, z) - nt^2 = \ell_1\ell_2 + c(\ell_3^2 - d\ell_4^2).$$

Conversely, if we have such linear forms then ℓ_1 defines a plane tangent to $\overline{X}$. Consider the quaternion algebra $\alpha = (\frac{\ell_1}{t}, d) \in \operatorname{Br}(\mathbb{Q}(\overline{X})) = \operatorname{Br}(\mathbb{Q}(X))$. By the identity in the l_i we get in $\operatorname{Br}(\mathbb{Q}(X))$ that

$$\alpha = \left(\frac{\ell_2}{t}, d\right)\left(\frac{\ell_1\ell_2}{t^2}, d\right) = \left(\frac{\ell_2}{t}, d\right)(c, d)\left(\frac{\ell_3^2 - d\ell_4^2}{t^2}, d\right) = \left(\frac{\ell_2}{t}, d\right)(c, d).$$

So α is defined on $U_1 = \{t\ell_1 \neq 0\}$ and on $U_2 = \{t\ell_2 \neq 0\}$. By Grothendieck purity [4, III: Theorem 6.1] this implies that α comes from the Brauer group of $\{t \neq 0\} = X$ since $\{\ell_1 = 0 = \ell_2\}$ is at least of codimension 2.

3. The proof of Theorem 1.1

We recall that the statement of Theorem 1.1 is the following inequalities:

$$B^{\frac{3}{2}}(\log B)^{\frac{1}{2}} \ll_n N_{Br}(B) \ll_n B^{\frac{3}{2}}(\log B)^{\frac{3}{2}}.$$

3.1. The lower bound. It suffices to do the case $n = 1$ since the surfaces $ax^2 + by^2 + cz^2 = 1$ and $anx^2 + bny^2 + cnz^2 = n$ are the same. We first construct a family with a Brauer–Manin obstruction. For this fix a prime $q \equiv 1 \bmod 8$, e.g. $q = 17$. For $a, c, d, e \in \mathbb{Z}\setminus\{0\}$ with c, d, e pairwise coprime consider the family of integral surfaces $Y_{a;c,d,e} : aq^2c^2x^2 - ad^2y^2 + e^2qz^2 = 1$. We start with a lemma showing when this family has a local solution everywhere, clearly we always have $Y_{a;c,d,e}(\mathbb{R}) \neq \emptyset$. From now on p is always a prime number. From now on, except for a single clearly marked exception, we will use the notation (a, b) without a subscript to mean the greatest common divisor of a and b. On the other hand $(a, b)_p$ with a subscript will be the Hilbert symbol.

Lemma 3.1. *$Y_{a;c,d,e}(\mathbb{Z}_p) \neq \emptyset$ for all primes p if and only if $(a, eq) = 1$, $(d, q) = 1$ and for all odd primes $p \mid a$ we have $(\frac{q}{p}) = 1$.*

Proof. The only if part is clear by looking modulo p, the other part we do by case analysis.

- If $p \nmid 2aq$, then the associated equation has a smooth point modulo p which lifts to a $\mathbb{Z}_p$-point by Hensel's lemma.
- If $p \mid a$ and if p is odd, then by assumption q is a non-zero square modulo p which implies we can write $q = \alpha^{-2}$ for $\alpha \in \mathbb{Z}_p$. Similarly, if $p = 2$ and $2 \nmid e$, then since $q \equiv 1 \pmod 8$ we can also write $q = \alpha^{-2}$ for $\alpha \in \mathbb{Z}_2^*$. In both cases e must be invertible in $\mathbb{Z}_p$ since $(a, e) = 1$. So $(0, 0, \alpha e^{-1}) \in Y_{a;c,d,e}(\mathbb{Z}_p)$.
- If $p = q$, then we can factorize $a = \prod_i p_i^{\alpha_i}$ where the p_i are prime numbers. Then $(\frac{a}{q}) = \prod_i (\frac{p_i}{q})^{\alpha_i} = 1$. Indeed, by our assumption and quadratic reciprocity $(\frac{p_i}{q}) = (\frac{q}{p_i}) = 1$ if p_i is odd. If $p_i = 2$ then also $(\frac{2}{q}) = 1$ since $q \equiv 1 \pmod 8$. So $a = \beta^{-2}$ for some $\beta \in \mathbb{Z}_q^*$. Then $(0, \beta d^{-1}, 0) \in Y_{a;c,d,e}(\mathbb{Z}_p)$.
- If $p = 2$ but $2 \mid e$, then by assumption $2 \nmid a, c, d$. A direct computation shows that the quadratic form $x'^2 - y'^2$ takes all values in $(\mathbb{Z}/8\mathbb{Z})^*$, letting it take the value a^{-1} and setting $z = 0, x = q^{-1}c^{-1}x', y = d^{-1}y'$ gives a solution to $aq^2c^2x^2 - ad^2y^2 + e^2qz^2 = 1$ modulo 8 which lifts to $\mathbb{Z}_2$ by Hensel's lemma. $\square$

From now on let a, c, d, e be as in the above lemma. We want to know when $Y_{a;c,d,e}$ has no integral point. By [1, Theorem 6.3] this only happens if there is a Brauer–Manin obstruction. In this case $\mathrm{Br}(Y_{a;c,d,e})/\mathrm{Br}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ since $-(aq^2c^2)(-ad^2)(e^2q) = q \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ is not a rational square as in Section 2.2. We use the procedure in that section to find a representative of the generator of this group. The projectivization of $Y_{a;c,d,e}$ is given by the equation $aq^2c^2X^2 - ad^2Y^2 + qe^2Z^2 = T^2$ with $[X : Y : Z : T] \in \mathbb{P}^3$. This variety has a rational point $[d : -qc : 0 : 0]$. The tangent plane to this point is defined by the equation $2aq^2c^2dX + 2ad^2qcY = 0$ so a representative for the generator of the group is given by the quaternion algebra $(qc\frac{X}{T} + d\frac{Y}{T}, q) = (qcx + dy, q)$.

We now need to find what the values of this Brauer element are when evaluated at points of $Y_{a;c,d,e}(\mathbb{Z}_p)$. Since the evaluation function is continuous we can restrict our attention to the dense open subset $U = \{qcx + dy \neq 0\}$. That is, we will only consider points in $Y_{a;c,d,e}(\mathbb{Z}_p) \cap U(\mathbb{Q}_p)$. We split this computation into the following cases:

- If $p = \infty$ or 2, then $(qcx + dy, q)_p = 1$ since q is a square in $\mathbb{R}$ and $\mathbb{Z}_2$.
- If $p \nmid 2q$ then the following equality follows from the computation of the Hilbert symbol [9, §III: Theorem 1].

$$(qcx + dy, q)_p = \left(\frac{q}{p}\right)^{v_p(qcx+dy)}.$$

  We may assume that $(\frac{q}{p}) = -1$ since the other case is trivial, thus $(a, p) = 1$. If $p \mid qcx + dy$, then $p \mid q^2c^2x^2 - d^2y^2$ so by looking at the defining equation modulo p we see that $e^2qz^2 \equiv 1 \pmod p$ which contradicts that $(\frac{q}{p}) = -1$.
- If $p = q$, then by looking at the defining equation modulo q we get $ad^2y^2 \equiv 1 \pmod q$ which shows that y is non-zero modulo q. Then $(qcx + dy, q)_q = (\frac{dy}{q})$ because of the computation of the Hilbert symbol. So it is equal to 1 if and only if dy is a square modulo q. Again looking at the defining equation modulo q we see that this happens if and only if $-a$ is a non-zero fourth power modulo q. Because $q \equiv 1 \pmod 8$ this is true if and only if a is a non-zero fourth power modulo q.

Combining all this we get that $Y_{a;c,d,e}(\mathbb{Z}) = \emptyset$ if and only if a is not a fourth power modulo q. On the other hand we already assumed that a was a square modulo q so the residue of a modulo q has to be an element of

$$S = (\mathbb{Z}/q\mathbb{Z})^{*2} \setminus (\mathbb{Z}/q\mathbb{Z})^{*4}. \tag{3.1}$$

The group isomorphism $(\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$ and the fact that $q \equiv 1 \pmod 8$ imply that the set S is non-empty and has size $\frac{q-1}{4}$.

We now want to count the amount of such equations with coefficients smaller than B, namely $N'_{\mathrm{Br}}(B) =$

$$|\{Y_{a;c,d,e} : H(aq^2c^2, ad^2, qe^2) \leq B, Y_{a;c,d,e}(\mathbb{A}_{\mathbb{Z}}) \neq \emptyset \text{ and } Y_{a;c,d,e}(\mathbb{Z}) = \emptyset\}| \tag{3.2}$$

We will first introduce some notation to encode the conditions above. First of all we will denote the indicator function of S by $1_{a\in S}$, we can encode this in the standard way as a sum of characters

$$1_{a\in S} = \frac{1}{q-1}\sum_{s\in S}\sum_{\chi \bmod q}\chi(s)\chi(a). \tag{3.3}$$

Note that we used that $s\in S$ if and only if $s^{-1}\in S$ to simplify the notation. We will also use $\alpha(a)$ to denote the indicator function of the set $\{a\in\mathbb{Z} : p \mid a \Rightarrow (\frac{p}{q}) = 1\}$. Similarly we use the notation $\beta(c,d,e)$ for the indicator function of the condition c,d,e pairwise coprime.

Since the sign of a is immaterial we have

$$N'_{\mathrm{Br}}(B) = 2\sum_{a\le \frac{B}{q^2}}\alpha(a)1_{a\in S}\sum_{c\le\frac{\sqrt{B}}{q\sqrt{a}}}\sum_{\substack{d\le\sqrt{\frac{B}{a}}\\(d,q)=1}}\sum_{\substack{e\le\sqrt{\frac{B}{q}}\\(e,a)=1}}\beta(c,d,e). \tag{3.4}$$

Note in particular that if $q|a$ then the associated term in this sum is zero. To remove the condition $(a,e)=1$ we can use that its indicator function is given by $\sum_{f|(a,e)}\mu(f)$. We can then swap the order of the summation so (3.4) turns into

$$N'_{\mathrm{Br}}(B) = 2\sum_{f\le\sqrt{\frac{B}{q}}}\mu(f)\sum_{a\le\frac{B}{q^2 f}}\alpha(af)1_{af\in S}\sum_{c\le\frac{\sqrt{B}}{q\sqrt{af}}}\sum_{\substack{d\le\sqrt{\frac{B}{af}}\\(d,q)=1}}\sum_{e\le\frac{\sqrt{B}}{\sqrt{q}f}}\beta(c,d,fe).$$

We will denote the triple sum over c,d,e by $V(B,a,f)$. Note that by definition $\beta(c,d,fe)=\beta(c,d,e)$ if $(f,cd)=1$ and equal to 0 otherwise. So we can also write this quantity as

$$V(B,a,f) = \sum_{\substack{c\le\frac{\sqrt{B}}{q\sqrt{af}}\\(c,f)=1}}\sum_{\substack{d\le\sqrt{\frac{B}{af}}\\(d,qf)=1}}\sum_{e\le\frac{\sqrt{B}}{\sqrt{q}f}}\beta(c,d,e). \tag{3.5}$$

It also follows from the definition of α that $\alpha(af)=\alpha(a)\alpha(f)$. Using this and (3.3) we obtain that $N'_{\mathrm{Br}}(B)$ is equal to

$$\frac{2}{q-1}\sum_{s\in S}\sum_{\chi \bmod q}\chi(s)\sum_{f\le\sqrt{\frac{B}{q}}}\alpha(f)\chi(f)\mu(f)\sum_{a\le\frac{B}{q^2 f}}\alpha(a)\chi(a)V(B,a,f).$$

We now introduce the following intermediary quantities for which we will find asympotic formulas one by one. First of all the sum over a is denoted by

$$W_\chi(B,f) = \sum_{a\le\frac{B}{q^2 f}}\alpha(a)\chi(a)V(B,a,f). \tag{3.6}$$

We will also consider the sum over f:

$$U_\chi(B) = \sum_{f \le \sqrt{\frac{B}{q}}} \alpha(f)\chi(f)\mu(f)W_\chi(B, f). \tag{3.7}$$

With this notation the quantity which we have to compute is

$$N'_{\mathrm{Br}}(B) = \frac{2}{q-1} \sum_{s \in S} \sum_{\chi \bmod q} \chi(s) U_\chi(B). \tag{3.8}$$

We begin by evaluating $V(B, a, f)$. Let k, ℓ, m be non-zero integers and let $X, Y, Z \ge 1$. We will start by investigating the following sum.

$$L_{k,\ell,m}(X, Y, Z) = \sum_{\substack{x \le X \\ (x,k)=1}} \sum_{\substack{y \le Y \\ (y,\ell)=1}} \sum_{\substack{z \le Z \\ (z,m)=1}} \beta(x, y, z).$$

A similar sum is the subject of [12], in particular if $X = Y = Z$ and $k = \ell = m$ the following lemma is a special case of the main theorem of [12].

Lemma 3.2. *There exists a non-zero constant $C_{k,\ell,m} = \prod_p C_p$ only depending on k, ℓ, m such that*

$$\begin{aligned} L_{k,\ell,m}(X, Y, Z) &= C_{k,\ell,m} XYZ \\ &\quad + O\left(\left(\frac{\tau(k)(\log X)^2}{X} + \frac{\tau(\ell)(\log Y)^2}{Y} + \frac{\tau(m)(\log Z)^2}{Z}\right) XYZ\right). \end{aligned}$$

For any prime p the constant C_p depends on how many of the k, ℓ, m are divisible by the prime p. If p divides exactly i of them, then $C_p = (1 - \frac{1}{p})^2(1 + \frac{2-i}{p})$.

In the proof of this lemma we will require the notion of a multivariable multiplicative function. A survey of this notion is the subject of [13].

Proof. We will first encode the conditions x, y, z pairwise coprime in a more useful way. Note that $\beta(x, y, z)$ is multiplicative. We can encode this condition as

$$\beta(x, y, z) = \sum_{t | (x,y,z)} \sum_{u | (x,y)} \sum_{v | (x,z)} \sum_{w | (y,z)} \mu(uvwt)\mu(t)\tau(t). \tag{3.9}$$

Indeed the right hand side is also multiplicative. It thus suffices to check the equality in the case where x, y, z are prime powers and this is a simple computation.

Use this encoding (3.9) of β in the definition of $L_{k,\ell,m}(X, Y, Z)$. Since the terms are non-zero unless t, u, v, w are pairwise coprime we can switch the order of summation and get that

$$\begin{aligned}(3.10)\quad & L_{k,\ell,m}(X,Y,Z)\\ &= \sum_{\substack{uvt\le X,\ (uvt,k)=1\\ uwt\le Y,\ (uwt,\ell)=1\\ vwt\le Z,\ (vwt,m)=1}} \mu(uvwt)\mu(t)\tau(t) \sum_{\substack{x\le \frac{X}{uvt}\\ (x,k)=1}} \sum_{\substack{y\le \frac{Y}{uwt}\\ (y,\ell)=1}} \sum_{\substack{z\le \frac{Z}{vwt}\\ (z,m)=1}} 1.\end{aligned}$$

Now for the inner sums use the standard fact that

$$\sum_{\substack{x\le X\\ (x,k)=1}} 1 = \sum_{x\le X} \sum_{d\mid (x,k)} \mu(d) = \sum_{d\mid k}\Big(\frac{\mu(d)X}{d} + O(1)\Big) = \frac{\phi(k)X}{k} + O(\tau(a)).$$

Applying this and the trivial inequality $\sum_{\substack{x\le X\\ (x,k)=1}} 1 \ll X$ if $X\le \tau(k)$ thrice one finds that

$$\begin{aligned}\sum_{\substack{x\le \frac{X}{uvt}\\ (x,k)=1}} \sum_{\substack{y\le \frac{Y}{uwt}\\ (y,\ell)=1}} \sum_{\substack{z\le \frac{Z}{vwt}\\ (z,m)=1}} 1 = \frac{XYZ}{u^2v^2w^2t^3}\Big(&\frac{\phi(k)\phi(\ell)\phi(m)}{k\ell m}\\ &+ O\Big(\frac{\tau(k)uvt}{X} + \frac{\tau(\ell)uwt}{Y} + \frac{\tau(m)vwt}{Z}\Big)\Big).\end{aligned}$$

If we apply this to (3.10) and use trivial inequalities for the sums over the error terms we get that

$$\begin{aligned}L_{k,\ell,m}(X,Y,Z) = K_{k,\ell,m}(X,Y,Z)XYZ\Bigg(&\frac{\phi(k)\phi(\ell)\phi(m)}{k\ell m}\\ &+ O\Bigg(\frac{\tau(k)(\log X)^2}{X} + \frac{\tau(\ell)(\log Y)^2}{Y} + \frac{\tau(m)(\log Z)^2}{Z}\Bigg)\Bigg),\end{aligned}$$

where

$$(3.11)\qquad K_{k,\ell,m}(X,Y,Z) = \sum_{\substack{uvt\le X,\ (uvt,k)=1\\ uwt\le Y,\ (uwt,\ell)=1\\ vwt\le Z,\ (vwt,m)=1}} \frac{\mu(uvwt)\mu(t)\tau(t)}{u^2v^2w^2t^3}.$$

We now show that $K_{k,\ell,m}(X,Y,Z)$ converges as $X,Y,Z\to\infty$ and decide its speed of convergence. For this we have to bound the size of

$$\Bigg|\sum_{\substack{uvt\ge X,\ (uvt,k)=1\\ \text{or } uwt\ge Y,\ (uwt,\ell)=1\\ \text{or } vwt\ge Z,\ (vwt,m)=1}} \frac{\mu(uvwt)\mu(t)\tau(t)}{u^2v^2w^2t^3}\Bigg| \le \sum_t \frac{\tau(t)}{t^3} \sum_{\substack{uv\ge \frac{X}{t}\\ \text{or } uw\ge \frac{Y}{t}\\ \text{or } vw\ge \frac{Z}{t}}} \frac{1}{u^2v^2w^2}.$$

We can bound this inner sum as a sum over the three regions $uv \geq \frac{X}{t}$, $uw \geq \frac{Y}{t}$ and $uv \geq \frac{X}{t}$. Since the sums over each region are analogous we only do the region $uv \geq \frac{X}{t}$. By putting $n = uv$ we can bound this sum as

$$\sum_{t} \frac{\tau(t)}{t^3} \sum_{w} \frac{1}{w^2} \sum_{n \geq \frac{X}{t}} \frac{\tau(n)}{n^2} \ll \sum_{t} \frac{\tau(t)}{t^3} \sum_{w} \frac{1}{w^2} \frac{t \log(\frac{X}{t})}{X} \ll \frac{\log X}{X}.$$

Here we have used partial summation and the classical fact [11, §I.3.2] that

$$\sum_{n \leq X} \tau(n) = X \log X + O(X).$$

This gives a total error term of size $O(\frac{\log X}{X} + \frac{\log Y}{Y} + \frac{\log Z}{Z})$.

It thus only remains to compute the value of the completed sum

$$\sum_{\substack{u,v,w,t \\ (uvt,k)=(uwt,\ell)=(vwt,m)=1}} \frac{\mu(uvwt)\mu(t)\tau(t)}{u^2v^2w^2t^3}. \tag{3.12}$$

Because the terms are multiplicative in u, v, w, t, [13, Proposition 11] implies that this sum converges to the Euler product $\prod_p C'_p$. Fix a prime p and let i be the number of elements of $\{k, \ell, m\}$ divisible by p.

- If $i = 0$ then $C'_p = 1 - \frac{3}{p^2} + \frac{2}{p^3} = (1 - \frac{1}{p})^2(1 + \frac{2}{p})$.
- If $i = 1$ then $C'_p = 1 - \frac{1}{p^2} = (1 - \frac{1}{p})(1 + \frac{1}{p})$
- If $i = 2, 3$ then $C'_p = 1$.

It remains to prove that $C_{k,\ell,m} = \frac{\phi(k)\phi(\ell)\phi(m)}{k\ell m} \prod_p C'_p$. This is clearly true since $C_p = C'_p(1 - \frac{1}{p})^i$. This completes the proof. $\square$

From this lemma it now follows by taking $X = \frac{\sqrt{B}}{q\sqrt{af}}, Y = \frac{\sqrt{B}}{\sqrt{af}}, Z = \frac{\sqrt{B}}{\sqrt{qf}}$ and $k = f, \ell = qf, m = 1$ that

$$V(B, a, f) = \frac{B^{\frac{3}{2}}}{q^{\frac{3}{2}}af^2}\left(C_f + O\left(\frac{\tau(f)}{\sqrt{B}}\left(f(\log B)^2 + \sqrt{af}\left(\log \frac{B}{a}\right)^2\right)\right)\right), \tag{3.13}$$

where

$$C_f = \frac{q+1}{q+2} \prod_{p|f} \left(1 + \frac{2}{p}\right)^{-1} \prod_{p} \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right).$$

This formula holds since $q \nmid f$ which is true since $f|a$ and $(q, a) = 1$. We will now compute $W_\chi(B, f)$. Using the formula (3.13) in the definition of

$W_\chi(B,f)$ (3.6) we find that

$$(3.14)\quad W_\chi(B,f) = \frac{B^{\frac{3}{2}}C_f}{q^{\frac{3}{2}}f^2}\sum_{a\le\frac{B}{q^2f}}\frac{\chi(a)\alpha(a)}{a}$$
$$+O\left(\frac{\tau(f)B(\log B)^2}{f}\sum_{a\le\frac{B}{q^2f}}\frac{\alpha(a)}{a}+\frac{B}{f^{\frac{3}{2}}}\sum_{a\le\frac{B}{q^2f}}\frac{\alpha(a)}{a^{\frac{1}{2}}}\left(\log\frac{B}{a}\right)^2\right).$$

To compute the main term we will first compute $\sum_{a\le\frac{B}{q^2f}}\chi(a)\alpha(a)$ and then apply partial summation. We will evaluate this sum using the Selberg–Delange method. See [11, II.5 Theorem 3] for a precise statement of the Selberg–Delange method and the preceding Section II.5.3 for the definition of type $\mathcal{T}$.

Lemma 3.3. *Let χ be a character modulo q and let ψ be the character $(\frac{\cdot}{q})$. Then we have the following. If $\chi=\psi$ or if χ is principal, then*

$$\sum_{a\le x}\chi(a)\alpha(a) = Dx(\log x)^{-\frac{1}{2}}+O(x(\log x)^{-\frac{3}{2}}),$$

where $D=\pi^{-\frac{1}{2}}(1-\frac{1}{q})^{\frac{1}{2}}\prod_p(1-\frac{1}{p})^{-\frac{\psi(p)}{2}}$. Otherwise,

$$\sum_{a\le x}\chi(a)\alpha(a) = O(xe^{-d_1\sqrt{\log x}})$$

for some constant $d_1>0$.

Proof. We first do the case $\chi=\psi$ or χ is principal. If $\chi=\psi$, then the only terms in the sum for which $\alpha(a)$ is non-zero, are by definition the ones such that for all primes $p|a$ we have $\psi(p)=1$. Since ψ is multiplicative this implies that $\psi(a)=1$. Now look at the associated Dirichlet series of this sum

$$F(s)=\sum_n\alpha(n)n^{-s} = \prod_{\substack{p\\ \psi(p)=1}}(1-p^{-s})^{-1}$$
$$=\left(1-\frac{1}{q^s}\right)^{\frac{1}{2}}\zeta(s)^{\frac{1}{2}}L(\psi,s)^{\frac{1}{2}}\prod_{\substack{p\\ \psi(p)=-1}}(1-p^{-2s})^{\frac{1}{2}}.$$

We were able to write the above as this Euler product since α is totally multiplicative. In the following we write $K(s)=\prod_{p,\psi(p)=-1}(1-p^{-2s})^{\frac{1}{2}}$. We will use the classical notation $s=\sigma+it$. For $\sigma>\frac{1}{2}$ we have the inequalities

$$\prod_{\substack{p\\ \psi(p)=-1}}|(1-p^{-2s})^{\frac{1}{2}}|\le\prod_p(1+p^{-2\sigma})^{\frac{1}{2}}\le\prod_p(1-p^{-2\sigma})^{-\frac{1}{2}}=\zeta(2\sigma)^{\frac{1}{2}}.$$

So K is holomorphic and bounded by $\zeta(\frac{3}{2})^{\frac{1}{2}}$ in the region $\operatorname{Reop}(s) > \frac{3}{4}$. It is known [2, Chapter 14] that there exists a constant $c_0 > 0$ such that for every character χ modulo q the Dirichlet series $L(\chi, s)$ has no zeroes in the region

$$\sigma \geq 1 - \frac{c_0}{1 + \log(1 + |t|)},$$

One can get rid of the possible Siegel zero by taking a smaller c_0. We will also require the bound $L(\sigma + it, \psi) \leq (\frac{q|\sigma+it|}{2\pi})^{\frac{3-2\sigma}{4}}\zeta(\frac{3}{2}) \leq (\frac{q}{2\pi})(1+|t|)^{\frac{1}{2}}\zeta(\frac{3}{2})$ for $\frac{1}{2} \leq \sigma \leq 1$, which is the case $\eta = \frac{1}{2}$ of [8, Theorem 3]. Here we used the fact that $q > 2\pi$. Let $c_1 = \min(c_0, \frac{1}{4})$, then the preceding discussion implies that $F(s)$ is of type $\mathcal{T}(\frac{1}{2}, \frac{1}{2}, c_1, \frac{3}{4}, (1+\frac{1}{q^{\frac{3}{4}}})^{\frac{1}{2}}(\frac{q}{2\pi})^{\frac{1}{2}}\zeta(\frac{3}{2}))$. The Selberg–Delange method immediately implies the desired asymptotic formula. For the other characters χ we use the Selberg–Delange method once again. The associated Dirichlet series is

$$\begin{aligned} F(s) = \sum_n \chi(n)\alpha(n)n^{-s} &= \prod_{\substack{p \\ \psi(p)=1}} (1 - \chi(p)p^{-s})^{-1} \\ &= L(\psi, s)^{\frac{1}{2}} L(\chi\psi, s)^{\frac{1}{2}} \prod_{\substack{p \\ \psi(p)=-1}} (1 - p^{-2s})^{\frac{1}{2}}. \end{aligned}$$

So for similar reasons as before $F(s)$ is of type $\mathcal{T}(0, \frac{1}{2}, c_1, \frac{1}{2}, \frac{q}{2\pi}\zeta(\frac{3}{2})^{\frac{3}{2}})$ which by the Selberg–Delange method implies the desired bound. □

To bound the error terms in (3.14) we proceed as follows. the first sum is bounded trivially and gives an error term of

$$O\left(\frac{B\tau(f)}{f}(\log B)^3\right).$$

For the second sum we first use that $(\log \frac{B}{a})^2 \ll (\frac{B}{a})^{\frac{1}{4}}$. We can then apply the lemma for the case of the principal character and partial summation to see that this contributes an error of size

$$O\left(\frac{B^{\frac{3}{2}}\tau(f)}{f^2}(\log B)^{-\frac{1}{2}}\right).$$

We then apply this lemma and partial summation to the sum over a in the main term of (3.14). Combining this with the error above gives us that

$W_\chi(B,f)$ is equal to

$$W_\chi(B,f) = \delta_\chi C_f 2D \frac{B^{\frac{3}{2}}}{q^{\frac{3}{2}} f^2} (\log B)^{\frac{1}{2}} + O\left(\frac{B\tau(f)}{f} (\log B)^3 + \frac{B^{\frac{3}{2}} \tau(f)}{f^2} (\log B)^{-\frac{1}{2}} \right). \tag{3.15}$$

Where $\delta_\chi = 1$ if χ is principal or $(\frac{\cdot}{q})$ and zero otherwise.

The next step is to compute $U_\chi(B)$. If we use (3.15) in its definition (3.7) and bound the sum over the error terms using the divisor bound $\tau(f) \ll_\epsilon f^\epsilon$ [11, Corollary I.5.1.1] with e.g. $\epsilon = \frac{1}{4}$ and the trivial bounds $|\mu(f)\chi(f)\alpha(f)| \leq 1$ we find that

$$U_\chi(B) = \delta_\chi \frac{2D}{q^{\frac{3}{2}}} B^{3/2} \sum_{f \leq \sqrt{\frac{B}{q}}} \frac{\mu(f) C_f}{f^2} \left(\log \frac{B}{f} \right)^{\frac{1}{2}} \alpha(f)\chi(f) + O\left(B^{\frac{3}{2}} (\log B)^{-\frac{1}{2}} \right). \tag{3.16}$$

Note that the only relevant cases are when χ is principal or $(\frac{\cdot}{q})$ since otherwise $\delta_\chi = 0$. In both cases the only non-zero terms are when $\alpha(f) = 1$, i.e. when for every prime $p|f$, one has $(\frac{p}{q}) = 1$. In this case $(\frac{f}{q}) = 1$ so in both cases $\chi(f) = 1$. By the definition of C_f we have $C_f = \prod_{p|f} (1 + \frac{2}{p})^{-1} C_1$ with $C_1 = \frac{q+1}{q+2} \prod_p (1 - \frac{3}{p^2} + \frac{2}{p^3})$, i.e. C_f for $f = 1$. Using trivial bounds we see that the sum $\sum_{f \leq \sqrt{\frac{B}{q}}} \frac{\mu(f)}{f^2} \prod_{p|f} (1 + \frac{2}{p})^{-1} \alpha(f)$ converges to its Euler product

$$\sum_{f \leq \sqrt{\frac{B}{q}}} \frac{\mu(f)}{f^2} \prod_{p|f} \left(1 + \frac{2}{p} \right)^{-1} \alpha(f) = \prod_{\substack{p \\ \psi(p)=1}} \left(1 - \frac{1}{p(p+2)} \right) + O(B^{-\frac{1}{2}}). \tag{3.17}$$

We then apply partial summation to the sum (3.16) and by (3.17) we get

$$U_\chi(B) = \delta_\chi \frac{2C_1 D}{q^{\frac{3}{2}}} \prod_{\substack{p \\ \psi(p)=1}} \left(1 - \frac{1}{p(p+2)} \right) B^{\frac{3}{2}} (\log B)^{\frac{1}{2}} + O\left(B^{\frac{3}{2}} (\log B)^{-\frac{1}{2}} \right). \tag{3.18}$$

Let us write $E = \frac{2C_1D}{q^{\frac{3}{2}}} \prod_{\substack{p \\ \psi(p)=1}} (1 - \frac{1}{p(p+2)})$ to simplify the notation. It then only remains to apply this formula to (3.8), this gives

$$N'_{\mathrm{Br}}(B) = \frac{2E}{q-1} \sum_{s \in S} \left(1 + \left(\frac{s}{q}\right)\right) B^{\frac{3}{2}} (\log B)^{\frac{1}{2}} + O(B^{\frac{3}{2}} \left(\log B)^{-\frac{1}{2}}\right).$$

But by the definition of S (3.1) we know that $(\frac{s}{q}) = 1$ for $s \in S$ and that $|S| = \frac{q-1}{4}$ so we can conclude that

$$N'_{\mathrm{Br}}(B) = EB^{\frac{3}{2}} (\log B)^{\frac{1}{2}} + O\left(B^{\frac{3}{2}} (\log B)^{-\frac{1}{2}}\right). \tag{3.19}$$

Since $N'_{\mathrm{Br}}(B) \leq N_{\mathrm{Br}}(B)$ this implies the desired bound

$$B^{\frac{3}{2}} (\log B)^{\frac{1}{2}} \ll_n N_{\mathrm{Br}}(B).$$

Remark 3.4. One might try to prove a better lower bound by considering multiple such families for varying primes q and adding all of these together. This will give no improvement since as q varies, C_1 and $\prod_{\substack{p \\ \psi(p)=1}} (1 - \frac{1}{p(p+2)})$ are bounded and D goes up to $L((\frac{\cdot}{q}), 1)^{\frac{1}{2}} \ll \log q$ [11, II.8 Theorem 6].

3.2. The upper bound. To find an upper bound we will use the following lemma from [7].

Lemma 3.5. *Let $a, b, c \in \mathbb{Z}$, if there exists an odd prime p such that $v_p(a)$ is odd and $p \nmid bcn$ then $X_{a,b,c} : ax^2 + by^2 + cz^2 = n$ has no integral Brauer–Manin obstruction.*

We can thus bound $N_{\mathrm{Br}}(B)$ by the amount of triples $(a, b, c) \in \mathbb{Z}^3 \cap [-B, B]^3$ such that for all prime divisors $p \mid a$ the integer $v_p(a)$ is even or $p \mid bcn$ and such that $ax^2 + by^2 + cy^2 = n$ has local solutions everywhere. Similarly, for b and c. Such a triple can be written as

$$\begin{aligned} a &= v_a u_{ab} u_{ac} w_{ab} w_{ac} w_{ba}^2 w_{ca}^2 a_1^2, \\ b &= v_b u_{ab} u_{bc} w_{ba} w_{bc} w_{ab}^2 w_{cb}^2 b_1^2, \\ c &= v_c u_{ac} u_{bc} w_{ca} w_{cb} w_{ac}^2 w_{bc}^2 c_1^2. \end{aligned}$$

Here the v_i have only prime factors dividing $2n$ and the u_{ij} and $w_{k\ell}$ are positive squarefree. The u_{ij} and $w_{k\ell}$ are jointly pairwise coprime and each of them is coprime to $2n$. Note first that the existence of local solutions implies that if a prime $p|(a, b, c)$ then $p|2n$. Such a decomposition can then be found as follows:

- The number v_a is the product of all the prime factors, counted with multiplicity, of a dividing $2n$. It also has the same sign as a. The numbers v_b, v_c are analogous.

- The positive squarefree number u_{ab} is the product of the primes $p|(a,b)$, not counted with multiplicity, such that $v_p(a)$ and $v_p(b)$ are both odd and $(p,2n)=1$. Completely analogous for u_{ac}, u_{bc}.
- The positive squarefree number w_{ab} is the product of the prime numbers $p|(a,b)$, also not counted with multiplicity, such that $v_p(a)$ is odd but $v_p(b)$ is even and $(p,2n)=1$. The other $w_{k\ell}$ are analogous.
- The products of the prime factors that are left are squares because of the conditions coming from Lemma 3.5 and can thus be written as a_1^2, b_1^2, c_1^2.

Because the equation $ax^2+by^2+cy^2=n$ needs to have solutions locally everywhere we see that for $p \mid u_{ab}$ we need $(\frac{v_c u_{ac} u_{bc} w_{ca} w_{cb} n}{p})=1$ by looking modulo p. We also have analogous conditions for u_{ac}, u_{bc}. Let now $\epsilon(v)$ be the indicator function of the set $\{v \in \mathbb{Z} : p \mid v \Rightarrow p \mid 2n\}$ and $\delta(u;v)$ be the indicator function of the set

$$\left\{u \in \mathbb{Z} : u \text{ squarefree, and } p \mid u \Rightarrow \left(\frac{v}{p}\right)=1\right\}. \tag{3.20}$$

In particular if u and v are not coprime then $\delta(u;v)=0$. The signs of a,b,c are immaterial in these conditions so we can assume that $a,b,c \geq 0$ and $u_{ab}, u_{ac}, u_{bc} \geq 1$. Summing over a_1, b_1, c_1 and using that there are $O(B^{\frac{1}{2}})$ squares less than B we get the following upper bound for $N_{\mathrm{Br}}(B)$:

$$\ll B^{\frac{3}{2}} \sum_{v_i \leq B} \frac{\epsilon(v_i)}{v_i^{\frac{1}{2}}} \sum_{w_{k\ell} \leq B} \frac{1}{w_{k\ell}^{\frac{3}{2}}} T(B; v_a w_{ab} w_{ac} n, v_b w_{ba} w_{bc} n, v_c w_{ca} w_{cb} n). \tag{3.21}$$

Where i,k,ℓ range over $\{a,b,c\}$ and $k \neq \ell$. We have gotten rid of the coprimality and squarefree conditions on the $w_{k\ell}$ by trivial bounds. Here $T(B;k,\ell,m)$ is the sum

$$\sum\sum\sum_{\substack{u_{ab},u_{ac},u_{bc} \leq B \\ (u_{ab}u_{ac}u_{bc},2k\ell m)=1}} \frac{\delta(u_{bc}; k u_{ab} u_{ac}) \delta(u_{ac}; \ell u_{ab} u_{bc}) \delta(u_{ab}; m u_{ac} u_{bc})}{u_{ab} u_{ac} u_{bc}}. \tag{3.22}$$

We note that the term in this sum is zero unless the u_{ij} are pairwise coprime.

To bound T we will first look at the related quantity

$$\begin{aligned} &S(X,Y,Z;k,\ell,m) \\ &\quad = \sum_{\substack{u_{bc} \leq X \\ (u_{ab}u_{ac}u_{bc},2k\ell m)=1}} \sum_{u_{ac} \leq Y} \sum_{u_{ab} \leq Z} \delta(u_{bc}; k u_{ab} u_{ac}) \delta(u_{ac}; \ell u_{ab} u_{bc}) \delta(u_{ab}; m u_{ac} u_{bc}). \end{aligned} \tag{3.23}$$

In particular, we will prove the following lemma.

Lemma 3.6. *For $X, Y, Z \geq 2$ and $k, \ell, m \in \mathbb{N} \setminus \{0\}$ we have the bound*

$$S(X,Y,Z;k,\ell,m) \ll (k\ell m)^{\frac{1}{4}} XYZ\Big[(\log X \log Y \log Z)^{-\frac{1}{2}} + (\log X \log Y \log Z)^{-2}\Big((\log X)^{\frac{5}{2}} + (\log Y)^{\frac{5}{2}} + (\log Z)^{\frac{5}{2}}\Big)\Big].$$

Now assuming this lemma and applying partial summation thrice we get the inequality

$$T(B;k,\ell,m) \ll (k\ell m)^{\frac{1}{4}} (\log B)^{\frac{3}{2}}.$$

Applying this to (3.21) and summing over the w_{ij} we find that

$$N_{\mathrm{Br}}(B) \ll_n B^{\frac{3}{2}} (\log B)^{\frac{3}{2}} \sum_{v_i \leq B} \frac{\epsilon(v_i)}{v_i^{\frac{1}{4}}}.$$

Since all the terms are positive and ϵ is completely multiplicative we can complete the sum and write it as a convergent Euler product. We conclude that

$$N_{\mathrm{Br}}(B) \ll_n B^{\frac{3}{2}} (\log B)^{\frac{3}{2}} \sum_{v_i} \frac{\epsilon(v_i)}{v_i^{\frac{1}{4}}} = B^{\frac{3}{2}} (\log B)^{\frac{3}{2}} \prod_{p \mid 2n} (1 - p^{-\frac{1}{4}})^{-3}$$

as desired.

We will now prove Lemma 3.6.

Proof. Note that $S(X,Y,Z;k,\ell,m)$ does not change if we permute $(X,k), (Y,\ell), (Z,m)$. Moreover, we have the trivial inequality

$$S(X,Y,Z;k,\ell,m) \leq XYZ. \tag{3.24}$$

If $\max(\log X, \log Y, \log Z) \geq \min(\log X \log Y, \log X \log Z, \log Y \log Z)^4$, then we can use the trivial inequality. Let us assume without loss of generality that $X \geq Y, Z$ so by assumption $\log X \geq (\log Y \log Z)^4$. We then find that

$$S(X,Y,Z;k,\ell,m) \ll XYZ(\log X)^{\frac{1}{2}} (\log Y \log Z)^{-2}.$$

In this case the lemma is true.

We now assume that

$$\max(\log X, \log Y, \log Z) \leq \min(\log X \log Y, \log X \log Z, \log Y \log Z)^4. \tag{3.25}$$

We can rewrite $S(X,Y,Z;k,\ell,m)$ using the equality

$$\delta(u;v) = 1_{(u,v)=1} \frac{\mu^2(u)}{\tau(u)} \sum_{d \mid u} \left(\frac{v}{d}\right). \tag{3.26}$$

By $1_{(u,v)=1}$ we mean the indicator function of the set $\{u \in \mathbb{Z} : (u,v) = 1\}$. This equality is true since both sides are multiplicative in u and it is trivial when u is a prime power from the definition (3.20). Then we can write $u_{bc} = d_1 f_1, u_{ac} = d_2 f_2, u_{bc} = d_3 f_3$ to get that $S(X, Y, Z; k, \ell, m)$ is equal to

$$(3.27) \quad \sum_{W(X,Y,Z)} \frac{\mu(d_1 d_2 d_3 f_1 f_2 f_3)^2}{\tau(d_1 d_2 d_3 f_1 f_2 f_3)} \left(\frac{k d_2 f_2 d_3 f_3}{d_1}\right)\left(\frac{\ell d_1 f_1 d_3 f_3}{d_2}\right)\left(\frac{m d_1 f_1 d_2 f_2}{d_3}\right).$$

Where $W(X, Y, Z)$ is the set of tuples $(d_1, d_2, d_3, f_1, f_2, f_3) \in (\mathbb{N}\backslash\{0\})^6$ such that

$$d_1 f_1 \le X, d_2 f_2 \le Y, d_3 f_3 \le Z \text{ and } (d_1 d_2 d_3 f_1 f_2 f_3, 2k\ell m) = 1$$

Now by quadratic reciprocity and since the d_i are odd, the factor

$$\left(\frac{d_2 d_3}{d_1}\right)\left(\frac{d_1 d_3}{d_2}\right)\left(\frac{d_1 d_2}{d_3}\right)$$

only depends on the classes of d_1, d_2, d_3 modulo 4. We can thus write this as a sum of characters

$$(3.28) \quad \left(\frac{d_2 d_3}{d_1}\right)\left(\frac{d_1 d_3}{d_2}\right)\left(\frac{d_1 d_2}{d_3}\right) = \sum_{\psi_1}\sum_{\psi_2}\sum_{\psi_3} a_{\psi_1,\psi_2,\psi_3}\psi_1(d_1)\psi_2(d_2)\psi_3(d_3).$$

Here ψ_1, ψ_2, ψ_3 range over all characters modulo 4 and a_{ψ_1,ψ_2,ψ_3} are some complex constants. After applying the equality (3.28) to (3.27) and switching the sums we see that we only have to bound each term corresponding to the characters ψ_1, ψ_2, ψ_3 separately. We put $\chi_1 = \psi_1(\,\cdot\,)(\frac{k}{\cdot}), \chi_2 = \psi_2(\,\cdot\,)(\frac{\ell}{\cdot}), \chi_3 = \psi_3(\,\cdot\,)(\frac{m}{\cdot})$, these are characters modulo $4k, 4\ell, 4m$ respectively. The corresponding term is

$$(3.29) \quad \sum_{W(X,Y,Z)} \frac{\mu(d_1 d_2 d_3 f_1 f_2 f_3)^2}{\tau(d_1 d_2 d_3 f_1 f_2 f_3)} \chi_1(d_1)\left(\frac{f_2 f_3}{d_1}\right)\chi_2(d_2)\left(\frac{f_1 f_3}{d_2}\right)\chi_3(d_3)\left(\frac{f_1 f_2}{d_3}\right).$$

A similar sum but with only 4 variables was investigated in [3]. We will follow their approach, for this we will need Lemma 1 and 2 from that paper.

Lemma 3.7. *Let α_n, β_m be complex numbers supported on odd integers of absolute value ≤ 1. For all real numbers $N, M > 1$ we have the inequality*

$$\sum_{\substack{n \le N \\ m \le M}} \alpha_n \beta_m \left(\frac{m}{n}\right) \ll \left(N^{\frac{5}{6}} M + N M^{\frac{5}{6}}\right)(\log NM)^{\frac{7}{6}}.$$

Lemma 3.8. *Let $\chi \bmod q$ be a Dirichlet character and d an integer such that $(d, q) = 1$, then for $x \ge 2$ and for all $C > 0$ we have*

$$\sum_{\substack{n \le x \\ (n,d)=1}} \frac{\mu(n)^2}{\tau(n)} \chi(n) = \delta_\chi c(dq) \frac{x}{\sqrt{\log x}} \left\{1 + O\left(\frac{(\log\log 3dq)^{\frac{3}{2}}}{\log x}\right)\right\} + O_C(\tau(d) q x (\log x)^{-C}).$$

Here $\delta_\chi = 1$ *if* χ *is principal,* $\delta_\chi = 0$ *otherwise and*

$$c(r) = \pi^{-\frac{1}{2}} \prod_p \Big(1 + \frac{1}{2p}\Big)\Big(1 - \frac{1}{p}\Big)^{\frac{1}{2}} \prod_{p|r} \Big(1 + \frac{1}{2p}\Big)^{-1}.$$

In particular when $d = 1$ and χ is principal this gives

$$\sum_{n \le x} \frac{\mu(n)^2}{\tau(n)} \ll x(\log x)^{-\frac{1}{2}}. \tag{3.30}$$

Let now $V \ge 1$ be a parameter which will be chosen later as a negative power of $k\ell m$ times a large power of $\log X \log Y \log Z$. We will split the sum (3.29) into different regions which we will bound separately. Some of these regions will overlap. Because of inclusion-exclusion it suffices to bound the intersections of these regions separately. The regions are as follows:

(1) The first regions are those of the form $d_i, f_j > V$ where $i \neq j$. All of these sums are analogous so we may assume that $i = 1, j = 2$. Certain regions will then be counted twice, to use inclusion-exclusion we will thus be required to bound regions of the type $d_1, f_2 > V$ and some subset of the integers d_2, d_3, f_1, f_3 will also have to be larger than V.
(2) Another type of region we consider is $d_i, d_j, f_i, f_j \le V$ and $d_k, f_k > V$ for $\{i, j, k\} = \{1, 2, 3\}$.
(3) The third regions are given by $d_1, d_2, d_3 \le V$ and $f_1, f_2, f_3 \le V$.
(4) The regions in (3) overlap so we will have also have to bound the region $d_1, d_2, d_3, f_1, f_2, f_3 \le V$.

We consider first the regions of the form $d_1, f_2 > V$ with a possible condition on d_2, d_3, f_1, f_3. Now look at this region in (3.29), move the sum over d_1, f_2 to the inside and apply trivial bounds to the terms which only depend on d_2, d_3, f_1, f_3, this also removes all the coprimality conditions except those of d_1, f_2. Put $t = 2k\ell m d_2 d_3 f_1 f_3$. After doing this we find that this region is bounded by

$$\ll \sum_{f_1 \le XV^{-1}} \sum_{d_2 \le YV^{-1}} \sum_{d_3 f_3 \le Z} \Bigg| \sum_{\substack{V < d_1 \le \frac{X}{f_1} \\ (d_1, t) = 1}} \sum_{\substack{V < f_2 \le \frac{Y}{d_2} \\ (f_2, t) = 1}} \frac{\mu(2 d_1 f_2)^2}{\tau(d_1 f_2)} \chi_1(d_1) \Big(\frac{f_2 f_3}{d_1}\Big) \Bigg|.$$

Apply Lemma 3.7 to the sum over d_1 and f_2 with $\alpha_n = \beta_m = 0$ for $n, m \le V$. We find that the above sum is bounded by

$$\begin{aligned} &\ll \sum_{f_1 \le XV^{-1}} \sum_{d_2 \le YV^{-1}} \sum_{d_3 f_3 \le Z} \Bigg(\Big(\frac{X}{f_1}\Big)^{\frac{5}{6}} \frac{Y}{d_2} + \frac{X}{f_1}\Big(\frac{Y}{d_2}\Big)^{\frac{5}{6}}\Bigg)(\log XY)^{\frac{7}{6}} \\ &\ll XYZV^{-\frac{1}{6}}(\log X \log Y)^{\frac{13}{6}} \log Z \ll XYZV^{-\frac{1}{6}}(\log X \log Y \log Z)^{\frac{13}{6}}. \end{aligned} \tag{3.31}$$

We can bound the regions $d_i, d_j, f_i, f_j \leq V$ and $d_k, f_k > V$ for $\{i,j,k\} = \{1,2,3\}$ via trivial bounds by

$$\ll V^4(X\log X + Y\log Y + Z\log Z). \tag{3.32}$$

The region $d_1, d_2, d_3, f_1, f_2, f_3 \leq V$ is trivially bounded by

$$V^6. \tag{3.33}$$

There remain two regions to be bounded, $f_1, f_2, f_3 \leq V$ and $d_1, d_2, d_3 \leq V$. These are analogous but the first one is slightly more involved due to the presence of the characters χ_i so we will only explain the treatment of that one here. The relevant sum is

$$\sum_{\substack{W(X,Y,Z) \\ f_1<V, f_2<V, f_3<V}} \frac{\mu(d_1d_2d_3f_1f_2f_3)^2}{\tau(d_1d_2d_3f_1f_2f_3)} \chi_1(d_1)\left(\frac{f_2f_3}{d_1}\right)\chi_2(d_2)\left(\frac{f_1f_3}{d_2}\right)\chi_3(d_3)\left(\frac{f_1f_2}{d_3}\right).$$

We will now estimate the inner sum depending on the values of f_1, f_2, f_3. Note that since the terms are zero unless f_1, f_2, f_3 are pairwise coprime squarefree integers, f_if_j is a square for $i \neq j$ only if $1 = f_i = f_j$. The first case is $1 = f_1 = f_2 = f_3$. One can first get rid of the coprimality conditions and the characters χ_1, χ_2, χ_3 by trivial bounds. After applying $\sum_{n \leq x} \mu(n)^2/\tau(n) \ll x(\log x)^{-\frac{1}{2}}$ three times to the sums over d_1, d_2, d_3 we see that the contribution of this part is

$$\ll XYZ(\log X \log Y \log Z)^{-\frac{1}{2}}. \tag{3.34}$$

The second part is when exactly two of f_1, f_2, f_3 are equal to 1, we may assume that $f_2 = f_3 = 1$ by symmetry. We first apply trivial bounds to remove all the coprimality conditions not involving d_2 and the characters χ_1, χ_3. By applying Lemma 3.8 to the sum over d_2 and using that $\chi_2(\,\cdot\,)(\frac{f_1}{\cdot})$ is a non-principal character of conductor at most $4\ell f_1$ since $(f_1, 2\ell) = 1$ we get a bound

$$\begin{aligned}
&\ll_C \ell \sum_{f_1 \leq V} \frac{f_1}{\tau(f_1)} \sum_{d_1 \leq \frac{X}{f_1}} \sum_{d_3 \leq Z} \frac{\mu(d_1d_3f_1)^2}{\tau(d_1d_3)} \tau(d_1d_3k\ell m) Y(\log Y)^{-C} \\
&\ll \tau(k\ell m)\ell XYZ \sum_{f_1 \leq V} \frac{1}{\tau(f_1)} \ll \tau(k\ell m)\ell VXYZ(\log Y)^{-C}
\end{aligned}$$

for all $C > 0$. By instead applying Lemma 3.8 to the sum over d_3 we get a similar bound with (ℓ, Y) and (m, Z) switched. Bounding by their geometric mean and finding similar contributions for the other situations when two of f_1, f_2, f_3 are equal to 1 we get a total bound for this part of

$$\begin{aligned}(3.35)\quad \ll_C \tau(k\ell m)VXYZ\Big(\sqrt{k\ell}(\log X\log Y)^{-\frac{C}{2}} + \sqrt{km}(\log X\log Z)^{-\frac{C}{2}}\\ + \sqrt{\ell m}(\log Y\log Z)^{-\frac{C}{2}}\Big).\end{aligned}$$

The last part is when none of the f_1f_2, f_1f_3, f_2f_3 are equal to 1. We apply Lemma 3.8 to the sum over d_1 where we use that $\chi_1(\cdot)(\frac{f_2f_3}{\cdot})$ is a non-principal character of conductor at most $4kf_2f_3$ since $(f_2f_3, 2k) = 1$. For the other sums use trivial bounds to get

$$\ll_C k \sum_{f_1,f_2,f_3\leq V} \frac{f_2f_3}{\tau(f_1f_2f_3)} \sum_{\substack{d_2\leq \frac{Y}{f_2}\\ d_3\leq\frac{Z}{f_3}}} \frac{\mu(d_2d_3f_1f_2f_3)^2}{\tau(d_2d_3)}\tau(f_1d_2d_3k\ell m)X(\log X)^{-C}$$

$$\ll \tau(k\ell m)kV^3XYZ(\log X)^{-C}.$$

By applying Lemma 3.8 instead to the sums over d_2, d_3 we get similar bounds so we may bound the sum by their geometric mean

$$(3.36)\qquad \ll_C \tau(k\ell m)(k\ell m)^{\frac{1}{3}}V^3XYZ(\log X\log Y\log Z)^{-\frac{C}{3}}.$$

We can now take for example $V = \frac{(\log X\log Y\log Z)^{20}}{\sqrt{k\ell m}}$ and $C = 300$, we have assumed that $V \geq 1$ but if $\frac{(\log X\log Y\log Z)^{20}}{\sqrt{k\ell m}} \leq 1$ then we can use the trivial inequality (3.24) to find that

$$S(X,Y,Z;k,\ell,m) \ll (k\ell m)^{\frac{1}{4}}XYZ(\log X\log Y\log Z)^{-10}.$$

Using this choice we get the desired bound for (3.31), (3.33), (3.34). By applying the divisor bound and the divisor bound $\tau(k\ell m) \ll (k\ell m)^{\frac{1}{4}}$ we get the correct bound in (3.36). If we use the assumption (3.25) to remove the large log power in the variable with the linear factor we can bound (3.32) correctly. Lastly, to bound (3.35) we use assumption (3.25) to get rid of the log powers in the variable with a positive exponent for the logarithm and apply the divisor bound $\tau(k\ell m) \ll (k\ell m)^{\frac{1}{4}}$. □

References

[1] J.-L. Colliot-Thélène & F. Xu, "Brauer–Manin obstruction for integral points of homogeneous spaces and representation by integral quadratic forms", *Compos. Math.* **145** (2009), no. 2, p. 309-363, With an appendix by Dasheng Wei and Xu.

[2] H. Davenport, *Multiplicative number theory*, second ed., Graduate Texts in Mathematics, vol. 74, Springer, 1980, Revised by Hugh L. Montgomery, xiii+177 pages.

[3] J. Friedlander & H. Iwaniec, "Ternary quadratic forms with rational zeros", *J. Théor. Nombres Bordeaux* **22** (2010), no. 1, p. 97-113.

[4] A. Grothendieck, "Le groupe de Brauer. I, II, III", in *Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics, vol. 3, North-Holland, 1968, p. 1-188.

[5] M. Kneser, "Darstellungsmasse indefiniter quadratischer Formen", *Math. Z.* **77** (1961), p. 188-194.

[6] Y. V. Matiyasevich, *Hilbert's tenth problem*, Foundations of Computing Series, MIT Press, 1993, Translated from the 1993 Russian original by the author, With a foreword by Martin Davis, xxiv+264 pages.

[7] V. Mitankin, "Failures of the integral Hasse principle for affine quadric surfaces", *J. Lond. Math. Soc.* **95** (2017), no. 3, p. 1035-1052.

[8] H. Rademacher, "On the Phragmén–Lindelöf theorem and some applications", *Math. Z.* **72** (1959/1960), p. 192-204.

[9] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer, 1973, Translated from the French, viii+115 pages.

[10] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001, viii+187 pages.

[11] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, 1995, Translated from the second French edition (1995) by C. B. Thomas, xvi+448 pages.

[12] L. Tóth, "The probability that k positive integers are pairwise relatively prime", *Fibonacci Q.* **40** (2002), no. 1, p. 13-18.

[13] ———, "Multiplicative arithmetic functions of several variables: a survey", in *Mathematics without boundaries*, Springer, 2014, p. 483-514.

Tim Santens
Departement Wiskunde
KU Leuven
Celestijnenlaan 200B
3001 Heverlee, Belgium
E-mail: tim.santens@kuleuven.be