Invent. math.
https://doi.org/10.1007/s00222-022-01114-z

Integral points on Markoff type cubic surfaces

Amit Ghosh[1] · **Peter Sarnak**[2,3]

Received: 14 September 2019 / Accepted: 24 March 2022

Abstract For integers k, we consider the affine cubic surface V_k given by $M(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3 = k$. We show that for almost all k the Hasse Principle holds, namely that $V_k(\mathbb{Z})$ is non-empty if $V_k(\mathbb{Z}_p)$ is non-empty for all primes p, and that there are infinitely many k's for which it fails. The Markoff morphisms act on $V_k(\mathbb{Z})$ with finitely many orbits and a numerical study points to some basic conjectures about these "class numbers" and Hasse failures. Some of the analysis may be extended to less special affine cubic surfaces.

Mathematics Subject Classification 11D25 · 11D45

1 Introduction

Little is known about the values at integers assumed by *affine cubic forms* F in three variables. Unless otherwise stated, by an *affine form* f in n-variables

✉ Peter Sarnak
sarnak@math.ias.edu

Amit Ghosh
ghosh@okstate.edu

[1] Department of Mathematics, Oklahoma State University, 401 MSCS, Monroe St., Stillwater, OK 74078, USA

[2] School of Mathematics, Institute for Advanced Study, Einstein Dr., Princeton, NJ 08540, USA

[3] Department of Mathematics, Princeton University, Fine Hall, Princeton, NJ 08540, USA

Published online: 30 May 2022

we mean $f \in \mathbb{Z}[x_1, \ldots, x_n]$ whose leading homogeneous term f_0 is non-degenerate [1] and such that $f - k$ is (absolutely) irreducible for all constants k. For $k \in \mathbb{Z}$, set

$$V_{k,F} = \{\mathbf{x} = (x_1, x_2, x_3) : \ F(\mathbf{x}) = k\}, \tag{1}$$

and $\mathfrak{v}_F(k) := |V_{k,F}(\mathbb{Z})|$. The basic question is for which k is $V_{k,F}(\mathbb{Z}) \neq \emptyset$, or more generally infinite or Zariski dense in $V_{k,F}$?

A prime example is $F = S$, the sum of three cubes:

$$S(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3. \tag{2}$$

There are obvious local congruence obstructions, namely that $V_{k,S}(\mathbb{Z}) = \emptyset$ if $k \equiv 4$ or 5 (m*od* 9), but beyond that it is possible that the answers to all three questions is yes for all the other k's, which we call the *admissible* values (see [20,38]). It is known that strong approximation in its strongest form fails for $V_{k,S}(\mathbb{Z})$; the global obstruction coming from an application of cubic reciprocity [16,18,28]. Moreover, [33] and [3] show that $V_{1,S}(\mathbb{Z})$ is Zariski dense in $V_{1,S}$.

The case when the cubic polynomial $F(x_1, x_2, x_3)$ factors into linear factors can be studied algebraically using divisor theory, and is apparently quite different to our irreducible F. If F is the split norm form $N(\mathbf{x}) = x_1x_2x_3$, then every $V_{k,N}$ is non-empty, and for k non-zero, $\mathfrak{v}_N(k)$ is finite and is a divisor function.

For a $\mathbb{Q}$-anistropic torus given by $N(\mathbf{x}) = Nm_{K/\mathbb{Q}}(\alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3)$, where α_1, α_2, α_3 is a $\mathbb{Z}$-basis of an order in a cubic number field K, the Dirichlet Unit Theorem coupled with the action $\mathbf{w} \to u\mathbf{w}$ of the unit group on the homogeneous space and the theory of divisors, allows for the study of $V_{k,N}(\mathbb{Z})$. It consists of a finite number $\mathfrak{h}_N(k)$ of orbits (putting $\mathfrak{h}_N(k) = \mathfrak{v}_N(k) = 0$ if $V_{k,N} = \emptyset$), is infinite if it is non-empty and is Zariski dense if K is totally real. The dependence of $\mathfrak{h}_N(k)$ on k is subtle, especially if the class number H of the order is not one. Most k's are not represented; in fact [40] shows that

$$\big|\{|k| \leq X : \mathfrak{v}_N(k) \neq 0\}\big| \sim \frac{1}{H}\big|\{|k| \leq X : k \text{ admissible}\}\big| \sim C\,X(\log X)^{-\frac{2}{3}}, \tag{3}$$

as $X \to \infty$. The question of the density of Hasse failures for norms of elements in a number field K is studied in [14].

To measure the richness of representations by f, we say that f is *perfect* if $V_{k,f}(\mathbb{Z})$ is Zariski dense in $V_{k,f}$ for all but finitely many admissible k's; we

[1] That is it cannot be transformed to a polynomial of fewer than n variables by a linear change of variables.

say it is *almost perfect* if the same holds for almost all admissible k (in the sense of natural density); and f is *full* if $\mathfrak{v}_f(k) \to \infty$ as $k \to \infty$ for almost all admissible k's. For an affine form, it follows from [32] and [41] that the admissible k's are given in terms of a congruence condition as in the case of S.

Much more is known about cubic forms in the "subcritical" case of forms in four or more variables or diagonal forms $f = x_1^{a_1} + \ldots + x_b^{a_b}$ with $\sum_{j=1}^{b} a_j^{-1} > 1$ and $b \geq 3$ (see [11,30,45] for example) and in the "super-critical" case of two variables [24]. The basic analytic feature in the subcritical case is that the average number of representations of k is $k^{\delta}(\log k)^A$ for some $\delta > 0$, while in the critical case, $\delta = 0$. If f is a cubic polynomial, $n \geq 10$ and f_0 is nonsingular then f is perfect [13].[2] In a recent paper [30], it is shown that if $f = f_0$ and is nonsingular with $n \geq 5$, then f is full, while conditional on the Riemann Hypothesis for certain Hasse-Weil L-functions, the same is true for $n \geq 4$. Moreover, it is conjectured there that any such f with $n \geq 4$ is perfect. For cubic f in two variables (supercritical case) the celebrated theorems [44], [43] assert that $V_{k,f}(\mathbb{Z})$ is finite and moreover only for very few of the admissible k's is $V_{k,f}(\mathbb{Z})$ non-empty [42].

Returning to the critical dimension $n = 3$ for affine cubic forms, there are well-known examples of F which are not perfect, see ([17,37])[3] and also our example of M below; however it is possible that F is always full (see the discussion at the end of the Introduction).

This paper is concerned with $F = M$ where

$$M(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3. \tag{4}$$

The affine cubic surface $V_{0,M}(\mathbb{Z})$ was studied by Markoff [35,36]; the points $(x_1, x_2, x_3) \in V_{0,M}(\mathbb{Z})$ with $x_j \in \mathbb{N}$ being essentially the "Markoff triples". The reason that one can study $V_{0,M}(\mathbb{Z})$, or more generally $V_{k,M}(\mathbb{Z})$ is that there is a descent group action albeit non-linear. The Vieta involutions $\mathcal{V}_j$ with $\mathcal{V}_1(x_1, x_2, x_3) = (x_2x_3 - x_1, x_2, x_3)$ and similarly for $\mathcal{V}_2$, $\mathcal{V}_3$, preserve M, as do permutations of the x_j's and switching the signs of two of the x_j's. We denote by Γ the group of polynomial affine transformations generated as above. Then, Γ preserves $V_{k,M}(\mathbb{Z})$ and except for the case of the Cayley cubic with $k = 4$ (see Sect. 4.3), $V_{k,M}(\mathbb{Z})$ decomposes into a finite number $\mathfrak{h}_M(k)$ of Γ-orbits. For example, if $k = 0$, then $\mathfrak{h}_M(0) = 2$ corresponds to the orbits

[2] They show that $|V_{k,f}(\mathbb{Z})| = \infty$ for k admissible from an asymptotic count which is flexible enough to deduce that $V_{k,f}(\mathbb{Z})$ is Zariski dense in $V_{k,f}$.

[3] The projective cubic surface for [17], namely $F(x_1, x_2, x_3) = 10x_4^3$ with $F(x_1, x_2, x_3) = 5x_1^3 + 12x_2^3 + 9x_3^3$, fails the Hasse principle over $\mathbb{Q}$; from which it follows that $V_{k,F}(\mathbb{Z})$ fails the Hasse principle over $\mathbb{Z}$ for $k = 10w^3$. There are many other such projective cubic surfaces over $\mathbb{Q}$ (see Sect. 4 of [12]).

of (0, 0, 0) and (3, 3, 3) [36]. If $V_{k,M}(\mathbb{Z}) \neq \emptyset$ (so that $\mathfrak{h}_M(k) > 0$) and $k \geq 5$ or $k < 0$ with k not a square, which will be our cases of interest, then each Γ-orbit is infinite and even Zariski dense in $V_{k,M}$ (see [15,21] and Sect. 5). In particular, for $k \geq 5$ and k not a square, or $k \leq 0$

$$V_{k,M}(\mathbb{Z}) \neq \emptyset \quad \text{iff} \quad V_{k,M}(\mathbb{Z}) \text{ is Zariski dense in } V_{k,M}. \tag{5}$$

Moreover, $V_{k,M}(\mathbb{Z})$ contains polynomial parametric solutions $\mathbf{x}(t)$ if and only if $k = 4 + \nu^2$, in which case it contains a line (see Sect. 5 for a direct proof). In [10] and [9], it is shown that these affine cubic surfaces with $V_{k,M}(\mathbb{Z}) \neq \emptyset$ satisfy a form of strong approximation,[4] after taking into account the possible finite orbits of Γ in $V_{k,M}(\bar{\mathbb{Q}})$. Our goal in this paper is to study the set of k's for which $\mathfrak{h}_M(k) > 0$.

The first issue is to determine the congruence obstructions for k. This is elementary and in Sect. 6 we show that $V_{k,M}(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset$ unless $k \equiv 3 \pmod 4$ or $k \equiv \pm 3 \pmod 9$. Recall that k is admissible means k does not satisfy any of these congruences. The number of $0 < k \leq K$ (or $0 < -k \leq K$) which are admissible is $\frac{7}{12}K + O(1)$. Any admissible k for which $\mathfrak{h}(k) = 0$ is called a Hasse failure (since in this case $V_{k,M}(\mathbb{Z})$ is empty but there is no congruence obstruction).

In order to study $\mathfrak{h}_M(k)$ both theoretically and numerically, we give an explicit reduction (descent) for the action of Γ on $V_{k,M}(\mathbb{Z})$. For this purpose, it is convenient to remove an explicit set of special admissible k's, namely those for which there is a point in $V_{k,M}(\mathbb{Z})$ with $|x_j| = 0,\ 1$ or 2. These k's take the form (i) $k = u^2 + v^2$ or (ii) $4(k-1) = u^2 + 3v^2$ or (iii) $k = 4 + u^2$. The number of these special k's (which we refer to as *exceptional*) with $0 \leq k \leq K$ is asymptotic to $C' \frac{K}{\sqrt{\log K}}$. The remaining admissible k's are called *generic* (all negative admissible k's are generic). For them, we have the following elegant reduced forms

Theorem 1.1 *(i). Let $k \geq 5$ be generic and consider the compact set*

$$\mathfrak{F}_k^+ = \{\mathbf{u} \in \mathbb{R}^3 : 3 \leq u_1 \leq u_2 \leq u_3\,,\ u_1^2 + u_2^2 + u_3^2 + u_1u_2u_3 = k\}.$$

The points in $\mathfrak{F}_k^+(\mathbb{Z}) = \mathfrak{F}_k^+ \cap \mathbb{Z}^3$ are Γ-inequivalent, and any $\mathbf{x} \in V_{k,M}(\mathbb{Z})$ is Γ-equivalent to a unique point $\mathbf{u}' = (-u_1, u_2, u_3)$ with $\mathbf{u} = (u_1, u_2, u_3) \in \mathfrak{F}_k^+(\mathbb{Z})$.

(ii). Let $k < 0$ be admissible and consider the compact set

$$\mathfrak{F}_k^- = \{\mathbf{u} \in \mathbb{R}^3 : 3 \leq u_1 \leq u_2 \leq u_3 \leq \frac{1}{2}u_1u_2\,,\ u_1^2 + u_2^2 + u_3^2 - u_1u_2u_3 = k\}.$$

[4] In its strongest form this fails as is shown using quadratic reciprocity in Sect. 8, see (20).

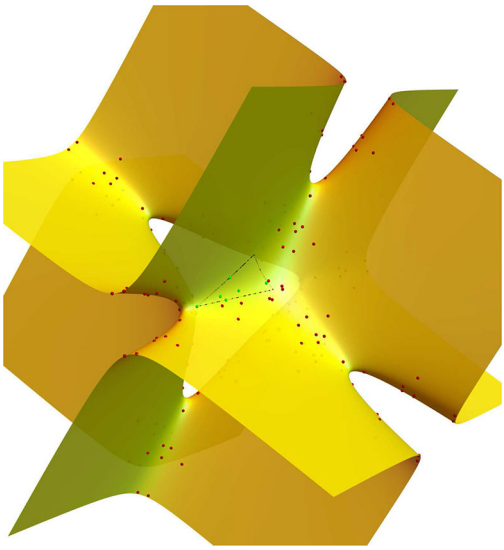

Fig. 1 Lattice points and fundamental set (triangular) for $k = 3685$

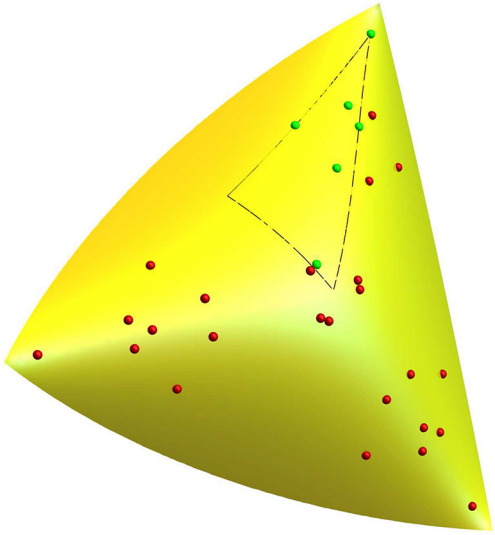

Fig. 2 Closeup of fundamental set (triangular) for $k = 3685$

The points in $\mathfrak{F}_k^-(\mathbb{Z}) = \mathfrak{F}_k^- \cap \mathbb{Z}^3$ *are* Γ*-inequivalent, and any* $\mathbf{x} \in V_{k,M}(\mathbb{Z})$ *is* Γ*-equivalent to a unique point* $\mathbf{u} = (u_1, u_2, u_3) \in \mathfrak{F}_k^-(\mathbb{Z})$.

The Theorem is illustrated for $k > 5$ in Figs. 1 and 2 with $k = 3685$ where $\mathfrak{h}_M(3685) = 6$, and for $k < 0$ in Figs. 3 and 4 with $k = -3691$, where $\mathfrak{h}_M(-3691) = 9$. The lattice points $V_{k,M}(\mathbb{Z})$ are highlighted and the fundamental sets indicated in a polygonal region.

Some simple consequences of Theorem 1.1 are (see the discussion in Sect. 2 and also Secs. 7 and 8) :

Fig. 3 Lattice points and fundamental set for $k = -3691$

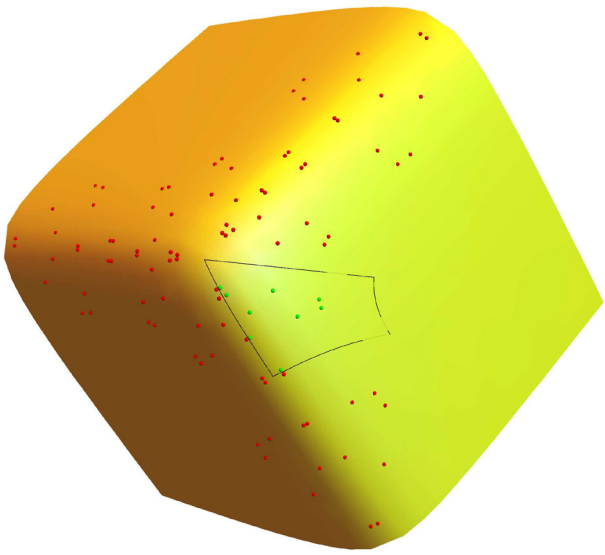

Fig. 4 Closeup of fundamental set for $k = -3691$

(a). $V_{46}(\mathbb{Z}) = \emptyset$, that is $\mathfrak{h}_M(46) = 0$, this being the first positive Hasse failure.
(b). $\mathfrak{h}_M(-2) = 1$ with all solutions equivalent to the point $(3, 3, 4)$; while $k = -4$ is the first negative Hasse failure.
(c). $\mathfrak{h}_M(k) \ll_\varepsilon |k|^{\frac{1}{3}+\varepsilon}$ as $k \to \pm\infty$. This follows from the fact that when considering the values taken by the corresponding indefinite quadratic

form in the y and z variable, for each fixed x, the units are bounded in number due to the restrictions imposed by the fundamental sets.

(d). Let $\mathfrak{h}_M^{\pm}(k) = |\mathfrak{F}_k^{\pm}(\mathbb{Z})|$ where $\pm = \mathrm{sgn}(k)$, this being defined for any k. Then Theorem 1.1 implies that for generic k, $\mathfrak{h}_M^{\pm}(k) = \mathfrak{h}_M(k)$ while otherwise $\mathfrak{h}_M(k) \leq \mathfrak{h}_M^{\pm}(k)$. We have

$$\sum_{\substack{k\neq 4\\ |k|\leq K}} \mathfrak{h}_M^{\pm}(k) \sim C^{\pm} K (\log K)^2, \tag{6}$$

where $C^{\pm} > 0$ and $K \to \infty$ (see Lemmas 7.2 and 7.3).

So, as expected in this case of critical dimension 3, the numbers $\mathfrak{h}_M(k)$ are small on average. On the other hand the fact that this average grows, albeit very slowly, is a key feature as it suggests that $\mathfrak{h}_M(k)$ might be non-zero for many k's. In Sect. 10, we report on some numerical experiments using Theorem 1.1 to find the Hasse failures among the generic k's when $0 < k < 6 \times 10^8$. These suggest that

$$\sum_{\substack{0<k\leq K\\ k \text{ admissible}\\ \mathfrak{h}_M(k)=0}} 1 \sim C_0 K^{\theta}, \tag{7}$$

with $C_0 > 0$ and $\theta \approx 0.8875\ldots$ We also provide results concerning other statistics for the $\mathfrak{h}_M(k)$'s for k near this range (see Sect. 10 for the numerics concerning the numbers $\mathfrak{h}_M(k)$ and some conjectures that these support).

Our main result concerns the values assumed by M and the Hasse failures in (7); we prove that M is almost perfect but not perfect.

Theorem 1.2 *(i). There are infinitely many Hasse failures. More precisely, the number of* $0 < k \leq K$ *and* $-K \leq k < 0$ *for which the Hasse Principle fails is at least* $\sqrt{K}(\log K)^{-\frac{1}{2}}$ *for* K *large.*

(ii). M is almost perfect, that is

$$\#\big\{|k| \leq K : k \text{ admissible},\ \mathfrak{h}_M(k) = 0\big\} = o(K),$$

as $K \to \infty$ and for almost all admissible k, $V_k(\mathbb{Z})$ is Zariski dense in V_k.

Remark 1.3(a). The proof of (i) is based on quadratic reciprocity and a global factorization that arises for special k's connected to the singular Cayley cubic $V_{4,M}$. If $k = 4 + \beta\nu^2$, with β carefully chosen and ν's having its prime factors in certain arithmetic progressions, we show that $V_{k,M}(\mathbb{Z}) = \emptyset$ even though k is generic. Explicit examples are given in Sect. 8. Some of these obstructions to integer solutions are similar to ones found by Mordell

[37] for similar cubic equations, and also to the "Integer Brauer-Manin obstructions" in [18]. Following our posting of an earlier version of this paper, [34] and [19] computed explicitly the Brauer groups of these affine Markoff surfaces, as well as the corresponding integral Brauer-Manin obstructions. They find that the Hasse failures in (i) and (ii) of Prop. 8.1 are accounted for by their obstructions. However, the analysis leading to Hasse failures in part (iii) of the Proposition uses both reciprocity and Markoff descent, and they are not accounted for by the integral Brauer-Manin obstruction alone. In any case, all of these algebraic obstructions are far fewer (they are of order of magnitude $\sqrt{K}$) than the Hasse failures that we found numerically, indicating that any simple description of the latter is perhaps not possible.

(b). In the recent paper [25], the Hasse failure (i) is exploited to give failures of profinite local to global principles for commutator equations in $SL_2(\mathcal{O})$ for $\mathcal{O}$ a ring of S-integers.

(c). The proof of (ii), when combined with Theorem 1.1 yields further information about the $\mathfrak{h}_M(k)$'s for generic k's. If $t \geq 0$ is fixed, then

$$\#\big\{0 \leq |k| \leq K : \mathfrak{h}_M(k) = t,\ k \text{ generic}\big\} = o(K),$$

as $K \to \infty$. So for generic k, $\mathfrak{h}_M(k) \to \infty$ for almost all k.

(d). Our approach to proving that M is full is to look for points in $V_{k,M}(\mathbb{Z})$ with $|k| \leq K$ in a region $\mathcal{R}$ where x_1 is small (roughly of size a power of $\log K$) and $x_2,\ x_3$ vary in a sector (so they are of the same size). $\mathcal{R}$ is contained in the fundamental domains $\mathfrak{F}_k^{\pm}$ and retains the *tentacles* (cusps) of the latter, this being critical to ensuring that the average for $|k| \leq K$, of the number of points in $V_{k,M}(\mathbb{Z}) \cap \mathcal{R}$ grows with k. For a given x_1, M is a (indefinite) binary quadratic form in $x_2,\ x_3$ and this allows one to use the methods developed in [8] and [6] to show that M assumes a positive proportion of the k's. Our proof that M is full is much more delicate. As with the proofs that cubic forms in many variables (starting with the case of a sum of four cubes [22]) represents almost all admissible numbers, we compare the number of points in $V_{k,M}(\mathbb{Z}) \cap \mathcal{R}$, to an arithmetic function $\delta^{(m)}(k)$ (see Sect. 9; here m is a secondary parameter) which is a product of local densities of solutions. While this heuristic for the count can be way off for certain k's (e.g. for the Hasse failures), we show that its variance from the actual count when averaged over k, is small enough to conclude that for almost all k's, $\delta^{(m)}(k)$ is a good approximation. The fullness then follows after showing that $\delta^{(m)}(k)$ is large for most k's. That M is almost perfect then follows from (5) and that M is full. The proof of the vanishing of the variance boils down to examining the "diagonal" and "off-diagonal" terms in (44). For the first, we make use of the divisor analysis

for varying quadratic forms [6], while for the second a modern treatment of Kloosterman's method for ternary quadratic forms [39] allows for uniform control of the contributions of the varying forms.

To end the introduction, we return to a discussion of the general affine cubic form F in three variables. The study of the level sets $V_{k,M}(\mathbb{Z})$, for example (5) using the Markoff group is very special. It applies to F's of the form $F = F_0 + G$, where

$$F_0 = cx_1x_2x_3 \quad \text{and} \quad G = \sum_{i,j} a_{ij}x_ix_j + \sum_i a_ix_i + a, \tag{8}$$

with $a_{jj} = \pm 1$ for $j = 1,\ 2,\ 3$ and $c,\ a,\ a_{ij},\ a_i \in \mathbb{Z}$, as well as F's obtained from these via integral affine linear substitutions (see Appendix A). Among these special affine forms are ones for which V_k carry explicit integral points and even parametric curves, for every k. This coupled with the action of the corresponding Markoff group leads to $V_k(\mathbb{Z})$ being Zariski dense for every k. Thus, the form is both perfect and 'universal' in the sense that it represents every k. Explicit examples are

$$U_1(x_1, x_2, x_3) = x_1 + x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3, \tag{9}$$

and

$$U_2(x_1, x_2, x_3) = x_2(x_3 - x_1) + x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3. \tag{10}$$

See Sect. 5 for an analysis of these forms. The only perfect F's that we are aware of are of the form (8).

On the other hand, our treatment of the fullness of M applies more generally. We leave the precise details and proofs of the following comments to a forthcoming paper. If F_0 is reducible in $\mathbb{Q}[x_1, x_2, x_3]$, then F is full. In this case F_0 has a linear factor, which is the condition that F has $\hbar$-invariant [23] equal to 1 (see Appendix A for a discussion of these arithmetic invariants of F). The linear factor yields a rational plane in $F_0(x_1, x_2, x_3) = 0$ which can be used as the small variable and to generate a family of planes and of binary quadratic forms and a tentacled region. If F_0 is irreducible in $\mathbb{Q}[x_1, x_2, x_3]$ then our moving plane method fails. Nevertheless one can still create tentacled regions $\mathcal{R}$ in $\mathbb{R}^3$ using neighborhoods at infinity of the curve $F_0(\mathbf{x}) = 0$ in $\mathbb{P}^2(\mathbb{R})$. As before, on average over k with $|k| \leq K$, the number of points $r_{\mathcal{R}}(k)$ in $V_{k,F}(\mathbb{Z}) \cap \mathbb{R}$ grows slowly with k. The study of the variance of $r_{\mathcal{R}}(k)$ from its expected number (i.e. a product of local densities) reduces to counting points on the hypersurface $F(\mathbf{x}) - F(\mathbf{y}) = 0$ with $(\mathbf{x}, \mathbf{y}) \in \mathcal{R} \times \mathcal{R}$. While this is well beyond the available tools from the circle method, a natural hypothesis

in this context along the lines of ([Hoo16]) [5] would lead to F being full. In particular, this applies to $F = S$ in (2). The much stronger suggestion that S is perfect ([28]),[6] which was mentioned at the start is a fascinating one, as is the question of the existence of any perfect homogeneous F. All k's are admissible for the homogeneous form $x_1^3 + x_2^3 + 2x_3^3$ and it is a candidate for being both perfect and universal over $\mathbb{Z}$. It is interesting to note that this form is universal when considered over the S-integer ring $\mathbb{Z}[\frac{1}{6}]$, and has infinitely many solutions for each k. This is seen by taking

$$x_1 = \frac{6k}{\varepsilon^2} + \frac{\varepsilon}{6}, \quad x_2 = \frac{6k}{\varepsilon^2} - \frac{\varepsilon}{6}, \quad x_3 = -\frac{6k}{\varepsilon^2},$$

for any unit ε.

We point out that the analogous problem for quadratic polynomials in two variables is very different in that f is never absolutely irreducible, and indeed the typical such f is never full.

Finally, we note that the $V_{k,F}$'s for $F = M$ are the relative character varieties for the representations of $\pi_1(\Sigma_{1,1})$ into SL_2 (here $\Sigma_{g,n}$ is a surface of genus g and n punctures) and the group Γ is essentially the mapping class group action on the $V_{k,M}$'s (see Goldman [27]). As such, many of the questions that we address in this simplest case make sense with $\Sigma_{1,1}$ replaced by $\Sigma_{g,n}$ (see Whang [47]). In particular it is shown there that the key feature that the integral points for these varieties consist of finitely many Γ-orbits, persists. However both for $\Sigma_{1,1}$ and in this more general setting, this finiteness fails when the integers are replaced by S-integers in a general number ring. This makes for a quite different picture and analysis to which we will return in a future work.

Notation: For the remainder of the paper we suppress the reference to the Markoff equation. So for example V_k would mean $V_{k,M}$. We also use $(\frac{*}{p})_L$ to denote the Legendre symbol $(\frac{*}{p})$ to avoid any confusion with fractions.

2 The descent argument revisited

The descent argument was first considered by Markoff in [36], and later extended by Hurwitz [31] and Mordell [37] (see also [2] for a study of fundamental solutions associated with a special case of these several variable hypersurfaces). In particular, Hurwitz used a "height" function given by $h(x_1, x_2, x_3) = |x_1| + |x_2| + |x_3|$, which was then utilized subsequently in

[5] Very recently, Wang [46] has shown that S is full if one assumes various standard conjectures about automorphic L-functions.

[6] Recently, $V_{k,S}(\mathbb{Z})$ for $k = 33$ and 42 were shown to be nonempty, completing the list of such for $1 \leq k \leq 100$ (see Booker [7] and Booker-Sutherland [48]).

the literature. The descent argument led to a finite number of points plus those with minimal height. Our initial analysis is a revisit of this descent argument but without the use of the height function (we later use a new function for a finer analysis).

For $k \in \mathbb{Z}$, consider the set of integral points on the Markoff surface

$$V_k : \qquad x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3 = k. \tag{11}$$

After invariance by permutations and also changing two signs but leaving out Vieta involutions (which we call narrow equivalence), we see that (i) if $k < 0$, we may consider only solutions $0 \le x_1 \le x_2 \le x_3$, and (ii) if $k \ge 0$, there are two types of solutions namely those with all variables non-negative and so $0 \le x_1 \le x_2 \le x_3$; and those in the compact set $\mathfrak{S}^+(k)$ with exactly one negative variable and two positive.

For $k < 0$ we note that $x = 0$, 1 or 2 are not possible (since they give $k = x_2^2 + x_3^2$, $4(k-1) = (2x_2 - x_3)^2 + 3x_3^2$ and $(x_2 - x_3)^2 = k - 4$ respectively) so that we assume $3 \le x_1 \le x_2 \le x_3$ in this case.

When $k \ge 0$, $x = 0$ and $x = 1$ give at most finitely many triples (x_1, x_2, x_3). and we denote this set by $\mathfrak{T}(k)$. Thus in this case, (x_1, x_2, x_3) is a solution implies it is equivalent (narrowly) to one in $\mathfrak{S}^+(k) \cup \mathfrak{T}(k)$ or it satisfies $2 \le x_1 \le x_2 \le x_3$.

We now consider the Vieta involution acting on (x_1, x_2, x_3), sending it to $(x_1, x_2, x_1x_2 - x_3)$. If $x_1x_2 - x_3 < 0$, so that $k \ge 0$, then (x_1, x_2, x_3) is equivalent to a solution in $\mathfrak{S}^+(k)$. Next suppose $x_1x_2 - x_3 \ge x_3$, so that $2x_3 \le x_1x_2$. Solving for x_3 in (11) gives $2x_3 = x_1x_2 \pm \sigma$ where $\sigma = \sqrt{x_1^2x_2^2 - 4(x_1^2 + x_2^2 - k)}$, so that necessarily $\sigma = x_1x_2 - 2x_3 \le (x_1 - 2)x_2$. Squaring and simplifying gives $(x_1 - 2)x_2^2 \le (x_1^2 - k)$.

If $x_1 \ge 3$ and $k > 0$, we conclude that $x_2^2 < x_1^2$, a contradiction. If $x_1 = 2$, we conclude that $k \le 4$. Thus we derive a contradiction for all $k > 4$, so that in this case we have $0 \le x_1x_2 - x_3 < x_3$. But more is true, namely $0 \le x_1x_2 - x_3 < x_2$ shown as follows: if $x_2 \le x_1x_2 - x_3 < x_3$, then $x_1x_2 < 2x_3 \le 2(x_1 - 1)x_2$, so that necessarily $2x_3 = x_1x_2 + \sigma$. Then $\sigma \le (x_1 - 2)x_2$ and the argument above gives a contradiction. Hence we have

Lemma 2.1 *If $k > 4$ and if (x_1, x_2, x_3) is a lattice point on V_k in (11), it is equivalent to one in the compact set $\mathfrak{S}^+(k) \cup \mathfrak{T}(k)$ where*

$$\mathfrak{S}^+(k) = \left\{(-x_1, x_2, x_3) : \ 3 \le x_1 \le x_2 \le x_3 ; \ x_1^2 + x_2^2 + x_3^2 + x_1x_2x_3 = k\right\} \cap \mathbb{Z}^3,$$

or if not then it is equivalent to $(x_1, x_1x_2 - x_3, x_2)$, with $3 \le x_1x_2 - x_3 < x_2 \le x_3$ and $x_1 \ge 3$.

The special cases $1 \le k \le 3$ are settled as follows: (i) there are no solutions when $k = 3$ since there are none modulo 4; (ii) for $k = 2$, we can use the descent argument above and conclude that we need only look for solutions to $x^2 + y^2 + z^2 + xyz = 2$ with all variables non-negative or we solve the Markoff equation with $x_1 \in \{0, \pm 1, \pm 2\}$, giving us the point $(0, 1, 1)$ and its infinite orbit under Γ; and for $k = 1$, the same analysis results in the point $(0, 0, 1)$, for which there is only a finite orbit under Γ. The cases $k = 0$ and 4 we consider in the next sections (they correspond to the original Markoff surface in Sect. 3.1 and the singular Cayley surface in Sect. 4.3).

For $k < 0$, the estimate $(x_1 - 2)x_2^2 \le (x_1^2 - k)$ given above is still valid when we assume $x_1x_2 - x_3 \ge x_3$, with $3 \le x_1 \le x_2 \le x_3$. Then, if $x_1 \ge 4$, it follows that $2x_2^2 \le x_1^2 + |k|$, which then implies $x_2 \le \sqrt{|k|}$, so that $x_3 \le \frac{x_1x_2}{2} \le \frac{|k|}{2}$. If $x_1 = 3$, then clearly $x_2 \le \sqrt{9 + |k|}$, and so $x_3 \le \frac{3}{2}\sqrt{9 + |k|}$. The same argument shows that for large values of $|k|$, $x_1 \ll |k|^{\frac{1}{3}}$, $x_2 \ll \sqrt{\frac{|k|}{x_1}}$ and $x_3 \ll \sqrt{|k|x_1}$. Next, supposing $x_2 \le x_1x_2 - x_3 < x_3$, we see that the point (x_1, x_2, x_3) is Γ-equivalent to $(y_1, y_2, y_3) = (x_1, x_2, x_1x_2 - x_3)$, where now $y_1y_2 - y_3 \ge y_3$, the same inequality considered above. Thus we have

Lemma 2.2 *For $k < 0$, if (x_1, x_2, x_3) is a lattice point on V_k in (11), it is then equivalent to one in the compact set $\mathfrak{S}^-(k) \subset \mathfrak{U}(k)$, where*

$$\mathfrak{S}^-(k) := \left\{(x_1, x_2, x_3) : 3 \le x_1 \le x_2 \le x_3 \le \frac{1}{2}x_1x_2\right\} \cap V_k(\mathbb{Z}),$$

and

$$\mathfrak{U}(k) := \left\{(x_1, x_2, x_3) : 3 \le x_1 \le x_2 \le \sqrt{|k| + 9};\ 3 \le x_3 \le \frac{3}{2}(|k| + 9)\right\},$$

or if not it is equivalent to $(x_1, x_1x_2 - x_3, x_2)$ with $3 \le x_1x_2 - x_3 < x_2 \le x_3$ and $x_1 \ge 3$.

The lemmas above form the basis of the descent argument with repeated application of the Vieta involution so that ultimately any integral solution is equivalent to one in a corresponding finite set.

3 Bhargava cubes and Markoff

To construct the fundamental sets in the next section, we utilize a function $\Delta(\mathbf{x})$ given in (12), that proves useful in tracking the images of points under the action of the group Γ. While we could define Δ without comment, we give here our original construction using Bhargava cubes.

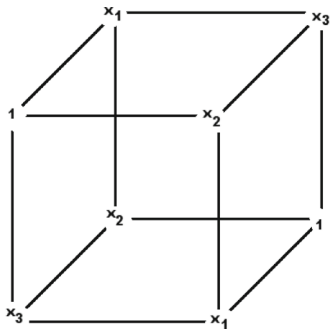

Fig. 5 Bhargava cube associated with M

Let x_1, x_2 and x_3 be arbitrary integers and consider the Bhargava cube ([4]) as shown in Fig. 5.

The Bhargava slicings give rise to the three matrix pairs:

$$M_1 = \begin{bmatrix} 1 & x_2 \\ x_3 & x_1 \end{bmatrix}, \quad N_1 = \begin{bmatrix} x_1 & x_3 \\ x_2 & 1 \end{bmatrix};$$
$$M_2 = \begin{bmatrix} 1 & x_3 \\ x_1 & x_2 \end{bmatrix}, \quad N_2 = \begin{bmatrix} x_2 & x_1 \\ x_3 & 1 \end{bmatrix};$$
$$M_3 = \begin{bmatrix} 1 & x_1 \\ x_2 & x_3 \end{bmatrix}, \quad N_3 = \begin{bmatrix} x_3 & x_1 \\ x_2 & 1 \end{bmatrix}.$$

These in turn give the following three quadratic forms $Q_i(u, v)$, where

$$Q_1 = (x_2x_3 - x_1)u^2 + (1 + x_1^2 - x_2^2 - x_3^2)uv + (x_2x_3 - x_1)v^2,$$
$$Q_2 = (x_1x_3 - x_2)u^2 + (1 + x_2^2 - x_1^2 - x_3^2)uv + (x_1x_3 - x_2)v^2,$$
$$Q_3 = (x_1x_2 - x_3)u^2 + (1 + x_3^2 - x_1^2 - x_2^2)uv + (x_1x_2 - x_3)v^2.$$

All three quadratic forms have the same discriminant $\Delta = \Delta(x_1, x_2, x_3)$ which also factorizes to give

$$\begin{aligned} \Delta &= (1 + x_2^2 - x_1^2 - x_3^2)^2 - 4(x_1x_3 - x_2)^2, \\ &= (1 + x_1 + x_2 + x_3)(1 + x_2 - x_1 - x_3)(1 + x_3 - x_1 - x_2)(1 + x_1 - x_2 - x_3). \end{aligned} \tag{12}$$

Note that

(a). $\Delta \equiv 0$ or $1 \pmod 4$ depending on if $x_1^2 + x_2^2 + x_3^2$ is odd or even respectively.
(b). Δ is invariant under permutations.
(c). Δ is invariant if one variable is fixed and the sign is changed on the other two variables.
(d). If $2 \le x_1 \le x_2 \le x_3$, then $\Delta < 0$ if and only if $x_2 \le x_3 \le x_1 + x_2 - 2$.

3.1 The case $k = 0$

Recall (Markoff [36]) that the solution set has two orbits with fundamental roots $(0, 0, 0)$ and $(3, 3, 3)$. We have $\Delta(0, 0, 0) = 1$ and $\Delta(3, 3, 3) = -80$. We show here that

$$\Delta(x_1, x_2, x_3) < 0 \text{ if and only if } (x_1, x_2, x_3) = (3, 3, 3). \tag{13}$$

Thus, the two orbits each have a minimal value for Δ, taken at the associated fundamental roots. In other words, there are two components of $V_0(\mathbb{Z})$ and in each component Δ has a minimum value, taken at a unique point, which can then be used as a generator for that component. This phenomenon repeats itself when $k \geq 5$ below.

We prove (13) as follows: since $x_1^2 + x_2^2 + x_3^2 = x_1x_2x_3$, it follows that x_1, x_2 and x_3 are all positive or exactly two are negative (we avoid the trivial solution here). By the properties of Δ itemized above, we may assume that $1 \leq x_1 \leq x_2 \leq x_3$. The Markoff equation is equivalent to the equation $(x_1^2 - 4)(x_2^2 - 4) - 16 = (2x_3 - x_1x_2)^2$, from which it follows that $3 \leq x_1 \leq x_2 \leq x_3$, which we assume. Suppose $\Delta(x_1, x_2, x_3) < 0$, so that $x_2 \leq x_3 \leq x_1 + x_2 - 2 < 2x_2$. Solving for x_3 in the Markoff equation gives us $2x_3 = x_1x_2 \pm \sigma$, where $\sigma = \sqrt{(x_1x_2)^2 - 4(x_1^2 + x_2^2)} \geq 1$.

If $x_1 \geq 4$ we must discard the positive sign since $x_3 < 2x_2$. So in this case, $x_1x_2 - \sigma = 2x_3 \geq 2x_2$, from which, by expanding and simplifying, one gets $4x_2^2 \leq x_1x_2^2 \leq x_1^2 + 2x_2^2 \leq 3x_2^2$, a contradiction.

For $x_1 = 3$, we have $x_2 \leq x_3 \leq x_1 + x_2 - 2 = x_2 + 1$, so that $x_3 = x_2$ or $x_3 = x_2 + 1$. If $x_3 = x_2$, we have $9 + 2x_2^2 - 3x_2^2 = 0$ so that $x_1 = x_2 = x_3 = 3$. Finally if $x_3 = x_2 + 1$, we must have $9 + x_2^2 + (x_2 + 1)^2 = 3(x_2^2 + x_2)$, which is impossible.

4 Fundamental sets and Theorem 1.1

The descent arguments of Markoff, Hurwitz and Mordell show that there is a finite set of lattice points from which all lattice points of the Markoff surface (11) can be obtained as images under Γ. This section provides a proof of Theorem 1.1 by showing the inequivalence of the points in the finite set.

4.1 The case $k \geq 5$

Recall from Sect. 2 that if $k \geq 5$, any solution $\mathbf{x} = (x_1, x_2, x_3)$ to the Markoff equation (11) is equivalent to one in a compact *reduced set* (by Lemma 2.1 and descent). We order the coordinates first such that $0 \leq |x_1| \leq |x_2| \leq |x_3|$.

In the next section, we show that the Markoff equation has no solutions for those k's (positive or negative) satisfying any of the following congruences: $k \equiv 3 \pmod 4$ and $k \equiv \pm 3 \pmod 9$, these then accounting for $\frac{5}{12}K + O(1)$ members in the interval $5 \le k \le K$, and we call them *non-admissible*; the non-admissible k's have local obstructions. The remaining k's we call *admissible*, and there are $\mathcal{A}(K) = \frac{7}{12}K + O(1)$ of them.

We say that k is *exceptional*[7] if there is a solution to (11) with $|x_j| = 0$, 1 or 2; these k's satisfy at least one of the equations (i) $u^2 + v^2 = k$, (ii) $u^2 + 3v^2 = 4(k-1)$, or (iii) $u^2 = k - 4$. Consequently, for k's in an interval of length K, they account for at most $O\left(K(\log K)^{-\frac{1}{2}}\right)$ members, and we will ignore them in what follows. The remaining $\frac{7}{12}K + O\left(K(\log K)^{-\frac{1}{2}}\right)$ numbers k in the interval $5 \le k \le K$ we shall call *generic*.

It follows from Sect. 2 that every solution $\mathbf{x}$ associated to a generic k is equivalent to one in the set $\mathfrak{S}^+(k)$ given in Lemma 2.1. We now show that the elements in this set, when non-empty, are inequivalent under Γ, so that $\mathfrak{S}^+(k)$ is a *fundamental set*.

We will use the Δ-function given in (12) to form an ordering on the tree of solutions to the Markoff equation. Given any $\mathbf{x} = (x_1, x_2, x_3)$, the three Vieta maps are $\mathcal{V}_1 : (x_1, x_2, x_3) \mapsto (x_2x_3 - x_1, x_2, x_3)$, $\mathcal{V}_2 : (x_1, x_2, x_3) \mapsto (x_1, x_1x_3 - x_1, x_3)$ and $\mathcal{V}_3 : (x_1, x_2, x_3) \mapsto (x_1, x_2, x_1x_2 - x_3)$. Recall that the group Γ is generated by permutations, double sign-changes and the Vieta maps. The Δ-function is invariant under the first two motions and we denote $\Delta_i = \Delta \circ \mathcal{V}_i$. Then, it is easy to check that when $\mathbf{x}$ is a solution of the Markoff equation, one has

$$\begin{aligned}
\Delta_1(\mathbf{x}) - \Delta(\mathbf{x}) &= x_2x_3(x_2x_3 - 2x_1)\left[2(k-5) + (x_2^2 - 4)(x_3^2 - 4)\right], \\
\Delta_2(\mathbf{x}) - \Delta(\mathbf{x}) &= x_1x_3(x_1x_3 - 2x_2)\left[2(k-5) + (x_1^2 - 4)(x_3^2 - 4)\right], \\
\Delta_3(\mathbf{x}) - \Delta(\mathbf{x}) &= x_1x_2(x_1x_2 - 2x_3)\left[2(k-5) + (x_1^2 - 4)(x_2^2 - 4)\right].
\end{aligned} \tag{14}$$

The expressions in the square brackets in all three formulae above are strictly positive when k is generic and if $\mathbf{x}$ is any solution of the corresponding Markoff equation.

We set up the tree associated with solutions as follows: each solution $\mathbf{x} = (x_1, x_2, x_3)$ will be a vertex and neighboring vertices are edge connected if they are obtained from $\mathbf{x}$ by one of the three Vieta maps. As such, we identify coordinates if they are obtained by permutations or double sign changes (noting that Δ is unchanged under them). By this latter identification, the coordinates

[7] The removal of the points $\mathbf{x}$ with one of its coordinates in $\{-2, -1, 0, 1, 2\}$ corresponds to avoiding the region at infinity on which Γ acts ergodically (when $k > 20$) in [27], and to the notion of "small" in [1] Sect. 5.

are one of two types, namely all positive or exactly one negative. It is then possible to rearrange them into the following canonical forms: (x_1, x_2, x_3) or $(-x_1, x_2, x_3)$ with $3 \le x_1 \le x_2 \le x_3$. We call the former *positive nodes* and the latter *negative nodes*. By Lemma 2.1, for $k \ge 5$, every positive node is equivalent to a negative node (or otherwise, by descent is equivalent to the node (3, 3, 3) which corresponds to $k = 0$).

We look at the action of the Vieta maps on a positive node. It is clear that $x_2x_3 - 2x_1$ and $x_1x_3 - 2x_2$ are strictly positive so that $\Delta_1(\mathbf{x}) > \Delta(\mathbf{x})$ and $\Delta_2(\mathbf{x}) > \Delta(\mathbf{x})$. Moreover, the nodes $\mathcal{V}_1(\mathbf{x})$ and $\mathcal{V}_2(\mathbf{x})$ are both positive, Next, the argument showing descent in Sect. 2 shows that $x_1x_2 - 2x_3 \ge 0$ is impossible so that $\Delta_3(\mathbf{x}) < \Delta(\mathbf{x})$. Here $\mathcal{V}_3(\mathbf{x})$ may be either positive or negative. We represent these observations by the images Fig. 6a, b, where square nodes are positive nodes, disc nodes are negative nodes, dark nodes are the Vieta images while the original point is a light node (the vertical ordering of the nodes is determined by the signs of the Δ-differences from (14)).

Next, if we begin with a negative node (so that one replaces x_1 with $-x_1$ in the formulae above, it is obvious that $\Delta_i(\mathbf{x}) > \Delta(\mathbf{x})$ for all i and (after a double sign change and reordering) that the $\mathcal{V}_i(\mathbf{x})$ are all positive. This is represented by Fig. 6c.

It follows now that the tree decomposes into components and each component has a root that is a negative node (Fig. 6). Moreover, the negative node occupies the lowest point on the tree, with all other nodes in that component being positive (in other words, Δ has a minimum on each component and that minimum is determined by a negative node). Thus the negative nodes form a fundamental set, giving us the first case of Theorem 1.1.

4.2 The case $k < 0$

From Sect. 2 and Lemma 2.2 every lattice point in V_k is equivalent to one in $\mathfrak{S}^-(k)$. We show that the points in this set are inequivalent. First using $(x_1^2 - 4)(x_2^2 - 4) = (2x_3 - x_1x_2)^2 - 4(k - 4)$ in (14) and the similar formulae with the variables permuted, we see that the three terms in square brackets in (14) are all positive. Thus the signs of the differences of the Δ-functions in (14) are determined by the three terms $x_2x_3 - 2x_1$, $x_1x_3 - 2x_2$ and $x_1x_2 - 2x_3$. The first two are obviously positive, and one sees that the last is non-negative if and only if $(x_1, x_2, x_3) \in \mathfrak{S}^-(k)$ Thus, in the tree determined by these points one sees that we have nodes of the type shown in Fig. 6c with two or three black square vertices emanating from points in $\mathfrak{S}^-(k)$, while for points in the complementary set, we have nodes of the type in Fig. 6a. It follows that the points in $\mathfrak{S}^-(k)$ can serve as the roots of the components of the tree, from which the second case of Theorem 1.1 follows.

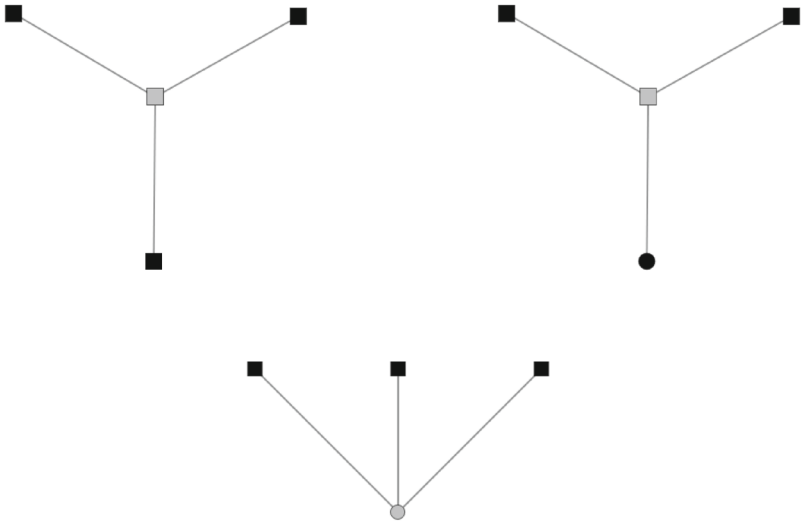

Fig. 6 Node blocks; top: (**a**, **b**); bottom: (**c**)

4.3 The Cayley surface $k = 4$

Most of the argument above for $k \geq 5$ can be applied to the case $k = 4$, and we indicate the necessary modifications. First, we consider solutions of the type $(-x_1, x_2, x_3)$ with $x_1,\ x_2,\ x_3 \geq 0$ satisfying $x_1^2 + x_2^2 + x_3^2 + x_1x_2x_3 = 4$. It is obvious that there are only two solutions up to equivalence, namely $(-2, 0, 0) \sim (0, 0, 2)$ and $(-1, 1, 1) \sim (1, 1, 2)$. Hence we need only consider solutions of the type (x_1, x_2, x_3) with $0 \leq x_1 \leq\ x_2 \leq x_3$. If $x_1 = 0$, the only solution is $(0, 0, 2)$ while if $x_1 = 1$, then the only choice is $(1, 1, 2)$. Then by the descent argument in Sect. 2, if $x_1 \geq 3$, the solution (x_1, x_2, x_3) is equivalent to one with one of the coordinates equal to 2. It is trivial that the only solutions of this kind are one of the type $(2, a, a)$, with $a \geq 0$ integers. It suffices now to check the equivalence of these solutions. It is easily checked that the orbits of $(2, 0, 0)$, $(2, 1, 1)$ and $(2, 2, 2)$ contain no other points of the type $(2, a, a)$ except themselves, so that we assume $a \geq 3$.

Following the three formulas in (14), if $\mathbf{x} = (2, a, a)$, then two of the Vieta transformations keep it fixed while the third creates a node above it, this new node not being of the same type (we say "above" to mean $\Delta_i(\mathbf{x}) > \Delta(\mathbf{x})$). Also following the argument used for $k \geq 5$, if $\mathbf{x} = (x_1, x_2, x_3)$, with $x_i \geq 3$, then two Vieta transformations create nodes above it while a third creates a node below it. It is then easily seen that a tree containing a node of the type $(2, a, a)$ cannot contain a different node of the same type. Hence we have

Proposition 4.1 *The Cayley surface $V_4(\mathbb{Z})$ has infinitely many inequivalent orbits, each determined by a solution of the type $(2, a, a)$, with $a \geq 0$.*

One checks that the $(2, 0, 0) \sim (-2, 0, 0)$-component has only 1 element (upto permutation and double sign-change) and so the minimal Δ-value is $\Delta(-2, 0, 0) = 9$. Next, the $(2, 1, 1)$-component has only 2 elements namely $(2, 1, 1)$ and $(-1, 1, 1)$. The minimal Δ-value is $\Delta(-1, 1, 1) = -16$ while $\Delta(2, 1, 1) = 5$. Finally, $\Delta(2, a, a) = 9 - 4a^2 < 0$ for $a \geq 2$. Then the same argument used in Sect. 3.1 can be used to show that any lattice point $\mathbf{x}$ not of these type satisfy $\Delta(\mathbf{x}) \geq 0$, so that the minimal Δ-value is uniquely determined. Thus, even here each component has a unique minimal Δ-value, whose point can be used as a generator.

One can use the Δ-function and the analysis above to deduce a descent procedure. One concludes that either every positive node descends to a negative node or if not, there is an infinite chain of positive nodes on which $\Delta(\mathbf{x})$ is strictly decreasing. The latter is not possible since $\Delta(\mathbf{x}) \geq 0$ on positive nodes. There are only finitely many negative nodes in $\mathfrak{S}^+(k)$. So we conclude that there are finitely many orbits. Repeating the analysis in the paper also shows that all the negative points are Γ-inequivalent and in each orbit Δ has a minimum value taken at the root of that orbit, so at the only (modulo double sign-changes) negative point on that orbit.

Using Lagrange multipliers on the region on V_k with $x_j \geq 3$ and $k \to \infty$, one can show that :

(i). $\min_{\mathbf{x}\in\mathfrak{S}^+(k)} \Delta(\mathbf{x}) \geq k^2 + 18k^{\frac{3}{2}} + 88k + \frac{621}{4}k^{\frac{1}{2}} + O(1)$;

(ii). $\max_{\mathbf{x}\in\mathfrak{S}^-(k)} \Delta(\mathbf{x}) \leq k^2 - 18k^{\frac{3}{2}} + 88k - \frac{45}{4}k^{\frac{1}{2}} + O(1)$;

(iii). $\min_{\mathbf{x}\in\mathfrak{S}^-(k)} \Delta(\mathbf{x}) \geq -3k^{\frac{4}{3}} + O(k)$.

Hence asymptotically, Δ behaves like a Minkowski gauge-function, with "successive minima" taken at the root of the orbits; that is if $\mathfrak{h}(k)$ is the number of orbits, the first $\mathfrak{h}(k)$ minimal values (counted with multiplicity) of Δ on the lattice points on V_k occur at the negative points.

5 Parametric solutions on Markoff-type surfaces and Zariski density

We show in this section that for generic k, the Markoff surface has no parametric integral points and that the solution set is Zariski dense. We also consider the surfaces given by U_1 and U_2 mentioned in the Introduction.

5.1 Parametric solutions

Lemma 5.1 *For any $k \in \mathbb{Z}$, let M_k^* be the surface given by $M^*(\mathbf{x}) = k$, where*

$$M^*(\mathbf{x}) = \sum_{j=1}^{3} \alpha_j x_j + (\beta_1 x_2 x_3 + \beta_2 x_1 x_3 + \beta_3 x_1 x_2) + x_1^2 + x_2^2 + \varepsilon x_3^2 - x_1 x_2 x_3, \quad (15)$$

where $\varepsilon = \pm 1$ and $\alpha_j, \beta_j \in \mathbb{Z}$ for all j. Suppose there are polynomials $P_j(t) \in \mathbb{Z}[t]$ each with non-zero degree, such that $M^*(P_1, P_2, P_3) = k$ identically in t. Then there are polynomials $Q_1, Q_2 \in \mathbb{Z}[t]$ of non-zero degree and a constant $q \in \mathbb{Z}$ such that $M^*(q, Q_1, Q_2) = k$ identically in t.

Proof Let P_j have degree $d_j \neq 0$ for $j = 1, 2, 3$ as above. By comparing degrees in (15) we cannot have $d_1 = d_2 = d_3$, so that there is either a unique d_j exceeding the other two or exactly two of the degrees are the same. The latter does not happen as it implies that at least one of the polynomials is a constant. Hence (comparing degrees in (15)) we have that $d'' = d' + d$ for some choice of the degrees. It will not matter which subscript represents the largest degree in what follows, so that we put $d_3 = d_1 + d_2$, with $d_1, d_2 \geq 1$.

There is a Vieta affine transformation acting on the surface given by $x_3 \mapsto x_4 = x_1 x_2 - \alpha_3 - \beta_1 x_2 - \beta_2 x_1 - \varepsilon x_3$, so that if $P_4(t)$ is the polynomial determined by x_4, we have

$$P_3 P_4 = k - P_1^2 - P_2^2 - \beta_3 P_1 P_2 - \alpha_1 P_1 - \alpha_2 P_2,$$

identically in t. If d_4 is the degree of P_4, we have $d_3 + d_4 \leq 2\max(d_1, d_2)$, so that $d_4 \leq \max(d_1, d_2) - \min(d_1, d_2) < \max(d_1, d_2)$. Thus we have polynomials P_1, P_2, P_4 in place of P_1, P_2, P_3 representing integral points on the surface, with the maximal degree reduced by at least one and the new maximum degree is determined by P_1 or P_2. Either P_4 has degree zero, in which case we are done, or if not, all the new polynomials have non-zero degree. Repeating this descent argument (with a different Vieta transformation) shows that there must be parametric solutions with at least one polynomial constant, and the other two polynomials of non-zero degree. □

It is not possible to have parametric solutions to (15) with two of the polynomials constant. It follows from the lemma that if parametric solutions exist then there exists $q \in \mathbb{Z}$ and $Q_1, Q_2 \in \mathbb{Z}[t]$ of the same degree d satisfying (15) (it is possible to show that $d \leq 2$, if it exists). We now consider some special cases:

1. For the Markoff equation we have $Q_1^2 + Q_2^2 - q Q_1 Q_2 = k - q^2$. Comparing the highest degree term shows that there are integers q_1, q_2 such that $q_1^2 + q_2^2 - q q_1 q_2 = 0$. It follows that $q = \pm 2$ and $k - 4 = \square$. Moreover if

$k = 4 + w^2$, then one has a parametric family of solutions $q = 2$, $Q_1 = t$ and $Q_2 = t + w$. In particular, this means that if k is generic, there are no parametric solutions to the associated Markoff level set.

2. Consider the Markoff-like surface $x_1^2 + x_2^2 - x_3^2 - x_1x_2x_3 = k$. If we have parametric solutions as above of the type (Q_1, Q_2, q), then the argument is identical to the Markoff case so that we conclude there are no such parametric solutions except when $k + 4 = w^2$, in which case we have the parametric family $(t + w, t, 2)$. Next, if either x_1 or x_2 is q, we have the equation $Q_1^2 - Q_2^2 - qQ_1Q_2 = k - q^2$, so like the case above, we have $q_1^2 - q_2^2 - qq_1q_2 = 0$. We conclude that $q = 0$ so that when $k \neq 0$, Q_1 and Q_2 have degree zero, a contradiction. When $k = 0$, we have the parametric family $(Q_1, 0, \pm Q_1)$ for any polynomial Q_1.

Remark 5.2 This surface has the following features: (i) there are no local obstructions, (ii) for $k = 4^\alpha k'$ with $\alpha \geq 0$ and k' odd, it has the integral points $(0, 2^\alpha \frac{k'+1}{2}, 2^\alpha \frac{k'-1}{2})$, (iii) if $k' \neq 1$ or $\alpha \geq 3$, there are infinitely many integral points, and (iv) there are infinitely many Hasse failures (in particular, $k = 94$ is a Hasse failure). This latter statement follows from an analysis similar to that in Prop. 8.1.

3. Consider the linear deformation U_1 of the Markoff equation considered in (9), namely $x_1 + x_1^2 + x_2^2 + \varepsilon x_3^2 - x_1x_2x_3 = k$. For any integer k, and $\varepsilon = \pm 1$, we have the parametric family of integral solutions $\big(-t^2 + k - 4\varepsilon, -t^2 + t + k - 4\varepsilon, 2\big)$.

4. Consider the quadratic deformation U_2 of (10): $x_2x_3 - x_1x_2 + x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3 = k$. For any k, we have the parametric solutions $(-t^2 + t + k - 1, -t^2 + k - 1, 1)$.

5.2 Zariski density

5.2.1

We prove (5) for the Markoff surface for k not a square (this ensures that if $V_{k,M}(\mathbb{Z}) \neq \emptyset$, then it has a lattice point with at most one coordinate zero). First note that if $\hat{\mathbf{x}} = (\hat{x}_1, \hat{x}_2, \hat{x}_3) \in V_k(\mathbb{Z})$ and $|\hat{x}_j| \geq 2$ for some j, then $|V_k(\mathbb{Z})| = \infty$. To see this, say $|\hat{x}_1| \geq 2$; then the composition of the Vieta transformation $\mathcal{V}_3$ with the permutation of x_2 and x_3 yields the transformation $(x_1, x_2, x_3) \mapsto (x_1, x_1x_2 - x_3, x_2)$ in Γ. This preserves the plane $x_1 = \hat{x}_1$ and V_k, and it induces the linear action $\begin{bmatrix} \hat{x}_1 & -1 \\ 1 & 0 \end{bmatrix}$ on this plane. Since $|\hat{x}_1| \geq 2$, this element in $SL_2(\mathbb{Z})$ is of infinite order, so that its orbit is infinite (since it is not acting on the origin) and its Zariski closure contains the conic section $\{x_1 = \hat{x}_1\} \cap V_k$. We now argue as in [21]. If $\overline{V_k(\mathbb{Z})}$, the Zariski closure of $V_k(\mathbb{Z})$

is not V_k, then it is contained in a finite union of curves in V_k. Hence there can be at most finitely many $\hat{x}_1$'s with $(\hat{x}_1, \hat{x}_2, \hat{x}_3) \in V_k(\mathbb{Z})$ with $|\hat{x}_1| \geq 2$ (since otherwise $\overline{V_k(\mathbb{Z})}$ contains infinitely many distinct conic sections as above). The same applies to $\hat{x}_2$ and $\hat{x}_3$, giving $|V_k(\mathbb{Z})| < \infty$. That is we have shown that $|V_k(\mathbb{Z})| = \infty$ implies that $\overline{V_k(\mathbb{Z})} = V_k$. To complete the proof of (5) note that if $|k| > 20$ and $(\hat{x}_1, \hat{x}_2, \hat{x}_3) \in V_k(\mathbb{Z})$ then for at least one of the j's, $|\hat{x}_j| \geq 2$ and so $|V_k(\mathbb{Z})| \neq \emptyset$ implies $\overline{V_k(\mathbb{Z})} = V_k$. For the k's with $|k| \leq 20$ we check directly that (5) holds. One can show that when $k = 1,\ 9,\ 49$, for example, $V_{k,M}(\mathbb{Z}) \neq \emptyset$ but has only a finite orbit. On the other hand, when $k = k_1^2$ with k_1 having an odd prime factor congruent to one modulo 4, then $V_{k,M}(\mathbb{Z})$ has an infinite orbit, and by the argument above, is Zariski dense.

5.2.2

We next consider the surface U_1 discussed above and in (9). The argument is almost the same as for the Markoff surface except that now we have an affine transformation and a lack of full symmetry in the variables.

As in the case for the Markoff equation, assume that $\overline{V_{k,U_1}(\mathbb{Z})} \neq V_{k,U_1}$ so that it is contained in a finite union of curves. Consider the two Vieta transformations: $\mathcal{V}_1(\mathbf{x}) = (x_2x_3 - 1 - x_1, x_2, x_3)$ and $\mathcal{V}_3(\mathbf{x}) = (x_1, x_2, x_1x_2 - x_3)$, keeping x_2 fixed. Put $\mathbf{w} = (x_1, x_3)^T$ so that $\mathcal{V}_1$ and $\mathcal{V}_3$ act on $\mathbf{w}$. By abuse of notation, we have

$$\mathcal{V}_1(\mathbf{w}) = \begin{bmatrix} -1 & x_2 \\ 0 & 1 \end{bmatrix} \mathbf{w} + \begin{bmatrix} -1 \\ 0 \end{bmatrix} \quad \text{and} \quad \mathcal{V}_3(\mathbf{w}) = \begin{bmatrix} 1 & 0 \\ -x_2 & -1 \end{bmatrix} \mathbf{w},$$

so that we write $\mathcal{V}_1\mathcal{V}_3(\mathbf{w}) = A\mathbf{w} + \mathbf{b}$, with

$$A = \begin{bmatrix} -1 - x_2^2 & -x_2 \\ -x_2 & -1 \end{bmatrix} \in SL(2, \mathbb{Z}), \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} -1 \\ 0 \end{bmatrix}.$$

Hence $(\mathcal{V}_1\mathcal{V}_3)^n\mathbf{w} = A^n\mathbf{w} + \sum_{j=0}^{n-1} A^j\mathbf{b}$ for $n \geq 1$. If $\mathcal{V}_1\mathcal{V}_3$ has order n, it follows that $(A^n - I)[(A - I)\mathbf{w} + \mathbf{b}] = 0$. Now, if $x_2 \neq 0$, then A has infinite order and $A^n - I$ is invertible, so that we have $(A - I)\mathbf{w} = -\mathbf{b}$. This is impossible since $(A - I)^{-1}\mathbf{b}$ is not integral. Hence $\mathcal{V}_1\mathcal{V}_3$ has infinite order so that the orbit $\mathcal{V}_1\mathcal{V}_3(x_1, x_2, x_3)$ with $x_2 \neq 0$ fixed is infinite. The assumption of Zariski density implies that there are only finitely many x_2's.

Since the surface given by U_1 is symmetric in x_2 and x_3, it follows that there are only finitely many x_2 and x_3's, from which we conclude that there are at most finitely many lattice points (since x_1 is determined). Starting with the base point $\mathbf{p} = (k - 4, k - 4, 2)$ which is on the surface, we see that this is impossible since the orbit $\mathcal{V}_1\mathcal{V}_3(\mathbf{p})$ is infinite if $k \neq 4$. Hence $V_{k,U_1}(\mathbb{Z})$ is Zariski dense in V_{k,U_1} for all $k \neq 4$. For $k = 4$, we use instead $\mathbf{p} = (-1, 2, 0)$ so that $\mathbf{w} \neq \mathbf{0}$, and the argument above gives an infinite orbit, and Zariski dense.

5.2.3

The argument for U_2 is almost identical: we use the Vieta transformations $\mathcal{V}_1(\mathbf{x}) = (x_2x_3 + x_2 - x_1, x_2, x_3)$ and $\mathcal{V}_3(\mathbf{x}) = (x_1, x_2, x_1x_2 - x_2 - x_3)$, and have the corresponding matrix equation for $\mathcal{V}_1\mathcal{V}_3(\mathbf{w}) = A\mathbf{w} + \mathbf{b}$, with

$$A = \begin{bmatrix} -1 + x_2^2 & -x_2 \\ x_2 & -1 \end{bmatrix} \in SL(2, \mathbb{Z}), \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} -x_2^2 + x_2 \\ -x_2 \end{bmatrix}.$$

The analysis is the same as for U_1 except now we have that $A^n - I$ is invertible if $|x_2| \geq 3$. As above, we derive a contadiction of the finite order assumption since $(A - I)^{-1}\mathbf{b}$ is not integral. In particular, taking the base point $\mathbf{p} = (k-1, k-1, 1)$, we conclude that $V_{k,U_2}(\mathbb{Z})$ is infinite if $|k| \geq 4$. The reasoning above using the Zariski density assumption shows that there are only finitely many x_2's.

Due to the lack of symmetry in the variables, we redo the analysis with x_1 fixed, using $\mathcal{V}_2\mathcal{V}_3(\mathbf{w}) = A\mathbf{w} + \mathbf{b}$, with $\mathcal{V}_2(\mathbf{x}) = (x_1, x_1x_3 + x_1 - x_3 - x_2, x_3)$, $\mathcal{V}_3$ as before, $\mathbf{w} = (x_2, x_3)^T$ and

$$A = \begin{bmatrix} x_1(x_1 - 2) & 1 - x_1 \\ x_1 - 1 & -1 \end{bmatrix} \in SL(2, \mathbb{Z}), \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} x_1 \\ 0 \end{bmatrix}.$$

If $|x_1 - 1| \geq 3$, we conclude $(A - I)\mathbf{w} = -\mathbf{b}$, and derive a contradiction regarding the finite order assumption. Thus the Zariski density hypothesis implies that there are only finitely many x_1's. Hence, again since x_3 is determined by x_1 and x_2, $V_{k,U_2}(\mathbb{Z})$ is finite, giving a contradiction. Thus $V_{k,U_2}(\mathbb{Z})$ is Zariski dense in V_{k,U_2} for all $|k| \geq 4$. For $|k| \leq 4$, a direct computation gives many eligible candidates for lattice points that lead to Zariski dense.

A much stronger theorem concerning Γ invariant holomorphic curves and structures for the surfaces corresponding to (8) is proved in ([15], Theorem D).

6 Local solutions in $\mathbb{Z}_p$

Proposition 6.1 *Given $k \in \mathbb{Z}$, the congruence $x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3 \equiv k \pmod{p^n}$ has solutions for all primes p and $n \geq 1$ except for the following exceptions : $k \equiv 3 \pmod 4$, $k \equiv \pm 3 \pmod 9$.*

We break up the proof into several cases.

It is particularly easy to verify the Proposition for powers of primes $p \geq 5$ as follows: recall the Fricke trace identity, namely for any real unimodular matrices A and B,

$$\mathfrak{S}(A)^2 + \mathfrak{S}(B)^2 + \mathfrak{S}(AB)^2 - \mathfrak{S}(A)\mathfrak{S}(B)\mathfrak{S}(AB) = \mathfrak{S}([A, B]) + 2, \tag{16}$$

where $[A, B] = ABA^{-1}B^{-1}$ is the commutator, and $\mathfrak{S}()$ denotes the trace of the matrix.

Restricting the matrices to $SL(2, \mathbb{Z})$, one obtains integral solutions to (11), with $k = t + 2$, where we denote $\mathfrak{S}([A, B])$ by t. We have

Lemma 6.2 *For any prime $p \geq 5$, $n \geq 1$ and any integer t, there exists matrices $A,\ B \in SL(2, \mathbb{Z}/p^n\mathbb{Z})$ such that*

$$\mathfrak{S}(A)^2 + \mathfrak{S}(B)^2 + \mathfrak{S}(AB)^2 - \mathfrak{S}(A)\mathfrak{S}(B)\mathfrak{S}(AB) \equiv t + 2 \,(\mathrm{mod}\, p^n)\,.$$

Proof For

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}, \quad A, B \in SL(2, \mathbb{Z}/p^n\mathbb{Z}),$$

we have $\mathfrak{S}([A, B]) = 2adef - bc(e^2 + f^2) \equiv 2 - bc(e - f)^2 \,(\mathrm{mod}\, p^n)$.

Since $p \geq 5$, there exists e and f such that $(e - f, p) = 1$ with $ef \equiv 1 \,(\mathrm{mod}\, p^n)$. Then, we choose c so that $c(e - f)^2 \equiv 1 \,(\mathrm{mod}\, p^n)$. Finally, we choose $a = 1$, $b = 2 - t$ and $d = 1 + bc$. □

Corollary 6.3 *For $p \geq 5$ and $n \geq 1$, the Markoff congruence $x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3 \equiv k \,(\mathrm{mod}\, p^n)$ has the solution $x_1 \equiv 2 - (k - 4)c$, $x_2 \equiv e + f$ and $x_3 \equiv e - f + fx_1$, with $e,\ f$ and c as in the proof of the Lemma.*

The argument above gives the existence of solutions for powers of $p \geq 5$. It is useful to have a precise count for the number of solutions modulo p. For this, it is not any harder to consider the more general problem in

Lemma 6.4 *For $p \geq 3$, let N_p denote the number of solutions to $x_1^2 + x_2^2 + x_3^2 - \alpha x_1x_2x_3 \equiv \beta$ modulo p. Then*

$$N_p = \begin{cases} p^2 + p\left(\frac{-\beta}{p}\right)_L & \text{if } p|\alpha, \\ p^2 + 1 + \left(\frac{\alpha^2\beta - 4}{p}\right)_L \left[3 + \left(\frac{\beta}{p}\right)_L\right] p & \text{otherwise.} \end{cases}$$

Proof It is clear we need only consider the cases $\alpha = 0$ and $\alpha = 1$, the latter when $p \nmid \alpha$, upon which we multiply through with α^2 and change variables.

Write $S_p(a) = \sum_u e_p(au^2)$ (where $e_p(x) = e^{\frac{2\pi i x}{p}}$) so that when $p \nmid a$, one has $S_p(a) = \left(\frac{a}{p}\right)_L S_p(1)$. When $\alpha = 1$, putting $u \equiv 2x_3 - x_1x_2 \,(\mathrm{mod}\, p)$ shows that we have the same number of solutions as the congruence

$$4(x_1^2 + x_2^2) + u^2 - x_1^2x_2^2 \equiv 4\beta \,(\mathrm{mod}\, p),$$

so that

$$N_p - p^2 = \frac{1}{p}\sum_{a\not\equiv 0} T_p(a)S_p(a)e_p(-4a\beta)\,; \tag{17}$$

here we obtained p^2 solutions when $a \equiv 0 \pmod p$, and we put

$$T_p(a) = \sum_{x_1,x_2} e_p\left(a(4x_1^2 + 4x_2^2 - x_1^2x_2^2)\right) = \sum_{x_1} e_p(4ax_1^2)S_p\left(a(4-x_1^2)\right).$$

Breaking the sum over x_1 in T_p above depending on when $x_1 \equiv \pm 2$ or not gives us

$$T_p(a) = 2p\, e_p(16a) + \left(\frac{a}{p}\right)_L S_p(1)\sum_{x_1}\left(\frac{4-x_1^2}{p}\right)_L e_p(4ax_1^2).$$

Summing over a in (17) gives $N_p = p^2 + \mathcal{E}_1 + \mathcal{E}_2$, where

$$\mathcal{E}_1 = 2S_p(1)\sum_a \left(\frac{a}{p}\right)_L e_p\left(a(16-4\beta)\right) = 2S_p(1)^2\left(\frac{4-\beta}{p}\right)_L, \tag{18}$$

and

$$\mathcal{E}_2 = \frac{1}{p}S_p(1)^2\sum_{x_1}\left(\frac{4-x_1^2}{p}\right)_L \sum_{a\not\equiv 0} e_p\left(4a(x_1^2-\beta)\right). \tag{19}$$

Summing over a in (19), we write $\mathcal{E}_2 = -\mathcal{E}_{2,1} + \mathcal{E}_{2,2}$ with

$$\begin{aligned}\mathcal{E}_{2,1} &= \frac{S_p(1)^2}{p}\sum_{x_1^2\not\equiv\beta}\left(\frac{4-x_1^2}{p}\right)_L,\\ &= \frac{S_p(1)^2}{p}\left[\sum_{x_1}\left(\frac{4-x_1^2}{p}\right)_L - \left(\frac{4-\beta}{p}\right)_L\left[1+\left(\frac{\beta}{p}\right)_L\right]\right],\end{aligned}$$

and

$$\mathcal{E}_{2,2} = \frac{S_p(1)^2}{p}(p-1)\left(\frac{4-\beta}{p}\right)_L\left[1+\left(\frac{\beta}{p}\right)_L\right].$$

Since $\sum_x \left(\frac{4-x_1^2}{p}\right)_L = -\left(\frac{-1}{p}\right)_L$, it follows from (18) and (19) that

$$N_p = p^2 + 2S_p(1)^2\left(\frac{4-\beta}{p}\right)_L + \frac{S_p(1)^2}{p}\left(\frac{-1}{p}\right)_L + S_p(1)^2\left(\frac{4-\beta}{p}\right)_L\left[1+\left(\frac{\beta}{p}\right)_L\right].$$

Using $S_p(1)^2 = p\left(\frac{-1}{p}\right)_L$ then gives us

$$N_p = p^2 + \left(\frac{\beta-4}{p}\right)_L\left[3+\left(\frac{\beta}{p}\right)_L\right]p + 1.$$

It follows that $N_p \geq p^2 - 4p + 1 = (p-2)^2 - 3 > 0$ if $p \geq 5$. This is also true of $p = 3$ as can be checked with different values of β.

Next, if $p|\alpha$,

$$N_p - p^2 = \frac{1}{p}\sum_{a\not\equiv 0} e_p(-\beta a)S_p(a)^3 = \frac{S_p(1)^3}{p}\sum_a e_p(-\beta a)\left(\frac{a}{p}\right)_L.$$

If $p|\beta$, then $N_p = p^2$. If $p\nmid\beta$, then the right hand side is $p\left(\frac{-\beta}{p}\right)_L$. □

6.1 Prime powers: $p \geq 5$

We have already considered this case in Corollary 6.3, but for completeness we give here the argument using Hensel's lemma. Let $f = x_1^2+x_2^2+x_3^2-x_1x_2x_3-k$, considered as three functions of each variable. We use Df to represent one of the three partial derivatives (the choice being understood from the context): $2x_1 - x_2x_3$, $2x_2 - x_1x_3$ or $2x_3 - x_1x_2$. To obtain solutions modulo p^{n+1} from those modulo p^n, it suffices that at least one of these derivatives not vanish modulo p^n. We call such triples non-singular. If (x_1, x_2, x_3) is such a non-singular solution modulo p^n with say $2x_1 - x_2x_3 \not\equiv 0 \pmod{p^n}$, then Hensel's lemma gives a solution to $f \equiv 0 \pmod{p^{n+1}}$ of the form (y_1, x_2, x_3) with $y_1 \equiv x_1 \pmod{p^n}$. This new triple is non-singular modulo p^{n+1} so that by induction a non-singular solution modulo p lifts to one modulo p^n for any $n \geq 1$, for any prime $p \geq 5$. Note that (3, 3, 3) is a non-singular solution when $p|k$, giving solutions modulo p^n.

Next suppose the triple (x_1, x_2, x_3) is a singular solution of the congruence $f \equiv 0 \pmod{p}$ for $p \nmid k$, so that we have $2x_1 \equiv x_2x_3$, $2x_2 \equiv x_1x_3$ and $2x_3 \equiv x_1x_2 \pmod{p}$. If we assume $p \nmid x_1x_2x_3$, then necessarily $x_1^2 \equiv x_2^2 \equiv x_3^2$ and $x_1x_2x_3 \equiv 2x_1^2 \pmod{p}$. Substituting into $f \equiv 0 \pmod{p}$ gives $x_1^2 \equiv k \pmod{p}$ so that k must be a non-zero quadratic residue modulo p, so say $k \equiv$

$u^2 \pmod p$. But then $(u, 0, 0)$ is a non-singular solution to $f \equiv 0 \pmod p$, and so by above, lifts to a non-singular solution modulo p^n for all $n \geq 1$.

Finally, suppose $p|x_1x_2x_3$ with (x_1, x_2, x_3) singular. Then p divides x_1, x_2 and x_3, so that $p^2|k$. But then $(3, 3, 3)$ is a non-singular solution modulo p^2 for all $p > 3$. We can now apply Hensel's lemma as above, starting modulo p^2 and lifting to solutions modulo p^n for all $n \geq 2$ and $p > 3$.

6.2 Prime powers: $p = 3$

The congruence $f \equiv 0 \pmod 3$ has the following non-singular solutions : when $k \equiv 1$, take $(1, 0, 0)$; and when $k \equiv -1$, take $(0, 1, 1)$. These solutions lift to solutions modulo 3^n for $n \geq 1$.

When $k \equiv 0 \pmod 3$, the only solution is the singular $(0, 0, 0)$. We now consider this case modulo 9. Since 3 divides each of x_1, x_2 and x_3, then necessarily when $k \equiv 3$ or 6 mod 9, there are no solutions. So assume $9|k$, in which case $(3, 0, 0)$ is a non-singular solution modulo 9 and so lifts to solutions modulo 3^n with $n \geq 2$.

6.3 Prime powers: $p = 2$

Modulo 2, $Df \equiv x_1x_2$ or x_1x_3 or x_2x_3. Thus if k is even, one may use the non-singular solution $(1, 1, 1)$ to obtain solutions modulo powers of 2. When k is odd, the only solution is the singular $(0, 0, 1)$. Then necessarily $k \equiv 3 \pmod 4$ has no solutions. So assume $k \equiv 1 \pmod 4$ and we find the non-singular solution $(1, 0, 0)$ modulo 4 (note that here one uses $Df \equiv 2x_1 - x_2x_3 \not\equiv 0 \pmod 4$). This then lifts to higher powers of 2.

7 The average of $\mathfrak{h}^{\pm}_M(k)$: counting lattice points

We show here that the average of $\mathfrak{h}^{\pm}_M(k)$ is $C^{\pm}(\log k)^2$, by counting lattice points in the domains given in Theorem 1.1 ((see the paragraph containing (6) for definitions). We provide the details for $k > 5$.

Fix $u_1 = a$ with $3 \leq a \ll K^{\frac{1}{3}}$ and write $u_2 = m$ and $u_3 = n$. We determine the asymptotics of $N_a(K)$, the number of pairs (m, n) satisfying the inequality $a^2 + m^2 + n^2 + amn \leq K$ with $a \leq m \leq n$. We have

$$m \leq n \leq \frac{1}{2}\left(-am + \sqrt{4(K - a^2) + (a^2 - 4)m^2}\right),$$

so that $m \leq K_a$, with $K_a = \sqrt{\frac{K-a^2}{a+2}}$. Hence

$$N_a(K) = \frac{1}{2} \sum_{a \leq m \leq K_a} \left\{\sqrt{4(K - a^2) + (a^2 - 4)m^2} - (a + 2)m\right\} + O\left(\sqrt{\frac{K}{a}}\right).$$

The function in the sum is decreasing in m and the contribution from the endpoints are $O(\sqrt{K})$. Hence

$$N_a(K) = \frac{1}{2}\int_a^{K_a} \left\{\sqrt{4(K-a^2)+(a^2-4)x^2} - (a+2)x\right\} dx + O\left(\sqrt{K}\right).$$

Changing variables gives

$$N_a(K) = 2\frac{K-a^2}{\sqrt{a^2-4}}\int_\alpha^\beta \left\{\sqrt{1+x^2} - \frac{a+2}{\sqrt{a^2-4}}x\right\} dx + O\left(\sqrt{K}\right),$$

where $\beta = \frac{\sqrt{a-2}}{2}$ and $\alpha = O(aK^{-\frac{1}{2}})$. Replacing α with zero gives an error of $O(\sqrt{K})$ and the integral becomes

$$\frac{1}{2}\left\{\beta\sqrt{1+\beta^2} + \log\left(\beta+\sqrt{1+\beta^2}\right) - \frac{a+2}{\sqrt{a^2-4}}\beta^2\right\}.$$

Simplifying gives us

Lemma 7.1 *For $3 \le a \ll K^{\frac{1}{3}}$, the number of pairs (m,n) satisfying the inequality $a^2+m^2+n^2+amn \le K$ with $a \le m \le n$ is*

$$N_a(K) = \log\left[\frac{\sqrt{a-2}+\sqrt{a+2}}{2}\right]\frac{K-a^2}{\sqrt{a^2-4}} + O(\sqrt{K}).$$

Lemma 7.2 *Let $R^+(K)$ be the number of points (x_1,x_2,x_3) satisfying $x_1^2+x_2^2+x_3^2+x_1x_2x_3 \le K$, with $3 \le x_1 \le x_2 \le x_3$. Then*

$$R^+(K) = \frac{1}{36}K(\log K)^2 + O(K\log K).$$

Proof It follows from the previous lemma that

$$R^+(K) = \sum_{3\le a\le K^{\frac{1}{3}}} \log\left[\frac{\sqrt{a-2}+\sqrt{a+2}}{2}\right]\frac{K}{\sqrt{a^2-4}} + O\left(K^{\frac{5}{6}}\right).$$

The main term is asymptotic to $\frac{K}{2}\sum_a \frac{\log a}{a} \sim \frac{K}{4}(\log K^{\frac{1}{3}})^2$. □

We also state, without details, the analogous count for the case of $k < 0$ in Theorem 1.1(ii).

Lemma 7.3 *Let $R^-(K)$ be the number of points (x_1, x_2, x_3) satisfying $x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3 = -k$, with $0 < k \le K$ and $3 \le x_1 \le x_2 \le x_3 \le \frac{1}{2}x_1x_2$. Then*

$$R^-(K) = \frac{1}{48}K(\log K)^2 + O(K \log K).$$

8 Failures of the Hasse Principle

The fundamental sets allows us to determine Hasse failures for small k very readily. For example, direct computations reveal that the smallest positive Hasse failure occurs with $k = 46$. That $k = 46$ is a Hasse failure can be verified by applying Theorem 1.1 as follows: either $k = 46$ is exceptional or there exist $3 \le x_1 \le x_2 \le x_3$ such that $x_1^2+x_2^2+x_3^2+x_1x_2x_3 = 46$. The latter cannot occur since the smallest value of the polynomial is 54. To determine if 46 is exceptional, since it is not a sum of two squares and since 42 is not a square, it remains to check if the equation $x_2^2 + x_3^2 - x_2x_3 = 45$ has any solutions with $x_2,\ x_3 \in \mathbb{Z}$. The equation implies that $3|x_2$ and $3|x_3$, so that we consider the solvability of $y_1^2 + y_2^2 - y_1y_2 = 5$. This is equivalent to the solvability of $u_1^2 + 3u_2^2 = 20$, which is impossible by congruence modulo 5 or otherwise.

Let $V_k(\mathbb{Z})$ denote the integral points on the surface $x_1^2+x_2^2+x_3^2-x_1x_2x_3 = k$, for $k \in \mathbb{Z}$. For $k = 4 + d$, the surface V_k is the singular Cayley surface when reduced modulo d. Its features, coupled with global quadratic reciprocity, yield failures of strong approximation (mod $4d$). For example, assume that $n \to \left(\frac{4d}{n}\right)$ is a primitive Dirichlet character (mod $4d$) and let $S_d \subset \mathbb{Z}/4d\mathbb{Z}$ be the multiplicative closed set $\left\{n : \left(\frac{4d}{n}\right) = 0 \text{ or } 1\right\}$. Then, for any $\mathbf{x} = (x_1, x_2, x_3) \in V_k(\mathbb{Z})$ one has

$$x_j^2 - 4 \in S_d \pmod{4d}, \text{ for } j = 1, 2, 3. \tag{20}$$

These congruences on x_j imposed by (20) are not consequences of local considerations and so strong approximation fails for $V_k(\mathbb{Z})$, at least (mod $4d$).

To see (20), we rewrite (11) as

$$w^2 - 4d = \left(x_1^2 - 4\right)\left(x_2^2 - 4\right), \tag{21}$$

with $w = 2x_3 - x_1x_2$. Now, if $x_1^2 - 4 = p_1p_2 \dots p_l$ with p_j primes (possibly with repetition), then $w^2 \equiv 4d \pmod{p_j}$ and hence $\left(\frac{4d}{p_j}\right) = 0$ or 1. Thus $p_j \in S_d$ for each j, and hence so does $x_1^2 - 4$. The same applies to $x_2^2 - 4$ and $x_3^2 - 4$. Quadratic reciprocity then implies that the x_j's must lie in certain congruence classes (mod $4d$).

As we now show, by specializing the k's and enhancing the analysis above, we can eliminate all the candidate congruence classes and produce families of Hasse failures. We turn to these and the proof of Theorem 1.2(i) in the Introduction, which follows from Prop. 8.1 below.

Proposition 8.1 *For the following choices of k, $V_k(\mathbb{Z})$ is empty but $V_k(\mathbb{Z}_p)$ is non-empty for all primes p :*

(i). For $k < 0$, choose $k = 4 - 2\nu^2$, with odd ν having all its prime factors congruent to 1 or 3 modulo 8.

(ii). For $k > 4$, choose $k = 4+2\nu^2$ with ν having all of its prime factors in the congruence classes $\{\pm 1\}$ modulo 8, and in addition with $\nu \in \{0, \pm 3, \pm 4\}$ modulo 9.

(iii). Suppose $\ell \geq 13$ is a prime number with $\ell \equiv \pm 4$ (mod 9). Then choose $k = 4 + 2\ell^2$.

The smallest positive k here is 342.

Proof Writing $k = 4 + 2\epsilon\nu^2$ with $\epsilon = \pm 1$, with odd ν, the congruence conditions ensure that Prop. 6.1 implies $V_k(\mathbb{Z}_p) \neq \varnothing$ for all primes p.

Let (x_1, x_2, x_3) be a solution to

$$x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3 = 4 + 2\epsilon\nu^2, \tag{22}$$

with the corresponding

$$w^2 - 8\epsilon\nu^2 = (x_1^2 - 4)(x_2^2 - 4), \tag{23}$$

with $w = 2x_3 - x_1x_2$.

Since ν is odd, $4 \pm 2\nu^2$ is not divisible by 4, so that at least one of x_1, x_2 or x_3 is odd, so say x_1. Then $x_1^2 - 4 \equiv 5 \equiv -3$ (mod 8).

Case (i): It follows that $x_1^2 - 4$ is divisible by a prime number $q \equiv -1$ or -3 (mod 8). Since $q \nmid \nu$, it follows from (23) that -2 is a quadratic residue modulo q, a contradiction.

Case (ii): It follows that $x_1^2 - 4$ is divisible by a prime number $q \equiv \pm 5$ (mod 8). Since $q \nmid \nu$, it follows from (23) that 2 is a quadratic residue modulo q, a contradiction.

Case (iii): Recall that for $k \geq 5$, if k is not exceptional, every solution is equivalent to one in the fundamental set $3 \leq x_1 \leq x_2 \leq x_3$ with $x_1^2 + x_2^2 + x_3^2 + x_1x_2x_3 = k = 4 + 2\ell^2$. This implies that $3 \leq x_1 \leq k^{\frac{1}{3}}$ and $x_1 \leq x_2 \leq \left(\frac{k}{x_1}\right)^{\frac{1}{2}}$. Now, the proof above requires that at least one of the variables is odd; but in fact at least 2 variables are odd (by considering the equation modulo 4). It follows that we derive a contradiction if we follow the proof above with $q \neq \ell$.

On the other hand, if $q = \ell$, since two variables are odd, we can choose one, say x_1 satisfying $3 \le x_1 \le \sqrt{\frac{k}{3}}$ with $\ell | (x_1^2 - 4)$. Then $\ell | (x_1 - 2)$ or $\ell | (x_1 + 2)$ so that $x_1 + 2 \ge \ell t$ for some $t \ge 1$. Then we get

$$\ell - 2 \le \ell t - 2 \le x_1 \le \sqrt{\frac{4 + 2\ell^2}{3}},$$

so that $3(\ell - 2)^2 \le 4 + 2\ell^2$, which implies that $\ell < 13$, a contradiction.

To complete the proof, it remains to check that our choice of k is not exceptional, that is there are no solutions with say x_1 equal to 0, ± 1 or ± 2. If $x_1 = 0$, then since two variables are odd, we have x_2 and x_3 are odd with $x_2^2 + x_3^2 = 4 + 2\ell^2$. The left side is congruent to 2 while the right is congruent to 6 modulo 8. Next, if $x_1 = \pm 1$, we have $x_2^2 + x_3^2 - x_2 x_3 = 3 + 2\ell^2$. Completing the square gives us $(2x_1 - x_3)^2 + 3x_3^2 = 4(3 + 2\ell^2)$, so that $8\ell^2$ is a quadratic residue modulo 3. This is a fallacy since $8\ell^2 \equiv 2$. Finally, the case $x_1 = \pm 2$ is trivially dealt with since it implies that 2 is a square. □

We continue below with variants of this construction of Hasse failures, their densities being no more than the k's in Prop. 8.1, which is $K^{\frac{1}{2}} (\log K)^{-\frac{1}{2}}$ and establishes Theorem 1.2(i).

Proposition 8.2 *Suppose $v^2 \equiv 25$ (mod 32) with v having all prime factors $\equiv \pm 1$ (mod 12). Then, $V_k(\mathbb{Z})$ is empty with $k = 4 + 12v^2$, but has local solutions. The smallest v is 37, with $k = 16432$.*

Proof It is obvious that with the choice of k, the conditions of Prop. 6.1 are satisfied so that local solutions exist.

We first consider congruences modulo 12, where the squares are in $\{0, 1, 4, 9\}$. Suppose (x_1, x_2, x_3) is a solution to

$$x_1^2 + x_2^2 + x_3^2 + x_1 x_2 x_3 = 4 + 12v^2, \tag{24}$$

with v as above.

If $2 \nmid x_1 x_2 x_3$, then $x_1^2 - 4 \equiv 5 \pmod{12}$ or is divisible by 3 (the same holding for x_2 and x_3). From (24) we have

$$w^2 - 48v^2 = (x_1^2 - 4)(x_2^2 - 4), \tag{25}$$

so that if $x_1^2 - 4 \equiv 5 \pmod{12}$, there is a prime $p \equiv \pm 5 \pmod{12}$ with $p | (x_1^2 - 4)$. This is not possible since $p \nmid v$ implies that 3 is a quadratic residue (mod p), a fallacy. The same holds for x_2 and x_3, so that we may assume that $x_1^2 \equiv x_2^2 \equiv x_3^2 \equiv 1 \pmod{12}$, so that each lies in the set $\{\pm 1, \pm 5\}$ modulo 12.

If $x_1 \equiv \pm 5$, then in $x_1^2 - 4 = (x_1 - 2)(x_2 + 2)$, at least one factor is congruent to ± 5, so that the argument above with a prime p gives a contradiction. Hence we may assume that $x_1 \equiv \pm 1 \pmod{12}$, and the same for x_2 and x_3. But then 9 divides the right hand side of (25), a contradiction.

Next, if $2 \nmid x_1 x_2$, but $2|x_3$, we see that a Vieta map gives the solution $(x_1, x_2, -(x_1 x_2 + x_3))$ with all coordinates odd, so that the previous analysis give a contradiction.

Hence we assume x_1, x_2 and x_3 are all even, so that changing variables gives us the equation

$$y_1^2 + y_2^2 + y_3^2 + 2y_1 y_2 y_3 = 1 + 3\nu^2, \tag{26}$$

with the corresponding

$$w_1^2 - 3\nu^2 = (y_1^2 - 1)(y_2^2 - 1). \tag{27}$$

If y_1 is odd, then $8|(y_1^2 - 1)$ so that 3 is a quadratic residue mod 8, a fallacy. Hence we assume all y_1, y_2 and y_3 are even. We now consider congruences modulo 16. We first note that $1 + 3\nu^2 \equiv 12 \pmod{16}$, so that we cannot have 4 dividing each of the variables.

Next, if $4|y_1, 4|y_2$ and $y_3 \equiv 2 \pmod 4$, then (26) gives us $y_3^2 \equiv 12 \pmod{16}$, an impossibility. Similarly if $4|y_1$ but $y_2 \equiv y_3 \equiv 2 \pmod 4$, then $y_2^2 + y_3^2 \equiv 12 \pmod{16}$, which we see again is impossible. Thus, we may assume that $y_1 \equiv y_2 \equiv y_3 \equiv 2 \pmod 4$, in which case we write $y_1 = 2z_1$, $y_2 = 2z_2$ and $y_3 = 2z_3$, with $2 \nmid z_1 z_2 z_3$. Then (26) becomes

$$z_1^2 + z_2^2 + z_3^2 + 4z_1 z_2 z_3 = 1 + 3\left(\frac{\nu^2 - 1}{4}\right).$$

The left hand side is congruent to 7 modulo 8, while the right is congruent to 3. Hence the result follows. □

Proposition 8.3 *Suppose $\nu \equiv \pm 4$ (mod 9) with ν having all prime factors $\equiv \pm 1$ (mod 20). Then, $V_k(\mathbb{Z})$ is empty with $k = 4 + 20\nu^2$, but has local solutions. The smallest ν is 41, with $k = 33624$.*

Proof The proof is very much the same as the one above, with a small change. The squares modulo 20 lie in the set $\{0, 1, \pm 4, 5, 9\}$ and the odd primes in $\{\pm 1, \pm 3, \pm 7, \pm 9\}$.

Write $w^2 - 80\nu^2 = (x_1^2 - 4)(x_2^2 - 4)$. If $5|x_1$, there must exist a prime $p \equiv \pm 2$ modulo 5 dividing $x_1^2 - 4$, so that since $p \nmid \nu$, 80 is a quadratic residue modulo p, which is false using quadratic reciprocity. So we may assume $5 \nmid x_1 x_2 x_3$ so that $x_j^2 - 4$ is not 1 modulo 20.

If $2 \nmid x_1x_2x_3$, since x_1 is odd, we have $x_1^2 - 4 \equiv -3$ or 5 modulo 20. Assume the former. Then, if there is a prime factor $p|(x_1^2 - 4)$, with $p \equiv \pm 3$ or ± 7 (mod 20), then $w^2 \equiv 80v^2 \pmod{p}$, so that 5 is a quadratic residue modulo p; that is p a quadratic residue modulo 5, which is not true. Hence $x_1^2 - 4$ must have a prime factor $p \equiv 9 \pmod{20}$. But then, $x_1^2 - 4 \equiv 3$ implies that there must be another prime factor $q \equiv \pm 3$ or ± 7 all modulo 20, and that leads to a contradiction. Hence we cannot have $x_1^2 - 4 \equiv -3 \pmod{20}$, and the same being so for x_2 and x_3. Hence we must have $x_1^2 - 4 \equiv x_2^2 - 4 \equiv 5 \pmod{20}$, so that $w^2 - 80v^2 = (x_1^2 - 4)(x_2^2 - 4)$ implies that $25|80$.

If $2 \nmid x_1x_2$, but $2|x_3$, the Vieta map gives the solution $(x_1, x_2, -(x_1x_2 + x_3))$ with all coordinates odd, so that the previous analysis give a contradiction. Hence we assume x_1, x_2 and x_3 are all even, so that changing variables gives us the equation

$$y_1^2 + y_2^2 + y_3^2 + 2y_1y_2y_3 = 1 + 5v^2, \tag{28}$$

with the corresponding

$$w_0^2 - 5v^2 = (y_1^2 - 1)(y_2^2 - 1). \tag{29}$$

If y_1, y_2 and y_3 are all even, then we have a contradiction in (28) since $v^2 \equiv 1 \pmod{4}$. If y_1 is odd, then $8|(y_1^2 - 1)$ so that 5 is a quadratic residue mod 8, a fallacy. The result follows. □

9 Proof of Theorem 1.2(ii)

The proofs for the case $k > 0$ and $k < 0$ are almost identical with the main difference being in the choice of our functions and the domains of the variables. We give here the details for the case $k > 0$ and indicate the modification for $k < 0$ in a remark below.

Let $K \to \infty$ be our main (large) parameter, and let A be a secondary parameter satisfying $(\log K)^2 < A \ll_\varepsilon K^\varepsilon$, with $\varepsilon > 0$ sufficiently small. Let $\mathcal{A}$ be the interval $[\sqrt{A}, A]$. Lastly we use a parameter $m = \prod_{p \le L} p^B$, where we put $L = \frac{\log A}{\log\log A}\Phi(A)$ and $B = \frac{\log\log A}{\Phi(A)^2}$ with $\Phi(A) \to \infty$ with A. Then, $m \sim A^{\frac{1}{\Phi(A)}}$ as $A \to \infty$.

For any $a \in \mathcal{A}$, put

$$g_a(x_1, x_2) = x_1^2 + x_2^2 + ax_1x_2 \quad \text{and} \quad f_a(x_1, x_1) = g_a(x_1, x_2) + a^2. \tag{30}$$

It will be convenient to denote by D_a the discriminant $a^2 - 4$ of the indefinite quadratic form g_a above, for each $a \in \mathcal{A}$. Completing the square shows that

$4g_a(x_1, x_2) = (2x_1 + ax_2)^2 - D_a x_2^2$, so that we consider the form $G_d(s_1, s_2) = s_1^2 - ds_2^2$ with $d = D_a$ (not a complete square). We then define the sector $\mathcal{S}_d$ in the plane as

$$\begin{aligned}\mathcal{S}_d &= \left\{(s_1, s_2) : s_1,\ s_2 \geq 0,\ \ 0 \leq G_d(s_1, s_2) \leq 1,\ \ 2\sqrt{d}s_2 \leq s_1 \leq 3\sqrt{d}s_2 \right\}, \\ &= \left\{(x_1, x_2) : \begin{array}{c} x_1,\ x_2 \geq 0,\ 0 \leq g_a(x_1,\ x_2) \leq \frac{1}{4}, \\ \frac{1}{2}\left(2\sqrt{d} - a\right)x_2 \leq x_1 \leq \frac{1}{2}\left(3\sqrt{d} - a\right)x_2 \end{array} \right\}. \end{aligned} \tag{31}$$

Remark 9.1 For $k < 0$ we define $g_a(x_1, x_2) = x_1^2 + x_2^2 - ax_1x_2$ and define the sector $\mathcal{S}_d$ with the constants 2 and 3 replaced by $\frac{1}{3}$ and $\frac{1}{2}$ respectively. This then leads to some minor changes for the sector in the variable x_1 and x_2.

Next, we define the scaled region

$$\sqrt{X}\mathcal{S}_d = \left\{\left(\sqrt{X}s_1, \sqrt{X}s_2\right) :\ (s_1, s_2) \in \mathcal{S}_a\right\}.$$

It is easily shown that

$$\mathrm{Vol}(\sqrt{X}\mathcal{S}_d) = C\frac{X}{\sqrt{d}},$$

with $C = \frac{1}{4}\log\frac{3}{2}$.

For $2 \leq k \leq K$, we define

$$R_d(k) = \#\left\{(s_1, s_2) \in \sqrt{K}\mathcal{S}_d \cap \mathbb{Z}^2 :\ G_d(s_1, s_2) = k \text{ and } 2|(s_1 - s_2)\right\}. \tag{32}$$

Lemma 9.2 *For d and m as above we have*

$$\sum_{k \leq K} R_d(k) = \frac{CK}{2\sqrt{d}} + O_\varepsilon\left(K^{\frac{1}{2}+\varepsilon}\right).$$

Proof By the definition of $\mathcal{S}_d$, we break up the sum in s_1 and s_2 into the ranges so that $\mathcal{S}_d = \mathcal{S}_d^{(1)} \cup \mathcal{S}_d^{(2)}$ with

$$\mathcal{S}_d^{(1)} = \left\{s_2 \leq \sqrt{\frac{K}{8d}},\ 2\sqrt{d}s_2 \leq s_1 \leq 3\sqrt{d}s_2,\ 2|(s_1 - s_2)\right\},$$

and

$$\mathcal{S}_d^{(2)} = \left\{ \sqrt{\frac{K}{8d}} \le s_2 \le \sqrt{\frac{K}{3d}},\ 2\sqrt{d}s_2 \le s_1 \le \sqrt{K + ds_2^2},\ 2|(s_1 - s_2) \right\}.$$

The sums are easily evaluated. □

Lemma 9.3 *For a and m as above and for any α_1 and α_2, we have*

$$\sum_{\substack{x_1 \equiv \alpha_1(m) \\ x_2 \equiv \alpha_2(m) \\ f_a(x_1,x_2) \le K \\ (x_1,x_2) \in \sqrt{4K}\mathcal{S}_{D_a} \cap \mathbb{Z}^2}} 1 = \frac{2CK}{\sqrt{D_a}m^2} + O_\varepsilon\left(K^{\frac{3}{4}+\varepsilon}\right),$$

with the error term uniform is all other variables.

Proof By (30) we have trivially $x_1,\ x_2 \ll \sqrt{K}$. Assuming $0 \le \alpha_j < m$, we put $x_j = \alpha_j + ml_j$ with $1 \le l_j \ll \frac{\sqrt{K}}{m}$. Then $(x_1, x_2) \in \sqrt{4K}\mathcal{S}_{D_a} \cap \mathbb{Z}^2$ and $x_2 \ll K^{\frac{1}{4}+\varepsilon}$ gives at most $O(K^{\frac{1}{2}+\varepsilon})$ lattice points, so that we may assume that $K^{\frac{1}{4}+\varepsilon} \ll x_1,\ x_2 \ll \sqrt{K}$. It is then easily checked that $C_1' l_2 \le l_1 \le C_2' l_2$, with $C_j' = C_j\left(1 + O(K^{-\frac{1}{4}+\varepsilon})\right)$, where we have put $C_1 = \frac{1}{2}\left(2\sqrt{d} - a\right)$ and $C_2 = \frac{1}{2}\left(3\sqrt{d} - a\right)$ as in (31).

Next $\left|f_a(x_1, x_2) - m^2 f_a(l_1, l_2)\right| \ll K^{\frac{1}{2}+\varepsilon}$. The error in replacing the condition $f_a(x_1, x_2) \le K$ with the condition $m^2 g_a(l_1, l_2) \le K$ is at most $O(K^{\frac{1}{2}+\varepsilon})$ since we are counting lattice points in a hyperbolic segment of width $K^{\frac{1}{2}+\varepsilon}$, with the variables restricted as above. Thus

$$\sum_{\substack{x_1 \equiv \alpha_1(m) \\ x_2 \equiv \alpha_2(m) \\ f_a(x_1,x_2) \le K \\ (x_1,x_2) \in \sqrt{4K}\mathcal{S}_{D_a} \cap \mathbb{Z}^2}} 1 = \sum_{\substack{g_a(l_1,l_2) \le \frac{K}{m^2} \\ (l_1,l_2) \in \sqrt{\frac{4K}{m^2}}\mathcal{S}^*_{D_a} \cap \mathbb{Z}^2}} 1 + O_\varepsilon\left(K^{\frac{1}{2}+\varepsilon}\right),$$

where $\mathcal{S}^*$ means the constants have been perturbed by about $O(K^{-\frac{1}{4}+\varepsilon})$, as discussed above. Completing the square shows that the last sum is over the s_1 and s_2 variables as in (31) with the constraint that $s_1 - s_2$ is even, and with the constants 2 and 3 defining the inequalities perturbed with the addition of $O(K^{-\frac{1}{4}+\varepsilon})$. Applying Lemma 9.2 with K replaced with $\frac{4K}{m^2}$ gives the result, with C replaced with $C + O(K^{-\frac{1}{4}+\varepsilon})$.

□

Corollary 9.4 *For $a \in \mathcal{A}$ and $k \leq K$ let*

$$r_a(k) = \#\left\{(x_1, x_2) \in \sqrt{4K}\mathcal{S}_a \cap \mathbb{Z}^2 : f_a(x_1, x_2) = k\right\}.$$

Then

$$\sum_{k \leq K} r_a(k) = \frac{2CK}{\sqrt{D_a}} + O_\varepsilon\left(K^{\frac{1}{2}+\varepsilon}\right).$$

We now set

$$b_{\mathcal{A}}(k) = \sum_{a \in \mathcal{A}} r_a(k), \tag{33}$$

and we are interested in this as a function of k for $1 \leq k \leq K$. From Corollary 9.4, we have

$$\sum_{1 \leq k \leq K} b_{\mathcal{A}}(k) = CK \log A + O(KA^{-1}), \tag{34}$$

so that the mean-value of $b_{\mathcal{A}}(k)$ is $C \log A$. Our main goal is to estimate the deviation of $b_{\mathcal{A}}(k)$ from its predicted value in terms of local masses. Let $\delta(V_k)$ denote the formal singular series for

$$V_k : \qquad x_1^2 + x_2^2 + x_3^2 + x_1x_2x_3 = k, \tag{35}$$

so that $\delta(V_k) = \prod_{p<\infty} \delta_p(V_k)$, with

$$\delta_p(V_k) = \lim_{\nu \to \infty} \frac{\#V_k(\mathbb{Z}/p^\nu\mathbb{Z})}{p^\nu}.$$

These are given explicitly in the Appendices and Section 5. Define

$$\delta^{(m)}(k) = \frac{\#V_k(\mathbb{Z}/m\mathbb{Z})}{m^2} := \frac{r_m(k)}{m^2}. \tag{36}$$

Note that $\delta^{(m)}(k)$ depends on k modulo m. With this, we define our variance

$$V(K) = V(K, A, m) = \sum_{k \leq K} \left(b_{\mathcal{A}}(k) - C(\log A)\delta^{(m)}(k)\right)^2. \tag{37}$$

We expand (37) as $\Sigma_1 + \Sigma_2 + \Sigma_3$. We have

$$\begin{aligned}\Sigma_3 &= C^2(\log A)^2 \sum_{l \,(\mathrm{mod}\, m)} \delta^{(m)}(l)^2 \sum_{\substack{k\le K\\ k\equiv l\,(\mathrm{mod}\, m)}} 1\,,\\ &= C^2(\log A)^2 \left(\frac{K}{m} + O(1)\right) \sum_{l \,(\mathrm{mod}\, m)} \delta^{(m)}(l)^2,\\ &= C^2(\log A)^2 \,(K + O(m))\, \delta_m\left(V^{(2)}\right),\end{aligned} \tag{38}$$

where we define

$$V^{(2)}: \qquad x_1^2 + x_2^2 + x_3^2 + x_1x_2x_3 = y_1^2 + y_2^2 + y_3^2 + y_1y_2y_3, \tag{39}$$

and $\delta_m\left(V^{(2)}\right)$ is the singular series for $V^{(2)}$ over $\mathbb{Z}/m\mathbb{Z}$.

Next,

$$\begin{aligned}\Sigma_2 &= -2C(\log A) \sum_{k\le K} b_{\mathcal{A}}(k)\delta^{(m)}(k) = -\log A \sum_{l \,(\mathrm{mod}\, m)} \delta^{(m)}(l) \sum_{\substack{k\le K\\ k\equiv l\,(\mathrm{mod}\, m)}} b_{\mathcal{A}}(k),\\ &= -2C\log A \sum_{l \,(\mathrm{mod}\, m)} \delta^{(m)}(l) \sum_{a\in\mathcal{A}} \sum_{\substack{k\le K\\ k\equiv l\,(\mathrm{mod}\, m)}} r_a(k).\end{aligned} \tag{40}$$

Now, for each $a \in \mathcal{A}$, the last sum in (40) above is

$$\sum_{\substack{k\le K\\ k\equiv l\,(\mathrm{mod}\, m)}} r_a(k) = \sum_{\substack{\alpha_1,\alpha_2\,(\mathrm{mod}\, m)\\ f_a(\alpha_1,\alpha_2)\equiv l\,(\mathrm{mod}\, m)}} \sum_{\substack{y_1\equiv\alpha_1\,(\mathrm{mod}\, m)\\ y_2\equiv\alpha_2\,(\mathrm{mod}\, m)\\ f_a(y_1,y_2)\le K\\ (y_1,y_2)\in\sqrt{4K}\mathcal{S}_a}} 1. \tag{41}$$

Applying Lemma 9.3 to the inner sum gives

$$\sum_{\substack{k\le K\\ k\equiv l\,(\mathrm{mod}\, m)}} r_a(k) = \sum_{\substack{\alpha_1,\alpha_2\,(\mathrm{mod}\, m)\\ f_a(\alpha_1,\alpha_2)\equiv l\,(\mathrm{mod}\, m)}} \frac{2CK}{am^2}\left(1 + O(a^{-2})\right),$$

so that

$$\begin{aligned}\sum_{\substack{k\le K\\ k\equiv l \pmod m}} b_{\mathcal{A}}(k) &= \frac{2CK}{m^2} \sum_{\substack{\beta \pmod m\\ \alpha_1,\alpha_2 \pmod m\\ f_\beta(\alpha_1,\alpha_2)\equiv l \pmod m}} \left(\sum_{\substack{a\in\mathcal{A}\\ a\equiv\beta \pmod m}} \left(a^{-1}+O(a^{-3})\right)\right),\\ &= \frac{2CK}{m^3}\left(\frac{1}{2}\log A + O(A^{-\frac{1}{2}})\right) \sum_{\substack{\beta \pmod m\\ \alpha_1,\alpha_2 \pmod m\\ f_\beta(\alpha_1,\alpha_2)\equiv l \pmod m}} 1, \qquad (42)\\ &= \frac{2CK}{m}\left(\frac{1}{2}\log A + O(A^{-\frac{1}{2}})\right)\delta^{(m)}(l).\end{aligned}$$

Combining (40) with (42) gives us

$$\begin{aligned}\Sigma_2 &= -2C^2\frac{K}{m}\left((\log A)^2 + O(A^{-\frac{1}{2}}\log A)\right)\sum_{l \pmod m}\delta^{(m)}(l)^2,\\ &= -2C^2K\left((\log A)^2 + O(A^{-\frac{1}{2}}\log A)\right)\delta_m(V^{(2)}).\end{aligned} \qquad (43)$$

It remains for us to analyze the difficult case Σ_1. We have

$$\begin{aligned}\Sigma_1 = \sum_{k\le K} b_{\mathcal{A}}^2(k) &= \sum_{a_1,\,a_2\in\mathcal{A}}\sum_{k\le K} r_{a_1}(k)r_{a_2}(k),\\ &= \sum_{a\in\mathcal{A}}\sum_{k\le K} r_a^2(k) + \sum_{\substack{a_1,\,a_2\in\mathcal{A}\\ a_1\ne a_2}}\sum_{k\le K} r_{a_1}(k)r_{a_2}(k).\end{aligned} \qquad (44)$$

The diagonal term above can be estimated from

Lemma 9.5

(a). For R_d as in (32), we have

$$\sum_{k\le K} R_d^2(k) \ll \frac{K}{\sqrt{d}} + \frac{K\log K}{d}\tau(d),$$

(b).

$$\sum_{a\in\mathcal{A}}\sum_{k\le K} r_a^2(k) \ll K\log A.$$

where $\tau(\,)$ is the divisor function, and all implied constants are absolute.

Proof Since we are obtaining upper-bounds, we will discard the condition that $s_1 - s_2$ is even in the definition of $R_d(k)$. By abuse of notation, we denote this

modified counting function by $R_d(k)$ in the proof. Part (b) follows from Part (a) in the same manner that Lemma 9.3 follows from Lemma 9.2, and summing over $a \in \mathcal{A}$, giving

$$\sum_{a\in\mathcal{A}}\sum_{k\le K} r_a^2(k) \ll K\log A + \frac{K\log K\log A}{\sqrt{A}} \ll K\log A,$$

since $(\log K)^2 \ll A \ll K^{\varepsilon}$.

For the proof of Part (a), we write $\mathbf{s}_j = (s_j, t_j)$ for $j = 1, 2$ to get

$$R_d^2(k) = \#\left\{(\mathbf{s}_1, \mathbf{s}_2) \,:\, s_1^2 - dt_1^2 = s_2^2 - dt_2^2 = k,\ \mathbf{s}_j \in \sqrt{K}\mathcal{S}_d,\ j = 1, 2\right\},$$

so that we have

$$\sum_{k\le K} R_d^2(k) = \#\left\{(\mathbf{s}_1, \mathbf{s}_2) :\, s_1^2 - dt_1^2 = s_2^2 - dt_2^2 \le K,\ \mathbf{s}_j \in \sqrt{K}\mathcal{S}_d,\ j = 1, 2\right\}. \tag{45}$$

Now $\mathbf{s}_j \in \sqrt{K}\mathcal{S}_d$ and $s_j^2 - dt_j^2 \le K$ imply that

$$s_1, s_2 \ll \sqrt{K} \quad \text{and} \quad t_1, t_2 \ll \sqrt{\frac{K}{d}}$$

Switching the roles of t_1 and t_2 in (45) shows that

$$\sum_{k\le K} R_d^2(k) \le \#\left\{(\mathbf{s}_1, \mathbf{s}_2) :\, s_1^2 + dt_2^2 = s_2^2 + dt_1^2,\ s_j \ll K^{\frac{1}{2}}, t_j \ll \left(\frac{K}{d}\right)^{\frac{1}{2}},\ j = 1, 2\right\}.$$

Since the forms are now positive definite, we apply Theorem 2 of [6], which gives the estimate in the Lemma. □

The inner sum in the off-diagonal term in (44) can be analyzed by using Kloostermann's method (see [29] and [39] for a modern treatment and uniformity with our parameters) to give, for $a_1 \ne a_2$

$$\sum_{k\le K} r_{a_1}(k) r_{a_2}(k) = \delta_\infty^{(K)}(a_1, a_2)\,\delta_{\text{fin}}(a_1, a_2) \ + O(K^{1-\varepsilon_0}), \tag{46}$$

for some $\varepsilon_0 > 0$. Here, $\delta_\infty^{(K)}(a_1, a_2)$ is the singular integral and $\delta_{\text{fin}}(a_1, a_2) = \prod_{p<\infty}\delta_p(a_1, a_2)$, where $\delta_p(a_1, a_2)$ is the singular series, both associated to the equation

$$V_{a_1,a_2} : \quad f_{a_1}(x_1, x_2) = f_{a_2}(y_1, y_2), \tag{47}$$

with

$$\delta_p(a_1, a_2) = \lim_{\nu\to\infty} \frac{\#V_{a_1,a_2}(\mathbb{Z}/p^\nu\mathbb{Z})}{p^{3\nu}}. \tag{48}$$

For the singular integral, let $\sqrt{4K}\mathcal{S}_{a_1,a_2} = \sqrt{4K}\mathcal{S}_{a_1} \times \sqrt{4K}\mathcal{S}_{a_2}$ and let χ_{a_1,a_2} be its characteristic function (here we abuse notation by writing $\mathcal{S}_{a_j}$ instead of $\mathcal{S}_{D_{a_j}}$). Then,

$$\begin{aligned}\delta_\infty^{(K)}(a_1, a_2) &= \int_{-\infty}^{\infty}\left[\int_{\mathbb{R}^4} \chi_{a_1,a_2}(\mathbf{x}, \mathbf{y})\, e\left(t(g_{a_1}(\mathbf{x}) - g_{a_2}(\mathbf{y}) + a_1^2 - a_2^2)\right) \mathrm{d}\mathbf{x}\mathrm{d}\mathbf{y}\right] \mathrm{d}t,\\ &= \lim_{\epsilon\to 0}\frac{1}{\epsilon}.\mathrm{Vol}\left((\mathbf{x}, \mathbf{y}) \in \sqrt{4K}\mathcal{S}_{a_1,a_2} : |g_{a_1}(\mathbf{x}) - g_{a_2}(\mathbf{y}) + a_1^2 - a_2^2| < \epsilon\right),\\ &= \frac{4C^2K}{a_1a_2}\left[1 + O(A^{-1})\right].\end{aligned} \tag{49}$$

Hence, from (44) and (46) we have

$$\Sigma_1 = 4C^2K\left(1 + O(A^{-1})\right) \sum_{\substack{a_1,\, a_2\in\mathcal{A}\\ a_1\neq a_2}} \frac{\delta_{\mathrm{fin}}(a_1, a_2)}{a_1a_2} + O\left(K\log A + K^{1-\varepsilon_0}A^2\right). \tag{50}$$

To analyse the main term in (50), we replace $\delta_{\mathrm{fin}}(a_1, a_2)$ with $\delta^{(m)}(a_1, a_2)$, where

$$\delta^{(m)}(a_1, a_2) := \frac{\#V_{a_1,a_2}(\mathbb{Z}/m\mathbb{Z})}{m^3}. \tag{51}$$

The error term in doing so in (50) has size

$$\ll K\sum_{s\geq 1} \sum_{\substack{a_1,a_2\in\mathcal{A}\\ a_1\neq a_2\\ \gcd(D_{a_1},D_{a_2})=s}} \frac{\left|\delta_{\mathrm{fin}}(a_1, a_2) - \delta^{(m)}(a_1, a_2)\right|}{a_1a_2}. \tag{52}$$

According to Appendix B, $\delta^{(m)}(a_1, a_2)$ is suitably close to $\delta_{\mathrm{fin}}(a_1, a_2)$ unless $s = \gcd\left(D_{a_1}, D_{a_2}\right)$ is in the set

$$S_{\mathcal{A},m} := \left\{ s : s = \prod_{j=1}^{t} p_j^{e_j} \text{ with either } e_j \geq B \text{ or } p_j > L \text{ for some } j \right\}.$$

Moreover, for such a_1 and a_2, the difference $\left|\delta_{\text{fin}}(a_1, a_2) - \delta^{(m)}(a_1, a_2)\right|$ is $O(\tau(s))$, with $\tau(.)$ the divisor function. Hence the contribution to (52) from these is at most

$$\sum_{s \in S_{\mathcal{A},m}} \tau(s) \sum_{\substack{a_1, a_2 \in \mathcal{A} \\ \gcd(D_{a_1}, D_{a_2}) = s}} \frac{1}{a_1 a_2}. \tag{53}$$

Since $D_a \equiv 0 \pmod{k}$ occurs only if $a \equiv \pm 2 \pmod{\frac{s}{2^\alpha}}$ with $0 \leq \alpha \leq 3$, the sums in (53) above are bounded by

$$(\log A)^2 \sum_{s \in S_{\mathcal{A},m}} \frac{\tau(s)}{s^2} \ll (\log A)^2 \ \min\left(L, 2^B\right)^{-\frac{1}{2}}, \tag{54}$$

because $s \in S_{\mathcal{A},m}$ implies $s \geq \min(L, 2^B)$ and $a_1,\ a_2 \neq \pm 2$.

Next, for $s \notin S_{\mathcal{A},m}$, we write

$$\delta_{\text{fin}}(a_1, a_2) = \prod_{p \leq L} \delta_p(a_1, a_2) \prod_{p > L} \delta_p(a_1, a_2).$$

Recall from Prop. B.5 that $\delta_p(a_1, a_2) = 1 + O(p^{-2})$ if $p \nmid D_{a_1} D_{a_2} \left(D_{a_1} - D_{a_2}\right)$ when $p \geq 3$. We denote these primes by $\mathcal{P}^{(1)}$ and include $p = 2$ in this set, and denote the remaining finite set of primes by $\mathcal{P}^{(2)}$. We decompose $\mathcal{P}^{(2)}$ further into $\mathcal{P}^{(3)} = \left\{p \geq 3 : p | \gcd\left(D_{a_1}, D_{a_2}\right)\right\}$ and its complement. Then we write

$$\begin{aligned}\prod_{p > L} \delta_p(a_1, a_2) &= \prod_{\substack{p \in \mathcal{P}^{(1)} \\ p > L}} \delta_p(a_1, a_2) \prod_{\substack{p \in \mathcal{P}^{(2)} \\ p > L}} \delta_p(a_1, a_2), \\ &= \prod_{\substack{p \in \mathcal{P}^{(2)} \\ p > L}} \delta_p(a_1, a_2) \left(1 + O\left(\frac{1}{L}\right)\right).\end{aligned}$$

Since $s \notin S_{\mathcal{A},m}$, if $p > L$ we have (using Prop. B.5 again)

$$\log \prod_{\substack{p \in \mathcal{P}^{(2)} \\ p > L}} \delta_p(a_1, a_2) = \sum_{\substack{p \in \mathcal{P}^{(2)} \\ p > L}} \frac{c_p}{p} + O\left(\frac{1}{L}\right),$$

with coefficients c_p satisfying $|c_p| \leq 1$. Since $a_1 \neq \pm a_2$ and $a_j \neq \pm 2$, the set $\mathcal{P}^{(2)}$ has the bound $\text{card}(\mathcal{P}^{(2)}) \ll \frac{\log A}{\log \log A}$, as it contains those primes dividing

D_{a_1} or D_{a_2} or $\left(D_{a_1} - D_{a_2}\right)$. Hence the sum over $\mathcal{P}^{(2)}$ above is bounded by $\frac{\log A}{L \log\log A} \ll \Phi(A)^{-1}$. Thus, for $s \notin S_{\mathcal{A},m}$ we have

$$\delta_{\text{fin}}(a_1, a_2) = \prod_{p \le L} \delta_p(a_1, a_2) \times \left(1 + O\left(\frac{1}{\Phi(A)}\right)\right).$$

To analyse this further, we write $\delta^{(m}(a_1, a_2) = \prod_{p \le L} \delta_p^{(m)}(a_1, a_2)$. Then one has

$$\delta_p(a_1, a_2) = 1 + \sum_{l=1}^{\infty} N_l(a_1, a_2) \quad \text{and} \quad \delta_p^{(m)}(a_1, a_2) = 1 + \sum_{l=1}^{B} N_l(a_1, a_2), \tag{55}$$

where

$$N_l(a_1, a_2) = p^{-4l} \sideset{}{^*}\sum_{b \,(\text{mod } p^l)} \sum_{\mathbf{x},\, \mathbf{y} \,(\text{mod } p^l)} e\left(\frac{g_{a_1}(\mathbf{x}) - g_{a_2}(\mathbf{y}) + D_{a_1} - D_{a_2}}{p^l} b\right). \tag{56}$$

Then for $s \notin S_{\mathcal{A},m}$, one has by Prop B.4 that $\delta_p(a_1, a_2) = \delta_p^{(m)}(a_1, a_2) + O(p^{-B})$. It follows that the contribution to (52) is

$$\begin{aligned} K \sum_{\substack{s \ge 1 \\ s \notin S_{\mathcal{A},m}}} \sum_{\substack{a_1,\, a_2 \in \mathcal{A} \\ a_1 \ne a_2 \\ \gcd(D_{a_1}, D_{a_2}) = s}} & \frac{\left|\delta_{\text{fin}}(a_1, a_2) - \delta^{(m)}(a_1, a_2)\right|}{a_1 a_2} \\ & \ll K \min\left(\Phi(A), 2^B\right)^{-1} \sum_{\substack{a_1,\, a_2 \in \mathcal{A} \\ a_1 \ne a_2}} \frac{\left|\delta^{(m)}(a_1, a_2)\right|}{a_1 a_2}, \\ & \ll K \min\left(\Phi(A), 2^B\right)^{-1} (\log A)^2, \end{aligned}$$

using $\delta^{(m)}(a_1, a_2) \ll \tau(\gcd(a_1, a_2))$.

We choose $\Phi(A) = \frac{1}{2}\sqrt{\frac{\log\log A}{\log\log\log A}}$ so that $\Phi(A)^2 \ll 2^B = o(L)$. Substituting into (50) gives us

$$\Sigma_1 = 4C^2 K \sum_{\substack{a_1,\, a_2 \in \mathcal{A} \\ a_1 \ne a_2}} \frac{\delta^{(m)}(a_1, a_2)}{a_1 a_2} + O\left(K \Phi(A)^{-1} (\log A)^2\right). \tag{57}$$

Since $\delta^{(m)}(a_1, a_2)$ is periodic modulo m, the sum in (57) can be analyzed as in (38), giving

$$\Sigma_1 = 4C^2K \sum_{\substack{\alpha_1 \,(\mathrm{mod}\, m)\\ \alpha_2 \,(\mathrm{mod}\, m)}} \delta^{(m)}(\alpha_1, \alpha_2) \frac{\left(\frac{1}{2}\log A\right)^2}{m^2} + O\left(K\Phi(A)^{-1}(\log A)^2\right), \tag{58}$$
$$= C^2K\,(\log A)^2\,\delta_m\left(V^{(2)}\right) + O\left(K\Phi(A)^{-1}(\log A)^2\right).$$

Combining (38), (43) and (57) into (37) gives us the key cancellation and hence the estimate on the variance $V(K)$.

Proposition 9.6 *Let $K \to \infty$, let $\mathcal{A}$ be the interval $[\sqrt{A},\ A]$ with A satisfying $(\log K)^2 < A \ll_\varepsilon K^\varepsilon$, with $\varepsilon > 0$ sufficiently small. Then with $\Phi(A) = \frac{1}{2}\sqrt{\frac{\log\log A}{\log\log\log A}}$, we have*

$$\frac{1}{K}\sum_{k\le K}\left[\frac{b_{\mathcal{A}}(k)}{\log A} - C\delta^{(m)}(k)\right]^2 \ll_\varepsilon \Phi(A)^{-1}.$$

Remark 9.7 One can remove the auxiliary parameter B in the Proposition above with

$$\delta^{(m)}(k) = \prod_{p\le L}\delta_p(k) + O(2^{-B}),$$

as follows. From (B4) and (35), we have $\delta(V_k) = \prod_{p<\infty}\delta_p(k)$ with $\delta_p(k) = 1 + \sum_{l\ge 1} N_l(k)$, where $N_l(k)$ is given in (B3) with all evaluated in the Appendix. Similarly, one shows that $\delta^{(m)}(k) = \prod_{p\le L}\delta_p^{(m)}(k)$, with $\delta_p^{(m)}(k) = 1 + \sum_{1\le l\le B} N_l(k)$. Then, it follows from Prop. B.1 that $\delta_p^{(m)}(k) = \delta_p(k) + O(p^{-B})$. Applying Prop B.2 then gives the result.

9.1 Lower bound for $\delta^{(m)}(k)$ for most admissible k's

To complete the proof of Theorem 1.2(ii), we need to estimate, for $\varepsilon > 0$

$$\left|\left\{0 \le k \le K\ :\ k \text{ admissible},\ \delta^{(m)}(k) < \varepsilon\right\}\right|. \tag{59}$$

By Props. B.5 and B.12 in the Appendix, and Remark 9.7 , we can write

$$\delta^{(m)}(k) = \prod_{p\le L}\left(1 + N_{1,p}(k) + \mathcal{C}_p(k)\right) + o(1), \tag{60}$$

where we indicate the dependence of p in the definition of N_l, and with $\mathcal{C}_p(k)$ coming from the $N_{l,p}$'s with $l \geq 2$. Since we are assuming that k is admissible, we can ignore the primes $p = 2$ and $p = 3$ since then these local factors are bounded from below. For $p \geq 5$, the problematic case of $\mathcal{C}_p(k)$ in (60) is, by Prop. B.1, of the form $4^{\beta} p^{-1} + O\left(p^{-2}\right)$. So, up to $O\left(p^{-2}\right)$, which can be ignored for our purposes of bounding $\delta^{(m)}(k)$ from below, we have that

$$\begin{aligned} \delta^{(m)}(k) &\gg \prod_{p \leq L} \left(1 + N_{1,p}(k) + O\left(\frac{1}{p^2}\right)\right) + o(1), \\ &\gg \prod_{p \leq L} \left(1 + \frac{\chi(k-4)\,(3 + \chi(k))}{p}\right), \end{aligned} \tag{61}$$

where χ is the Legendre symbol modulo p. Hence

$$\begin{aligned} \left[\delta^{(m)}(k)\right]^{-1} &\ll \prod_{p \leq L} \left(1 - \frac{\chi(k-4)\,(3 + \chi(k))}{p}\right), \\ &= \sum_{n \leq M} \frac{\mu(n) A(k,n)}{n}, \end{aligned} \tag{62}$$

where $A(k,n) = A(k,p_1) \ldots A(k,p_l)$ if $n = p_1 \ldots p_l$, $M = \left(\prod_{p \leq L} p\right) \leq m \ll K^{\varepsilon}$, and

$$A(k,p) = \begin{cases} \chi(k-4)\,(3 + \chi(k)) & \text{if } p \geq 5, \\ 0 & \text{otherwise.} \end{cases} \tag{63}$$

Since $A(k,n)$ as a function of k is periodic of period n, we have

$$\sum_{k \leq K} A(k,n) = \frac{K}{n} \sum_{k \,(\mathrm{mod}\, n)} A(k,n) + O(n). \tag{64}$$

By multiplicativity, the completed sum

$$\sum_{k \,(\mathrm{mod}\, n)} A(k,n) = \prod_{p \mid n} \left(\sum_{k \,(\mathrm{mod}\, p)} A(k,p) \right) = \mu(n),$$

since $\sum_{k \,(\mathrm{mod}\, p)} \chi(k-4) = 0$ and $\sum_{k \,(\mathrm{mod}\, p)} \chi(k-4)\chi(k) = -1$. Hence

$$\sum_{k \leq K} A(k,n) = \frac{\mu(n)}{n} K + O(n),$$

so that by (62) we have

$$\sum_{\substack{k\le K\\ k \text{ admissible}}} \left[\delta^{(m)}(k)\right]^{-1} \ll K\left(\sum_n \frac{1}{n^2}\right) + M \ll K.$$

Hence, it follows that for any $\varepsilon > 0$

$$\left|\left\{0 \le k \le K : k \text{ admissible}, \ \delta^{(m)}(k) < \varepsilon\right\}\right| \ll \varepsilon K. \tag{65}$$

Finally, combining (65) with the variance estimate in Prop. 9.6 gives Theorem 1.2(ii). □

10 Computations

We computed all the Hasse failures (HF), and also the number of orbits $\mathfrak{h}(k)$ for positive generic k's with $k \le K$ where K is about $K_0 = 564 \times 10^6$ (the limitation imposed by memory usage and computation time). An extended version of this section can be found in Sect. 10 of our preprint [26]. We state some conjectures based on these computations.

The number of admissible k's (see Sect. 3) in the interval $[1, K]$ we denote by $\mathcal{A}(K)$, and is asymptotically $\frac{7}{12}K$. The admissibles consist of the exceptional k's, of which there are $O(\frac{K}{\sqrt{\log K}})$ members, the generic k's consisting of the Hasse failures (HF) and the generic k's with $\mathfrak{h}(k) > 0$. For $K \ge 5$, let $\mathcal{A}_{HF}(K)$ denote the number of HF's in the interval $[5, K]$. By the arguments in Sect. 7, $\mathcal{A}_{HF}(K) \gg_\epsilon K^{\frac{1}{2}-\epsilon}$ for any $\epsilon > 0$. While we do not know the exact order of $\mathcal{A}_{HF}(K)$, Theorem 1.2(ii) shows that it is $o(K)$, and we consider this question computationally, for which we compare $\mathcal{A}_{HF}(K)$ with $\mathcal{A}(K)$.

There are two possible models to consider, namely (1) $\mathcal{A}_{HF}(K) \sim C\mathcal{A}(K)^\theta$ for some $0 < \theta < 1$ or (2) $\mathcal{A}_{HF}(K) \sim C\mathcal{A}(K)/(\log \mathcal{A}(K))^\theta$. Since K is of limited size in our computations, we cannot distinguish between these two cases with confidence, but the latter seemed unlikely from the data. For the former, the graphical data for $\log \mathcal{A}_{HF}(K)/\log \mathcal{A}(K)$ with $\mathcal{A}(K) = \frac{7}{12}K$ is in Fig. 7. Our data suggests that

$$\mathcal{A}_{HF}(K) \sim C K^{0.8875\ldots + o(1)}, \tag{66}$$

for some constant C, at least for K in this range. The error is smaller than 0.1% for $K \ge 10^7$ and gets better for larger values of K.

For further justification that $\mathcal{A}_{HF}(K) \sim C\mathcal{A}(K)^\theta$ rather than $\mathcal{A}_{HF}(K) \sim C\mathcal{A}(K)/(\log \mathcal{A}(K))^\theta$, we look at the distribution of HF's within subintervals. Taking $K = K_0$ and subdividing the interval $[5, K_0]$ into subintervals

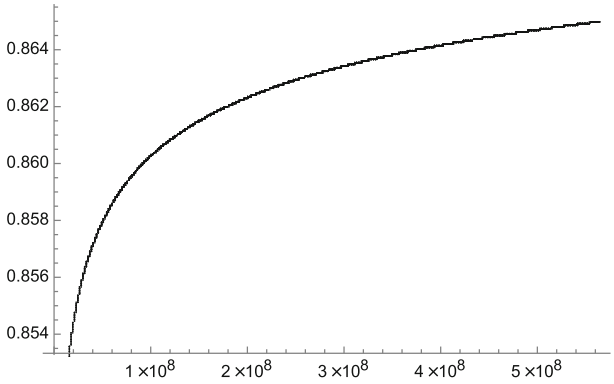

Fig. 7 Plot of $\frac{\log \mathcal{A}_{HF}(K)}{\log \mathcal{A}(K)}$

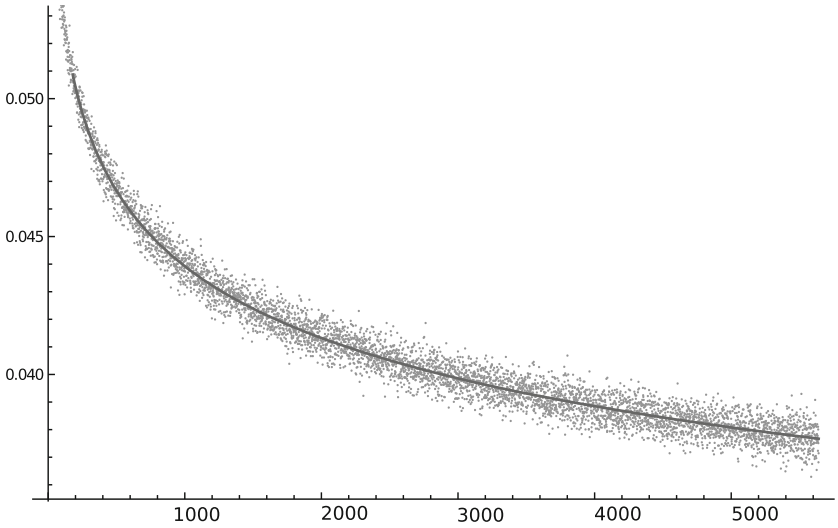

Fig. 8 Average of Hasse failures in subintervals

of length h, we compare the average number of HF's in each subinterval $\frac{1}{h}\left(\mathcal{A}_{HF}((l+1)h) - \mathcal{A}_{HF}(lh)\right)$ for $1 \leq l \leq \frac{K_0}{h}$ with what we might expect from the derivative of our predicted function. Taking $h = 10^5$ (chosen to be comparable to $\sqrt{K_0}$), we plot $\frac{1}{h}\left(\mathcal{A}_{HF}((l+1)h) - \mathcal{A}_{HF}(lh)\right)$ against l in Fig. 8. The curve in the graph is an approximation, given by $g(x) \approx x^{-0.0908}$. This power decay suggests $\mathcal{A}_{HF}(K) \sim C\mathcal{A}(K)^{\theta}$ with a θ close to that given in (66).

Finally we include graphical data in Fig. 9 on the distribution of the number of orbits $\mathfrak{h}(k)$ with generic $k \leq K$ with $K = 10^7$ (this smaller value compared to K_0 above due to long computational times). Here, $\mathfrak{n}(h) = \mathfrak{n}_K(h)$ is the number of occurrences of $h = \mathfrak{h}(k)$ with k running through generic integers

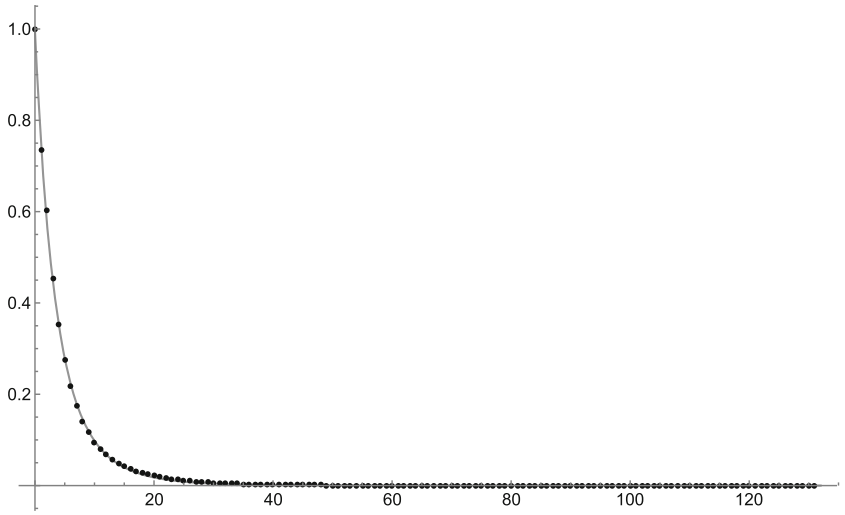

Fig. 9 Occurences of relative number of orbits: $\mathfrak{n}(\mathfrak{h}(k))/\mathfrak{n}(0)$, generic $k \leq 10^7$. Approximation curve $\frac{\mathfrak{n}(h)}{\mathfrak{n}(0)} \approx e^{-1.92905\sqrt{h+1}}$, $h = \mathfrak{h}(k)$ on x-axis

in $[1, K]$. Our count also includes the number of Hasse failures, denoted by $\mathfrak{n}(0)$. Since $\mathfrak{n}(0)$ grows with K, we normalize our counts and consider the distribution of $\frac{\mathfrak{n}(h)}{\mathfrak{n}(0)}$. We find that this quantity appears to behave like the graph of $e^{-\sqrt{h+1}}$. If so, this suggests that $\frac{\mathfrak{n}(h+1)}{\mathfrak{n}(h)} \sim 1 - \frac{1}{2}h^{-\frac{1}{2}}$ as $h \to \infty$. This is roughly consistent with our data where for example with $h = 21$, we have $\frac{\mathfrak{n}(h+1)}{\mathfrak{n}(h)} = 0.88921$ while $1 - \frac{1}{2}h^{-\frac{1}{2}} = 0.89089$. By Lemma 7.2, the average value of $\mathfrak{h}(k)$ with $0 \leq k \leq K$ has size about $(\log K)^2$. Since $\mathfrak{n}(0)$ has size a power of K, the data with its suggested exponential decay (at least in this short range for K) suggests that the maximal value of $\mathfrak{h}(k)$ is probably a power of $\log K$, or at worst $\mathfrak{h}(k) \ll_\epsilon k^\epsilon$, for $\epsilon > 0$. As mentioned in the introduction, the best we know is $\mathfrak{h}(k) \ll_\varepsilon k^{\frac{1}{3}+\varepsilon}$. For $K = 10^7$, the maximum value for $\mathfrak{h}(k)$ in our data was 131, while $(\log K)^2 \approx 61$ and $K^{\frac{1}{3}} \approx 412$.

We end this section with some basic Conjectures concerning the class numbers $\mathfrak{h}(k)$, suggested by our theoretical results as well as the discussion above.

Conjecture 10.1 For any $\varepsilon > 0$ and generic k

$$\mathfrak{h}(k) \ll_\varepsilon |k|^\varepsilon.$$

Conjecture 10.2 1. The number of Hasse failures for $0 \leq k \leq K$ satisfies

$$\left| \{0 \leq k \leq K : \mathfrak{h}(k) = 0 \text{ and } k \text{ admissible } \} \right| \sim C_0 K^\theta,$$

for some $C_0 > 0$ and some $\frac{1}{2} < \theta < 1$.

2. More generally, for $t \geq 1$

$$\left| \{0 \leq k \leq K : \mathfrak{h}(k) = t \ \} \right| \sim C_t K^{\theta},$$

with $C_t \approx e^{-\alpha\sqrt{t}}$, for some $\alpha > 0$.

Acknowledgements We thank V. Blomer, E. Bombieri, J. Bourgain, T. Browning, C. McMullen, P. Whang and U. Zannier for insightful discussions. AG thanks the Institute for Advanced Study and Princeton University for making possible visits during part of the years 2015-2017 when much of this work took place. He also acknowledges support from the IAS, a Simons Foundation grant No. 634846 and his home Department. He dedicates this article to his family Priscilla, Armand and Saskia. PS was supported by NSF grant DMS 1302952. The softwares Eureqa® and Mathematica© were used on a PC running Linux to generate some of the data. Additional computations were done at the OSU-HPCC at Oklahoma State University, which is supported in part through the NSF grant OCI-1126330. We also thank the referees for suggestions that improved the paper.

Appendix

The appendix consists of (A) a discussion of invariants of affine cubic forms referred to in the Introduction, and (B) computation of local masses δ_p, for primes $p \geq 2$ (with some details omitted); their structure is used in the proofs in Sect. 9.

Notation: To reduce clutter we will use $\chi(*)$ to denote the Legendre symbol $(\frac{*}{p})_L$, with p fixed. We also use χ_4 and χ_8 to denote some characters modulo 4 and 8 respectively.

Appendix A: Arithmetic invariants of affine cubic forms

A number of invariants of f as an element of the unique factorization domain $R = \mathbb{Q}[x_1, x_2, \ldots, x_n]$, enter into the study of the values assumed by such an affine cubic form f. The first is the $\hbar$-invariant from [23]: $\hbar(f)$ is the minimal integer h for which

$$f_0 = L_1 Q_1 + L_2 Q_2 + \ldots + L_h Q_h, \tag{A1}$$

where the L_j's are homogeneous linear and the Q_j's are homogeneous quadratic members of R; equivalently $n - \hbar(f)$ is the dimension of the largest $\mathbb{Q}$-linear subspace contained in $W_0 = \{\mathbf{x} : f_0(\mathbf{x}) = 0\}$, the linear space given by $L_1 = L_2 = \ldots = L_h = 0$. Note that $\hbar(f) = 1$ iff f_0 is reducible in R, and in this case W_0 contains a rational hypersurface.

Closely related are the $\mathbb{Q}$-invariants $\ell(f)$ and $q(f)$ defined as the dimensions of the largest $\mathbb{Q}$-affine linear subspaces U_ℓ and U_q of $\mathbb{A}^n$ on which the restriction of f to U_ℓ is linear (non-constant) and to U_q is quadratic. So, $\ell(f)$ and $q(f)$ lie in $[0, n-1]$. Of particular interest to us is that

$$\hbar(f) = 1 \quad \text{iff} \quad q(f) = n - 1. \tag{A2}$$

The group $\mathrm{Aff}_n(\mathbb{Z})$ consisting of integral affine linear maps $\mathbf{x} \to A\mathbf{x} + \mathbf{b}$ with $A \in \mathrm{GL}_n(\mathbb{Z})$ and $\mathbf{b} \in \mathbb{Z}^n$, acts on the integral cubic polynomials by a change of variable. The arithmetic invariants as well as the diophantine questions concerning $V_{k,f}(\mathbb{Z})$ are all preserved by this action. On the leading homogeneous cubic term f_0, the action is that of $\mathrm{GL}_n(\mathbb{Z})$, which has been well studied in terms of its invariants. With these fixed, there are finitely many $\mathrm{GL}_n(\mathbb{Z})$ orbits, see [5] for a recent discussion of the case $n = 3$, which is our interest. In this case the vector space of f_0's is 10-dimensional and it's quotient by SL_3 is 2-dimensional, given by the Aronhold invariants I and J. The vector space of f's is 20-dimensional and its quotient by Aff_3 is 9-dimensional. The invariants for this action up to the additive constant term and at a generic point are $I(f_0)$, $J(f_0)$ together with the 6-dimensional vector space associated with the homogeneous quadratic part of f.

We end with some examples of affine cubic forms and their invariants.

(1). $S(\mathbf{x}) = x_1^3 + x_2^3 + x_3^3$, $\hbar(S) = 3, \ell(S) = q(S) = 0$;
(2). $M(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 - x_1x_2x_3$, $\hbar(M) = 1, \ell(M) = 0, q(M) = 2$;
(3). $T(\mathbf{x}) = x_1x_2x_3 + x_1 + x_2$ (perhaps the mildest perturbation of the fully split form $x_1x_2x_3$), $\hbar(M) = 1, \ell(M) = q(M) = 2$ (the restriction of T to $x_3 = 0$ is linear). From the last it follows that $\mathfrak{v}_T(k) = |V_{k,T}(\mathbb{Z})| = \infty$; however T is not perfect or even almost perfect since $V_{k,T}(\mathbb{Z})$ is not Zariski dense in $V_{k,T}$ for $k \neq 0$.
(4). $P(\mathbf{x}) = x_1x_2x_3 + (x_1 - 1)Q_1(\mathbf{x}) + (x_2 - 1)Q_2(\mathbf{x})$, with Q_1, Q_2 generic quadratics. Then, $\ell(P) = q(P) = 1$ (with $x_1 = x_2 = 1$ giving the line U_ℓ). In particular, $V_{k,P}(\mathbb{Z}) \neq \emptyset$ for every k. We expect that P is full.

Appendix B: Analysis of the local masses

B.1 Computation of $\delta_p(k)$ for odd primes

For any integer k and prime $p \geq 3$, we determine

$$\delta_p(k) = \lim_{l \to \infty} |V_k(\mathbb{Z}/\, p^l\mathbb{Z})|\, p^{-2l}.$$

Define

$$N_l(k) = p^{-3l} \sideset{}{^*}\sum_{b \,(\mathrm{mod}\, p^l)} \sum_{\mathbf{x} \,(\mathrm{mod}\, p^l)} e\left(\frac{f(\mathbf{x}) - k}{p^l} b\right), \tag{B3}$$

where $\mathbf{x} = (x_1, x_2, x_3)$, $f(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 - x_1 x_2 x_3$ and the asterisk denotes a sum over those b's not divisible by p. Then one has

$$\delta_p(k) = 1 + \sum_{l=1}^{\infty} N_l(k). \tag{B4}$$

In what follows, we analyze the case $l \geq 2$ (the case $l = 1$ is determined by Lemma 6.4). For $p \geq 3$ one has

$$N_l(k) = p^{-3l} \sideset{}{^*}\sum_{b \,(\mathrm{mod}\, p^l)} e\left(\frac{4(4-k)}{p^l} b\right) \sum_{\mathbf{x}} e\left(\frac{(2x_3 - x_1 x_2)^2 - (x_1^2 - 4)(x_2^2 - 4)}{p^l} b\right). \tag{B5}$$

Making a change of variable shows that the inner sum over $\mathbf{x}$ is

$$\sum_u \sum_{x_1, x_2} e\left(\frac{bu^2}{p^l}\right) e\left(\frac{-b(x_1^2 - 4)(x_2^2 - 4)}{p^l}\right) = S(b; p^l) \times \sum_x e\left(\frac{4b(x^2 - 4)}{p^l}\right) \times \overline{S\left(b(x^2 - 4); p^l\right)}, \tag{B6}$$

where for $q \geq 1$ we put

$$S(b; q) = \sum_{r \,(\mathrm{mod}\, q)} e\left(\frac{br^2}{q}\right). \tag{B7}$$

Using properties of the Gauss sum, we get

Proposition B.1 *For $p \geq 3$ we have*

(a). $$N_1(k) = \chi(k-4)\,[3 + \chi(k)]\,\frac{1}{p} + \frac{1}{p^2};$$

(b). if $l \geq 3$ is odd,

$$N_l(k) = \begin{cases} 4p^{-\frac{1}{2}(l+1)} \chi\left(\frac{k-4}{p^{l-1}}\right) & \text{if } p^{l-1} | (k-4), \\ p^{-\frac{1}{2}(l+1)} \chi\left(\frac{k}{p^{l-1}}\right) & \text{if } p^{l-1} | k, \\ 0 & \text{otherwise;} \end{cases}$$

(c). if $l \geq 2$ is even, then

$$N_l(k) = \begin{cases} -p^{-\frac{l+2}{2}} \{4\eta_{l-1}(k-4) + \eta_{l-1}(k)\} & \text{if } p^{l-1}||k(k-4), \\ p^{-\frac{l}{2}} \left(1 - \frac{1}{p}\right) \{4\eta_l(k-4) + \eta_l(k)\} & \text{if } p^l|k(k-4), \\ 0 & \text{otherwise}, \end{cases}$$

where we define $\eta_l(m) = 1$ if $p^l|m$ and is zero otherwise.

To compute $\delta_p(k)$ for $p \geq 3$ in (B4), we write $\delta_p(k) = 1 + N_1(k) + \mathfrak{S}_p(k)$. Define $\mu \geq 0$ by $p^\mu||k(k-4)$. By Prop. B.1, $\mu = 0$ implies $N_l(k) = 0$ for $l \geq 2$, so that we have $\mathfrak{S}_p(k) = 0$ for this case. For $\mu \geq 1$, we have $p^\mu||(k - 4\beta)$, with $\beta = 0$ or 1. Then we combine Prop. B.1 in (B4), to get

$$\mathfrak{S}_p(k) = 4^\beta \times \begin{cases} p^{-1} - p^{-\frac{1}{2}(\mu+1)} - p^{-\frac{1}{2}(\mu+3)} & \text{if } 2 \nmid \mu, \\ p^{-1} - p^{-\frac{\mu}{2}-1} \left(1 - \chi\left(\frac{k-4\beta}{p^\mu}\right)\right) & \text{if } 2|\mu. \end{cases} \tag{B8}$$

In particular, we see that if $\mu = 1$, then $\mathfrak{S}_p(k) = -4^\beta p^{-2}$ while if $\mu \geq 2$ then $\mathfrak{S}_p(k) = 4^\beta p^{-1} + O(p^{-2})$.

Combining (B8) with Prop. B.1(a) in (B4) gives

Proposition B.2 *For $p \geq 3$, suppose $p^\mu||k(k-4)$ with $\mu \geq 0$. We have*

(a). if $\mu = 0$, then $\delta_p(k) = 1 + \chi(k-4)\,[3 + \chi(k)]\,\frac{1}{p} + \frac{1}{p^2}$;

(b). if $p||k$, then $\delta_p(k) = 1 + 3\chi(-1)\frac{1}{p}$;

(c). if $p||(k-4)$, then $\delta_p(k) = 1 - \frac{3}{p^2}$;

(d). if $\mu \geq 2$ and $p|k$, then

$$\delta_p(k) = 1 + \begin{cases} (1 + 3\chi(-1))\, p^{-1} + p^{-2} - p^{-\frac{1}{2}(\mu+1)} - p^{-\frac{1}{2}(\mu+3)} & \text{if } 2 \nmid \mu, \\ (1 + 3\chi(-1))\, p^{-1} + p^{-2} - p^{-\frac{\mu}{2}-1} \left(1 - \chi\left(\frac{k}{p^\mu}\right)\right) & \text{if } 2|\mu; \end{cases}$$

(e). if $\mu \geq 2$ and $p|(k-4)$, then

$$\delta_p(k) = 1 + \begin{cases} 4p^{-1} + p^{-2} - 4p^{-\frac{1}{2}(\mu+1)} - 4p^{-\frac{1}{2}(\mu+3)} & \text{if } 2 \nmid \mu, \\ 4p^{-1} + p^{-2} - 4p^{-\frac{\mu}{2}-1} \left(1 - \chi\left(\frac{k}{p^\mu}\right)\right) & \text{if } 2|\mu. \end{cases}$$

Remark B.3 The case (b) shows that $\delta_3(k) = 0$ if $k \equiv 3$ or 6 (mod 9), while case (a) and (d) shows that $\delta_3(k) > 0$ otherwise.

B.2 Local factors associated with V_{a_1,a_2}, odd primes

We next state (without details) the analogous results for the density function $\delta_p(a_1, a_2)$ in (48) for the surface V_{a_1,a_2} in (47). Recalling the properties in (55) and (56), since p is odd, completing the square gives us

$$N_l(a_1, a_2) = p^{-3l} \sum_{b \,(\mathrm{mod}\, p^l)}^{*} e\left(4b\frac{D_{a_1} - D_{a_2}}{p^l}\right) \overline{S(bD_{a_1}; p^l)} S(bD_{a_2}; p^l). \tag{B9}$$

Again, using properties of the Gauss sums gives us

Proposition B.4 *Let $a_1 \neq a_2$ be fixed, and let $p \geq 3$.*

(a). Suppose $p \nmid D_{a_1} D_{a_2} \left(D_{a_1} - D_{a_2}\right)$. Then

$$N_l(a_1, a_2) = \begin{cases} -\frac{\chi\left(D_{a_1} D_{a_2}\right)}{p^2} & \text{if } l = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(b). Suppose $p \nmid D_{a_1} D_{a_2}$ and $p^{\mu} || \left(D_{a_1} - D_{a_2}\right)$ with $\mu \geq 1$. Then

$$N_l(a_1, a_2) = \begin{cases} \frac{1}{p^l}\left(1 - \frac{1}{p}\right) & \text{if } l \leq \mu, \\ -p^{-\mu-2} & \text{if } l = \mu + 1, \\ 0 & \text{otherwise.} \end{cases}$$

(c). Suppose $p^{\alpha} || D_{a_1}$ but $p \nmid D_{a_2}$ with $\alpha \geq 1$. Then

$$N_l(a_1, a_2) = \begin{cases} p^{-1} & \text{if } l = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(d). Suppose $p^{\eta_1} || D_{a_1}$, $p^{\eta_2} || D_{a_2}$ and $p^{\mu} || \left(D_{a_1} - D_{a_2}\right)$ with η_1, η_2 and $\mu \geq 1$. Putting $\eta = \min(\eta_1, \eta_2)$ gives us

$$N_l(a_1, a_2) = \begin{cases} \left(1 - \frac{1}{p}\right) & \text{if } 1 \leq l \leq \eta, \\ p^{-1} & \text{if } l = \eta + 1,\ \eta_1 \neq \eta_2, \\ -p^{-\eta-2} \chi\left(\frac{D_{a_1}}{p^{\eta}}\right) \chi\left(\frac{D_{a_2}}{p^{\eta}}\right) & \text{if } l = \eta + 1,\ \eta_1 = \eta_2 \leq \mu, \\ 0 & \text{otherwise.} \end{cases}$$

It then follows that

Proposition B.5 *Let $a_1 \neq a_2$ be fixed, and let $p \geq 3$.*

(a). Suppose $p \nmid D_{a_1} D_{a_2} \left(D_{a_1} - D_{a_2}\right)$. Then

$$\delta_p(a_1, a_2) = 1 - \frac{\chi\left(D_{a_1} D_{a_2}\right)}{p^2}.$$

(b). Suppose $p \nmid D_{a_1} D_{a_2}$ and $p^\mu || \left(D_{a_1} - D_{a_2}\right)$ with $\mu \geq 1$. Then

$$\delta_p(a_1, a_2) = \left(1 + \frac{1}{p}\right)\left(1 - \frac{1}{p^{\mu+1}}\right).$$

(c). Suppose $p | D_{a_1} D_{a_2}$ but $p \nmid \left(D_{a_1} - D_{a_2}\right)$. Then

$$\delta_p(a_1, a_2) = \left(1 + \frac{1}{p}\right).$$

(d). Suppose $p^{\eta_1} || D_{a_1}$, $p^{\eta_2} || D_{a_2}$ and $p^\mu || \left(D_{a_1} - D_{a_2}\right)$ with η_1, η_2 and $\mu \geq 1$. Putting $\eta = \min(\eta_1, \eta_2)$ gives us

$$\delta_p(a_1, a_2) = \begin{cases} (1+\eta) - \frac{\eta-1}{p} & \text{if } \eta_1 \neq \eta_2, \\ (1+\eta) - \frac{\eta}{p} - \frac{1}{p^2}\chi\left(\frac{D_{a_1}}{p^\eta}\right)\chi\left(\frac{D_{a_2}}{p^\eta}\right) & \text{if } \eta_1 = \eta_2 = \mu, \\ (1+\eta) - \frac{\eta-1}{p} - \frac{1}{p^{\mu-\eta+1}}\left(1 + \frac{1}{p}\right) & \text{if } \eta_1 = \eta_2 < \mu. \end{cases}$$

Remark B.6 If $a_1 = a_2 = a$ and $p \geq 3$, one can deduce the result for $\delta_p(a, a)$ from parts (c) and (d) above, with $\mu \to \infty$, giving

(a). if $p \nmid D_a$, then $\delta_p(a, a) = 1 + p^{-1}$, and
(b). if $p^\eta || D_a$ with $\eta \geq 1$, then $\delta_p(a, a) = (1+\eta) - \frac{\eta-1}{p}$.

B.3 The even local factor $\delta_2(k)$

Since the analysis here is a bit more delicate, we provide some additional details. Let $l \geq 0$ and define $F_l(c) = \sum_{x \bmod 2^l} e\left(\frac{cx^2}{2^l}\right)$. Recall the three primitive real characters modulo powers of two: χ_4 modulo 4, χ_8 and $\chi_4\chi_8$ modulo 8, where

$$\chi_4(x) = \left(\frac{-4}{x}\right)_{\mathrm{J}} = \begin{cases} 1 & \text{if } x \equiv 1 \bmod 4, \\ -1 & \text{if } x \equiv 3 \bmod 4, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\chi_8(x) = \left(\frac{8}{x}\right)_{\mathrm{J}} = \begin{cases} 1 & \text{if } x \equiv \pm 1 \bmod 8, \\ -1 & \text{if } x \equiv \pm 3 \bmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

For $l \geq 1$ we define $\omega_l(k)$ to be 1 if $2^l | k$ and 0 otherwise; if $l \leq 0$, we define $\omega_l(k)$ to be 1 always. Given a term $\omega_l(k)$, we define $\hat{k} = \frac{k}{2^l}$. While $\omega_l(k) = \omega_l(-k)$, the corresponding "hat" function is not the same, and the appropriate choice is determined by the ω-function.

We have

Lemma B.7 *Define $\theta \geq 0$ so that $2^\theta || c$. We have*

(a). if $\theta \geq l$, $F_l(c) = 2^l$;
(b). if $\theta = l - 1$, $F_l(c) = 0$;
(c). if $l \geq 2$ and $2 \nmid c$, then $F_l(c) = 2^{\frac{l}{2}} \chi_8(c)^l \, [1 + \chi_4(c) i]$;
(d). if $l \geq 3$ and $1 \leq \theta \leq l - 2$, we have

$$F_l(c) = 2^{\frac{l+\theta}{2}} \chi_8\left(\frac{c}{2^\theta}\right)^{l+\theta} \left[1 + \chi_4\left(\frac{c}{2^\theta}\right) i\right];$$

(e). for $l \geq 1$ and $q \in \mathbb{Z}$,

$$\sum_{b \,(\mathrm{mod}\, 2^l)}^{*} e\left(\frac{qb}{2^l}\right) F_l(b) = \omega_{l-3}(q)\, 2^{\frac{3(l-1)}{2}} \cos\left(\frac{\hat{q}+1}{4}\pi\right) [1 + (-1)^{l+\hat{q}}],$$

where $\hat{q} = \frac{q}{2^{l-3}}$, and the sum over b runs through odd numbers.

Lemma B.8 *For any b and $l \geq 0$, put*

$$Q_l(b; a) = \sum_{x_1, x_2 \,(\mathrm{mod}\, 2^l)} e\left(b \frac{x_1^2 + x_2^2 - a x_1 x_2}{2^l}\right).$$

(a). If $2 | a$, then $Q_l(b; a) = F_l(b) \overline{F_l\left(b(\frac{a^2}{4} - 1)\right)}$,
(b). If $2 \nmid ab$, then $Q_l(b; a) = (-2)^l$.

We now compute $N_l(k)$ given in (B3) with $p = 2$, where the sum over b runs through odd numbers. It will be convenient to compute $N_l(k)$ for some small values and we give it as

Lemma B.9

(a). $N_0(k) = 1$;
(b). $N_1(k) = \frac{1}{4}(-1)^k$;
(c). $N_2(k) = \frac{1}{4}\cos(k\frac{\pi}{2}) + \frac{3}{4}\sin(k\frac{\pi}{2})$;
(d).

$$N_3(k) = \begin{cases} \frac{3}{4}(-1)^{\frac{k+3}{4}} & \text{if } k \equiv 1 \ (mod\ 4), \\ 0 & \text{otherwise.} \end{cases}$$

For $l \geq 4$, we have

$$N_l(k) = 2^{-3l} \sideset{}{^*}\sum_{b \ (\mathrm{mod}\ 2^l)} e\left(-\frac{kb}{2^l}\right) \sum_{a \ (\mathrm{mod}\ 2^l)} e\left(\frac{ba^2}{2^l}\right) Q_l(b; a). \quad \text{(B10)}$$

Using the lemmas above, we conclude

Lemma B.10

(a). If k is odd and $l \geq 4$, $N_l(k) = 0$;
(b). if $l = 4$ then $N_4(k) = 0$ unless $4|k$, in which case

$$N_4(k) = \begin{cases} \frac{1}{2}\chi_4\left(\frac{k}{4}\right) & \text{if } 4||k, \\ \frac{1}{4}(-1)^{\frac{k}{8}+1} & \text{if } 8|k; \end{cases}$$

(c). if $l = 5$, $N_5(k) = 0$ unless $8|k$, in which case $N_5(k) = \frac{3}{4}\chi_4\left(\frac{k}{8}\right)$;
(d). if $l \geq 6$, define $\hat{k} = \frac{k}{2^{l-3}}$ or $\frac{4-k}{2^{l-3}}$. Then, $N_l(k) = 0$ unless $\hat{k} \in \mathbb{Z}$, in which case

$$N_l(k) = \begin{cases} -2^{-\frac{l+1}{2}} \cos\left(\frac{\hat{k}+1}{4}\pi\right)\left[1 + (-1)^{l+\hat{k}}\right] & \text{if } 2^{l-3}|k, \\ 2^{\min(3,\, l-5)-\frac{l+1}{2}} \cos\left(\frac{\hat{k}+1}{4}\pi\right)\left[1 + (-1)^{l+\hat{k}}\right] & \text{if } 2^{l-3}|(k-4). \end{cases}$$

Remark B.11 Note that $\cos\left(\frac{w+1}{4}\pi\right) = \frac{1}{2}\chi_8(w)\,(1 - \chi_4(w)) = \frac{1}{2}\left(\left(\frac{8}{w}\right)_{\mathrm{J}} - \left(\frac{-8}{w}\right)_{\mathrm{J}}\right)$ for odd w.

Combining Lemmas B.9 and B.10 gives us

Proposition B.12 *Suppose $k \neq 0$ or 4. Let $\delta_2(k)$ denote the mass at $p = 2$. Then $\delta_2(k) = 0$ only when $k \equiv 3$ (mod 4). Otherwise $\delta_2(k) \geq \frac{3}{4}$. More precisely,*

(1). If k is odd then

$$\delta_2(k) = \frac{3}{4}\left(1 + \chi_4(k)\right)\left(2 - \chi_8(k)\right);$$

(2). if $2||k$, then $\delta_2(k) = 1$;
(3). if $4||k$, define $\eta \geq 3$ with $2^\eta||(k-4)$, and put $4 - k = 2^\eta w$ with w odd.
(a). if $\eta \geq 6$ is even,

$$\delta_2(k) = \frac{13}{4} - 2^{-\frac{\eta-6}{2}} - \left(\frac{-4}{w}\right)_{\mathrm{J}} 2^{-\frac{\eta-4}{2}} + \left(\left(\frac{8}{w}\right)_{\mathrm{J}} - \left(\frac{-8}{w}\right)_{\mathrm{J}}\right) 2^{-\frac{\eta-2}{2}},$$

(b). if $\eta \geq 7$ is odd, $\delta_2(k) = \frac{13}{4} - 2^{-\frac{\eta-6}{2}} + (-1)^w 2^{-\frac{\eta-5}{2}}$,
(c). if $\eta = 3$, $\delta_2(k) = 1$,
(d). if $\eta = 4$, $\delta_2(k) = 2 + \frac{1}{4}\left(\left(\frac{8}{w}\right)_{\mathrm{J}} - \left(\frac{-8}{w}\right)_{\mathrm{J}}\right)$,
(e). if $\eta = 5$, $\delta_2(k) = 2 + \frac{1}{4}(-1)^w$;
(4). if $8|k$, define $\eta \geq 3$ with $2^\eta||k$, and put $k = 2^\eta w$ with w odd.
(a). if $\eta \geq 6$ is even,

$$\delta_2(k) = \frac{5}{2} - 2^{-\frac{\eta-6}{2}} + \left(\frac{-4}{w}\right)_{J} 2^{-\frac{\eta-4}{2}} - \left(\left(\frac{8}{w}\right)_{\mathrm{J}} - \left(\frac{-8}{w}\right)_{\mathrm{J}}\right) 2^{-\frac{\eta-2}{2}},$$

(b). if $\eta \geq 7$ is odd, $\delta_2(k) = \frac{5}{2} - 2^{-\frac{\eta-6}{2}} - (-1)^w 2^{-\frac{\eta-5}{2}}$,
(c). if $\eta = 3$, $\delta_2(k) = \frac{5}{2}$,
(d). if $\eta = 4$, $\delta_2(k) = \frac{5}{4} - \frac{1}{4}\left(\left(\frac{8}{w}\right)_{\mathrm{J}} - \left(\frac{-8}{w}\right)_{\mathrm{J}}\right)$,
(e). if $\eta = 5$, $\delta_2(k) = \frac{5}{4} - \frac{1}{4}(-1)^w$;

B.4 Local factors associated with V_{a_1,a_2} for $p = 2$

The analog of (B9) is

$$N_l(a_1, a_2) = 2^{-4l} \sideset{}{^*}\sum_{b \,(\mathrm{mod}\, 2^l)} e\left(b\frac{a_1^2 - a_2^2}{2^l}\right) Q_l(b, a_1)\overline{Q_l(b, a_2)}, \quad \text{(B11)}$$

with $\delta_2(a_1, a_2) = 1 + \sum_{l=1}^{\infty} N_l(a_1, a_2)$. In what follows we have $l \geq 1$.
B.4.1

Suppose $2 \nmid a_1 a_2$ and $2^\eta||(D_{a_1} - D_{a_2})$ with $\eta \geq 3$. Then, by Lemma B.8 we have $Q_l(b, a_1)\overline{Q_l(b, a_2)} = 2^{2l}$.

Hence we get

$$N_l(a_1,a_2)=\begin{cases}2^{-l-1} & \text{if } 1\le l\le \eta,\\ -2^{-l-1} & \text{if } l=\eta+1,\\ 0 & \text{if } l\ge \eta+2,\end{cases} \tag{B12}$$

so that $\delta_2(a_1,a_2)=\frac{3}{2}\left(1-2^{-\eta-1}\right)$.

B.4.2

Next suppose $2|a_1$ and $2\nmid a_2$, so that $\eta=0$. Put $A_1=\frac{a_1^2}{4}-1$ and $2^\theta||A_1$, with $\theta=0$ or $\theta\ge 3$. By Lemmas B.8, B.7 and (B11), we have $N_l(a_1,a_2)=0$ if $l=1$ or $l=\theta+1$. Otherwise, with $l\ge 2$ we have

$$N_l(a_1,a_2)=\frac{(-1)^l}{2^{3l}}\sideset{}{^*}\sum_{b\,(\mathrm{mod}\,2^l)} e\left(b\frac{\sigma}{2^l}\right)F_l(b)F_l(bA_1), \tag{B13}$$

where $\sigma=a_1^2-a_2^2$ is odd.

If $2\le l\le\theta$, Lemma B.7 shows that

$$N_l(a_1,a_2)=(-1)^l 2^{-\frac{3}{2}l}\sideset{}{^*}\sum_{b\,(\mathrm{mod}\,2^l)} e\left(b\frac{\sigma}{2^l}\right)\chi_8(b)\left(1+\chi_4(b)i\right).$$

We now use

Lemma B.13 *Suppose $2^\mu||\sigma$ with $\mu\ge 0$. Then,*

(1). If $l\ge 2$,

$$\sideset{}{^*}\sum_{b\,(\mathrm{mod}\,2^l)} e\left(b\frac{\sigma}{2^l}\right)\chi_4(b)=\begin{cases}2^{\mu+1}\chi_4\left(\frac{\sigma}{2^\mu}\right)i & \text{if } l=2+\mu,\\ 0 & \text{otherwise};\end{cases}$$

(2). If $l\ge 3$, and $\mathfrak{a}=0$ or 1,

$$\sideset{}{^*}\sum_{b\,(\mathrm{mod}\,2^l)} e\left(b\frac{\sigma}{2^l}\right)\chi_4(b)^{\mathfrak{a}}\chi_8(b)=\begin{cases}2^{\mu+\frac{3}{2}}\chi_4\left(\frac{\sigma}{2^\mu}\right)^{\mathfrak{a}}\chi_8\left(\frac{\sigma}{2^\mu}\right)i^{\mathfrak{a}} & \text{if } l=3+\mu,\\ 0 & \text{otherwise},\end{cases}$$

If $\theta\ge 3$, then for $2\le l\le\theta$, we have

$$N_l(a_1,a_2)=\begin{cases}\frac{1}{4} & \text{if } l=2 \text{ or } 3,\\ 0 & \text{if } l\ge 4.\end{cases} \tag{B14}$$

Here we have used the fact that $\sigma=a_1^2-a_2^2=(2u^2)-v^2$ with u and v both odd.

For $l \geq \theta + 2$, with $\theta \geq 0$, we get in (B13)

$$N_l(a_1, a_2) = \frac{(-1)^l}{2^{2l-\theta}} \sideset{}{^*}\sum_{b \,(\mathrm{mod}\, 2^l)} e\left(b\frac{\sigma}{2^l}\right) \chi_8(b)^\theta \left[\left(1 - \chi_4\left(\frac{A_1}{2^\theta}\right)\right) + i\,\chi(b)\left(1 - \chi_4\left(\frac{A_1}{2^\theta}\right)\right)\right].$$

Applying Lemma B.13 shows that $N_l(a_1, a_2) = 0$ for all $l \geq \theta + 2$.

Thus, if $\theta = 0$, then $\delta_2(a_1, a_2) = 1$, while for $\theta \geq 3$ we get $\delta_2(a_1, a_2) = \frac{3}{2}$.

B.4.3

Assume a_1 and a_2 are both even and put $A_j = \left(\frac{a_j}{2}\right)^2 - 1$, so that $A_j \equiv 0,\ 3$ modulo 4. Put $2^{\theta_j} || A_j$ with $\theta_j \geq 0$ but $\theta_j \neq 1,\ 2$ and $C_j = A_j 2^{-\theta_j}$ odd. We will assume that $\theta_1 \leq \theta_2$. Then $a_1^2 - a_2^2 = 4(A_1 - A_2)$ so that $\eta = 2 + t$, say, with $2^t || (A_1 - A_2)$ with $t \neq 1$. We have

$$N_l(a_1, a_2) = 2^{-4l} \sideset{}{^*}\sum_{b \,(\mathrm{mod}\, 2^l)} e\left(b\frac{4\sigma'}{2^l}\right) |F_l(b)|^2 F_l(bA_1)\overline{F_l(bA_2)}, \quad \text{(B15)}$$

where we put $\sigma' = A_1 - A_2$.

Note that $N_l(a_1, a_2) = 0$ if $l = 1$ or $l = \theta_j + 1$, so we assume $l \geq 2$.

(I). If $2 \leq l \leq \theta_1$, then $F_l(bA_j) = 2^l$. Using $|F_l(b)|^2 = 2^{l+1}$ and (B12) shows that $N_l(a_1, a_2) = 1$.

(II). If $\theta_1 + 2 \leq l \leq \theta_2$, using $F_l(bA_2) = 2^l$ and Lemma B.7(d) gives us

$$N_l(a_1, a_2) = 2^{-\frac{3}{2}l + \frac{1}{2}\theta_1 + 1} \chi_8(C_1)^{l+\theta_1} \mathfrak{S}_l(a_1, a_2),$$

where

$$\mathfrak{S}_l(a_1, a_2) = \sideset{}{^*}\sum_{b \,(\mathrm{mod}\, 2^l)} e\left(b\frac{4\sigma'}{2^l}\right) \chi_8(b)^{l+\theta_1} \left[1 + i\,\chi_4(bC_1)\right]. \quad \text{(B16)}$$

Applying (B12) and Lemma B.13 shows that $\mathfrak{S}_l(a_1, a_2) = 0$ except for the cases $\mathfrak{S}_{\theta_1+2}(a_1, a_2) = 2^{\theta_1+1}$ and $\mathfrak{S}_{\theta_1+4}(a_1, a_2) = -2^{\theta_3+1}$.

Thus in this range, if $\theta_1 + 2 \leq \theta_2$ then $N_{\theta_1+2}(a_1, a_2) = \frac{1}{2}$; if $\theta_1 + 4 \leq \theta_2$, then $N_{\theta_1+4}(a_1, a_2) = -\frac{1}{4}$ and $N_l(a_1, a_2) = 0$ for all other l.

(III). For $l \geq \theta_2 + 2$ we get

$$N_l(a_1, a_2) = 2^{-2l+1+\frac{1}{2}(\theta_1+\theta_2)} \chi_8(C_1)^{l+\theta_1} \chi_8(C_2)^{l+\theta_2} \mathfrak{S}_l(a_1, a_2),$$

with

$$\mathfrak{S}_l(a_1,a_2) = \sum_{b(\mathrm{mod}\ 2^l)}^{*} e\left(b\frac{4\sigma'}{2^l}\right)\chi_8(b)^{\theta_1+\theta_2}\left[(1+\chi_4(C_1C_2))+i\left(\chi_4(bC_1)-\chi_4(bC_2)\right)\right].$$

Since C_1 and C_2 are both odd, we have $C_1 \equiv (-1)^{\mathfrak{a}}C_2$ modulo 4 with $\mathfrak{a} = 0,\ 1$. Hence

$$\mathfrak{S}_l(a_1,a_2) = 2i^{\mathfrak{a}} \sum_{b\ (\mathrm{mod}\ 2^l)}^{*} e\left(b\frac{4\sigma'}{2^l}\right)\chi_4(b)^{\mathfrak{a}}\chi_8(b)^{\theta_1+\theta_2}. \tag{B17}$$

If $\theta_1 \neq \theta_2$, then $t = \theta_1$ and $l \geq \theta_2 + 2 \geq 3$. We apply (B12) and Lemma B.13 with $\mu = \theta_1 + 2$ so that $N_l(a_1,a_2) = 0$ except possibly when $l = \theta_1+3, \theta_1+4$ or θ_1+5.

If $l = \theta_1 + 3$ then necessarily $\theta_2 = \theta_1 + 1$, in which case we get $N_l(a_1,a_2) = 0$.

If $l = \theta_1 + 4$ then $\theta_2 = \theta_1 + 1$ or $\theta_2 = \theta_1 + 2$. If the former, then $N_l(a_1,a_2) = 0$. For the latter we get $\mathfrak{S}_l(a_1,a_2) = -(1-\chi_4(C_1C_2))\,2^{\theta_1+3}$ so that $N_l(a_1,a_2) = -\frac{1}{4}(1-\chi_4(C_1C_2))$.

If $l = \theta_1 + 5$ then $\theta_2 = \theta_1+1, \theta_1+2$ or θ_1+3. If $\theta_2 = \theta_1+2$, then $N_l(a_1,a_2) = 0$. If $\theta_2 = \theta_1+1$, then $\mathfrak{S}_l(a_1,a_2) = 2^{l-\frac{1}{2}}\chi_4(C_1)\chi_4\chi_8(C_2)$ while if $\theta_2 = \theta_1+3$, then $\mathfrak{S}_l(a_1,a_2) = 2^{l-\frac{1}{2}}\chi_4\chi_8(C_1)\chi_4(C_2)$. In these latter cases, we get $N_l(a_1,a_2) = 2^{-4}\chi_4\chi_8(C_1)\chi_4(C_2)$ if $\theta_2 = \theta_1+1$ and $N_l(a_1,a_2) = 2^{-3}\chi_4(C_1)\chi_4\chi_8(C_2)$ if $\theta_2 = \theta_1+3$.

Next, suppose $\theta_1 = \theta_2 = \theta$ with $t \geq \theta$ and $l \geq \theta+2$. Then, from (B17), we have $N_l(a_1,a_2) = 0$ if $l \geq t+5$. For the remaining cases we have

(a). if $l = t+4$, $\mathfrak{S}_l(a_1,a_2) = -\chi_4\left(\frac{A_1-A_2}{2^t}\right)\left[\chi_4(C_1)-\chi_4(C_2)\right]2^{l-1}$;
(b). if $l = t+3$, then $\mathfrak{S}_l(a_1,a_2) = -(1+\chi_4(C_1C_2))\,2^{l-1}$;
(c). if $\theta+2 \leq l \leq t+2$, then $\mathfrak{S}_l(a_1,a_2) = (1+\chi_4(C_1C_2))\,2^{l-1}$.

Combining give us the following

Proposition B.14 *Let $a_1 \neq \pm a_2$ and $a_j \neq \pm 2$.*

(1). Suppose $2 \nmid a_1a_2$ *and* $2^\eta || (D_{a_1} - D_{a_2})$ *with* $\eta \geq 3$. *Then*

$$N_l(a_1, a_2) = \begin{cases} 2^{-l-1} & \text{if } 1 \leq l \leq \eta, \\ -2^{-l-1} & \text{if } l = \eta + 1, \\ 0 & \text{if } l \geq \eta + 2; \end{cases}$$

(2). Suppose $2|a_1$ *and* $2 \nmid a_2$, *and let* $2^{2+\theta} || D_{a_1}$. *Then*

$$N_l(a_1, a_2) = \begin{cases} \frac{1}{4} \text{ if } \theta \geq 3 \text{ and } l \in \{2, 3\}, \\ 0 \text{ otherwise } ; \end{cases}$$

(3). For $j = 1,\ 2$ *suppose* $2|a_j$, *and put* $A_j = \frac{1}{4} D_{a_j}$, $C_j = A_j 2^{-\theta_j}$ *with* $2^{\theta_j} || A_j$ *and assume* $\theta_1 \leq \theta_2$. *Also suppose* $2^t || (A_1 - A_2)$ *so that* $t \geq \theta_1$. *We have*

(i). $N_l(a_1, a_2) = 0$ *for* $l = 1, \theta_1 + 1$ *and* $\theta_2 + 1$.

(ii). For $2 \leq l \leq \theta_1$, $N_l(a_1, a_2) = 1$.

(iii). For $l \geq \theta_1 + 2$, *and* $\theta_1 \neq \theta_2$ *we have* $N_l(a_1, a_2) = 0$ *except for the following cases:*

$$N_l(a_1, a_2) = \begin{cases} 2^{-4} \chi_4\chi_8(C_1)\chi_4(C_2) & \text{if } l = \theta_1 + 5 \text{ and } \theta_2 = \theta_1 + 1, \\ 2^{-1} & \text{if } l = \theta_1 + 2 \text{ and } \theta_2 \geq \theta_1 + 2, \\ -2^{-2} \left(1 - \chi_4(C_1C_2)\right) & \text{if } l = \theta_1 + 4 \text{ and } \theta_2 = \theta_1 + 2, \\ 2^{-3} \chi_4(C_1)\chi_4\chi_8(C_2) & \text{if } l = \theta_1 + 5 \text{ and } \theta_2 = \theta_1 + 3, \\ -2^{-2} & \text{if } l = \theta_1 + 4 \text{ and } \theta_2 \geq \theta_1 + 4. \end{cases}$$

(iv). If $\theta_1 = \theta_2 = \theta$, *then*

$$N_l(a_1, a_2) = \begin{cases} -2^{-(l-\theta)} \chi_8(C_1C_2)^{l+\theta} \left(1 + \chi_4(C_1C_2)\right), & \text{if } \theta + 2 \leq l \leq t + 2, \\ -2^{-(t-\theta+3)} \chi_8(C_1C_2)^{t+\theta+1} \left(1 + \chi_4(C_1C_2)\right), & \text{if } l = t + 3, \\ -2^{-(t-\theta+4)} \chi_8(C_1C_2)^{t+\theta} \chi_4\left(\frac{C_1 - C_2}{2^{t-\theta}}\right) \left[\chi_4(C_1) - \chi_4(C_2)\right], & \text{if } l = t + 4, \\ 0, & \text{if } l \geq t + 5. \end{cases}$$

Corollary B.15 *For* $a_1 \neq \pm a_2$ *and* $a_j \neq \pm 2$, *suppose* $2^\theta || \gcd(D_{a_1}, D_{a_2})$. *Then* $\delta_2(a_1, a_2) = \theta + O(1)$ *and* $\delta_2(a_1, a_2) - \delta_2^{(m)}(a_1, a_2) = O\left(2^{-B}\right)$, *where the implied constants are absolute.*

References

1. Auroux, D.: Factorizations in $SL(2, \mathbb{Z})$ and simple examples of inequivalent Stein fillings. J. Symplectic Geom. **13**(2), 261–277 (2015)
2. Baragar, A.: Integral solutions of Markov–Hurwitz equations. J. Number Theory **49**(1), 27–44 (1994)

3. Beukers, F.: Ternary form equations. J. Number Theory **54**, 113–133 (1995)
4. Bhargava, M.: Higher composition laws I: a new view on Gauss composition, and quadratic generalizations. Ann. Math. **159**(1), 217–250 (2004)
5. Bhargava, M., Shankar, A.: Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. Ann. Math. **181**(2), 587–621 (2015)
6. Blomer, V., Granville, A.: Estimates for representation numbers of quadratic forms. Duke Math. J. **135**(2), 261–302 (2006)
7. Booker, A.R.: Cracking the problem with 33. Res. Number Theory **5**(26) (2019)
8. Bourgain, J., Fuchs, E.: A proof of the positive density conjecture for integer Apollonian circle packings. J. Am. Math. Soc. **24**, 945–967 (2011)
9. Bourgain, J., Gamburd, A., Sarnak, P.: Markoff surfaces and strong approximation: 1, arXiv: 1607.01530 (2016)
10. Bourgain, J., Gamburd, A., Sarnak, P.: Markoff triples and strong approximation. Comptes Rendus Math. **354**(2), 131–135 (2016)
11. Browning, T.D.: A survey of applications of the circle method to rational points. Lond. Math. Soc. Lecture Note Series, pp. 89–113, Cambridge University Press (2015)
12. Browning, T.D.: How often does the Hasse principle hold? In: Proceedings of the AMS Summer Institute in Algebraic Geometry, Salt Lake City, 2015, (2018)
13. Browning, T.D., Heath-Brown, D.R.: Integral points on cubic hypersurfaces. Analytic Number Theory: Essays in honour of Klaus Roth, CUP, pp. 75–90 (2009)
14. Browning, T.D., Newton, R.: The proportion of failures of the Hasse norm principle. Mathematika **62**(2), 337–347 (2016)
15. Cantat, S., Loray, F.: Dynamics on character varieties and Malgrange irreducibility of Painlevé VI equation. Ann. de l'institut Fourier **59**(7), 2927–2978 (2009)
16. Cassels, J.W.S.: A note on the Diophantine equation $x^3 + y^3 + z^3 = 3$. Math. Comput. **44**, 265–266 (1985)
17. Cassels, J.W.S., Guy, M.J.T.: On the Hasse principle for cubic surfaces. Mathematika **13**(2), 111–120 (1966)
18. Colliot-Thélène, J., Wittenberg, O.: Groupe de Brauer et points entiers de deux familles de surfaces cubiques affines. Am. J. Math. **134**(5), 1303–1327 (2012)
19. Colliot-Thélène, J.L., Wei, D., Xu, F.: Brauer-Manin obstruction for Markoff surfaces. Annali della Scuola Normale Superiore di Pisa **vol. XXI**, 1257–1313 (2020)
20. Conn, W., Vaserstein, L.N.: On sums of three integral cubes, Contemp. Math., vol. 166, American Mathematical Society, pp. 285–294 (1994)
21. Corvaja, P., Zannier, P.: On the greatest prime factor of Markov pairs, Rendiconti del Seminario Mat. della Università di Padova **116**, 253–260 (eng) (2006)
22. Davenport, H.: On Waring's problem for cubes. Acta Math. **71**, 123–143 (1939)
23. Davenport, H., Lewis, D.J.: Non-homogeneous cubic equations. J. Lond. Math. Soc. **s1–39**(1), 657–671 (1964)
24. Fuchs, C., Zannier, U.: Integral points on curves: Siegel's theorem after Siegel's proof, On Some Applications of Diophantine Approximations (Pisa), Scuola Normale Superiore, pp. 139–157 (2014)
25. Ghosh, A., Meiri, C., Sarnak, P.: Commutators in SL_2 and Markoff surfaces I. N. Z. J. Math. **52**, 773–819 (2022)
26. Ghosh, A., Sarnak, P.: Integral points on Markoff type cubic surfaces, arXiv:1706.06712 [math.NT] (2017)
27. Goldman, W.M.: The modular group action on real characters of a one-holed torus. Geom. Topol. **7**, 443–486 (2003)
28. Heath-Brown, D.R.: The density of zeros of forms for which weak approximation fails. Math. Comput. **59**(200), 613–623 (1992)

29. Heath-Brown, D.R.: A new form of the circle method, and its application to quadratic forms. J. für die reine und Angewandte Math. **481**, 149–206 (1996)
30. Hooley, C.: On the representation of numbers by quaternary and quinary cubic forms: I. Acta Arith **173**(1), 19–39 (2016)
31. Hurwitz, A.: Über eine aufgabe der unbestimmten analysis. Archiv. Math. Phys. **3**, 185–196 (1907)
32. Lang, S., Weil, A.: Number of points of varieties in finite fields. Am. J. Math. **76**(4), 819–827 (1954)
33. Lehmer, D.H.: On the Diophantine equation $x^3+y^3+z^3 = 1$. J. Lond. Math. Soc. **s1–31**(3), 275–280 (1956)
34. Loughran, D., Mitankin, V.: Integral Hasse principle and strong approximation for Markoff surfaces. IMRN /imrn/rnz114 **10**, 1093 (2020)
35. Markoff, A.: Sur les formes quadratiques binaires indéfinies. Math. Annalen **15**, 381–406 (1879)
36. Markoff, A.: Sur les formes quadratiques binaires indéfinies. (second mémoire). Math. Annalen **17**, 379–399 (1880)
37. Mordell, L.J.: Integer solutions of the equation $x^2 + y^2 + z^2 + 2xyz = n$. J. Lond. Math. Soc. **s1–28**(4), 500–510 (1953)
38. Mordell, L.J.: Diophantine Equations. Academic Press, London (1969)
39. Niedermowwe, N.: The circle method with weights for the representation of integers by quadratic forms. J. Math. Sci. **171**(6), 753–764 (2010)
40. Odoni, R.W.K.: A new equidistribution property of norms of ideals in given classes. Acta Arith. **33**(1), 53–63 (1977)
41. Schmidt, W.M.: Equations Over Finite Fields: An Elementary Approach. Lectures Notes in Mathematics, vol. 536. Springer, New York (1976)
42. Schmidt, W.M.: Thue equations with few coefficients. Trans. Am. Math. Soc. **303**(1), 241–255 (1987)
43. Siegel, C.L.: Über einige Anwendungen diophantischer Approximationen. Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. **1**, 209–226 (1929)
44. Thue, A.: Über Annäherungswerte algebraischer Zahlen. J. für die reine und angewandte Math **135**, 284–305 (1909)
45. Vaughan, R.C., Wooley, T.D.: Waring's problem: a survey, Number Theory for the Millennium. III, A. K. Peters, pp. 301–340 (2002)
46. Wang, V.Y.: Approaching cubic Diophantine statistics via mean-value L-function conjectures of Random Matrix Theory type, arXiv:2108.03398 [math.NT] (2021)
47. Whang, J.P.: Nonlinear descent on moduli of local systems. Israel J. Math. **240**, 935–1004 (2020)
48. Wikipedia contributors, Sums of three cubes — Wikipedia, the free encyclopedia, 2019, [Online; accessed 8-September-2019]