

# *Pacific Journal of Mathematics*

**BINARY QUARTIC FORMS WITH BOUNDED INVARIANTS  
AND SMALL GALOIS GROUPS**

CINDY (SIN YI) TSANG AND STANLEY YAO XIAO

# BINARY QUARTIC FORMS WITH BOUNDED INVARIANTS AND SMALL GALOIS GROUPS

CINDY (SIN YI) TSANG AND STANLEY YAO XIAO

We consider integral and irreducible binary quartic forms whose Galois group is isomorphic to a subgroup of the dihedral group of order eight. We first show that the set of all such forms is a union of families indexed by integral binary quadratic forms  $f(x, y)$  of nonzero discriminant. Then, we shall enumerate the  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of all such forms associated to a fixed  $f(x, y)$ .

1. Introduction	249
2. Characterization of forms with small Galois groups	258
3. Basic properties of forms in $V_{\mathbb{R}, f}$ of nonzero discriminant	260
4. Parametrizing forms in $V_{\mathbb{R}, f}$ of nonzero discriminant	266
5. Definition of a bounded semialgebraic set	272
6. Error estimates and the main theorem	281
Acknowledgments	289
References	289

## 1. Introduction

The problem of enumerating  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of integral and irreducible binary forms of a fixed degree has a long history. The quadratic and cubic cases were solved in [Gauss 1801; Siegel 1944] and [Davenport 1951b; 1951c], respectively, where the forms are ordered by the natural height, namely the discriminant  $\Delta(-)$ . The quartic case turns out to be more challenging. This is because the ring of polynomial invariants of quartic forms have two independent generators, usually denoted  $I(-)$  and  $J(-)$ . For

$$(1-1) \quad F(x, y) = a_4x^4 + a_3x^3y + a_2x^2y^2 + a_1xy^3 + a_0y^4,$$

they are given by the explicit formulae

$$I(F) = 12a_4a_0 - 3a_3a_1 + a_2^2,$$

$$J(F) = 72a_4a_2a_0 + 9a_3a_2a_1 - 27a_4a_1^2 - 27a_3^2a_0 - 2a_2^3,$$

MSC2010: 11E76, 11R45.

Keywords: binary quartic forms, coregular spaces, arithmetic statistics.

which are of degrees two and three, respectively. Bhargava and Shankar [2015], instead of using the discriminant, introduced the height function

$$(1-2) \quad H_{\text{BS}}(F) = \max\{|I(F)|^3, J(F)^2/4\}.$$

For  $X > 0$ , let us define

$$N_{\mathbb{Z}}(X) = \#\{[F] : \text{integral and irreducible binary quartic forms } F \text{ such that } H_{\text{BS}}(F) \leq X\},$$

where  $[-]$  denotes  $\text{GL}_2(\mathbb{Z})$ -equivalence class. In [loc. cit.], they proved that

$$(1-3) \quad N_{\mathbb{Z}}(X) = \frac{44\zeta(2)}{135} X^{\frac{5}{6}} + O_{\epsilon}(X^{\frac{3}{4}+\epsilon}) \quad \text{for any } \epsilon > 0.$$

This is the first result ever obtained, and as far as we know, the only known result in the literature, for the quartic case.

**1A. Set-up and notation.** In this paper, we shall also be interested in the quartic case, but only the integral and irreducible binary quartic forms  $F$  with *small* Galois group  $\text{Gal}(F)$ , which is defined to be the Galois group of the splitting field of  $F(x, 1)$  over  $\mathbb{Q}$ . We know that  $\text{Gal}(F)$  is isomorphic to one of the following:

- $S_4$  = the symmetric group on four letters,
- $A_4$  = the alternating group on four letters,
- $D_4$  = the dihedral group of order eight,
- $C_4$  = the cyclic group of order four,
- $V_4$  = the Klein-four group.

We shall say that  $\text{Gal}(F)$  is *small* if it is isomorphic to  $D_4$ ,  $C_4$ , or  $V_4$ . Recall that the *cubic resolvent* of  $F$  is defined by

$$\mathcal{Q}_F(x) = x^3 - 3I(F)x + J(F).$$

Then, equivalently, we have the classical characterization that for irreducible  $F$

$$\text{Gal}(F) \text{ is small if and only if } \mathcal{Q}_F(x) \text{ is reducible.}$$

It turns out that whether  $\text{Gal}(F)$  is small or not may also be characterized in terms of binary quadratic forms and the following so-called *twisted action* of  $\text{GL}_2(\mathbb{R})$ .

Given a complex binary form  $\xi(x, y)$ , let  $\text{GL}_2(\mathbb{R})$  act on it via

$$\xi_T(x, y) = \frac{1}{\det(T)^{\deg \xi/2}} \xi(t_1x + t_2y, t_3x + t_4y) \quad \text{for } T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}.$$

Observe that this is only an action up to sign when  $\deg \xi$  is odd, in the sense that for  $T_1, T_2 \in \text{GL}_2(\mathbb{R})$ , we only have  $\xi_{T_1 T_2} = \pm(\xi_{T_1})_{T_2}$  in general. Now, given a real

binary quadratic form  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  with  $\Delta(f) \neq 0$ , write

$$M_f = \begin{pmatrix} \beta & 2\gamma \\ -2\alpha & -\beta \end{pmatrix}$$

for its associated matrix in  $\mathrm{GL}_2(\mathbb{R})$ . Its action on binary quartic forms clearly remains unchanged if we scale  $f(x, y)$  by a constant in  $\mathbb{R}^\times$ . The second author, Xiao, proved [2019] that for any real binary quartic form  $F$  with  $\Delta(F) \neq 0$ , elements of

$$\{T \in \mathrm{GL}_2(\mathbb{R}) : T \text{ is not a scalar multiple of } I_{2 \times 2} \text{ and } F_T = F\}$$

all arise from binary quadratic forms in this way; see Proposition 2.1. Recall that an integral binary quadratic form is called *primitive* if its coefficients are coprime. Using this result from [Xiao 2019], in Section 2, we shall first show:

**Theorem 1.1.** *Let  $F$  be an integral binary quartic form with  $\Delta(F) \neq 0$ . Then, the following are equivalent.*

- (1)  $\mathcal{Q}_F(x)$  is reducible.
- (2)  $F_T = F$  for some  $T \in \mathrm{GL}_2(\mathbb{Q})$  which is not a scalar multiple of  $I_{2 \times 2}$ .
- (3)  $F_{M_f} = F$  for an integral and primitive binary quadratic form  $f$  with  $\Delta(f) \neq 0$ .

Moreover, in the case that  $\mathcal{Q}_F(x)$  is reducible:

- (a) If  $\Delta(F) \neq \square$ , then there is a unique such  $f$  up to sign.
- (b) If  $\Delta(F) = \square$ , then there are exactly three such  $f$  up to sign, among which one is definite and two are indefinite.

Given a real binary quadratic form  $f(x, y)$  with  $\Delta(f) \neq 0$ , let us further make the following definitions. First put

$$V_{\mathbb{R},f} = \{\text{real binary quartic forms } F \text{ such that } F_{M_f} = F\},$$

$$V_{\mathbb{Z},f} = \{\text{integral binary quartic forms } F \text{ such that } F_{M_f} = F\}.$$

Clearly  $V_{\mathbb{R},f}$  is a vector space over  $\mathbb{R}$  and  $V_{\mathbb{Z},f}$  a lattice over  $\mathbb{Z}$ . A straightforward calculation shows that  $\dim_{\mathbb{R}} V_{\mathbb{R},f}$  is three; see (3-1) and (3-2) below. Also, put

$$V_{\mathbb{R},f}^0 = \{F \in V_{\mathbb{R},f} : \Delta(F) \neq 0\} \quad \text{and} \quad V_{\mathbb{Z},f}^0 = \{F \in V_{\mathbb{Z},f} : \Delta(F) \neq 0\}.$$

For  $F \in V_{\mathbb{R},f}^0$ , we shall define two new invariants as follows. As we shall see in (2-3), there is a unique root  $\omega_f(F)$  of  $\mathcal{Q}_F(x)$  corresponding to  $f$ . Let  $\omega'_f(F)$ ,  $\omega''_f(F)$  denote the other two roots of  $\mathcal{Q}_F(x)$  and define

$$(1-4) \quad L_f(F) = \omega_f(F) \quad \text{and} \quad K_f(F) = -\omega'_f(F)\omega''_f(F).$$

By [Proposition 3.2](#) below, they have degrees one and two, respectively, in the coefficients of  $F$ . Following [\(1-2\)](#), let us define the *height of  $F$  associated to  $f$*  by

$$H_f(F) = \max\{L_f(F)^2, |K_f(F)|\}.$$

This is comparable to the height [\(1-2\)](#) because by comparing coefficients in

$$x^3 - I(F)x + J(F) = (x - \omega_f(F))(x - \omega'_f(F))(x - \omega''_f(F)),$$

we easily deduce the relations

$$(1-5) \quad 3I(F) = L_f(F)^2 + K_f(F) \quad \text{and} \quad J(F) = L_f(F)K_f(F),$$

which in turn imply that

$$(1-6) \quad (H_f(F)/10)^3 \leq H_{\text{BS}}(F) \leq H_f(F)^3.$$

Let us note that

$$(1-7) \quad \begin{aligned} \Delta(F) &= \frac{4I(F)^3 - J(F)^2}{27} \\ &= \left( \frac{L_f(F)^2 + 4K_f(F)}{9} \right) \left( \frac{2L_f(F)^2 - K_f(F)}{9} \right)^2, \end{aligned}$$

where the first equality is well-known, and the second equality holds by [\(1-5\)](#). Also, our height  $H_f(-)$  is an invariant in the sense that for any  $T \in \text{GL}_2(\mathbb{R})$ , we have

$$H_{f_T}(F_T) = H_f(F),$$

as shown in [Proposition 3.1](#) below. This implies that the map

$$(1-8) \quad V_{\mathbb{R},f} \rightarrow V_{\mathbb{R},f_T}, \quad F \mapsto F_T,$$

which is a well-defined bijection because  $M_{f_T} = T^{-1}M_fT$ , is height-preserving when restricted to the forms of nonzero discriminant.

Now, let us return to the integral and irreducible binary quartic forms with small Galois group. Write  $V_{\mathbb{Z}}^{\text{sm}}$  for the set of all such forms and set

$$V_{\mathbb{Z}}^{\text{sm},\dagger} = \{F \in V_{\mathbb{Z}}^{\text{sm}} : \text{Gal}(F) \not\cong V_4\}.$$

By [Theorem 1.1](#), we know that

$$(1-9) \quad \begin{aligned} V_{\mathbb{Z}}^{\text{sm}} &= \bigcup_{f \in \mathfrak{F}^*} \{F \in V_{\mathbb{Z},f}^0 : F \text{ is irreducible}\}, \\ V_{\mathbb{Z}}^{\text{sm},\dagger} &= \bigsqcup_{f \in \mathfrak{F}^*} \{F \in V_{\mathbb{Z},f}^0 : F \text{ is irreducible and } \text{Gal}(F) \not\cong V_4\}, \end{aligned}$$

where  $\mathfrak{F}^*$  denotes the set of all integral and primitive binary quadratic forms of nonzero discriminant, up to sign. In particular, given  $F \in V_{\mathbb{Z}}^{\text{sm}, \dagger}$ , there is a unique  $f \in \mathfrak{F}^*$  such that  $F \in V_{\mathbb{Z}, f}^0$ , and we may define the *height of  $F$*  by setting

$$H(F) = H_f(F).$$

For  $X > 0$ , let us define

$$\begin{aligned} N_{\mathbb{Z}}^{\dagger}(X) &= \#\{[F] : F \in V_{\mathbb{Z}}^{\text{sm}, \dagger} \text{ such that } H(F) \leq X\}, \\ N_{\mathbb{Z}, f}^{\dagger}(X) &= \#\{[F] : F \in V_{\mathbb{Z}}^{\text{sm}, \dagger} \cap V_{\mathbb{Z}, f}^0 \text{ such that } H(F) \leq X\}. \end{aligned}$$

Then, by (1-8) and (1-9), we have

$$N_{\mathbb{Z}}^{\dagger}(X) = \sum_{f \in \mathfrak{F}} N_{\mathbb{Z}, f}^{\dagger}(X),$$

where  $\mathfrak{F}$  denotes a set of representatives of the  $\text{GL}_2(\mathbb{Z})$ -equivalence classes on  $\mathfrak{F}^*$ . In Theorem 1.2, which is our main result, for  $f \in \mathfrak{F}^*$ , we shall determine the asymptotic formula for  $N_{\mathbb{Z}, f}^{\dagger}(X)$ . In fact, we shall consider the finer counts

$$\begin{aligned} N_{\mathbb{Z}, f}^{(D_4)}(X) &= \#\{[F] : F \in V_{\mathbb{Z}}^{\text{sm}} \cap V_{\mathbb{Z}, f}^0 \text{ such that } \text{Gal}(F) \simeq D_4 \text{ and } H(F) \leq X\}, \\ N_{\mathbb{Z}, f}^{(C_4)}(X) &= \#\{[F] : F \in V_{\mathbb{Z}}^{\text{sm}} \cap V_{\mathbb{Z}, f}^0 \text{ such that } \text{Gal}(F) \simeq C_4 \text{ and } H(F) \leq X\}, \\ N_{\mathbb{Z}, f}^{(V_4)}(X) &= \#\{[F] : F \in V_{\mathbb{Z}}^{\text{sm}} \cap V_{\mathbb{Z}, f}^0 \text{ such that } \text{Gal}(F) \simeq V_4 \text{ and } H_f(F) \leq X\}, \end{aligned}$$

and show that the latter two are negligible compared to  $N_{\mathbb{Z}, f}^{(D_4)}(X)$ . This means that most of the forms in  $V_{\mathbb{Z}}^{\text{sm}} \cap V_{\mathbb{Z}, f}^0$  have Galois group isomorphic to  $D_4$ . However, all of our error estimates depend upon  $f$ . Currently, we do not know how to control them in a uniform way, and so we are unable to obtain an asymptotic formula for  $N_{\mathbb{Z}}^{\dagger}(X)$  by summing over  $f \in \mathfrak{F}$ .

Finally, let us explain, for each  $f \in \mathfrak{F}^*$ , how counting forms in  $V_{\mathbb{Z}}^{\text{sm}} \cap V_{\mathbb{Z}, f}^0$  may be reduced to counting lattice points. Write  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  with  $\alpha, \beta, \gamma \in \mathbb{Z}$ . By (3-1) and (3-2), the set  $V_{\mathbb{R}, f}$  is a vector space isomorphic to  $\mathbb{R}^3$  via

$$\begin{aligned} \Theta_1 : a_4 x^4 + a_3 x^3 y + a_2 x^2 y^2 + a_1 x y^3 + a_0 y^4 &\mapsto (a_4, a_3, a_2) \quad \text{if } \alpha \neq 0, \\ \Theta_2 : a_4 x^4 + a_3 x^3 y + a_2 x^2 y^2 + a_1 x y^3 + a_0 y^4 &\mapsto (a_4, a_2, a_0) \quad \text{if } \beta, \beta^2 + 4\alpha\gamma \neq 0. \end{aligned}$$

Recall that the subset  $V_{\mathbb{Z}, f}$  has the structure of a rank-three  $\mathbb{Z}$ -lattice, which may be identified with the lattices

$$(1-10) \quad \Lambda_{f,1} = \Theta_1(V_{\mathbb{Z}, f}) \quad \text{and} \quad \Lambda_{f,2} = \Theta_2(V_{\mathbb{Z}, f})$$

in  $\mathbb{Z}^3$ . Let us mention here that we shall use the isomorphism

$$\Theta_{w(f)}, \quad \text{where } w(f) = \begin{cases} 1 & \text{if } f \text{ is irreducible,} \\ 2 & \text{if } f \text{ is reducible.} \end{cases}$$

Thus, the problem is reduced to counting points in  $\Lambda_{f,1}$  or  $\Lambda_{f,2}$ , and then sieving out those which come from reducible forms. In turn, counting lattice points amounts to computing certain volumes by a result of Davenport [1951a]; see Proposition 5.1.

**1B. Statement of the main theorem.** It is clear that we may choose the set  $\mathfrak{F}$  of representatives to be such that for all  $f \in \mathfrak{F}$ , the  $x^2$ -coefficient is positive, and

$$(1-11) \quad f(x, y) = \alpha x^2 + \beta xy, \quad \text{where } \gcd(\alpha, \beta) = 1 \text{ and } 0 < \alpha \leq \beta$$

when  $f$  is reducible. Let  $\sim$  denote  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence. Then, our main result is:

**Theorem 1.2.** *Let  $f(x, y)$  be an integral and primitive binary quadratic form of nonzero discriminant and with positive  $x^2$ -coefficient. Write  $D_f = |\Delta(f)|$ , and put*

$$s_f = \begin{cases} 8 & \text{if } D_f \text{ is odd,} \\ 1 & \text{if } D_f \text{ is even.} \end{cases}$$

(a) *Suppose that  $f$  is positive definite. Then, we have*

$$N_{\mathbb{Z},f}^{(D_4)}(X) = \frac{1}{s_f r_f} \frac{13\pi}{27 D_f^{3/2}} X^{3/2} + O_f(X^{1+\epsilon}) \quad \text{for any } \epsilon > 0,$$

where

$$r_f = \begin{cases} 6 & \text{if } f(x, y) \sim x^2 + xy + y^2, \\ 2 & \text{if } f(x, y) \sim ax^2 + cy^2 \text{ or } f(x, y) \sim ax^2 + bxy + ay^2 \text{ with } a \neq b, \\ 1 & \text{otherwise.} \end{cases}$$

(b) *Suppose that  $f$  is reducible and that  $f$  has the shape (1-11). Then, we have*

$$N_{\mathbb{Z},f}^{(D_4)}(X) = \frac{1}{s_f r_f} \frac{8}{9\beta^{3/2}} X^{3/2} \log X + O_f(X^{3/2}),$$

where

$$r_f = \begin{cases} 1 & \text{if } \beta \nmid \alpha^2 + 1 \text{ and } \beta \nmid \alpha^2 - 1, \\ 2 & \text{otherwise.} \end{cases}$$

(c) *Suppose that  $f$  is indefinite and irreducible. Define  $t_{D_f} \in \mathbb{R}$  to be such that  $e^{t_{D_f}}$  is the fundamental unit of the quadratic order  $\mathbb{Z}[(D_f + \sqrt{D_f})/2]$ , or equivalently*

$$t_{D_f} = \log((u_{D_f} + v_{D_f}\sqrt{D_f})/2),$$

where  $(u_{D_f}, v_{D_f}) \in \mathbb{N}^2$  is the least solution to  $x^2 - D_f y^2 = \pm 4$ . Then, we have

$$N_{\mathbb{Z},f}^{(D_4)}(X) = \frac{1}{s_f r_f} \frac{32t_{D_f}}{9D_f^{3/2}} X^{3/2} + O_f(X^{1+\epsilon}) \quad \text{for any } \epsilon > 0,$$

where

$$r_f = \begin{cases} 2 & \text{if } f(x, y) \sim ax^2 + bxy - ay^2 \\ & \text{or } f(x, y) \sim ax^2 + bxy + cy^2 \text{ with } a \mid b, \\ 1 & \text{otherwise.} \end{cases}$$

(d) In all three cases, for any  $\epsilon > 0$ , we have

$$N_{\mathbb{Z},f}^{(V_4)}(X) = O_{f,\epsilon}(X^{1+\epsilon}),$$

and also

$$N_{\mathbb{Z},f}^{(C_4)}(X) = \begin{cases} O_{f,\epsilon}(X^{1/2+\epsilon}) & \text{if } -\Delta(f) \neq \square, \\ O_f(X) & \text{if } -\Delta(f) = \square. \end{cases}$$

Notice that the error terms in [Theorem 1.2](#) depend upon  $f$ . Hence, we are unable to obtain an asymptotic formula for  $N_{\mathbb{Z}}^{\dagger}(X)$  by summing over  $f \in \mathfrak{F}$ . However, there are only three  $f \in \mathfrak{F}$  that need to be considered if we restrict to the forms in

$$V_{\mathbb{Z}}^{\text{sm},*} = \{F \in V_{\mathbb{Z}}^{\text{sm}} : F_T = F \text{ for some } T \in \text{GL}_2(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}\}.$$

This is because by [Proposition 2.1](#) below, such a matrix  $T$  must be of the shape  $M_f$  or  $M_f/2$  up to sign, where  $f \in \mathfrak{F}^*$ . From (1-9), we then deduce that

$$\begin{aligned} V_{\mathbb{Z}}^{\text{sm},*} &= \bigcup_{\substack{f \in \mathfrak{F}^* \\ \Delta(f) \in \{-4, 1, 4\}}} \{F \in V_{\mathbb{Z},f}^0 : F \text{ is irreducible}\}, \\ V_{\mathbb{Z}}^{\text{sm},*,\dagger} &= \bigsqcup_{\substack{f \in \mathfrak{F}^* \\ \Delta(f) \in \{-4, 1, 4\}}} \{F \in V_{\mathbb{Z},f}^0 : F \text{ is irreducible and } \text{Gal}(F) \not\cong V_4\}. \end{aligned}$$

For  $X > 0$ , let us put

$$N_{\mathbb{Z}}^{*,\dagger}(X) = \#\{[F] : F \in V_{\mathbb{Z}}^{\text{sm},*,\dagger} \text{ such that } H(F) \leq X\}.$$

Then, by (1-8) and the above discussion, we have

$$N_{\mathbb{Z}}^{*,\dagger}(X) = N_{\mathbb{Z},f^{(1)}}^{*,\dagger}(X) + N_{\mathbb{Z},f^{(2)}}^{*,\dagger}(X) + N_{\mathbb{Z},f^{(3)}}^{*,\dagger}(X),$$

where we may take

$$f^{(1)}(x, y) = x^2 + y^2, \quad f^{(2)}(x, y) = x^2 + xy, \quad f^{(3)}(x, y) = x^2 + 2xy,$$

whose discriminants are  $-4$ ,  $1$ , and  $4$ , respectively. We have:

**Corollary 1.3.** *We have*

$$N_{\mathbb{Z}}^{*,\dagger}(X) = \frac{1}{9}X^{3/2} \log X + O(X^{3/2}).$$

*Proof.* [Theorem 1.2](#) implies that

$$N_{\mathbb{Z},f^{(1)}}^{\dagger}(X) = O(X^{3/2}) \quad \text{and} \quad N_{\mathbb{Z},f^{(i)}}^{\dagger}(X) = \frac{1}{18}X^{3/2} \log X + O(X^{3/2}) \quad \text{for } i = 2, 3.$$

Summing these terms up then yields the claim.  $\square$

Finally, as a consequence of the proof of [Theorem 1.2](#), we also have:



**Theorem 1.4.** *Let  $D = \beta^2 + 4\alpha^2$ , where  $\alpha, \beta \in \mathbb{N}$  are coprime and  $D$  is not a square. Then, the negative Pell's equation  $x^2 - Dy^2 = -4$  has integer solutions if and only if the integral binary quadratic form  $\alpha x^2 + \beta xy - \alpha y^2$  is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to a form of the shape  $ax^2 + bxy + cy^2$  with a dividing  $b$ .*

We now discuss some potential applications of our [Theorem 1.2](#) and [Corollary 1.3](#).

First, it is natural to ask whether the asymptotic formula (1-3), which was proven using [Proposition 5.1](#), admits a secondary main term. From the arguments in [\[Bhargava and Shankar 2015\]](#), we see that the error term arising from volumes of the lower dimensional projections in [Proposition 5.1](#) is only of order  $O(X^{3/4})$ . Thus, possibly  $X^{3/4}$  is the order of a second main term, but it is dominated by another error term coming from

$$N_{\mathbb{Z}, \mathrm{BS}}^*(X) = \#\{[F] : F \in V_{\mathbb{Z}}^{\mathrm{sm},*} \text{ such that } H_{\mathrm{BS}}(F) \leq X\}.$$

In particular, it was shown in [\[Bhargava and Shankar 2015, Lemma 2.4\]](#) that

$$N_{\mathbb{Z}, \mathrm{BS}}^*(X) = O_{\epsilon}(X^{3/4+\epsilon}) \quad \text{for any } \epsilon > 0.$$

Our [Corollary 1.3](#) removes this obstacle, because

$$N_{\mathbb{Z}}^{*,\dagger}(X^{1/3}) \leq N_{\mathbb{Z}, \mathrm{BS}}^*(X) \leq N_{\mathbb{Z}}^{*,\dagger}(10X^{1/3}) + O_{\epsilon}(X^{1/3+\epsilon})$$

by (1-6) and [Theorem 1.2\(d\)](#), whence we have

$$N_{\mathbb{Z}, \mathrm{BS}}^*(X) \asymp X^{1/2} \log X.$$

This improvement potentially allows one to prove a secondary main term for (1-3) by using similar methods from [\[Bhargava et al. 2013\]](#), where it was shown that the counting theorem in [\[Davenport and Heilbronn 1971\]](#) for cubic fields has a secondary main term of order  $X^{5/6}$ ; this latter fact was proven independently in [\[Taniguchi and Thorne 2013\]](#) as well.

Next, integral binary quartic forms are closely related to quartic orders, and maximal irreducible quartic orders may be regarded as quartic fields. More generally, by the construction of Birch and Merriman [\[1972\]](#) or Nakagawa [\[1989\]](#), any integral binary form  $F$  gives rise to a  $\mathbb{Z}$ -order  $Q_F$  whose rank is the degree of  $F$ , where  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence class of  $F$  corresponds to isomorphism class of  $Q_F$ . By [\[Delone and Faddeev 1964\]](#), it is well-known that all cubic orders come from integral binary cubic forms, which enabled the enumeration of cubic orders having a nontrivial automorphism as well as cubic fields by their discriminant; see [\[Bhargava and Shnidman 2014\]](#) and [\[Davenport and Heilbronn 1971\]](#), respectively. But this is not true for orders of higher rank. Parametrizations of quartic and quintic orders were given by Bhargava in his seminal work [\[2004; 2008\]](#). Wood [\[2012\]](#) further showed that the quartic orders arising from integral binary quartic forms are exactly

those having a monogenic *cubic resolvent*; see [Bhargava 2004] for the definition. This implies that the forms in

$$V_{\mathbb{Z}}^{\text{sm},\star} = \{F \in V_{\mathbb{Z}}^{\text{sm}} : Q_F \text{ is maximal}\}$$

correspond to quartic  $D_4$ -,  $C_4$ -, and  $V_4$ -fields whose ring of integers has a monogenic cubic resolvent. In our upcoming paper [Tsang and Xiao 2017], we shall enumerate  $\text{GL}_2(\mathbb{Z})$ -equivalence classes of forms in  $V_{\mathbb{Z}}^{\text{sm},\star}$  with respect to a height corresponding to the conductor of fields, as motivated by [Altuğ et al. 2017]. In fact, we shall that show that

$$\text{for all } f \in \mathfrak{F}^* : \quad F \in V_{\mathbb{Z}}^{\text{sm},\star} \cap V_{\mathbb{Z},f}^0 \neq \emptyset \quad \text{if and only if} \quad \Delta(f) \in \{-4, 1, 4\}.$$

Thus, our counting theorem in [Tsang and Xiao 2017] may be regarded as a refinement and an extension of Corollary 1.3 above.

Last but not least, binary quartic forms are connected to elliptic curves as well. In particular, any integral binary quartic form  $F$  gives rise to an elliptic curve

$$E_F : y^2 = x^3 - \frac{I(F)}{3}x - \frac{J(F)}{27}$$

defined over  $\mathbb{Q}$ . Bhargava and Shankar [2015] applied (1-3) as well as a parametrization of 2-Selmer groups due to Birch and Swinnerton-Dyer to show that the average rank of elliptic groups over  $\mathbb{Q}$ , when ordered by a *naïve* height analogous to (1-2), is at most  $\frac{3}{2}$ . This result is remarkable in that it is the first to show, unconditional on the BSD-conjecture and the Grand Riemann Hypothesis, boundedness of the average rank of large families of elliptic curves over  $\mathbb{Q}$ . Conditional bounds were obtained by Brumer [1992], Heath-Brown [2004], and Young [2006] previously. Now, the relations in (1-5) imply that for  $F \in V_{\mathbb{Z}}^{\text{sm}} \cap V_{\mathbb{Z},f}^0$  with  $f \in \mathfrak{F}^*$ , we have

$$E_F : y^2 = \left(x + \frac{L_f(F)}{3}\right) \left(x^2 - \frac{L_f(F)}{3}x - \frac{K_f(F)}{9}\right),$$

which has a rational 2-torsion point. Hence, our Theorem 1.2 potentially allows one to study arithmetic properties of elliptic curves with 2-torsion over  $\mathbb{Q}$ . Let us remark that unlike a *large* family of elliptic curves over  $\mathbb{Q}$ , in the sense of [Bhargava and Shankar 2015, Section 3], the family consisting of those curves with a rational 2-torsion exhibits a rather peculiar behavior. Indeed, Klagsbrun and Lemke Oliver [2014] proved that the average size of the 2-Selmer groups in this family is unbounded, and they conjectured an asymptotic growth rate. One might be able to obtain such an asymptotic growth rate using our Theorem 1.2 and a sieve that detects local solubility; this line of inquiry is pursued in an upcoming paper due to D. Kane and Z. Klagsbrun.

## 2. Characterization of forms with small Galois groups

**2A. Cremona covariants.** Let  $F$  be a real binary quartic form with  $\Delta(F) \neq 0$ . As Cremona defined [1999], we have three quadratic covariants  $\mathfrak{C}_{F,\omega}(x, y)$ , each of which is associated to a root  $\omega$  of  $\mathcal{Q}_F(x)$ ; see [Xiao 2019, Subsection 4.2] for the explicit definition. They satisfy the syzygy

$$(2-1) \quad \mathfrak{C}_{F,\omega}(x, y)^2 = \frac{1}{3}(F_4(x, y) + 4\omega F(x, y)),$$

where  $F_4$  is the *Hessian covariant* of  $F$  and is given by

$$F_4(x, y) = 3(a_3^2 - 8a_4a_2)x^4 + 4(a_3a_2 - 6a_4a_1)x^3y + 2(2a_2^2 - 24a_4a_0 - 3a_3a_1)x^2y^2 \\ + 4(a_2a_1 - 6a_3a_0)xy^3 + (3a_1^2 - 8a_2a_0)y^4.$$

We shall label the roots  $\omega_1(F)$ ,  $\omega_2(F)$ ,  $\omega_3(F)$  of  $\mathcal{Q}_F(x)$  such that

$$\mathfrak{C}_{F,\omega_i(F)}(x, y) = \mathfrak{C}_{F,i}(x, y) \quad \text{for all } i = 1, 2, 3,$$

where  $\mathfrak{C}_{F,i}(x, y)$  is defined as in [Xiao 2019, (4.6)]. Then, from (2-1) and the explicit expressions for  $\mathfrak{C}_{F,\omega}(x, y)$  given in [Xiao 2019], we have the following observations:

- (1) For  $\omega = \omega_1(F)$ , the binary quadratic form  $\mathfrak{C}_{F,\omega}(x, y)$  has real coefficients.
- (2) For  $\omega = \omega_2(F)$ ,  $\omega_3(F)$ , we have:
  - If  $\Delta(F) > 0$ , then  $\lambda_\omega \cdot \mathfrak{C}_{F,\omega}(x, y)$  has real coefficients for some  $\lambda_\omega \in \{1, \sqrt{-1}\}$ .
  - If  $\Delta(F) < 0$ , then  $\lambda \cdot \mathfrak{C}_{F,\omega}(x, y)$  does not have real coefficients for all  $\lambda \in \mathbb{C}^\times$ .

Also, it is easy to check that

$$(2-2) \quad \Delta(\mathfrak{C}_{F,\omega_1(F)}) > 0 \quad \text{and} \quad \Delta(\mathfrak{C}_{F,\omega_2(F)}) < 0.$$

We shall require the following result by Xiao [2019].

**Proposition 2.1.** *Let  $F$  be a real binary quartic form with  $\Delta(F) \neq 0$ . Then, a set of representatives for the quotient group*

$$\{T \in \text{GL}_2(\mathbb{R}) : F_T = F\} / \{\lambda \cdot I_{2 \times 2} : \lambda \in \mathbb{R}^\times\}$$

is given by

$$\begin{cases} \{I_{2 \times 2}, M_f : f \in \{\mathfrak{C}_{F,\omega_1(F)}, \lambda_{\omega_2(F)} \cdot \mathfrak{C}_{F,\omega_2(F)}, \lambda_{\omega_3(F)} \cdot \mathfrak{C}_{F,\omega_3(F)}\}\} & \text{if } \Delta(F) > 0, \\ \{I_{2 \times 2}, M_f : f \in \{\mathfrak{C}_{F,\omega_1(F)}\}\} & \text{if } \Delta(F) < 0. \end{cases}$$

Furthermore, the quadratic forms  $\mathfrak{C}_{F,\omega_1(F)}(x, y)$ ,  $\mathfrak{C}_{F,\omega_2(F)}(x, y)$ , and  $\mathfrak{C}_{F,\omega_3(F)}(x, y)$ , are pairwise nonproportional over  $\mathbb{C}^\times$ .

*Proof.* For the first statement, see [Xiao 2019, Proposition 4.6]. As for the second statement, since  $\mathfrak{C}_{F, \omega_i(F)}(x, y)$  are covariants, replacing  $F$  by a  $\mathrm{GL}_2(\mathbb{R})$ -translate if necessary, we may assume that

$$F(x, y) = a_4x^4 + a_2x^2y^2 \pm a_4y^4.$$

In this special case, it is not hard to verify the claim using the explicit expressions for  $\mathfrak{C}_{F, \omega_i(F)}(x, y)$  in [Xiao 2019, (4.6)].  $\square$

Let  $F$  be a real binary quartic form with  $\Delta(F) \neq 0$ . Proposition 2.1 implies that for any real binary quadratic form  $f$  with  $\Delta(f) \neq 0$ , we have  $F \in V_{\mathbb{R}, f}$  if and only if

$$(2-3) \quad f(x, y) \text{ is proportional to } \mathfrak{C}_{F, \omega}(x, y) \text{ for a root } \omega \text{ of } \mathcal{Q}_F(x).$$

Moreover, this root  $\omega$  is unique, and we shall denote it by  $\omega_f(F)$ . This was required in order to define the  $L_f$ - and  $K_f$ -invariants in (1-4).

**2B. Proof of Theorem 1.1.** The key is the following lemma.

**Lemma 2.2.** *Let  $F$  be an integral binary quartic form with  $\Delta(F) \neq 0$  and let  $\omega$  be a root of  $\mathcal{Q}_F(x)$ . Then, the quadratic form  $\mathfrak{C}_{F, \omega}(x, y)$  is proportional over  $\mathbb{C}^\times$  to a form with integer coefficients if and only if  $\omega \in \mathbb{Z}$ .*

*Proof.* If  $\omega \in \mathbb{Z}$ , then we easily see from (2-1) that  $\lambda \cdot \mathfrak{C}_{F, \omega}(x, y)$  has integer coefficients for some  $\lambda \in \mathbb{C}^\times$ . Conversely, if  $\lambda \cdot \mathfrak{C}_{F, \omega}(x, y)$  has integer coefficients for some  $\lambda \in \mathbb{C}^\times$ , then consider the action of an element  $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ , where  $\bar{\mathbb{Q}}$  is an algebraic closure of  $\mathbb{Q}$ . It is clear from the definition of  $\mathfrak{C}_{F, \omega}(x, y)$  that  $\lambda \in \bar{\mathbb{Q}}$ . From (2-1), we have

$$\frac{4}{3}(\omega - \sigma(\omega))F(x, y) = \mathfrak{C}_{F, \omega}(x, y)^2 - \sigma(\mathfrak{C}_{F, \omega}(x, y)^2) = \left(1 - \frac{\lambda^2}{\sigma(\lambda)^2}\right) \mathfrak{C}_{F, \omega}(x, y)^2,$$

and this last binary quartic form has zero discriminant. This shows that  $\omega - \sigma(\omega) = 0$  for all  $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ . Thus, we have  $\omega \in \mathbb{Q}$ , and so  $\omega \in \mathbb{Z}$  since  $\mathcal{Q}_F(x)$  is monic.  $\square$

The first claim in Theorem 1.1 now follows from Proposition 2.1, Lemma 2.2, and (2-3). Note that

$$\Delta(F) = 27^2 \Delta(\mathcal{Q}_F),$$

which means that  $\mathcal{Q}_F(x)$  has three integer roots if and only if  $\mathcal{Q}_F(x)$  is reducible and  $\Delta(F) = \square$ . The second claim then follows from this fact and (2-2).

### 3. Basic properties of forms in $V_{\mathbb{R},f}$ of nonzero discriminant

Throughout this section, let  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  be a real binary quadratic form with  $\Delta(f) \neq 0$ . It is not hard to check, by a direct calculation, that

$$(3-1) \quad V_{\mathbb{R},f} = \left\{ Ax^4 + Bx^3y + Cx^2y^2 + \left( \frac{4\beta\gamma A - (\beta^2 + 2\alpha\gamma)B + 2\alpha\beta C}{2\alpha^2} \right) xy^3 \right. \\ \left. + \left( \frac{4\gamma(\beta^2 + 2\alpha\gamma)A - \beta(\beta^2 + 4\alpha\gamma)B + 2\alpha\beta^2 C}{8\alpha^3} \right) y^4 : A, B, C \in \mathbb{R} \right\}$$

if  $\alpha \neq 0$ , and similarly that

$$(3-2) \quad V_{\mathbb{R},f} = \left\{ Ax^4 + \left( \frac{\gamma(4\beta^2 + 8\alpha\gamma)A + 2\alpha\beta^2 B - 8\alpha^3 C}{\beta(\beta^2 + 4\alpha\gamma)} \right) x^3y + Bx^2y^2 \right. \\ \left. - \left( \frac{8\gamma^3 A - 2\beta^2\gamma B - \alpha(4\beta^2 + 8\alpha\gamma)C}{\beta(\beta^2 + 4\alpha\gamma)} \right) xy^3 + Cy^4 : A, B, C \in \mathbb{R} \right\}$$

if  $\beta, \beta^2 + 4\alpha\gamma \neq 0$ . Below, we shall give some basic properties of  $V_{\mathbb{R},f}^0$  and  $V_{\mathbb{Z},f}^0$ .

**3A. The two new invariants.** Recall the definitions of the  $L_f$ - and  $K_f$ -invariants given in (1-4). First, we shall show that they are indeed invariants under the twisted action of  $\mathrm{GL}_2(\mathbb{R})$  in the following sense.

**Proposition 3.1.** *For all  $F \in V_{\mathbb{R},f}^0$  and  $T \in \mathrm{GL}_2(\mathbb{R})$ , we have*

$$L_{f_T}(F_T) = L_f(F) \quad \text{and} \quad K_{f_T}(F_T) = K_f(F).$$

*Proof.* Notice that  $\mathcal{Q}_F(x) = \mathcal{Q}_{F_T}(x)$ . For any root  $\omega$  of  $\mathcal{Q}_F(x)$ , because  $\mathfrak{C}_{F,\omega}(x, y)$  is a covariant up to sign by (2-1), if  $\mathfrak{C}_{F,\omega}(x, y)$  is proportional to  $f(x, y)$ , then  $\mathfrak{C}_{F_T,\omega}(x, y)$  is proportional to  $f_T(x, y)$ . It then follows from the definition that  $L_{f_T}(F_T) = L_f(F)$ . Since  $I(F_T) = I(F)$ , we also have  $K_{f_T}(F_T) = K_f(F)$  by the first equality in (1-5).  $\square$

We shall give explicit formulae for  $L_f(-)$  and  $K_f(-)$  in two special cases.

**Proposition 3.2.** *The following holds.*

(a) *Assume that  $\alpha \neq 0$ . Then, for all  $F \in V_{\mathbb{R},f}^0$  as in (3-1), we have*

$$L_f(F) = -(12\gamma A - 3\beta B + 2\alpha C)/(2\alpha), \\ K_f(F) = (72\beta^2\gamma A^2 + 9\alpha(\beta^2 + 4\alpha\gamma)B^2 + 8\alpha^3 C^2 \\ - 18\beta(\beta^2 + 4\alpha\gamma)AB + 12\alpha(3\beta^2 - 4\alpha\gamma)AC - 24\alpha^2\beta BC)/(4\alpha^3).$$

Moreover, we have

$$\frac{4(L_f(F)^2 + 4K_f(F))}{9} = \frac{L_{f,1}(F)^2 - \Delta(f)L_{f,2}(F)^2}{\alpha^4},$$

where

$$L_{f,1}(F) = 4(\beta^2 - \alpha\gamma)A - 3\alpha\beta B + 2\alpha^2 C \quad \text{and} \quad L_{f,2}(F) = 2(2\beta A - \alpha B).$$

(b) Assume that  $\gamma = 0$ . Then, for all  $F \in V_{\mathbb{R},f}^0$  as in (3-2), we have

$$\begin{aligned} L_f(F) &= (2\beta^2 B - 12\alpha^2 C)/\beta^2, \\ K_f(F) &= (-\beta^4 B^2 + 144\alpha^4 C^2 + 36\beta^4 AC - 24\alpha^2 \beta^2 BC)/\beta^4. \end{aligned}$$

Moreover, we have

$$\frac{4(L_f(F)^2 + 4K_f(F))}{9} = \frac{8C}{\beta^2} \left( 8\beta^2 A - 8\alpha^2 B + \frac{40\alpha^4}{\beta^2} C \right).$$

*Proof.* This may be verified by explicit computation. □

We shall also need the following observation.

**Proposition 3.3.** Assume that  $f$  is integral. Then, for all  $F \in V_{\mathbb{Z},f}^0$ , we have

$$L_f(F), K_f(F), (L_f(F)^2 + 4K_f(F))/9, (2L_f(F)^2 - K_f(F))/9 \in \mathbb{Z}.$$

Moreover, when  $f$  is primitive in addition, we have

$$4(2L_f(F)^2 - K_f(F))/(9\Delta(f)) \in \mathbb{Z}.$$

*Proof.* We have  $L_f(F) \in \mathbb{Z}$  by Lemma 2.2. Since  $I(F) \in \mathbb{Z}$ , we deduce from the first equality in (1-5) that  $K_f(F) \in \mathbb{Z}$  holds as well. Observe that

$$\begin{aligned} I(F) + K_f(F) &= (L_f(F)^2 + 4K_f(F))/3, \\ 2I(F) - K_f(F) &= (2L_f(F)^2 - K_f(F))/3, \end{aligned}$$

both of which are integers. Since  $\Delta(F) \in \mathbb{Z}$ , we deduce from (1-7) that at least one of the above expressions is divisible by 3. But again by (1-5), we have

$$3I(F) = (L_f(F)^2 + 4K_f(F))/3 + (2L_f(F)^2 - K_f(F))/3,$$

so in fact both expressions are divisible by 3. This proves the first claim.

Next, assume that  $f$  is primitive in addition. In view of Proposition 3.1, by applying a  $\mathrm{GL}_2(\mathbb{Z})$ -action on  $f$  if necessary, we may assume that  $\alpha \neq 0$  and that  $\alpha$  is coprime to  $\Delta(f)$ . Using Proposition 3.2(a), we then compute that

$$\frac{4(2L_f(F)^2 - K_f(F))}{9} = \Delta(f) \left( \frac{\alpha(B^2 - 4AC) + 2A(\beta B - 4\gamma A)}{\alpha^3} \right).$$

This expression is an integer by the first claim, and hence must be divisible by  $\Delta(f)$ , because  $\alpha$  is taken to be coprime to  $\Delta(f)$ . This proves the second claim.  $\square$

**3B. Determinants of the two lattices.** In this subsection, assume that  $f$  is integral and primitive. Let  $\Lambda_{f,1}$  and  $\Lambda_{f,2}$  denote the lattices defined in (1-10). Below, we shall compute their determinants in terms of the number  $s_f$  as in Theorem 1.2.

**Proposition 3.4.** *We have  $\det(\Lambda_{f,1}) = s_f |\alpha|^3$  and  $\det(\Lambda_{f,2}) = s_f |\beta(\beta^2 + 4\alpha\gamma)|/8$ .*

*Proof.* Observe that the linear transformation defined by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ * & -B & * \end{pmatrix}, \quad \text{where } B = \frac{\beta(\beta^2 + 4\alpha\gamma)}{8\alpha^3},$$

has determinant  $B$ , and it sends  $\Lambda_{f,1}$  to  $\Lambda_{f,2}$ . Thus, it suffices to prove the first claim. Recall from (3-1) that  $\Lambda_{f,1}$  is the set of tuples  $(A, B, C) \in \mathbb{Z}^3$  satisfying

$$\begin{aligned} 4\beta\gamma A - (\beta^2 + 2\alpha\gamma)B + 2\alpha\beta C &\equiv 0 \pmod{2\alpha^2}, \\ 4\gamma(\beta^2 + 2\alpha\gamma)A - \beta(\beta^2 + 4\alpha\gamma)B + 2\alpha\beta^2 C &\equiv 0 \pmod{8\alpha^3}. \end{aligned}$$

If  $\beta\gamma = 0$ , then it is easy to check that  $\det(\Lambda_{f,1}) = s_f |\alpha|^3$ . If  $\beta\gamma \neq 0$ , then we shall use the fact that

$$\det(\Lambda_{f,1}) = \prod_p \det(\Lambda_{f,1}^{(p)}) = \prod_{p|2\alpha} \det(\Lambda_{f,1}^{(p)}), \quad \text{where } \Lambda_{f,1}^{(p)} = \mathbb{Z}_p \otimes_{\mathbb{Z}} \Lambda_{f,1},$$

and so  $\det(\Lambda_{f,1}) = s_f |\alpha|^3$  indeed holds by Lemma 3.5 below.  $\square$

**Lemma 3.5.** *Let  $p$  be a prime dividing  $2\alpha$  and let  $p^k \parallel \alpha$ . Then, we have*

$$\det(\Lambda_{f,1}^{(p)}) = s_f^{\epsilon_p} p^{3k}, \quad \text{where } \epsilon_p = \begin{cases} 1 & \text{if } p = 2, \\ 0 & \text{if } p \geq 3. \end{cases}$$

*Proof.* For brevity, write

$$\alpha = p^k a \quad \text{and} \quad \beta = p^\ell b, \quad \text{where } k, \ell, a, b \in \mathbb{Z} \text{ with } k, \ell \geq 0 \text{ and } p \nmid a, b.$$

Then, the claim may be restated as

$$\det(\Lambda_{f,1}^{(p)}) = \begin{cases} p^{3k+3\epsilon_p} & \text{if } \ell = 0, \\ p^{3k} & \text{if } \ell \geq 1. \end{cases}$$

By definition, the lattice  $\Lambda_{f,1}^{(p)}$  is the set  $(A, B, C) \in \mathbb{Z}_p^3$  of tuples satisfying

$$\mathcal{T}_1(A, B, C) \equiv 0 \pmod{p^{2k+\epsilon_p}} \quad \text{and} \quad \mathcal{T}_2(A, B, C) \equiv 0 \pmod{p^{3k+3\epsilon_p}},$$

where

$$\mathcal{T}_1(A, B, C) = p^\ell b(4\gamma A - p^\ell bB) - 2p^k a\gamma B + 2p^{k+\ell} abC,$$

$$\mathcal{T}_2(A, B, C) = (p^{2\ell} b^2 + 4p^k a\gamma)(4\gamma A - p^\ell bB) - 8p^k a\gamma^2 A + 2p^{k+2\ell} ab^2 C.$$

Observe that we have the relation

$$(3-3) \quad \mathcal{T}_2(A, B, C) - p^\ell b \mathcal{T}_1(A, B, C) = 2p^k a \gamma (4\gamma A - p^\ell b B).$$

For  $\ell = 0$ , we deduce from (3-3) that  $\Lambda_{f,1}^{(p)}$  is defined solely by

$$\mathcal{T}_2(A, B, C) \equiv 0 \pmod{p^{3k+3\epsilon_p}}.$$

For  $\ell \geq 1$  and  $\ell \geq k + 2\epsilon_p$ , it is easy to see that  $\Lambda_{f,1}^{(p)}$  is in fact defined by

$$A \equiv 0 \pmod{p^{2k}} \quad \text{and} \quad B \equiv 0 \pmod{p^k}.$$

For  $\ell \geq 1$  and  $\ell \leq k + \epsilon_p$ , we shall first show that  $\Lambda_{f,1}^{(p)}$  is also defined by

$$(3-4) \quad \begin{cases} A \equiv 0 & \pmod{p^{2\ell-2\epsilon_p}}, \\ B \equiv 0 & \pmod{p^{\ell-\epsilon_p}}, \\ (4\gamma A - p^\ell b B)/p^{2\ell-\epsilon_p} \equiv 0 & \pmod{p^{k-\ell+\epsilon_p}}, \\ \mathcal{T}_2(A, B, C)/p^{k+2\ell+\epsilon_p} \equiv 0 & \pmod{p^{2k-2\ell+2\epsilon_p}}. \end{cases}$$

If (3-4) is satisfied, then from (3-3), it is easy to see that  $(A, B, C) \in \Lambda_{f,1}^{(p)}$ . Conversely, if  $(A, B, C) \in \Lambda_{f,1}^{(p)}$ , then the assumption  $\ell \leq k + \epsilon_p$  implies that

$$\mathcal{T}_1(A, B, C) \equiv 0 \pmod{p^{k+\ell}} \quad \text{and} \quad \mathcal{T}_2(A, B, C) \equiv 0 \pmod{p^{k+2\ell+\epsilon_p}},$$

while reducing (3-3) mod  $p^{2k+\ell+\epsilon_p}$  also yields

$$4\gamma A - p^\ell b B \equiv 0 \pmod{p^{k+\ell}}.$$

From these three congruence equations, it follows that (3-4) is indeed satisfied. In all cases, we then see that  $\det(\Lambda_{f,1}^{(p)})$  is as claimed.  $\square$

**3C. Forms with abelian Galois groups.** In this subsection, assume that  $f$  is integral. Consider an irreducible form  $F \in V_{\mathbb{Z},f}^0$ . By Theorem 1.1, we have  $\text{Gal}(F) \simeq D_4$ ,  $C_4$ , or  $V_4$ . To distinguish among these three possibilities, note that the *cubic resolvent polynomial of  $F$* , defined by

$$R_F(x) = a_4^3 X^3 - a_4^2 a_2 X^2 + a_4(a_3 a_1 - 4a_4 a_0)X - (a_3^2 a_0 + a_4 a_1^2 - 4a_4 a_2 a_0)$$

when  $F$  has the shape (1-1), is reducible since  $\text{Gal}(F)$  is small. Also, it has a unique root  $r_F \in \mathbb{Q}$  precisely when  $\Delta(F) \neq \square$ , in which case we define

$$\theta_1(F) = (a_3^2 - 4a_4(a_2 - r_F a_4))\Delta(F) \quad \text{and} \quad \theta_2(F) = a_4(r_F^2 a_4 - 4a_0)\Delta(F).$$

Then, we have the well-known criterion

$$\text{Gal}(F) \simeq V_4 \iff \Delta(F) = \square,$$

$$\text{Gal}(F) \simeq C_4 \iff \Delta(F) \neq \square \text{ and } \theta_1(F), \theta_2(F) = \square \text{ in } \mathbb{Q}.$$



See [Conrad 2012], for example. We then deduce:

**Proposition 3.6.** *Let  $F \in V_{\mathbb{Z},f}^0$  be an irreducible form. Then, we have*

$$\text{Gal}(F) \simeq V_4 \iff L_f(F)^2 + 4K_f(F) = \square,$$

as well as

$$\text{Gal}(F) \simeq C_4 \iff \begin{cases} L_f(F)^2 + 4K_f(F) \neq \square, \\ (L_f(F)^2 + 4K_f(F))(2L_f(F)^2 - K_f(F))/\Delta(f) = \square. \end{cases}$$

*Proof.* Observe that by (1-7), we have

$$\Delta(F) = \square \quad \text{if and only if} \quad L_f(F)^2 + 4K_f(F) = \square.$$

The first claim is then clear. Next, suppose that  $\Delta(F) \neq \square$ . By Proposition 3.1, we may assume that  $\alpha \neq 0$ . For  $F$  in the shape as in (3-1), a direct computation yields

$$r_F = (-4\gamma A + \beta B)/(2\alpha A).$$

Using Proposition 3.2 (a), we further compute that

$$\begin{aligned} \theta_1(F) &= 4\alpha^2(2L_f(F)^2 - K_f(F))\Delta(F)/(9\Delta(f)), \\ \theta_2(F) &= \beta^2(2L_f(F)^2 - K_f(F))\Delta(F)/(9\Delta(f)). \end{aligned}$$

By (1-7) and the criterion above, it follows that  $\theta_1(F), \theta_2(F)$  are squares if and only if  $(L_f(F)^2 + 4K_f(F))(2L_f(F)^2 - K_f(F))/\Delta(f)$  is a square, as desired.  $\square$

**3D. Reducible forms.** In this subsection, assume that  $f$  is integral. We shall study the reducible forms in  $V_{\mathbb{Z},f}^0$ . Let us first make a definition and an observation.

**Definition 3.7.** Let  $F \in V_{\mathbb{Z},f}^0$  be a reducible form.

- (1) We say that  $F$  is of *type 1* if  $F = m \cdot pp_{M_f}$  for some  $m \in \mathbb{Q}^\times$  and integral binary quadratic form  $p$ .
- (2) We say that  $F$  is of *type 2* if  $F = pq$  for some integral binary quadratic forms  $p$  and  $q$  satisfying  $p_{M_f} = -p$  and  $q_{M_f} = -q$ .

**Lemma 3.8.** *For all reducible forms  $F \in V_{\mathbb{Z},f}^0$  of type 1, we have*

$$L_f(F)^2 + 4K_f(F) = \square.$$

*Proof.* This may be verified by a direct computation.  $\square$

Below, we shall show that the two reducibility types in Definition 3.7 are in fact the only possibilities. We shall require two further lemmas.

**Lemma 3.9.** *Let  $\ell(x, y) = \ell_1 x + \ell_0 y$  be a nonzero complex binary linear form, and suppose that  $\ell_{M_f} = \lambda \cdot \ell$  for some  $\lambda \in \mathbb{C}^\times$ . Then, we have  $\lambda = \pm\sqrt{-1}$ , with*

$$\lambda = \begin{cases} -\sqrt{-1} & \text{if and only if } \ell_0 = (\beta + \sqrt{\Delta(f)})\ell_1/(2\alpha), \\ \sqrt{-1} & \text{if and only if } \ell_0 = (\beta - \sqrt{\Delta(f)})\ell_1/(2\alpha), \end{cases}$$

in the case that  $\alpha \neq 0$ .

*Proof.* The hypothesis implies that

$$\frac{1}{\sqrt{-\Delta(f)}} \begin{pmatrix} \beta & -2\alpha \\ 2\gamma & -\beta \end{pmatrix} \begin{pmatrix} \ell_1 \\ \ell_0 \end{pmatrix} = \lambda \begin{pmatrix} \ell_1 \\ \ell_0 \end{pmatrix}.$$

Then, by computing the eigenvalues and eigenspaces of the  $2 \times 2$  matrix above, we see that the claim holds.  $\square$

**Lemma 3.10.** *Let  $p(x, y) = p_2 x^2 + p_1 xy + p_0 y^2$  be a nonzero complex binary quadratic form, and suppose that  $p_{M_f} = \lambda \cdot p$  for some  $\lambda \in \mathbb{C}^\times$ . Then, we have  $\lambda = \pm 1$ , with*

$$\lambda = \begin{cases} -1 & \text{if and only if } p_0 = (\beta p_1 - 2\gamma p_2)/(2\alpha), \\ 1 & \text{if and only if } p = (p_2/\alpha)f, \end{cases}$$

in the case that  $\alpha \neq 0$ .

*Proof.* The hypothesis implies that

$$\frac{1}{-\Delta(f)} \begin{pmatrix} \beta^2 & -2\alpha & 4\alpha^2 \\ 4\beta\gamma & -(\beta^2 + 4\alpha\gamma) & 4\alpha\beta \\ 4\gamma^2 & -2\beta\gamma & \beta^2 \end{pmatrix} \begin{pmatrix} p_2 \\ p_1 \\ p_0 \end{pmatrix} = \lambda \begin{pmatrix} p_2 \\ p_1 \\ p_0 \end{pmatrix}.$$

Then, by computing the eigenvalues and eigenspaces of the  $3 \times 3$  matrix above, it is not hard to check that the claim holds.  $\square$

**Proposition 3.11.** *Any reducible form  $F \in V_{\mathbb{Z}, f}^0$  is either of type 1 or of type 2.*

*Proof.* Write  $F = g^{(1)}g^{(2)}g^{(3)}g^{(4)}$ , where the  $g^{(k)}$  are complex binary linear forms, and are pairwise nonproportional because  $\Delta(F) \neq 0$ . Since  $F$  is reducible, by renumbering if necessary, we may assume that

$$\begin{cases} g^{(1)}, g^{(2)}g^{(3)}g^{(4)} & \text{when } F \text{ has exactly one rational linear factor,} \\ g^{(1)}, g^{(2)}, g^{(3)}g^{(4)} & \text{when } F \text{ has exactly two rational linear factors,} \\ g^{(1)}g^{(2)}, g^{(3)}g^{(4)} & \text{when } F \text{ has no rational linear factor,} \\ g^{(1)}, g^{(2)}, g^{(3)}, g^{(4)} & \text{when } F \text{ has four rational linear factors,} \end{cases}$$

have integer coefficients and are irreducible. We have  $M_f^2 = \Delta(f) \cdot I_{2 \times 2}$  and  $F_{M_f} = F$  by definition. Hence, up to scaling, the matrix  $M_f$  acts on the  $g^{(k)}$  via a permutation  $\sigma$  on four letters of order dividing two. This has two consequences.

By (1-8), without loss of generality, we may assume that  $\alpha \neq 0$ . First, the form  $F$  cannot have exactly one rational linear factor, for otherwise

$$\sigma(1) = 1 \quad \text{and} \quad \sigma(k_0) = k_0 \text{ for at least one } k_0 \in \{2, 3, 4\}.$$

From Lemma 3.9, it would follow that  $\Delta(f)$  is a square and that  $g^{(k_0)}$  is proportional to a form with integer coefficients, which is a contradiction. Second, when  $F$  has four rational linear factors, by further renumbering if necessary, we may assume that

$$\sigma \in \{(1), (12), (12)(34)\}.$$

Now, in all three of the possible cases for the factorization of  $F$ , define

$$p = g^{(1)}g^{(2)} \quad \text{and} \quad q = g^{(3)}g^{(4)},$$

which are integral binary quadratic forms by definition. We then deduce that

$$(p_{M_f}, q_{M_f}) = (\lambda \cdot q, \lambda^{-1} \cdot p) \quad \text{or} \quad (p_{M_f}, q_{M_f}) = (\lambda \cdot p, \lambda^{-1} \cdot q)$$

for some  $\lambda \in \mathbb{Q}^\times$ . In the former case, it is clear that  $F$  is of type 1. In the latter case, we have  $\lambda = -1$  by Lemma 3.10 and the fact that  $\Delta(F) \neq 0$ , so  $F$  is of type 2.  $\square$

#### 4. Parametrizing forms in $V_{\mathbb{R},f}$ of nonzero discriminant

Throughout this section, let  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  be a real binary quadratic form with  $\Delta(f) \neq 0$  and  $\alpha > 0$ . We shall give an alternative parametrization of  $V_{\mathbb{R},f}^0$ , different from (3-1) and (3-2), in terms of the regions

$$(4-1) \quad \begin{cases} \Omega^0 = \{(L, K) \in \mathbb{R}^2 : L^2 + 4K \neq 0 \text{ and } 2L^2 - K \neq 0\}, \\ \Omega^+ = \{(L, K) \in \mathbb{R}^2 : L^2 + 4K > 0 \text{ and } 2L^2 - K \neq 0\}, \\ \Omega^- = \{(L, K) \in \mathbb{R}^2 : L^2 + 4K < 0 \text{ and } 2L^2 - K > 0\}, \end{cases}$$

corresponding to the  $L_f$ - and  $K_f$ -invariants, as well as a parameter  $t \in \mathbb{R}$  arising from the *orthogonal group of  $f$* , defined by

$$O_f(\mathbb{R}) = \{T \in \text{GL}_2(\mathbb{R}) : \det(T) = \pm 1 \text{ and } f_T = \pm f\}.$$

Note that by (1-7), for any  $F \in V_{\mathbb{R},f}^0$ , we have

$$\begin{aligned} (L_f(F), K_f(F)) \in \Omega^+ &\iff \Delta(F) > 0, \\ (L_f(F), K_f(F)) \in \Omega^- &\iff \Delta(F) < 0. \end{aligned}$$

First, we shall show that it suffices to consider  $x^2 + y^2$  and  $x^2 - y^2$ . It shall be helpful to recall (1-8) as well as the isomorphisms  $\Theta_1$  and  $\Theta_2$  defined in Section 1A.

**Lemma 4.1.** *Define a matrix*

$$T_f = \begin{pmatrix} \delta_f^{-1/4} & 0 \\ 0 & \delta_f^{1/4} \end{pmatrix} \cdot \frac{1}{2\sqrt{\alpha}} \begin{pmatrix} 2\alpha & \beta \\ 0 & 2 \end{pmatrix}, \quad \text{where } \delta_f = \frac{|\Delta(f)|}{4}.$$

*Then, we have a well-defined bijective linear map*

$$\begin{cases} \Psi_f : V_{\mathbb{R}, x^2+y^2} \rightarrow V_{\mathbb{R}, f}, & \Psi_f(F) = F_{T_f} \quad \text{if } f \text{ is positive definite,} \\ \Psi_f : V_{\mathbb{R}, x^2-y^2} \rightarrow V_{\mathbb{R}, f}, & \Psi_f(F) = F_{T_f} \quad \text{if } f \text{ is indefinite,} \end{cases}$$

*and we have  $\det(\Psi_f) = 8\alpha^3 |\Delta(f)|^{-3/2}$ .*

*Proof.* The first claim holds by (1-8) and the fact

$$\delta_f^{-1/2} \cdot f = \begin{cases} (x^2 + y^2)_{T_f} & \text{if } f \text{ is positive definite,} \\ (x^2 - y^2)_{T_f} & \text{if } f \text{ is indefinite.} \end{cases}$$

Identifying  $V_{\mathbb{R}, x^2 \pm y^2}$  and  $V_{\mathbb{R}, f}$  with  $\mathbb{R}^3$  via  $\Theta_1$ , we see from (3-1) that

$$(4-2) \quad \Psi_f : \begin{pmatrix} a_4 \\ a_3 \\ a_2 \end{pmatrix} \mapsto \begin{pmatrix} \alpha^2/\delta_f & 0 & 0 \\ 2\alpha\beta/\delta_f & \alpha/\sqrt{\delta_f} & 0 \\ 3\beta^2/2\delta_f & 3\beta/(2\sqrt{\delta_f}) & 1 \end{pmatrix} \begin{pmatrix} a_4 \\ a_3 \\ a_2 \end{pmatrix},$$

from which the second claim follows. □

In the subsequent subsections, we shall prove the following propositions.

**Proposition 4.2.** *There exists an explicit bijection*

$$\Phi : \Omega^+ \times [-\pi/4, \pi/4] \rightarrow V_{\mathbb{R}, x^2+y^2}^0,$$

*defined as in (4-4), such that*

- (a) *we have  $L_{x^2+y^2}(\Phi(L, K, t)) = L$  and  $K_{x^2+y^2}(\Phi(L, K, t)) = K$ ,*
- (b) *the Jacobian matrix of  $\Theta_1 \circ \Phi$  has determinant  $-\frac{1}{18}$ .*

**Proposition 4.3.** *There exist explicit injections*

$$\Phi^{(1)}, \Phi^{(2)} : \Omega^+ \times \mathbb{R} \rightarrow V_{\mathbb{R}, x^2-y^2}^0 \quad \text{and} \quad \Phi^{(3)}, \Phi^{(4)} : \Omega^- \times \mathbb{R} \rightarrow V_{\mathbb{R}, x^2-y^2}^0,$$

*defined as in (4-6), with*

$$V_{\mathbb{R}, x^2-y^2}^0 = \Phi^{(1)}(\Omega^+ \times \mathbb{R}) \sqcup \Phi^{(2)}(\Omega^+ \times \mathbb{R}) \sqcup \Phi^{(3)}(\Omega^- \times \mathbb{R}) \sqcup \Phi^{(4)}(\Omega^- \times \mathbb{R})$$

*such that, for all  $i = 1, 2, 3, 4$ ,*

- (a) *we have  $L_{x^2-y^2}(\Phi^{(i)}(L, K, t)) = L$  and  $K_{x^2-y^2}(\Phi^{(i)}(L, K, t)) = K$ ,*
- (b) *the Jacobian matrix of  $\Theta_1 \circ \Phi^{(i)}$  has determinant  $-\frac{1}{18}$ .*

In view of (1-11), we shall give another parametrization of  $V_{\mathbb{R}, f}$  when  $\gamma = 0$ , which does not require reducing to the form  $x^2 - y^2$  via Lemma 4.1.

**Proposition 4.4.** *Suppose that  $\gamma = 0$ . Then, there exist explicit injections*

$$\Phi_f^{(1)}, \Phi_f^{(2)} : \Omega^0 \times \mathbb{R} \rightarrow V_{\mathbb{R},f}^0,$$

*defined as in (4-9), with*

$$V_{\mathbb{R},f}^0 = \Phi_f^{(1)}(\Omega^0 \times \mathbb{R}) \sqcup \Phi_f^{(2)}(\Omega^0 \times \mathbb{R})$$

*such that, for both  $i = 1, 2$ ,*

(a) *we have  $L_f(\Phi^{(i)}(L, K, t)) = L$  and  $K_f(\Phi^{(i)}(L, K, t)) = K$ ,*

(b) *the Jacobian matrix of  $\Theta_2 \circ \Phi_f^{(i)}$  has determinant  $-\frac{1}{18}$ .*

For  $t \in \mathbb{R}$ , we shall use the notation

$$(4-3) \quad T^+(t) = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix} \quad \text{and} \quad T^-(t) = \begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix},$$

which is an element of  $O_{x^2+y^2}(\mathbb{R})$  and  $O_{x^2-y^2}(\mathbb{R})$ , respectively.

**4A. Positive definite case.** Define

$$(4-4) \quad \Phi : \Omega^+ \times [-\pi/4, \pi/4] \rightarrow V_{\mathbb{R},x^2+y^2}^0, \quad \Phi(L, K, t) = (F_{(L,K)})_{T^+(t)},$$

where

$$\begin{aligned} F_{(L,K)}(x, y) &= \frac{-3L + \sqrt{L^2 + 4K}}{24} x^4 + \frac{-L - \sqrt{L^2 + 4K}}{4} x^2 y^2 + \frac{-3L + \sqrt{L^2 + 4K}}{24} y^4. \end{aligned}$$

The image of  $\Phi$  lies in  $V_{\mathbb{R},x^2+y^2}$  by (3-1) and (1-8). Using Propositions 3.1 and 3.2(a), it is easy to check that Proposition 4.2(a) holds.

Now, by (3-1), an arbitrary  $F \in V_{\mathbb{R},x^2+y^2}^0$  has the shape

$$F(x, y) = a_4 x^4 + a_3 x^3 y + a_2 x^2 y^2 - a_3 x y^3 + a_4 y^4.$$

Write  $L = L_{x^2+y^2}(F)$  and  $K = K_{x^2+y^2}(F)$ . Note that  $(L, K) \in \Omega^+$  because  $\Delta(F) > 0$  by (1-7). For  $t \in \mathbb{R}$ , a direct computation yields

$$F_{T^+(t)}(x, y) = A(t)x^4 + B(t)x^3 y + C(t)x^2 y^2 - B(t)xy^3 + A(t)y^4,$$

where

$$\begin{cases} A(t) = \frac{6a_4 + a_2}{8} + \frac{2a_4 - a_2}{8} \cos(4t) - \frac{a_3}{4} \sin(4t), \\ B(t) = a_3 \cos(4t) + \frac{2a_4 - a_2}{2} \sin(4t), \\ C(t) = \frac{6a_4 + a_2}{4} - \frac{3(2a_4 - a_2)}{4} \cos(4t) + \frac{3a_3}{2} \sin(4t). \end{cases}$$

It is not hard to show that there exists a unique  $t_0 \in (-\pi/4, \pi/4]$  such that  $B(t_0) = 0$  and  $2A(t_0) - C(t_0) > 0$ . Put  $(A, C) = (A(t_0), C(t_0))$ . Then, we have

$$(L, K) = (L_{x^2+y^2}(F_{T^+(t_0)}), K_{x^2+y^2}(F_{T^+(t_0)})) = (-6A - C, -2C(6A - C))$$

by Propositions 3.1 and 3.2(a). We solve that  $F_{T^+(t_0)} = F_{(L,K)}$ , or equivalently

$$F = (F_{(L,K)})_{T^+(-t_0)} = \Phi(L, K, -t_0).$$

Since  $-t_0 \in [-\pi/4, \pi/4)$  is uniquely determined by  $F$ , this shows that  $\Phi$  is a bijection.

Finally, the above calculation also yields

$$(\Theta_1 \circ \Phi)(L, K, t) = (\Phi_1(L, K, t), \Phi_2(L, K, t), \Phi_3(L, K, t)),$$

where

$$(4-5) \quad \begin{cases} \Phi_1(L, K, t) = -\frac{L}{8} + \frac{\sqrt{L^2+4K}}{24} \cos(4t), \\ \Phi_2(L, K, t) = \frac{\sqrt{L^2+4K}}{6} \sin(4t), \\ \Phi_3(L, K, t) = -\frac{L}{4} - \frac{\sqrt{L^2+4K}}{4} \cos(4t). \end{cases}$$

By a direct computation, we then see that Proposition 4.2(b) holds.

**4B. Indefinite case.** Define

$$(4-6) \quad \begin{cases} \Phi^{(i)} : \Omega^+ \times \mathbb{R} \rightarrow V_{\mathbb{R}, x^2-y^2}^0, & \Phi^{(i)}(L, K, t) = (F_{(L,K)}^{(i)})_{T^-(t)} \quad \text{for } i = 1, 2, \\ \Phi^{(i)} : \Omega^- \times \mathbb{R} \rightarrow V_{\mathbb{R}, x^2-y^2}^0, & \Phi^{(i)}(L, K, t) = (F_{(L,K)}^{(i)})_{T^-(t)} \quad \text{for } i = 3, 4, \end{cases}$$

where

$$F_{(L,K)}^{(i)}(x, y) = \frac{3L + (-1)^i \sqrt{L^2+4K}}{24} x^4 + \frac{-L + (-1)^i \sqrt{L^2+4K}}{4} x^2 y^2 + \frac{3L + (-1)^i \sqrt{L^2+4K}}{24} y^4$$

for  $i = 1, 2$ , and

$$F_{(L,K)}^{(i)}(x, y) = \frac{(-1)^i \sqrt{2L^2-K}}{3} x^3 y - L x^2 y^2 + \frac{(-1)^i \sqrt{2L^2-K}}{3} x y^3$$

for  $i = 3, 4$ . The images of  $\Phi^{(1)}, \Phi^{(2)}, \Phi^{(3)}, \Phi^{(4)}$  lie in  $V_{\mathbb{R}, x^2-y^2}$  by (3-1) and (1-8). Using Propositions 3.1 and 3.2(a), it is easy to check that Proposition 4.3(a) holds.

Now, by (3-1), an arbitrary  $F \in V_{\mathbb{R}, x^2-y^2}^0$  has the shape

$$F(x, y) = a_4 x^4 + a_3 x^3 y + a_2 x^2 y^2 + a_3 x y^3 + a_4 y^4.$$

Write  $L = L_{x^2-y^2}(F)$  and  $K = K_{x^2-y^2}(F)$ . For  $t \in \mathbb{R}$ , a direct computation yields

$$F_{T^-(t)}(x, y) = A(t)x^4 + B(t)x^3y + C(t)x^2y^2 + B(t)xy^3 + A(t)y^4,$$

where

$$\begin{cases} A(t) = \frac{6a_4 - a_2}{8} + \frac{2a_4 + a_2}{8} \cosh(4t) + \frac{a_3}{4} \sinh(4t), \\ B(t) = a_3 \cosh(4t) + \frac{2a_4 + a_2}{2} \sinh(4t), \\ C(t) = -\frac{6a_4 - a_2}{4} + \frac{3(2a_4 + a_2)}{4} \cosh(4t) + \frac{3a_3}{2} \sinh(4t). \end{cases}$$

Note that  $\frac{d}{dt}A(t) = \frac{1}{2}B(t)$ . It is not hard to check that:

- If  $\Delta(F) > 0$ , then there is a unique  $t_0 \in \mathbb{R}$  such that  $B(t_0) = 0$ .
- If  $\Delta(F) < 0$ , then  $B(t) \neq 0$  for all  $t \in \mathbb{R}$ , and there is a unique  $t_0 \in \mathbb{R}$  such that  $A(t_0) = 0$ .

Put  $(A, B, C) = (A(t_0), B(t_0), C(t_0))$ . Then, we have

$$\begin{aligned} (L, K) &= (L_{x^2-y^2}(F_{T^-(t_0)}), K_{x^2-y^2}(F_{T^-(t_0)})) \\ &= \begin{cases} (6A - C, 2C(6A + C)) & \text{if } \Delta(F) > 0, \\ (-C, -9B^2 + 2C^2) & \text{if } \Delta(F) < 0. \end{cases} \end{aligned}$$

by Propositions 3.1 and 3.2(a). We solve that  $F_{T^-(t_0)} = F_{(L,K)}^{(i)}$ , or equivalently

$$F = (F_{(L,K)}^{(i)})_{T^-(-t_0)} = \Phi^{(i)}(L, K, -t_0), \quad \text{for exactly one } i \in \{1, 2, 3, 4\}.$$

Since  $t_0$  is uniquely determined by  $F$ , this shows that  $\Phi^{(1)}, \Phi^{(2)}, \Phi^{(3)}, \Phi^{(4)}$  are all injections, and that the stated disjoint union holds.

Finally, the above calculation also yields

$$(\Theta_1 \circ \Phi^{(i)})(L, K, t) = (\Phi_1^{(i)}(L, K, t), \Phi_2^{(i)}(L, K, t), \Phi_3^{(i)}(L, K, t)),$$

where

$$(4-7) \quad \begin{cases} \Phi_1^{(i)}(L, K, t) = \frac{L}{8} + \frac{(-1)^i \sqrt{L^2 + 4K}}{24} \cosh(4t), \\ \Phi_2^{(i)}(L, K, t) = \frac{(-1)^i \sqrt{L^2 + 4K}}{6} \sinh(4t), \\ \Phi_3^{(i)}(L, K, t) = -\frac{L}{4} + \frac{(-1)^i \sqrt{L^2 + 4K}}{4} \cosh(4t), \end{cases}$$

for  $i = 1, 2$ , and

$$(4-8) \quad \begin{cases} \Phi_1^{(i)}(L, K, t) = \frac{L}{8} - \frac{L}{8} \cosh(4t) + \frac{(-1)^i \sqrt{2L^2 - K}}{12} \sinh(4t), \\ \Phi_2^{(i)}(L, K, t) = \frac{(-1)^i \sqrt{2L^2 - K}}{3} \cosh(4t) - \frac{L}{2} \sinh(4t), \\ \Phi_3^{(i)}(L, K, t) = -\frac{L}{4} - \frac{3L}{4} \cosh(4t) + \frac{(-1)^i \sqrt{2L^2 - K}}{2} \sinh(4t), \end{cases}$$

for  $i = 3, 4$ . By a direct computation, we then see that [Proposition 4.3\(b\)](#) holds.

**4C. Reducible case.** Suppose  $\gamma = 0$ . For  $t \in \mathbb{R}$ , put

$$T(t) = \begin{pmatrix} e^{-t} & 0 \\ \frac{2\alpha \sinh t}{\beta} & e^t \end{pmatrix},$$

which is an element of  $O_f(\mathbb{R})$ . Define

$$(4-9) \quad \Phi_f^{(i)} : \Omega^0 \times \mathbb{R} \rightarrow V_{\mathbb{R}, f}^0, \quad \Phi_f^{(i)}(L, K, t) = (F_{f, (L, K)}^{(i)})_{T(t)} \quad \text{for } i = 1, 2,$$

where

$$\begin{aligned} F_{f, (L, K)}^{(i)}(x, y) = & \left( \frac{L^2 + (-1)^i 72\alpha^2 L + 4K + 144\alpha^4}{(-1)^i 144\beta^2} \right) x^4 + \left( \frac{\alpha L + (-1)^i 4\alpha^3}{\beta} \right) x^3 y \\ & + \left( \frac{L + (-1)^i 12\alpha^2}{2} \right) x^2 y^2 + (-1)^i 4\alpha\beta x y^3 + (-1)^i \beta^2 y^4. \end{aligned}$$

The images of  $\Phi_f^{(1)}, \Phi_f^{(2)}$  lie in  $V_{\mathbb{R}, f}$  by [\(3-2\)](#) and [\(1-8\)](#). Using [Propositions 3.1](#) and [3.2\(b\)](#), it is easy to check that [Proposition 4.4\(a\)](#) holds.

Now, by [\(3-2\)](#), an arbitrary  $F \in V_{\mathbb{R}, f}^0$  has the shape

$$(4-10) \quad F(x, y) = a_4 x^4 + \left( \frac{2\alpha(\beta^2 a_2 - 4\alpha^2 a_0)}{\beta^3} \right) x^3 y + a_2 x^2 y^2 + \left( \frac{4\alpha a_0}{\beta} \right) x y^3 + a_0 y^4.$$

Write  $L = L_f(F)$  and  $K = K_f(F)$ . For  $t \in \mathbb{R}$ , a direct computation yields

$$F_{T(t)}(x, y) = A(t)x^4 + (*)x^3 y + B(t)x^2 y^2 + (*)xy^3 + C(t)y^4,$$

where

$$\begin{cases} A(t) = e^{-4t} a_4 + \frac{\alpha^2}{\beta^2} (e^{4t} - 1) e^{-4t} a_2 + \frac{\alpha^4}{\beta^4} (e^{4t} - 1) (e^{4t} - 5) e^{-4t} a_0, \\ B(t) = a_2 + \frac{6\alpha^2}{\beta^2} (e^{4t} - 1) a_0, \\ C(t) = e^{4t} a_0. \end{cases}$$



Since  $\Delta(F) \neq 0$ , we have  $(-1)^i a_0 > 0$  for a unique  $i \in \{1, 2\}$ , and there is a unique  $t_0 \in \mathbb{R}$  such that  $C(t_0) = (-1)^i \beta^2$ . Put  $(A, B) = (A(t_0), B(t_0))$ . Then, we have

$$\begin{aligned} (L, K) &= (L_f(F_{T(t_0)}), K_f(F_{T(t_0)})) \\ &= (2B - (-1)^i 12\alpha^2, -B^2 + (-1)^i 36\beta^2 A - (-1)^i 24\alpha^2 B + 144\alpha^4), \end{aligned}$$

by Propositions 3.1 and 3.2(b). We solve that  $F_{T(t_0)} = F_{f,(L,K)}^{(i)}$ , or equivalently

$$F = (F_{f,(L,K)}^{(i)})_{T(-t_0)} = \Phi_f^{(i)}(L, K, -t_0).$$

Since  $t_0$  and  $i$  are uniquely determined by  $F$ , this shows that  $\Phi_f^{(1)}$  and  $\Phi_f^{(2)}$  are both injections, and that the stated disjoint union holds.

Finally, the above calculation also yields

$$(\Theta_2 \circ \Phi_f^{(i)})(L, K, t) = (\Phi_{f,1}^{(i)}(L, K, t), \Phi_{f,2}^{(i)}(L, K, t), \Phi_{f,3}^{(i)}(L, K, t)),$$

where

$$(4-11) \quad \begin{cases} \Phi_{f,1}^{(i)}(L, K, t) = \frac{(-1)^i e^{-4t}}{144\beta^2} (L^2 + 4K) + \frac{\alpha^2}{2\beta^2} L + \frac{(-1)^i \alpha^4 e^{4t}}{\beta^2}, \\ \Phi_{f,2}^{(i)}(L, K, t) = \frac{L}{2} + (-1)^i 6\alpha^2 e^{4t}, \\ \Phi_{f,3}^{(i)}(L, K, t) = (-1)^i \beta^2 e^{4t}. \end{cases}$$

By a direct computation, we then see that Proposition 4.4(b) holds.

## 5. Definition of a bounded semialgebraic set

Throughout this section, let  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  be an integral and primitive binary quadratic form with  $\Delta(f) \neq 0$  and  $\alpha > 0$ , in the shape (1-11) whenever  $f$  is reducible. As we have already explained in Section 1A, the proof of Theorem 1.2 is reduced to counting points in the lattices in (1-10), which in turn amounts to certain volume computations, by the result below.

**Proposition 5.1** (Davenport's lemma). *Let  $\mathcal{R}$  be a bounded semialgebraic multiset in  $\mathbb{R}^n$  having maximum multiplicity  $m$  and which is defined by at most  $k$  polynomial inequalities, each having degree at most  $\ell$ . Then, the number of integral lattice points (counted with multiplicity) contained in the region  $\mathcal{R}$  is*

$$\text{Vol}(\mathcal{R}) + O(\max\{\text{Vol}(\bar{\mathcal{R}}), 1\}),$$

where  $\text{Vol}(\bar{\mathcal{R}})$  denotes the greatest  $d$ -dimensional volume of any projection of  $\mathcal{R}$  onto a coordinate subspace by equating  $n - d$  coordinates to zero, with  $1 \leq d \leq n - 1$ . The implied constant in the second summand depends only on  $n, m, k, \ell$ .

*Proof.* This is a result of Davenport [1951a], and the above formulation is due to Bhargava and Shankar [2015, Proposition 2.6].  $\square$

For  $X > 0$ , define

$$V_{\mathbb{R},f}^0(X) = \{F \in V_{\mathbb{R},f}^0 : H_f(F) \leq X\} \quad \text{and} \quad V_{\mathbb{Z},f}^0(X) = \{F \in V_{\mathbb{Z},f}^0 : H_f(F) \leq X\}.$$

However, to prove [Theorem 1.2](#), we cannot apply [Proposition 5.1](#) directly to

$$\Theta_{w(f)}(V_{\mathbb{R},f}^0(X)), \quad \text{where } w(f) = \begin{cases} 1 & \text{if } f \text{ is irreducible,} \\ 2 & \text{if } f \text{ is reducible,} \end{cases}$$

as in [Section 1A](#), to count the lattice points in  $\Theta_{w(f)}(V_{\mathbb{Z},f}^0(X)) \subset \Lambda_{f,w(f)}$  because

(1) the set  $\Theta_{w(f)}(V_{\mathbb{R},f}^0(X))$  is unbounded when  $f$  is indefinite,

(2) distinct forms in  $V_{\mathbb{Z},f}^0(X)$  might be  $\text{GL}_2(\mathbb{Z})$ -equivalent.

Recall [\(4-1\)](#) and define

$$\Omega^*(X) = \{(L, K) \in \Omega^* : \max\{L^2, |K|\} \leq X\} \quad \text{for } * \in \{0, +, -\}.$$

In the notation of [Lemma 4.1](#) as well as [Propositions 4.2, 4.3](#), and [4.4](#), we have

$$(5-1) \quad V_{\mathbb{R},f}^0(X) = \begin{cases} (\Psi_f \circ \Phi)(\Omega^+(X) \times [-\pi/4, \pi/4]), \\ \bigsqcup_{i=1}^2 (\Psi_f \circ \Phi^{(i)})(\Omega^+(X) \times \mathbb{R}) \sqcup \bigsqcup_{i=3}^4 (\Psi_f \circ \Phi^{(i)})(\Omega^-(X) \times \mathbb{R}), \\ \bigsqcup_{i=1}^2 \Phi_f^{(i)}(\Omega^0(X) \times \mathbb{R}), \end{cases}$$

respectively, if  $f$  is positive definite, indefinite, and reducible. We shall overcome the two issues above by restricting the values for  $t \in \mathbb{R}$ .

For brevity, in this section, write

$$D_f = |\Delta(f)| \quad \text{and} \quad \delta_f = D_f/4,$$

as in [Theorem 1.2](#) and [Lemma 4.1](#), respectively.

**Definition 5.2.** If  $f$  is positive definite, define

$$\mathcal{S}_f(X) = (\Psi_f \circ \Phi)(\Omega^+(X) \times [-\pi/4, \pi/4)).$$

If  $f$  is reducible, define

$$\mathcal{S}_f(X) = \bigsqcup_{i=1}^2 \Phi_f^{(i)}(\Omega^0(X) \times [t_{f,1}, t_{f,2}]) \quad \text{for } t_{f,1} = -\frac{\log 8}{4} \text{ and } t_{f,2} = \frac{\log(5X/18)}{4}.$$

If  $f$  is indefinite and irreducible, define

$$\mathcal{S}_f(X) = \bigsqcup_{i=1}^2 (\Psi_f \circ \Phi^{(i)})(\Omega^+(X) \times [0, t_{D_f})) \sqcup \bigsqcup_{i=3}^4 (\Psi_f \circ \Phi^{(i)})(\Omega^-(X) \times [0, t_{D_f})),$$

where  $t_{D_f}$  is defined as in [Theorem 1.2\(c\)](#).

The goal of this section to prove the following preliminary results and estimates:

**Proposition 5.3.** *The set  $\Theta_{w(f)}(S_f(X))$  is bounded, semialgebraic, and definable by an absolutely bounded number of polynomial inequalities whose degrees are absolutely bounded.*

**Proposition 5.4.** *The following statements hold.*

- (a) *A form in  $V_{\mathbb{Z},f}^0(X)$  is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to at least one form in  $S_f(X)$ .*
- (b) *A form in  $V_{\mathbb{Z},f}^0(X)$  for which  $\Delta(F) \neq \square$  is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to exactly  $r_f$  forms in  $S_f(X)$ , where  $r_f$  is defined as in [Theorem 1.2](#).*

**5A. Alternative description.** First, we shall give an alternative description of the set  $S_f(X)$  in terms of the coefficients of the forms in  $V_{\mathbb{R},f}^0(X)$ .

**Lemma 5.5.** *If  $f$  is positive definite, then  $S_f(X) = V_{\mathbb{R},f}^0(X)$ .*

*Proof.* This is clear from [\(5-1\)](#). □

**Lemma 5.6.** *If  $f$  is reducible, then*

$$S_f(X) = \{F \in V_{\mathbb{R},f}^0(X) : \beta^2/8 \leq |C_F| \leq 5\beta^2 X/18\},$$

where  $C_F$  denotes the  $y^4$ -coefficient of  $F$ .

*Proof.* For  $i = 1, 2$  and for any  $F = \Phi_f^{(i)}(L, K, t)$ , we have  $C_F = (-1)^i \beta^2 e^{4t}$  by [\(4-11\)](#), and the claim is then clear from [\(5-1\)](#). □

**Lemma 5.7.** *If  $f$  is an indefinite and irreducible, then*

$$S_f(X) = \{F \in V_{\mathbb{R},f}^0(X) : 1 \leq E_{f,1}(F)Z_f(F)/E_{f,2}(F) < e^{8t_{D_f}}\},$$

where in the notation of [Proposition 3.2\(a\)](#), we define

$$E_{f,1}(F) = L_{f,1}(F) - \sqrt{D_f}L_{f,2}(F) \quad \text{and} \quad E_{f,2}(F) = L_{f,1}(F) + \sqrt{D_f}L_{f,2}(F),$$

and for  $F$  in the image of  $\Psi_f \circ \Phi^{(i)}$ , we define

$$Z_f(F) = \begin{cases} 1 & \text{for } i = 1, 2, \\ \frac{L_f(F)^2 + 4K_f(F)}{(4L_f(F) - (-1)^i 2\sqrt{2}L_f(F)^2 - K_f(F))^2} & \text{for } i = 3, 4. \end{cases}$$

*Proof.* For  $i = 1, 2, 3, 4$ , consider  $F = (\Psi_f \circ \Phi^{(i)})(L, K, t)$ . For  $k = 1, 2$ , we have

$$E_{f,k}(F) = \begin{cases} (-1)^i 2\alpha^2 \sqrt{L_f(F)^2 + 4K_f(F)} e^{(-1)^{k+1}4t} / 3 & \text{if } i = 1, 2, \\ -2\alpha^2 (3L_f(F) + (-1)^{k+i} 2\sqrt{2}L_f(F)^2 - K_f(F)) e^{(-1)^{k+1}4t} / 3 & \text{if } i = 3, 4, \end{cases}$$

by a direct computation using [\(4-2\)](#), [\(4-7\)](#), and [\(4-8\)](#). We then see that

$$E_{f,1}(F)Z_f(F)/E_{f,2}(F) = e^{8t},$$

from which the claim follows. □

**5B. Proof of Proposition 5.3.** From (4-5), (4-7), (4-8), and (4-11), it is clear that the set  $\mathcal{S}_f(X)$  is bounded. Thus, it remains to show that  $\mathcal{S}_f(X)$  is a semialgebraic set definable by an absolutely bounded number of polynomial inequalities whose degrees are absolutely bounded.

**5B1.** *The case when  $f$  is positive definite or reducible.* The claim follows immediately from Lemmas 5.5 and 5.6 as well as Proposition 3.2.

**5B2.** *The case when  $f$  is indefinite and irreducible.* The only problem is that, for  $F$  in the image of  $\Psi_f \circ \Phi^{(i)}$  for  $i = 3, 4$ , the expression  $Z_f(F)$  is not a polynomial in the  $x^4$ ,  $x^3y$ , and  $x^2y^2$ -coefficients of  $F$ . We shall resolve this issue in Lemma 5.8 below. The claim then follows from Lemma 5.7 and Proposition 3.2.

**Lemma 5.8.** *For  $i = 3, 4$ , let  $F \in (\Psi_f \circ \Phi^{(i)})(\Omega^- \times \mathbb{R})$ . Then, the condition*

$$1 \leq E_{f,1}(F)Z_f(F)/E_{f,2}(F) < e^{8t_{Df}}$$

*is equivalent to an absolutely bounded number of polynomial inequalities in the variables  $L_f(F)$ ,  $K_f(F)$ ,  $E_{f,1}(F)$ ,  $E_{f,2}(F)$  whose degrees are absolutely bounded.*

*Proof.* For brevity, define

$$Y_{f,1}(F) = -E_{f,1}(F)(L_f(F)^2 + 4K_f(F)) + E_{f,2}(F)(17L_f(F)^2 - 4K_f(F)),$$

$$Y_{f,2}(F) = -E_{f,1}(F)(L_f(F)^2 + 4K_f(F)) + e^{8t_{Df}} E_{f,2}(F)(17L_f(F)^2 - 4K_f(F)),$$

as well as write

$$\begin{aligned} (L, K, E_1, E_2, Z, Y_1, Y_2) \\ = (L_f(F), K_f(F), E_{f,1}(F), E_{f,2}(F), Z_f(F), Y_{f,1}(F), Y_{f,2}(F)). \end{aligned}$$

Note that  $L^2 + 4K < 0$  by (1-7) because  $\Delta(F) < 0$ . This implies that  $Z < 0$  and so the stated condition may be rewritten as

$$\begin{cases} E_2 \leq E_1 Z < e^{8t_{Df}} E_2 & \text{if } E_2 > 0, \text{ which is equivalent to } i = 3, \\ E_2 \geq E_1 Z > e^{8t_{Df}} E_2 & \text{if } E_2 < 0, \text{ which is equivalent to } i = 4. \end{cases}$$

By rearranging, we may further rewrite the above as

$$12E_2L\sqrt{2L^2 - K} \leq (-1)^i Y_1 \quad \text{and} \quad 12e^{8t_{Df}} E_2L\sqrt{2L^2 - K} > (-1)^i Y_2.$$

From here, we shall consider the different possibilities for the signs of  $E_2$ ,  $L$ ,  $Y_1$ ,  $Y_2$ . For example, when  $E_2 > 0$  and  $L \geq 0$ , the above is equivalent to  $Y_1 \leq 0$  and

$$\begin{cases} (12E_2L)^2(2L^2 - K) \leq Y_1^2 & \text{if } Y_2 > 0, \\ (12E_2L)^2(2L^2 - K) \leq Y_1^2 \text{ and } (12e^{8t_{Df}} E_2L)^2(2L^2 - K) > Y_2^2 & \text{if } Y_2 \leq 0. \end{cases}$$

The other cases are analogous. We then see that the claim holds.  $\square$

**5C. Integral orthogonal groups.** We shall require an explicit description of

$$O_f(\mathbb{Z}) = O_f(\mathbb{R}) \cap \mathrm{GL}_2(\mathbb{Z}).$$

In the notation of [Lemma 4.1](#), observe that

$$(5-2) \quad O_f(\mathbb{R}) = \begin{cases} T_f^{-1}(O_{x^2+y^2}(\mathbb{R}))T_f & \text{if } f \text{ is positive definite,} \\ T_f^{-1}(O_{x^2-y^2}(\mathbb{R}))T_f & \text{if } f \text{ is indefinite.} \end{cases}$$

Moreover, it is well-known that

$$\begin{aligned} O_{x^2+y^2}(\mathbb{R}) &= \{J_k T^+(t) : k \in \{1, 4\} \text{ and } t \in \mathbb{R}\}, \\ O_{x^2-y^2}(\mathbb{R}) &= \{\pm J_k T^-(t) : k \in \{1, 2, 3, 4\} \text{ and } t \in \mathbb{R}\}, \end{aligned}$$

where  $T^+(t)$  and  $T^-(t)$  are defined as in [\(4-3\)](#), and

$$(5-3) \quad J_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad J_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We shall need the following lemma.

**Lemma 5.9.** *Suppose that  $T \in O_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$  has finite order. Then, the form  $f$  is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to a form of the shape*

$$\begin{cases} x^2 + y^2, x^2 + xy + y^2, \text{ or } ax^2 + bxy - ay^2 & \text{if } \det(T) = 1, \\ xy, x^2 - y^2, ax^2 + cy^2, \text{ or } ax^2 + bxy + ay^2 & \text{if } \det(T) = -1, \end{cases}$$

for some integers  $a, b$ , and  $c$ .

*Proof.* By [\[Newman 1972, Chapter IX\]](#), for example, a finite cyclic subgroup of  $\mathrm{GL}_2(\mathbb{Z})$  not contained in  $\{\pm I_{2 \times 2}\}$  is conjugate to the subgroup generated by one of the following:

$$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We then deduce that there exists  $P \in \mathrm{GL}_2(\mathbb{Z})$  such that  $Q = P^{-1}TP$  is equal to one of the following matrices up to sign:

$$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Since  $f$  is primitive with  $\alpha > 0$  by assumption and  $(f_P)_Q = \pm f_P$ , we then check that  $f_P$  must have one of the stated shapes.  $\square$

**Proposition 5.10.** *Suppose that  $f$  is positive definite. Then, we have*

$$O_f(\mathbb{Z}) = \{\pm I_{2 \times 2}\}$$

if  $f$  is not  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to the forms below, and the group  $O_f(\mathbb{Z})$  is equal to

$$\left\{ \begin{array}{ll} \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} & \text{if } f(x, y) = x^2 + y^2, \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \right\} & \text{if } f(x, y) = x^2 + xy + y^2, \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} & \text{if } f(x, y) = \alpha x^2 + \gamma y^2 \text{ for } \alpha \neq \gamma, \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} & \text{if } f(x, y) = \alpha x^2 + \beta xy + \alpha y^2 \text{ for } \beta \notin \{0, \alpha\}. \end{array} \right.$$

*Proof.* Elements in  $O_f(\mathbb{Z})$  have finite order by (5-2) and so the first claim follows from Lemma 5.9. Using (5-2), we compute that elements in  $O_f(\mathbb{R})$  are of the forms

$$\begin{pmatrix} \phi_t + \frac{\beta \psi_t}{2\sqrt{\delta_f}} & \frac{\gamma \psi_t}{\sqrt{\delta_f}} \\ -\frac{\alpha \psi_t}{\sqrt{\delta_f}} & \phi_t - \frac{\beta \psi_t}{2\sqrt{\delta_f}} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \phi_t - \frac{\beta \psi_t}{2\sqrt{\delta_f}} & \frac{\beta}{\alpha} \left( \phi_t - \frac{\beta \psi_t}{2\sqrt{\delta_f}} \right) + \frac{\gamma \psi_t}{\sqrt{\delta_f}} \\ \frac{\alpha \psi_t}{\sqrt{\delta_f}} & -\phi_t - \frac{\beta \psi_t}{2\sqrt{\delta_f}} \end{pmatrix},$$

where  $t \in \mathbb{R}$  and  $(\phi_t, \psi_t) = (\cos t, \sin t)$ . With the help of the proof of Lemma 5.9, it is not hard to check that  $O_f(\mathbb{Z})$  is as claimed.  $\square$

**Proposition 5.11.** *Suppose that  $f$  is reducible. Then, the group  $O_f(\mathbb{Z})$  is equal to*

$$\left\{ \begin{array}{ll} \{ \pm I_{2 \times 2} \} & \text{if } \beta \nmid \alpha^2 + 1 \text{ and } \beta \nmid \alpha^2 - 1, \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} \alpha & \beta \\ -(\alpha^2 + 1)/\beta & -\alpha \end{pmatrix} \right\} & \text{if } \beta \mid \alpha^2 + 1 \text{ and } \beta \nmid \alpha^2 - 1, \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} \alpha & \beta \\ -(\alpha^2 - 1)/\beta & -\alpha \end{pmatrix} \right\} & \text{if } \beta \nmid \alpha^2 + 1 \text{ and } \beta \mid \alpha^2 - 1, \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\} & \text{if } f(x, y) = x^2 + xy, \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \right\} & \text{if } f(x, y) = x^2 + 2xy. \end{array} \right.$$

*Proof.* Using (5-2), we compute that elements in  $O_f(\mathbb{R})$  are of the forms

$$\pm \begin{pmatrix} \phi_t - \psi_t & 0 \\ 2\alpha \psi_t / \beta & \phi_t + \psi_t \end{pmatrix} \quad \text{and} \quad \pm \begin{pmatrix} \phi_t + \psi_t & (\beta/\alpha)(\phi_t + \psi_t) \\ -2\alpha \psi_t / \beta & -\phi_t - \psi_t \end{pmatrix},$$

where  $t \in \mathbb{R}$  and  $(\phi_t, \psi_t) \in \{(\cosh t, \sinh t), (\sinh t, \cosh t)\}$ . For the matrix on the left to have integer entries, necessarily

$$2 \cosh t, 2 \sinh t \in \mathbb{Z}, \quad \text{so} \quad (2 \cosh t, 2 \sinh t) = (2, 0).$$

Similarly, for the matrix on the right to have integer entries, necessarily

$$2\alpha \cosh t, 2\alpha \sinh t, (\cosh t + \sinh t)/\alpha \in \mathbb{Z},$$

$$\text{so} \quad (2\alpha \cosh t, 2\alpha \sinh t) = (\alpha^2 + 1, \alpha^2 - 1).$$

We then deduce that

$$O_f(\mathbb{Z}) = \{\pm I_{2 \times 2}, \pm \begin{pmatrix} -1 & 0 \\ 2\alpha/\beta & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ -(\alpha^2 \pm 1)/\beta & -\alpha \end{pmatrix}\} \cap \mathrm{GL}_2(\mathbb{Z}).$$

Since  $f$  has the shape (1-11) by assumption, we have

$$\beta \mid \alpha^2 + 1 \text{ and } \beta \mid \alpha^2 - 1 \iff \alpha = 1 \text{ and } \beta \in \{1, 2\},$$

and we see that the claim indeed holds.  $\square$

**Proposition 5.12.** *Suppose that  $f$  is indefinite and irreducible. Define*

$$G_f(\mathbb{Z}) = \{\pm T_{D_f}^n : n \in \mathbb{Z}\}, \quad \text{where } T_{D_f} = \begin{pmatrix} \frac{1}{2}(u_{D_f} - \beta v_{D_f}) & -\gamma v_{D_f} \\ \alpha v_{D_f} & \frac{1}{2}(u_{D_f} + \beta v_{D_f}) \end{pmatrix}$$

and  $(u_{D_f}, v_{D_f}) \in \mathbb{N}^2$  is the least solution to  $x^2 - D_f y^2 = \pm 4$ . Then, we have

$$O_f(\mathbb{Z}) = G_f(\mathbb{Z})$$

if  $f$  is not  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to the forms below, and the group  $O_f(\mathbb{Z})$  is equal to

$$\begin{cases} G_f(\mathbb{Z}) \sqcup G_f(\mathbb{Z}) \begin{pmatrix} 1 & \beta/\alpha \\ 0 & -1 \end{pmatrix} & \text{if } f(x, y) = \alpha x^2 + \beta xy + \gamma y^2 \text{ with } \alpha \mid \beta, \\ G_f(\mathbb{Z}) \sqcup G_f(\mathbb{Z}) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \text{if } f(x, y) = \alpha x^2 + \beta xy - \alpha y^2. \end{cases}$$

*Proof.* By (5-2), elements in  $O_f(\mathbb{R})$  of infinite order are of the shape

$$\pm \begin{pmatrix} \phi_t - \beta \psi_t / (2\sqrt{\delta_f}) & -\gamma \psi_t / \sqrt{\delta_f} \\ \alpha \psi_t / \sqrt{\delta_f} & \phi_t + \beta \psi_t / (2\sqrt{\delta_f}) \end{pmatrix},$$

where  $t \in \mathbb{R}$  and  $(\phi_t, \psi_t) \in \{(\cosh t, \sinh t), (\sinh t, \cosh t)\}$ . We then see that

$$G_f(\mathbb{Z}) = \{\pm I_{2 \times 2}\} \sqcup \{T \in O_f(\mathbb{Z}) : T \text{ has infinite order}\}.$$

Hence, the first claim follows from Lemma 5.9 and the fact that  $ax^2 + bxy + ay^2$  is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to the form

$$(5-4) \quad (2a - b)x^2 + (2a - b)xy + ay^2 \quad \text{via } \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Now, again by (5-2), elements in  $O_f(\mathbb{R})$  of finite order have the shape

$$(5-5) \quad \begin{pmatrix} \frac{-\beta}{\sqrt{D_f}} & -\frac{2\gamma}{\sqrt{D_f}} \\ \frac{2\alpha}{\sqrt{D_f}} & \frac{\beta}{\sqrt{D_f}} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \phi_t + \frac{\beta \psi_t}{2\sqrt{\delta_f}} & \frac{\beta}{\alpha} \left( \phi_t + \frac{\beta \psi_t}{2\sqrt{\delta_f}} \right) - \frac{\gamma \psi_t}{\sqrt{\delta_f}} \\ -\frac{\alpha \psi_t}{\sqrt{\delta_f}} & -\phi_t - \frac{\beta \psi_t}{2\sqrt{\delta_f}} \end{pmatrix}$$

where  $t \in \mathbb{R}$  and  $(\phi_t, \psi_t) \in \{(\cosh t, \sinh t), (\sinh t, \cosh t)\}$ . Notice that the matrix on the left cannot lie in  $\mathrm{GL}_2(\mathbb{Z})$  because  $D_f$  is not square when  $f$  is irreducible. Using the description of  $O_{x^2-y^2}(\mathbb{R})$ , it is then not hard to check that  $[O_f(\mathbb{Z}) : G_f(\mathbb{Z})] \leq 2$ , from which the second claim follows.  $\square$

**5D. Proof of Theorem 1.4.** Suppose that  $f(x, y) = \alpha x^2 + \beta xy - \alpha y^2$  and that  $D_f$  is not a square. In the notation of Proposition 5.12, we have

$$x^2 - D_f y^2 = -4 \quad \text{has integer solutions if and only if} \quad \det(T_{D_f}) = -1$$

by definition. But Proposition 5.12 also implies that  $\det(T_{D_f}) = -1$  is equivalent to

$$O_f(\mathbb{Z}) \text{ has an element of finite order and negative determinant.}$$

The theorem now follows from Lemma 5.9 and (5-4).

**5E. Proof of Proposition 5.4.** We shall need the following lemma.

**Lemma 5.13.** *For all  $F \in V_{\mathbb{Z},f}^0$  with  $\Delta(F) \neq \square$  and  $T \in \mathrm{GL}_2(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$ , we have*

- (a)  $F_T \in V_{\mathbb{Z},f}^0 \quad \text{if and only if} \quad T \in O_f(\mathbb{Z}),$
- (b)  $F_T = F \quad \text{if and only if} \quad T = \pm D_f^{-1/2} M_f.$

*Proof.* Note that  $F_T \in V_{\mathbb{Z},f}^0$  by (1-8). By Theorem 1.1(a), we then have  $F_T \in V_{\mathbb{Z},f}^0$  if and only if  $f_T = \pm f$ , whence part (a) holds. By Theorem 1.1(a) and Proposition 2.1, we have  $F_T = F$  if and only if  $T$  is proportional to  $M_f$ , from which part (b) follows since  $\det(T) = \pm 1$ .  $\square$

**5E1. The case when  $f$  is positive definite or reducible.** Let us first observe that:

**Lemma 5.14.** *We have  $V_{\mathbb{Z},f}^0(X) \subset \mathcal{S}_f(X)$ .*

*Proof.* Let  $F \in V_{\mathbb{Z},f}^0(X)$  be given. If  $f$  is positive definite, then clearly  $F \in \mathcal{S}_f(X)$  by Lemma 5.5. If  $f$  is reducible, then recall Lemma 5.6, and we have  $F \in \mathcal{S}_f(X)$  since

$$\frac{8C_F}{\beta^2} \in \mathbb{Z} \quad \text{and} \quad \left| \frac{8C_F}{\beta^2} \right| \leq \left| \frac{4(L_f(F)^2 + 4K_f(F))}{9} \right| \leq \frac{20X}{9}$$

by (4-10) and Proposition 3.2(b), respectively.  $\square$

Lemma 5.14 implies that part (a) holds. Together with Lemma 5.13(a), it further implies that for  $F \in V_{\mathbb{Z},f}^0(X)$  with  $\Delta(F) \neq \square$ , the number of forms in  $\mathcal{S}_f(X)$  which are  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to  $F$  is equal to

$$[O_f(\mathbb{Z}) : \mathrm{Stab}_{O_f(\mathbb{Z})}(F)].$$

By Lemma 5.13(b), we in turn have

$$[O_f(\mathbb{Z}) : \mathrm{Stab}_{O_f(\mathbb{Z})}(F)] = [O_f(\mathbb{Z}) : O_f(\mathbb{Z}) \cap \{\pm I_{2 \times 2}, \pm D_f^{-1/2} M_f\}],$$

which may be verified to be equal to  $r_f$  using Propositions 5.10 and 5.11.



**5E2.** *The case when  $f$  is indefinite and irreducible.* We shall use the notation from Lemma 4.1, Proposition 5.12, (4-3), and (5-3). Then, by definition, we have

$$T_{D_f} = T_f^{-1} J_{k(f)} T^{-}(t_{D_f}) T_f, \quad \text{where } k(f) = \begin{cases} 1 & \text{if } u_{D_f}^2 - D_f v_{D_f}^2 = -4, \\ 2 & \text{if } u_{D_f}^2 - D_f v_{D_f}^2 = 4. \end{cases}$$

Now, by (5-1) and (4-6), a form in  $V_{\mathbb{Z}, f}^0(X)$  is of the shape

$$F = (F_{(L, K)}^{(i)})_{T^{-}(t)T_f}, \quad \text{where } (L, K, t) \in \Omega^0(X) \times \mathbb{R} \text{ and } i \in \{1, 2, 3, 4\}.$$

Observe that  $J_1$  and  $J_2$  commute with  $T^{-}(t)$  as well as fix the forms in  $V_{\mathbb{R}, x^2 - y^2}$ . For any  $n \in \mathbb{Z}$ , we then deduce that

$$F_{T_{D_f}^n} = (F_{(L, K)}^{(i)})_{T^{-}(t)J_{k(f)}^n T^{-}(nt_{D_f})T_f} = (F_{(L, K)}^{(i)})_{T^{-}(t+nt_{D_f})T_f}.$$

Let  $n_1 \in \mathbb{Z}$  be the unique integer such that  $0 \leq t + n_1 t_{D_f} < t_{D_f}$ . The existence of  $n_1$  then implies part (a).

Next, suppose that  $\Delta(F) \neq \square$ , in which case

$$\text{for } T \in \text{GL}_2(\mathbb{Z}) : \quad F_T \in V_{\mathbb{Z}, f}^0 \quad \text{if and only if} \quad T \in O_f(\mathbb{Z})$$

by Lemma 5.13(a). If  $O_f(\mathbb{Z}) = G_f(\mathbb{Z})$ , then part (b) holds by the uniqueness of  $n_1$ . If  $O_f(\mathbb{Z}) \neq G_f(\mathbb{Z})$ , then recall from Proposition 5.12 that

$$O_f(\mathbb{Z}) = G_f(\mathbb{Z}) \sqcup G_f(\mathbb{Z})M, \quad \text{where } M \text{ has finite order.}$$

From (5-2), we see that

$$M = \pm T_f^{-1} J_{k_0} T^{-}(t_0) T_f, \quad \text{where } t_0 \in \mathbb{R} \text{ and } k_0 \in \{3, 4\}.$$

Then, for any  $n \in \mathbb{Z}$ , it is straightforward to verify that

$$\begin{aligned} F_{T_{D_f}^n} M &= (F_{(L, K)}^{(i)})_{T^{-}(t+nt_{D_f})J_{k_0} T^{-}(t_0)T_f} \\ &= \begin{cases} (F_{(L, K)}^{(i)})_{T^{-}(-(t+nt_{D_f})+t_0)T_f} & \text{for } i \in \{1, 2\}, \\ (F_{(L, K)}^{(j)})_{T^{-}(-(t+nt_{D_f})+t_0)T_f} & \text{for } i \in \{3, 4\}, \text{ where } j \in \{3, 4\} \setminus \{i\}. \end{cases} \end{aligned}$$

There is a unique  $n_2 \in \mathbb{Z}$  such that  $0 \leq -(t + n_2 t_{D_f}) + t_0 < t_{D_f}$ . Observe that

$$F_{T_{D_f}^{n_1}} = F_{T_{D_f}^{n_2} M} \quad \text{would imply} \quad F_{T_{D_f}^{n_1}} = (F_{T_{D_f}^{n_1}})_{T_{D_f}^{n_2 - n_1} M}.$$

But  $T_{D_f}^{n_2 - n_1} M$  has finite order, and so it cannot be proportional to  $M_f$  by (5-5), which is a contradiction by Lemma 5.13(b). Then, we conclude from Proposition 5.12 that part (b) indeed holds.

## 6. Error estimates and the main theorem

Throughout this section, let  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  be an integral and primitive binary quadratic form with  $\Delta(f) \neq 0$  and  $\alpha > 0$ , in the shape (1-11) whenever  $f$  is reducible. Let  $D_f$ ,  $r_f$  and  $s_f$  be as in Theorem 1.2.

In Subsections 6A and 6B, respectively, we shall first prove:

**Proposition 6.1.** *For any  $\epsilon > 0$ , we have*

$$\#\{F \in \mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0 : L_f(F)^2 + 4K_f(F) = \square\} = O_{f,\epsilon}(X^{1+\epsilon}),$$

and

$$\begin{aligned} \#\{F \in \mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0 : \\ (L_f(F)^2 + 4K_f(F))(2L_f(F) - K_f(F))/\Delta(f) = \square \text{ and } L_f(F) \neq 0\} \\ = O_f(X^{1/2+\epsilon}). \end{aligned}$$

Further, the number

$$\#\{F \in \mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0 : -4K_f(F)^2/\Delta(f) = \square \text{ and } L_f(F) = 0\}$$

is equal to zero if  $-\Delta(f) \neq \square$ , and is bounded by  $O_f(X)$  otherwise.

Propositions 6.1, 3.6, and 5.4 then imply part (d) of Theorem 1.2.

**Proposition 6.2.** *We have*

$$\#\{F \in \mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0 : F \text{ is reducible}\} = \begin{cases} O_f(X(\log X)^2) & \text{if } f \text{ is irreducible,} \\ O_f(X(\log X)^3) & \text{if } f \text{ is reducible.} \end{cases}$$

Now, from Propositions 5.4, 6.1, and 6.2, we also easily see that

$$(6-1) \quad N_{\mathbb{Z},f}^{(D_4)}(X) = \frac{1}{r_f} \#(\mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0) + O_{f,\epsilon}(X^{1+\epsilon}) \quad \text{for any } \epsilon > 0.$$

Let  $\mathcal{L}_{f,w(f)}$  be a linear transformation on  $\mathbb{R}^3$  which takes  $\Lambda_{f,w(f)}$  to  $\mathbb{Z}^3$ , and define

$$\mathcal{R}_f(X) = (\mathcal{L}_{f,w(f)} \circ \Theta_{w(f)})(\mathcal{S}_f(X)), \quad \text{where } w(f) = \begin{cases} 1 & \text{if } f \text{ is irreducible,} \\ 2 & \text{if } f \text{ is reducible,} \end{cases}$$

as before. Observe that then

$$\#(\mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0) = \#(\Theta_{w(f)}(\mathcal{S}_f(X)) \cap \Lambda_{f,w(f)}) = \#(\mathcal{R}_f(X) \cap \mathbb{Z}^3).$$

By [Proposition 5.3](#), we may apply [Proposition 5.1](#) to obtain

$$\begin{aligned}
 (6-2) \quad & \#(S_f(X) \cap V_{\mathbb{Z},f}^0) \\
 &= \text{Vol}(\mathcal{R}_f(X)) + O(\max\{\text{Vol}(\overline{\mathcal{R}_f(X)}), 1\}) \\
 &= \frac{1}{\det(\Lambda_{f,w(f)})} \text{Vol}(\Theta_{w(f)}(S_f(X))) + O_f(\max\{\text{Vol}(\overline{\Theta_{w(f)}(S_f(X))}), 1\}),
 \end{aligned}$$

where by [Proposition 3.4](#), we know that

$$\det(\Lambda_{f,w(f)}) = \begin{cases} s_f \alpha^3 & \text{if } f \text{ is irreducible,} \\ s_f \beta^3 / 8 & \text{if } f \text{ is reducible.} \end{cases}$$

Hence, it remains to compute the above volumes, which we shall do in [Section 6C](#).

**6A. Proof of [Proposition 6.1](#).** Recall the notation from [Proposition 3.2](#). By definition and [Proposition 3.3](#), we then have a well-defined map

$$\iota : V_{\mathbb{Z},f}^0 \rightarrow \mathbb{Z}^3, \quad \iota(F) = (L_f(F), L_{f,1}(F), L_{f,2}(F)).$$

Using [Proposition 3.2](#), it is easy to verify that  $\iota$  is in fact injective. We shall also need the following result.

**Lemma 6.3** [[Heath-Brown 2002](#), Corollary 2]. *Let  $\xi(x_1, x_2, x_3)$  be a ternary quadratic form such that its corresponding matrix  $M_\xi$  has nonzero determinant. For  $B_1, B_2, B_3 > 0$ , let  $N_\xi(B_1, B_2, B_3)$  denote the number of tuples  $(x_1, x_2, x_3) \in \mathbb{Z}^3$  such that*

$$|x_1| \leq B_1, \quad |x_2| \leq B_2, \quad |x_3| \leq B_3, \quad \gcd(x_1, x_2, x_3) = 1, \quad \xi(x_1, x_2, x_3) = 0.$$

*Then, we have*

$$N_\xi(B_1, B_2, B_3) \ll_\epsilon \left( 1 + \left( B_1 B_2 B_3 \cdot \frac{\det_0(M_\xi)^2}{|\det(M_\xi)|} \right)^{1/3+\epsilon} \right) d_3(|\det(M_\xi)|),$$

*where  $\det_0(M_\xi)$  denotes the greatest common divisor of the  $2 \times 2$  minors of  $M_\xi$ , and  $d_3(|\det(M_\xi)|)$  is the number of ways to write  $|\det(M_\xi)|$  as a product of three positive integers.*

In what follows, consider  $F \in S_f(X) \cap V_{\mathbb{Z},f}^0$ , and for brevity, write

$$(L, K, L_1, L_2) = (L_f(F), K_f(F), L_{f,1}(F), L_{f,2}(F)).$$

Since  $\iota$  is injective, it is enough to estimate the number of choices for  $(L, L_1, L_2)$ . To that end, let us put  $\mathcal{D}_f = \Delta(f)$ . Recall from [Propositions 3.2](#) and [3.3](#) that

$$L, K, L_1, L_2 \in \mathbb{Z}, \quad \text{as well as} \quad L_1^2 - \mathcal{D}_f L_2^2 = 4\alpha^4(L^2 + 4K)/9,$$

which is nonzero by (1-7). By the definition of our height, we also have

$$(6-3) \quad \begin{cases} L = O_f(X^{1/2}) & \text{and} & K = O_f(X) & \text{in all cases,} \\ L_1 = O_f(X^{1/2}) & \text{and} & L_2 = O_f(X^{1/2}) & \text{if } f \text{ is irreducible.} \end{cases}$$

The latter estimate holds by

$$\begin{cases} (4-5), (4-2) & \text{if } f \text{ is positive definite,} \\ (4-7), (4-8), (4-2), \text{ and } 0 \leq t < t_{D_f} & \text{if } f \text{ is indefinite and irreducible,} \end{cases}$$

as well as the fact that  $L_1$  and  $L_2$  are linear in the coefficients of  $F$ . Finally, we shall write  $d(-)$  for the divisor function.

*Proof of Proposition 6.1: first claim.* Suppose that  $L^2 + 4K = \square$ . Then, we have

$$L_1^2 - \mathcal{D}_f L_2^2 = U^2, \quad \text{where } U \in \mathbb{N} \text{ is such that } U = O_f(X^{1/2}).$$

If  $f$  is reducible, then  $\mathcal{D}_f = \square$  and so clearly there are

$$O_f\left(\sum_{U=1}^{X^{1/2}} d(U^2)\right) = O_{f,\epsilon}\left(\sum_{U=1}^{X^{1/2}} X^\epsilon\right) = O_{f,\epsilon}(X^{1/2+\epsilon})$$

choices for the pair  $(L_1, L_2)$ . If  $f$  is irreducible, then note that

$$(L_1/n)^2 - \mathcal{D}_f (L_2/n)^2 = (U/n)^2, \quad \text{where } n = \gcd(L_1, L_2, U),$$

and applying Lemma 6.3 to the ternary quadratic form  $\xi$  with matrix

$$M_\xi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\mathcal{D}_f & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \text{with } \begin{cases} \det(M_\xi) = \mathcal{D}_f, \\ \det_0(M_\xi) = 1, \end{cases}$$

we deduce from (6-3) that there are

$$O_f\left(\sum_{n=1}^{X^{1/2}} N_\xi\left(\frac{X^{1/2}}{n}, \frac{X^{1/2}}{n}, \frac{X^{1/2}}{n}\right)\right) = O_{f,\epsilon}\left(\sum_{n=1}^{X^{1/2}} \left(1 + \frac{X^{1/2+\epsilon}}{n^{1+\epsilon}}\right)\right) = O_{f,\epsilon}(X^{1/2+\epsilon})$$

choices for the pair  $(L_1, L_2)$ . In both cases, we see that there are

$$O_f(X^{1/2}) \cdot O_{f,\epsilon}(X^{1/2+\epsilon}) = O_{f,\epsilon}(X^{1+\epsilon})$$

choices for  $(L, L_1, L_2)$  in total, whence the claim.  $\square$

*Proof of Proposition 6.1: second claim.* Suppose that  $(L^2 + 4K)(2L^2 - K)/\mathcal{D}_f = \square$ . By Proposition 3.3, we may write

$$\gcd(L^2 + 4K, 4(2L^2 - K)/\mathcal{D}_f) = 9ma^2, \quad \text{where } m, a \in \mathbb{N} \text{ and } m \text{ is square-free.}$$

From the hypothesis, we then easily see that

$$L^2 + 4K = 9mU^2 \quad \text{and} \quad 4(2L^2 - K)/\mathcal{D}_f = 9mV^2, \quad \text{where } U, V \in \mathbb{N},$$

as well as that  $m$  divides  $L$ . In particular, a simple calculation yields

$$L^2 = m(U^2 + \mathcal{D}_f V^2), \quad \text{whence } mW^2 = U^2 + \mathcal{D}_f V^2, \quad \text{where } W \in \mathbb{Z} \text{ with } L = mW.$$

Now, suppose also that  $L \neq 0$ , in which case  $m = O_f(X^{1/2})$  by (6-3). Note also that

$$m(W/n)^2 = (U/n)^2 + \mathcal{D}_f(V/n)^2, \quad \text{where } n = \gcd(W, U, V).$$

Applying Lemma 6.3 to the ternary quadratic form  $\xi_m$  with matrix

$$M_{\xi_m} = \begin{pmatrix} m & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -\mathcal{D}_f \end{pmatrix}, \quad \text{with} \quad \begin{cases} \det(M_{\xi_m}) = m\mathcal{D}_f, \\ \det_0(M_{\xi_m}) = \gcd(m, \mathcal{D}_f) \leq |\mathcal{D}_f|, \end{cases}$$

we then see from (6-3) that there are

$$\begin{aligned} O_f\left(\sum_{n=1}^{X^{1/2}/m} N_{\xi_m}\left(\frac{X^{1/2}}{mn}, \frac{X^{1/2}}{m^{1/2}n}, \frac{X^{1/2}}{m^{1/2}n}\right)\right) &= O_{f,\epsilon}\left(\sum_{n=1}^{X^{1/2}/m} \left(1 + \frac{X^{1/2+\epsilon}}{(mn)^{1+\epsilon}}\right) m^\epsilon\right) \\ &= O_{f,\epsilon}\left(\frac{X^{1/2}}{m^{1-\epsilon}} + \frac{X^{1/2+\epsilon}}{m}\right) \end{aligned}$$

choices for  $(x, u, v)$  when  $m$  is fixed. It follows that we have

$$O_{f,\epsilon}\left(\sum_{m=1}^{X^{1/2}} \left(\frac{X^{1/2}}{m^{1-\epsilon}} + \frac{X^{1/2+\epsilon}}{m}\right)\right) = O_{f,\epsilon}(X^{1/2+\epsilon})$$

choices for  $(m, x, u, v)$  and hence for  $(L, K)$ .

Next, regard  $(L, K)$  as being fixed, and recall that

$$L_1^2 - \mathcal{D}_f L_2^2 = T, \quad \text{where } T = 4\alpha^4(L^2 + 4K)/9.$$

We claim that there are  $O_f(d(T))$  choices for  $(L_1, L_2)$ . If  $f$  is positive definite or if  $f$  is reducible, then this is clear. If  $f$  is indefinite and irreducible, then by Definition 5.2 as well as Propositions 3.1 and 4.3, we have

$$F = (\Psi_f \circ \Phi^{(i)})(L, K, t), \quad \text{where } 0 \leq t < t_{\mathcal{D}_f} \text{ and } i \in \{1, 2, 3, 4\}.$$

Since  $\mathcal{D}_f > 0$ , we must have  $L^2 + 4K > 0$  by the hypothesis, and so in fact  $i \in \{1, 2\}$ . From the proof of Lemma 5.7, we know that

$$L_1 - \sqrt{\mathcal{D}_f} L_2 = (-1)^i \sqrt{T} e^{4t} \quad \text{and} \quad L_1 + \sqrt{\mathcal{D}_f} L_2 = (-1)^i \sqrt{T} e^{-4t},$$

which implies that

$$L_1 = (-1)^i \sqrt{T} \cosh(4t) \quad \text{and} \quad L_2 = (-1)^i \sqrt{T} \sinh(4t) / \sqrt{D_f}.$$

Since  $t = O_f(1)$ , we then deduce that indeed there are  $O_f(d(T))$  choices for  $(L_1, L_2)$ . Using the bound  $d(T) = O_\epsilon(T^\epsilon) = O_{f,\epsilon}(X^\epsilon)$ , we conclude that there are

$$O_{f,\epsilon}(X^{1/2+\epsilon}) \cdot O_{f,\epsilon}(X^\epsilon) = O_{f,\epsilon}(X^{1/2+\epsilon})$$

choices for  $(L, L_1, L_2)$  in total, whence the claim.  $\square$

*Proof of Proposition 6.1: third claim.* Suppose that  $L = 0$  and that  $F$  is in the shape as in (3-1). Using Proposition 3.2, we then deduce that

$$C = (-12\gamma A + 3\beta B)/(2\alpha), \quad \text{and so} \quad K = -9\mathcal{D}_f(\alpha B^2 - 4\beta AB + 16\gamma A^2)/(4\alpha^3).$$

Clearly  $-4K2/\Delta(f) = \square$  if and only if  $-\Delta(f) = \square$ .

We now suppose that  $-\Delta(f) = \square$ , so in particular  $f$  is positive definite. The form  $F$  is then determined by  $(A, B) \in \mathbb{Z}^2$ , and that  $|K| \leq X$  implies

$$\left| \left( B - \frac{2\beta}{\alpha} A \right)^2 - \frac{4\mathcal{D}_f}{\alpha^2} A^2 \right| \ll_f X.$$

Hence there are  $O_f(X)$  choices for  $(A, B)$ . It follows that the claim holds.  $\square$

**6B. Proof of Proposition 6.2.** By Lemma 3.8 and Proposition 6.1, we have

$$(6-4) \quad \#\{F \in \mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0 : F \text{ is reducible of type 1}\} = O_{f,\epsilon}(X^{1+\epsilon}),$$

whence it is enough to consider the reducible forms in  $\mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0$  of type 2; recall Definition 3.7. By definition, such a form has the shape

$$F(x, y) = p_2 q_2 x^4 + (p_2 q_1 + p_1 q_2) x^3 y + (p_2 q_0 + p_1 q_1 + p_0 q_2) x^2 y^2 + (*) x y^3 + (*) y^4,$$

where  $p_2, p_1, p_0, q_2, q_1, q_0 \in \mathbb{Z}$ , and we have

$$p_0 = (\beta p_1 - 2\gamma p_2)/(2\alpha) \quad \text{and} \quad q_0 = (\beta q_1 - 2\gamma q_2)/(2\alpha)$$

by Lemma 3.10. We have the condition

$$(6-5) \quad |(\alpha p_1^2 - 2\beta p_1 p_2 + 4\gamma p_2^2)/\alpha|, |(\alpha q_1^2 - 2\beta q_1 q_2 + 4\gamma q_2^2)/\alpha|, |p_2|, \\ |\alpha p_1 - \beta p_2|, |q_2|, |\alpha q_1 - \beta q_2| \geq 1$$

since the above numbers are all integers. Using Proposition 3.2(a), we compute that

$$\frac{L_f(F)^2 + 4K_f(F)}{9} = \frac{\alpha p_1^2 - 2\beta p_1 p_2 + 4\gamma p_2^2}{\alpha} \cdot \frac{\alpha q_1^2 - 2\beta q_1 q_2 + 4\gamma q_2^2}{\alpha}.$$

Now, by the definition of our height, we clearly have

$$(6-6) \quad |(\alpha p_1^2 - 2\beta p_1 p_2 + 4\gamma p_2^2)/\alpha|, |(\alpha q_1^2 - 2\beta q_1 q_2 + 4\gamma q_2^2)/\alpha| \leq X.$$

Observe also that

$$(6-7) \quad p_2q_2, p_2q_1 + p_1q_2, p_1q_1 = O_f(X^{1/2}) \quad \text{if } f \text{ is indefinite and irreducible}$$

by (4-7), (4-8), (4-2), and the bound  $0 \leq t < t_{D_f}$ . We then deduce that

$$(6-8) \quad \#\{F \in \mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^0 : F \text{ is reducible of type 2}\} \leq \#(\mathcal{R}'_f(X) \cap \mathbb{Z}^4),$$

where we define

$$\mathcal{R}'_f(X) = \{(p_2, p_1, q_2, q_1) \in \mathbb{R}^4 : (6-5), (6-6), \text{ and } (6-7)\}.$$

It is clear that this set is bounded and semialgebraic. Hence, we may apply [Proposition 5.1](#) to estimate the number of integral points it contains.

**6B1.** *The case when  $f$  is irreducible.* Let us define

$$\mathcal{R}''_f(X) = \mathcal{L}_{D_f}(\mathcal{R}'_f(X)), \quad \text{where } \mathcal{L}_{D_f} = \begin{pmatrix} \sqrt{D_f} & 0 & 0 & 0 \\ -\beta & \alpha & 0 & 0 \\ 0 & 0 & \sqrt{D_f} & 0 \\ 0 & 0 & -\beta & \alpha \end{pmatrix}.$$

Applying [Proposition 5.1](#), we then obtain

$$\begin{aligned} \#(\mathcal{R}'_f(X) \cap \mathbb{Z}^4) &= \text{Vol}(\mathcal{R}'_f(X)) + O(\max\{\text{Vol}(\overline{\mathcal{R}'_f(X)}), 1\}) \\ &= \frac{1}{\det(\mathcal{L}_{D_f})} \text{Vol}(\mathcal{R}''_f(X)) + O_f(\max\{\text{Vol}(\overline{\mathcal{R}''_f(X)}), 1\}) \end{aligned}$$

For any  $(u_2, u_1, v_2, v_1) \in \mathcal{R}''_f(X)$ , from (6-5) and (6-6), we deduce that

$$|u_2|, |u_1|, |v_2|, |v_1| \geq 1$$

as well as that

$$(6-9) \quad \begin{cases} 1 \leq |u_1^2 + u_2^2|, |v_1^2 + v_2^2| \leq \alpha^4 X & \text{if } f \text{ is positive definite,} \\ 1 \leq |u_1^2 - u_2^2|, |v_1^2 - v_2^2| \leq \alpha^4 X & \text{if } f \text{ is indefinite.} \end{cases}$$

This, together with (6-7), implies that in fact

$$1 \leq |u_2|, |u_1|, |v_2|, |v_1|, |u_2v_2|, |u_1v_1| \ll_f X^{1/2}.$$

We then compute that

$$\text{Vol}(\mathcal{R}''_f(X)) = O_f\left(\prod_{i=1}^2 \int_1^{X^{1/2}/v_i} du_i dv_i\right) = O_f(X(\log X)^2),$$

$$\text{Vol}(\overline{\mathcal{R}''_f(X)}) = O_f(X \log X).$$

The claim now follows from (6-4) and (6-8).

**6B2.** *The case when  $f$  is reducible.* Let us define

$$\mathbb{R}''_f(X) = \mathcal{L}_{0,D_f}(\mathbb{R}'_f(X)), \quad \text{where } \mathcal{L}_{0,D_f} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{D_f} & 0 & 0 & 0 \\ -\beta & \alpha & 0 & 0 \\ 0 & 0 & \sqrt{D_f} & 0 \\ 0 & 0 & -\beta & \alpha \end{pmatrix}.$$

Since  $D_f = \square$  in this case, we see that

$$\mathcal{L}_{0,D_f}(\mathcal{R}'_f(X) \cap \mathbb{Z}^4) \subset \mathcal{R}''_f(X) \cap \mathbb{Z}^4 \quad \text{and so} \quad \#(\mathcal{R}'_f(X) \cap \mathbb{Z}^4) \leq \#(\mathcal{R}''_f(X) \cap \mathbb{Z}^4).$$

Now, applying [Proposition 5.1](#), we have

$$\#(\mathcal{R}''_f(X) \cap \mathbb{Z}^4) = \text{Vol}(\mathcal{R}''_f(X)) + O(\max\{\text{Vol}(\overline{\mathcal{R}''_f(X)}), 1\}).$$

For any  $(z_1, z_2, z_3, z_4) \in \mathcal{R}''_f(X)$ , the conditions [\(6-5\)](#) and [\(6-6\)](#) imply that

$$|z_1|, |z_2|, |z_3|, |z_4| \geq 1 \quad \text{and} \quad |z_1 z_2 z_3 z_4| \leq \alpha^4 X,$$

which is analogous to [\(6-9\)](#). We then compute that

$$\begin{aligned} \text{Vol}(\mathcal{R}''_f(X)) &= O_f \left( \int_1^X \int_1^{X/z_4} \int_1^{X/(z_3 z_4)} \int_1^{X/(z_2 z_3 z_4)} dz_1 dz_2 dz_3 dz_4 \right) \\ &= O_f(X(\log X)^3), \\ \text{Vol}(\overline{\mathcal{R}''_f(X)}) &= O_f(X(\log X)^2). \end{aligned}$$

The claim now follows from [\(6-4\)](#) and [\(6-8\)](#).

**6C. Proof of [Theorem 1.2](#).** We have already proven part (d). To prove parts (a) through (c), it remains to compute the volumes in [\(6-2\)](#).

**6C1.** *The case when  $f$  is positive definite.* We have

$$\text{Vol}(\Theta_1(\mathcal{S}_f(X))) = \frac{8\alpha^3}{D_f^{3/2}} \cdot \frac{1}{18} \cdot \text{Vol}(\Omega^+(X) \times [-\pi/4, \pi/4])$$

by [Lemma 4.1](#) and [Proposition 4.2\(b\)](#), as well as

$$\text{Vol}(\Omega^+(X) \times [-\pi/4, \pi/4]) = \int_{-X^{1/2}}^{X^{1/2}} \int_{-L^{2/4}}^X \frac{\pi}{2} dK dL = \frac{13\pi}{12} X^{3/2}.$$

Observe also that

$$\text{Vol}(\overline{\Theta_1(\mathcal{S}_f(X))}) = O_f(X)$$

because  $\Theta_1(\mathcal{S}_f(X))$  lies in the cube centered at the origin of side length  $O_f(X^{1/2})$  by [\(4-5\)](#) and [\(4-2\)](#). We then deduce part (a) from [\(6-1\)](#) and [\(6-2\)](#).



**6C2.** *The case when  $f$  is reducible.* We have

$$\text{Vol}(\Theta_2(\mathcal{S}_f(X))) = \frac{1}{18} \cdot 2 \cdot \text{Vol}(\Omega^0(X) \times [t_{f,1}, t_{f,2}])$$

by [Proposition 4.4](#), as well as

$$\text{Vol}(\Omega^0(X) \times [t_{f,1}, t_{f,2}]) = \int_{-X^{1/2}}^{X^{1/2}} \int_{-X}^X \frac{1}{4} \log\left(\frac{20X}{9}\right) dK dL = X^{3/2} \log(20X/9).$$

We then deduce part (b) from [Lemma 6.4](#) below as well as [\(6-1\)](#) and [\(6-2\)](#).

**Lemma 6.4.** *We have  $\text{Vol}(\overline{\Theta_2(\mathcal{S}_f(X))}) = O_f(X^{3/2})$ .*

*Proof.* By [Definition 5.2](#), an element in  $\Theta_2(\mathcal{S}_f(X))$  takes the form

$$(A, B, C) = (\Theta_2 \circ \Phi_f)(L, K, t), \quad \text{where } (L, K, t) \in \Omega^0(X) \times [t_{f,1}, t_{f,2}].$$

Let us recall that

$$(6-10) \quad |L| \leq X^{1/2}, \quad |K| \leq X, \quad 4t_{f,1} = -\log 8, \quad 4t_{f,2} = \log(5X/18).$$

Then, from [\(4-11\)](#), we see that 1-dimensional projections of  $\Theta_2(\mathcal{S}_f(X))$  have lengths of order  $O_f(X)$ . As for the 2-dimensional projections, note that [\(5-1\)](#) and [\(6-10\)](#) yield

$$|C| = \beta^2 e^{4t} \quad \text{and} \quad 1 \ll_f |C| \ll_f X,$$

as well as the estimates

$$\left| B - \frac{6\alpha^2 C}{\beta^2} \right| \leq \frac{1}{2} X^{1/2} \quad \text{and} \quad \left| A - \frac{\alpha^4 C}{\beta^4} \right| \leq \frac{5}{144|C|} X + \frac{\alpha^2}{2\beta^2} X^{1/2}.$$

Hence, the projections of  $\Theta_2(\mathcal{S}_f(X))$  onto the  $BC$ -plane and  $AC$ -plane, respectively, have areas bounded by

$$O_f\left(\int_1^X X^{1/2} dC\right) \quad \text{and} \quad O_f\left(\int_1^X \left(\frac{1}{C} X + X^{1/2}\right) dC\right).$$

Similarly, from [\(5-1\)](#) and [\(6-10\)](#), we deduce that

$$|2B - L| = 12\alpha^2 e^{4t}, \quad 1 \ll_f |2B - L| \ll_f X, \quad |B| \ll_f X,$$

as well as the estimate

$$\left| A - \frac{\alpha^2 B}{6\beta^2} \right| \leq \frac{5\alpha^2}{12\beta^2} \left( \frac{1}{|2B - L|} X + X^{1/2} \right).$$

Note that  $|L| \leq X^{1/2}$  also implies that

$$|2B - L| \geq |2|B| - |L|| \geq 2|B| - X^{1/2} \quad \text{when } |B| \geq X^{1/2}/2.$$

Hence, the projection of  $\Theta_2(\mathcal{S}_f(X))$  onto the  $AB$ -plane has area bounded by

$$O_f \left( \int_0^{1+X^{1/2}/2} (X + X^{1/2}) dB + \int_{1+X^{1/2}/2}^X \left( \frac{1}{2B - X^{1/2}} X + X^{1/2} \right) dB \right).$$

It follows that all of the 2-dimensional projections of  $\Theta_2(\mathcal{S}_f(X))$  have areas of order  $O_f(X^{3/2})$ , and this proves the lemma.  $\square$

**6C3.** *The case when  $f$  is indefinite and irreducible.* We have

$$\text{Vol}(\Theta_1(\mathcal{S}_f(X))) = \frac{8\alpha^3}{D_f^{3/2}} \cdot \frac{1}{18} \cdot 2 \cdot (\text{Vol}(\Omega^+(X) \times [0, t_{D_f})) + \text{Vol}(\Omega^-(X) \times [0, t_{D_f})))$$

by [Lemma 4.1](#) and [Proposition 4.3](#), as well as

$$\begin{aligned} \text{Vol}(\Omega^+(X) \times [0, t_{D_f})) &= \int_{-X^{1/2}}^{X^{1/2}} \int_{-L^2/4}^X t_{D_f} dK dL = \frac{13t_{D_f}}{6} X^{3/2}, \\ \text{Vol}(\Omega^-(X) \times [0, t_{D_f})) &= \int_{-X^{1/2}}^{X^{1/2}} \int_{-X}^{-L^2/4} t_{D_f} dK dL = \frac{11t_{D_f}}{6} X^{3/2}, \end{aligned}$$

Observe also that

$$\text{Vol}(\overline{\Theta_1(\mathcal{S}_f(X))}) = O_f(X)$$

because  $\Theta_1(\mathcal{S}_f(X))$  lies in the cube centered at the origin of side length  $O_f(X^{1/2})$  by (4-7), (4-8), (4-2), and the bound on  $t$ . We then deduce part (c) from (6-1) and (6-2).

## Acknowledgments

Tsang was partially supported by the China Postdoctoral Science Foundation Special Financial Grant (grant number: 2017T100060). We would like to thank the referee for many useful suggestions which helped improve the exposition of the paper significantly.

## References

- [Altuğ et al. 2017] S. A. Altuğ, A. Shankar, I. Varma, and K. H. Wilson, “The number of quartic  $D_4$ -fields ordered by conductor”, preprint, 2017. [arXiv](#)
- [Bhargava 2004] M. Bhargava, “[Higher composition laws, III: The parametrization of quartic rings](#)”, *Ann. of Math.* (2) **159**:3 (2004), 1329–1360. [MR](#) [Zbl](#)
- [Bhargava 2008] M. Bhargava, “[Higher composition laws, IV: The parametrization of quintic rings](#)”, *Ann. of Math.* (2) **167**:1 (2008), 53–94. [MR](#) [Zbl](#)

- [Bhargava and Shankar 2015] M. Bhargava and A. Shankar, “Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves”, *Ann. of Math.* (2) **181**:1 (2015), 191–242. [MR](#) [Zbl](#)
- [Bhargava and Shnidman 2014] M. Bhargava and A. Shnidman, “On the number of cubic orders of bounded discriminant having automorphism group  $C_3$ , and related problems”, *Algebra Number Theory* **8**:1 (2014), 53–88. [MR](#) [Zbl](#)
- [Bhargava et al. 2013] M. Bhargava, A. Shankar, and J. Tsimerman, “On the Davenport–Heilbronn theorems and second order terms”, *Invent. Math.* **193**:2 (2013), 439–499. [MR](#) [Zbl](#)
- [Birch and Merriman 1972] B. J. Birch and J. R. Merriman, “Finiteness theorems for binary forms with given discriminant”, *Proc. London Math. Soc.* (3) **24**:3 (1972), 385–394. [MR](#) [Zbl](#)
- [Brumer 1992] A. Brumer, “The average rank of elliptic curves, I”, *Invent. Math.* **109**:1 (1992), 445–472. [MR](#) [Zbl](#)
- [Conrad 2012] K. Conrad, “Galois groups of cubics and quartics (not in characteristic 2)”, expository notes, 2012, <http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf>.
- [Cremona 1999] J. E. Cremona, “Reduction of binary cubic and quartic forms”, *LMS J. Comput. Math.* **2** (1999), 64–94. [MR](#) [Zbl](#)
- [Davenport 1951a] H. Davenport, “On a principle of Lipschitz”, *J. London Math. Soc.* **26**:3 (1951), 179–183. [MR](#) [Zbl](#)
- [Davenport 1951b] H. Davenport, “On the class-number of binary cubic forms, I”, *J. London Math. Soc.* **26**:3 (1951), 183–192. [MR](#) [Zbl](#)
- [Davenport 1951c] H. Davenport, “On the class-number of binary cubic forms, II”, *J. London Math. Soc.* **26**:3 (1951), 192–198. [MR](#) [Zbl](#)
- [Davenport and Heilbronn 1971] H. Davenport and H. Heilbronn, “On the density of discriminants of cubic fields, II”, *Proc. Roy. Soc. London Ser. A* **322**:1551 (1971), 405–420. [MR](#) [Zbl](#)
- [Delone and Faddeev 1964] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Trans. Math. Monographs **10**, Amer. Math. Soc., Providence, RI, 1964. [MR](#) [Zbl](#)
- [Gauss 1801] C. F. Gauss, *Disquisitiones arithmeticae*, Fleischer, Leipzig, 1801.
- [Heath-Brown 2002] D. R. Heath-Brown, “The density of rational points on curves and surfaces”, *Ann. of Math.* (2) **155**:2 (2002), 553–598. [MR](#) [Zbl](#)
- [Heath-Brown 2004] D. R. Heath-Brown, “The average analytic rank of elliptic curves”, *Duke Math. J.* **122**:3 (2004), 591–623. [MR](#) [Zbl](#)
- [Klagsbrun and Lemke Oliver 2014] Z. Klagsbrun and R. J. Lemke Oliver, “The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point”, *Res. Math. Sci.* **1**:1 (2014), art. id. 15. [MR](#) [Zbl](#)
- [Nakagawa 1989] J. Nakagawa, “Binary forms and orders of algebraic number fields”, *Invent. Math.* **97**:2 (1989), 219–235. Correction in **105**:2 (1991), 443. [MR](#) [Zbl](#)
- [Newman 1972] M. Newman, *Integral matrices*, Pure Appl. Math. **45**, Academic Press, New York, 1972. [MR](#) [Zbl](#)
- [Siegel 1944] C. L. Siegel, “The average measure of quadratic forms with given determinant and signature”, *Ann. of Math.* (2) **45**:4 (1944), 667–685. [MR](#) [Zbl](#)
- [Taniguchi and Thorne 2013] T. Taniguchi and F. Thorne, “Secondary terms in counting functions for cubic fields”, *Duke Math. J.* **162**:13 (2013), 2451–2508. [MR](#) [Zbl](#)
- [Tsang and Xiao 2017] C. Tsang and S. Y. Xiao, “The number of quartic  $D_4$ -fields with monogenic cubic resolvent ordered by conductor”, preprint, 2017. [arXiv](#)

- [Wood 2012] M. M. Wood, “Quartic rings associated to binary quartic forms”, *Int. Math. Res. Not.* **2012**:6 (2012), 1300–1320. [MR](#) [Zbl](#)
- [Xiao 2019] S. Y. Xiao, “On binary cubic and quartic forms”, *J. Théor. Nombres Bordeaux* **31**:2 (2019), 323–341.
- [Young 2006] M. P. Young, “Low-lying zeros of families of elliptic curves”, *J. Amer. Math. Soc.* **19**:1 (2006), 205–250. [MR](#) [Zbl](#)

Received February 27, 2018. Revised October 21, 2018.

CINDY (SIN YI) TSANG  
YAU MATHEMATICAL SCIENCES CENTER  
TSINGHUA UNIVERSITY  
BEIJING  
CHINA

*Current address:*

SCHOOL OF MATHEMATICS (ZHUHAI)  
SUN YAT-SEN UNIVERSITY  
TANGJIAWAN, ZHUHAI  
GUANGDONG  
CHINA

[zengshy26@mail.sysu.edu.cn](mailto:zengshy26@mail.sysu.edu.cn)

STANLEY YAO XIAO  
MATHEMATICAL INSTITUTE  
UNIVERSITY OF OXFORD  
UNITED KINGDOM

*Current address:*

DEPARTMENT OF MATHEMATICS  
UNIVERSITY OF TORONTO  
CANADA

[syxiao@math.toronto.edu](mailto:syxiao@math.toronto.edu)

# PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

[msp.org/pjm](http://msp.org/pjm)

## EDITORS

Don Blasius (Managing Editor)  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[blasius@math.ucla.edu](mailto:blasius@math.ucla.edu)

Matthias Aschenbrenner  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[matthias@math.ucla.edu](mailto:matthias@math.ucla.edu)

Daryl Cooper  
Department of Mathematics  
University of California  
Santa Barbara, CA 93106-3080  
[cooper@math.ucsb.edu](mailto:cooper@math.ucsb.edu)

Jiang-Hua Lu  
Department of Mathematics  
The University of Hong Kong  
Pokfulam Rd., Hong Kong  
[jhlu@maths.hku.hk](mailto:jhlu@maths.hku.hk)

Paul Balmer  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[balmer@math.ucla.edu](mailto:balmer@math.ucla.edu)

Wee Teck Gan  
Mathematics Department  
National University of Singapore  
Singapore 119076  
[matgwt@nus.edu.sg](mailto:matgwt@nus.edu.sg)

Sorin Popa  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[popa@math.ucla.edu](mailto:popa@math.ucla.edu)

Paul Yang  
Department of Mathematics  
Princeton University  
Princeton NJ 08544-1000  
[yang@math.princeton.edu](mailto:yang@math.princeton.edu)

Vyjayanthi Chari  
Department of Mathematics  
University of California  
Riverside, CA 92521-0135  
[chari@math.ucr.edu](mailto:chari@math.ucr.edu)

Kefeng Liu  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[liu@math.ucla.edu](mailto:liu@math.ucla.edu)

Jie Qing  
Department of Mathematics  
University of California  
Santa Cruz, CA 95064  
[qing@cats.ucsc.edu](mailto:qing@cats.ucsc.edu)

## PRODUCTION

Silvio Levy, Scientific Editor, [production@msp.org](mailto:production@msp.org)

## SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI  
CALIFORNIA INST. OF TECHNOLOGY  
INST. DE MATEMÁTICA PURA E APLICADA  
KEIO UNIVERSITY  
MATH. SCIENCES RESEARCH INSTITUTE  
NEW MEXICO STATE UNIV.  
OREGON STATE UNIV.

STANFORD UNIVERSITY  
UNIV. OF BRITISH COLUMBIA  
UNIV. OF CALIFORNIA, BERKELEY  
UNIV. OF CALIFORNIA, DAVIS  
UNIV. OF CALIFORNIA, LOS ANGELES  
UNIV. OF CALIFORNIA, RIVERSIDE  
UNIV. OF CALIFORNIA, SAN DIEGO  
UNIV. OF CALIF., SANTA BARBARA

UNIV. OF CALIF., SANTA CRUZ  
UNIV. OF MONTANA  
UNIV. OF OREGON  
UNIV. OF SOUTHERN CALIFORNIA  
UNIV. OF UTAH  
UNIV. OF WASHINGTON  
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.

---

See inside back cover or [msp.org/pjm](http://msp.org/pjm) for submission instructions.

---

The subscription price for 2019 is US \$490/year for the electronic version, and \$665/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by [Mathematical Reviews](#), [Zentralblatt MATH](#), [PASCAL CNRS Index](#), [Referativnyi Zhurnal](#), [Current Mathematical Publications](#) and [Web of Knowledge \(Science Citation Index\)](#).


---

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

---

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2019 Mathematical Sciences Publishers

# PACIFIC JOURNAL OF MATHEMATICS

Volume 302      No. 1      September 2019

---

On masas in $q$ -deformed von Neumann algebras	1
MARTIJN CASPERS, ADAM SKALSKI and MATEUSZ WASILEWSKI	
The compact picture of symmetry-breaking operators for rank-one orthogonal and unitary groups	23
JAN FRAHM and BENT ØRSTED	
On the Landsberg curvature of a class of Finsler metrics generated from the navigation problem	77
LIBING HUANG, HUAIFU LIU and XIAOHUAN MO	
Symplectic and odd orthogonal Pfaffian formulas for algebraic cobordism	97
THOMAS HUDSON and TOMOO MATSUMURA	
A compactness theorem on Branson's $Q$ -curvature equation	119
GANG LI	
A characterization of Fuchsian actions by topological rigidity	181
KATHRYN MANN and MAXIME WOLFF	
Fundamental domains and presentations for the Deligne–Mostow lattices with 2-fold symmetry	201
IRENE PASQUINELLI	
Binary quartic forms with bounded invariants and small Galois groups	249
CINDY (SIN YI) TSANG and STANLEY YAO XIAO	
Obstructions to lifting abelian subalgebras of corona algebras	293
ANDREA VACCARO	
Schwarz lemma at the boundary on the classical domain of type $\mathcal{IV}$	309
JIANFEI WANG, TAISHUN LIU and XIAOMIN TANG	
Cyclic $\eta$ -parallel shape and Ricci operators on real hypersurfaces in two-dimensional nonflat complex space forms	335
YANING WANG	
Finsler spheres with constant flag curvature and finite orbits of prime closed geodesics	353
MING XU	
Degeneracy theorems for two holomorphic curves in $\mathbb{P}^n(\mathbb{C})$ sharing few hypersurfaces	371
KAI ZHOU and LU JIN	