ON THE REPRESENTATION OF INTEGERS BY BINARY FORMS

C. L. STEWART AND STANLEY YAO XIAO

Abstract. Let F be a binary form with integer coefficients, non-zero discriminant and degree d with d at least 3. Let $R_F(Z)$ denote the number of integers of absolute value at most Z which are represented by F. We prove that there is a positive number C_F such that $R_F(Z)$ is asymptotic to $C_F Z^{\frac{2}{d}}$.

1. Introduction

Let F be a binary form with integer coefficients, non-zero discriminant $\Delta(F)$ and degree d with $d \geq 2$. For any positive number Z let $\mathcal{R}_F(Z)$ denote the set of non-zero integers h with $|h| \leq Z$ for which there exist integers x and y with $F(x,y) = h$. Denote the cardinality of a set $\mathcal{S}$ by $|\mathcal{S}|$ and put $R_F(Z) = |\mathcal{R}_F(Z)|$. There is an extensive literature, going back to the foundational work of Fermat, Lagrange, Legendre and Gauss [12], concerning the set $\mathcal{R}_F(Z)$ and the growth of $R_F(Z)$ when F is a binary quadratic form. For instance in 1908 Landau [26] proved that if $F_0(x,y) = x^2 + y^2$ then

$$R_{F_0}(Z) \sim C_0 Z/(\log Z)^{1/2} \tag{1.1}$$

with C_0, the Landau-Ramanujan constant [14], given by

$$C_0 = \left(\frac{1}{2} \prod_{p \equiv 3 \pmod 4} \frac{1}{1 - p^{-2}} \right)^{1/2} \tag{1.2}$$

where the product is over primes congruent to 3 modulo 4. See [6], [7] and [8] for more recent treatments of these topics. For forms of higher degree much less is known. In 1938 Erdős and Mahler [11] proved that if F is irreducible over $\mathbb{Q}$ and d is at least 3 then there exist positive numbers c_1 and c_2, which depend on F, such that

$$R_F(Z) > c_1 Z^{\frac{2}{d}}$$

for $Z > c_2$.

Put

$$A_F = \mu(\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leq 1\}) \tag{1.3}$$

where μ denotes the area of a set in $\mathbb{R}^2$. In 1967 Hooley [18] determined the asymptotic growth rate of $R_F(Z)$ when F is an irreducible binary cubic form with discriminant which is not a square. He proved that

Date: May 30, 2019.

2010 *Mathematics Subject Classification.* Primary 11D45, Secondary 11D59, 11E76.

Key words and phrases. binary forms, determinant method.

The research of the first author was supported in part by the Canada Research Chairs Program and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

$$R_F(Z) = A_F Z^{\frac{2}{3}} + O\left(Z^{\frac{2}{3}}(\log\log Z)^{-\frac{1}{600}}\right). \tag{1.4}$$

In 2000 Hooley [23] treated the case when the discriminant is a perfect square. Suppose that

$$F(x,y) = b_3x^3 + b_2x^2y + b_1xy^2 + b_0y^3.$$

The Hessian covariant of F is

$$q_F(x) = Ax^2 + Bx + C,$$

where

$$A = b_2^2 - 3b_3b_1,\ B = b_2b_1 - 9b_3b_0 \text{ and } C = b_1^2 - 3b_2b_0.$$

Put

$$m = \frac{\sqrt{\Delta(F)}}{\gcd(A,B,C)}. \tag{1.5}$$

Hooley proved that if F is an irreducible cubic with b_1 and b_2 divisible by 3 and $\Delta(F)$ a square then there is a positive number γ such that

$$R_F(Z) = \left(1 - \frac{2}{3m}\right) A_F Z^{\frac{2}{3}} + O\left(Z^{\frac{2}{3}}(\log Z)^{-\gamma}\right). \tag{1.6}$$

We remark that if F is a binary cubic form then

$$|\Delta(F)|^{\frac{1}{6}} A_F = \begin{cases} \dfrac{3\Gamma^2(1/3)}{\Gamma(2/3)} & \text{if } \Delta(F) > 0, \\ \\ \dfrac{\sqrt{3}\Gamma^2(1/3)}{\Gamma(2/3)} & \text{if } \Delta(F) < 0, \end{cases}$$

where $\Gamma(s)$ denotes the gamma function. In [1] Bean gives a simple representation for A_F when F is a binary quartic form.

Hooley [22] also studied irreducible quartic forms of the shape

$$F(x,y) = ax^4 + 2bx^2y^2 + cy^4.$$

Let $\varepsilon > 0$. He proved that if a/c is not the fourth power of a rational number then

$$R_F(Z) = \frac{A_F}{4} Z^{\frac{1}{2}} + O_{F,\varepsilon}\left(Z^{\frac{18}{37}+\varepsilon}\right). \tag{1.7}$$

Further if $a/c = A^4/C^4$ with A and C coprime positive integers then

$$R_F(Z) = \frac{A_F}{4}\left(1 - \frac{1}{2AC}\right) Z^{\frac{1}{2}} + O_{F,\varepsilon}\left(Z^{\frac{18}{37}+\varepsilon}\right). \tag{1.8}$$

In addition to these results, when d is at least 3 and F is the product of d linear forms with integer coefficients Hooley [24], [25] proved that there is a positive number C_F such that for each positive number ε

$$R_F(Z) = C_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\eta_d+\varepsilon}\right), \tag{1.9}$$

where η_3 is $\frac{5}{9}$ and η_d is $\frac{2}{d} - \frac{d-2}{d^2(d-1)}$ if d exceeds 3.

Browning [5], Greaves [13], Heath-Brown [16], Hooley [19], [20], [21], Skinner and Wooley [33] and Wooley [36] have obtained asymptotic estimates for $R_F(Z)$ when F is of the form $x^d + y^d$ with $d \geq 3$. Furthermore, Bennett, Dummigan and Wooley [2] have obtained an asymptotic estimate for $R_F(Z)$ when $F(x, y) = ax^d + by^d$ with $d \geq 3$ and a and b non-zero integers.

For each binary form F with integer coefficients, non-zero discriminant and degree d with $d \geq 3$ we define β_F in the following way. If F has a linear factor in $\mathbb{R}[x, y]$ we put

$$\beta_F = \begin{cases} \dfrac{12}{19} & \text{if } d = 3 \text{ and } F \text{ is irreducible over } \mathbb{Q} \\[2ex] \dfrac{4}{7} & \text{if } d = 3 \text{ and } F \text{ has exactly one linear factor over } \mathbb{Q} \\[2ex] \dfrac{5}{9} & \text{if } d = 3 \text{ and } F \text{ has three linear factors over } \mathbb{Q} \\[2ex] \dfrac{3}{(d-2)\sqrt{d}+3} & \text{if } 4 \leq d \leq 8 \\[2ex] \dfrac{1}{d-1} & \text{if } d \geq 9. \end{cases} \tag{1.10}$$

If F does not have a linear factor over $\mathbb{R}$ then d is even and we put

$$\beta_F = \begin{cases} \dfrac{3}{d\sqrt{d}} & \text{if } d = 4, 6, 8 \\[2ex] \dfrac{1}{d} & \text{if } d \geq 10. \end{cases} \tag{1.11}$$

We shall employ a similar strategy to the one used by Hooley [25] to prove (1.9) in order to establish the following result.

Theorem 1.1. *Let F be a binary form with integer coefficients, non-zero discriminant and degree d with $d \geq 3$. Let $\varepsilon > 0$. There exists a positive number C_F such that*

$$R_F(Z) = C_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F + \varepsilon}\right), \tag{1.12}$$

where β_F is given by (1.10) and (1.11).

The proof of Theorem 1.1 depends on some results of Salberger in [30] and [31], which are based on a refinement of Heath-Brown's p-adic determinant method in [17], an argument of Heath-Brown [17] and a classical result of Mahler [27]. When d is 3 and F is reducible we appeal to a result of Heath-Brown on integer points on non-singular cubic forms [16] and to work of Hooley [24] and Xiao [38], [39]. In addition, and crucial for our proof, we shall elucidate the structure of the lattices associated with the automorphism group of F and its subgroups. Theorem 1.1, together with

Theorem 1.2, contains all previous estimates for $R_F(Z)$.

Let A be an element of $\mathrm{GL}_2(\mathbb{Q})$ with

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Put $F_A(x,y) = F(a_1x + a_2y, a_3x + a_4y)$. We say that A fixes F if $F_A = F$. The set of A in $\mathrm{GL}_2(\mathbb{Q})$ which fix F is the automorphism group of F and we shall denote it by $\mathrm{Aut}\, F$. Let G_1 and G_2 be subgroups of $\mathrm{GL}_2(\mathbb{Q})$. We say that they are equivalent under conjugation if there is an element T in $\mathrm{GL}_2(\mathbb{Q})$ such that $G_1 = TG_2T^{-1}$.

The positive number C_F in (1.12) is a rational multiple of A_F and the rational multiple depends on $\mathrm{Aut}\, F$. There are 10 equivalence classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Q})$ under $\mathrm{GL}_2(\mathbb{Q})$-conjugation to which $\mathrm{Aut}\, F$ might belong and we give a representative of each equivalence class together with its generators in Table 1.

Table 1

Group	Generators	Group	Generators
$\mathbf{C}_1$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\mathbf{D}_1$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\mathbf{C}_2$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\mathbf{D}_2$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\mathbf{C}_3$	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$	$\mathbf{D}_3$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$
$\mathbf{C}_4$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\mathbf{D}_4$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
$\mathbf{C}_6$	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	$\mathbf{D}_6$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$

Since the matrix $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is in $\mathrm{Aut}\, F$ if and only if the degree of F is even, we see from an examination of Table 1 that if the degree of F is odd then $\mathrm{Aut}\, F$ is equivalent to one of $\mathbf{C}_1, \mathbf{C}_3, \mathbf{D}_1$ and $\mathbf{D}_3$ and if the degree of F is even then $\mathrm{Aut}\, F$ is equivalent to one of $\mathbf{C}_2, \mathbf{C}_4, \mathbf{C}_6, \mathbf{D}_2, \mathbf{D}_4$ and $\mathbf{D}_6$.

Note that the table has fewer entries than Table 1 of [34] which gives representatives for the equivalence classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ under $\mathrm{GL}_2(\mathbb{Z})$-conjugation. This is because for $i = 1, 2, 3$ the groups $\mathbf{D}_i$ and $\mathbf{D}_i^*$ are equivalent under conjugation in $\mathrm{GL}_2(\mathbb{Q})$ but are not equivalent under conjugation in $\mathrm{GL}_2(\mathbb{Z})$. Further every finite subgroup of $\mathrm{GL}_2(\mathbb{Q})$ is conjugate to a finite subgroup of $\mathrm{GL}_2(\mathbb{Z})$, see [28].

Let Λ be the sublattice of $\mathbb{Z}^2$ consisting of (u,v) in $\mathbb{Z}^2$ for which $A\begin{pmatrix}u\\v\end{pmatrix}$ is in $\mathbb{Z}^2$ for all A in $\operatorname{Aut} F$, and put

$$m = d(\Lambda), \tag{1.13}$$

where $d(\Lambda)$ denotes the determinant of Λ. Note that $m = 1$ when $\operatorname{Aut} F$ is equal to either $\mathbf{C}_1$ or $\mathbf{C}_2$. Observe that the conjugacy classes of $\mathbf{C}_1$ and $\mathbf{C}_2$ in $\mathrm{GL}_2(\mathbb{Q})$ consist only of themselves.

When $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_3$ it has three subgroups G_1, G_2 and G_3 of order 2 with generators A_1, A_2 and A_3 respectively, and one, G_4 say, of order 3 with generator A_4. Let $\Lambda_i = \Lambda(A_i)$ be the sublattice of $\mathbb{Z}^2$ consisting of (u,v) in $\mathbb{Z}^2$ for which $A_i\begin{pmatrix}u\\v\end{pmatrix}$ is in $\mathbb{Z}^2$ and put

$$m_i = d(\Lambda_i) \tag{1.14}$$

for $i = 1,2,3,4$. We remark that m_4 is well defined since, by (3.7), Λ_4 does not depend on the choice of generator A_4.

When $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_4$ there are three subgroups G_1, G_2 and G_3 of order 2 of $\operatorname{Aut} F/\{\pm I\}$. Let Λ_i be the sublattice of $\mathbb{Z}^2$ consisting of (u,v) in $\mathbb{Z}^2$ for which $A\begin{pmatrix}u\\v\end{pmatrix}$ is in $\mathbb{Z}^2$ for A in a generator of G_i and put

$$m_i = d(\Lambda_i) \tag{1.15}$$

for $i = 1,2,3$.

Finally when $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_6$ there are three subgroups G_1, G_2 and G_3 of order 2 and one, G_4 say, of order 3 in $\operatorname{Aut} F/\{\pm I\}$. Let A_i be in a generator of G_i for $i = 1,2,3,4$. Let $\Lambda_i = \Lambda(A_i)$ be the sublattice of $\mathbb{Z}^2$ consisting of (u,v) in $\mathbb{Z}^2$ for which $A_i\begin{pmatrix}u\\v\end{pmatrix}$ is in $\mathbb{Z}^2$ and put

$$m_i = d(\Lambda_i) \tag{1.16}$$

for $i = 1,2,3,4$.

Theorem 1.2. *The positive number C_F in the statement of Theorem 1.1 is equal to $W_F A_F$ where A_F is given by (1.3) and W_F is given by the following table:*

Rep(F)	W_F	Rep(F)	W_F
$\mathbf{C}_1$	1	$\mathbf{D}_1$	$1-\frac{1}{2m}$
$\mathbf{C}_2$	$\frac{1}{2}$	$\mathbf{D}_2$	$\frac{1}{2}\left(1-\frac{1}{2m}\right)$
$\mathbf{C}_3$	$1-\frac{2}{3m}$	$\mathbf{D}_3$	$1-\frac{1}{2m_1}-\frac{1}{2m_2}-\frac{1}{2m_3}-\frac{2}{3m_4}+\frac{4}{3m}$
$\mathbf{C}_4$	$\frac{1}{2}\left(1-\frac{1}{2m}\right)$	$\mathbf{D}_4$	$\frac{1}{2}\left(1-\frac{1}{2m_1}-\frac{1}{2m_2}-\frac{1}{2m_3}+\frac{3}{4m}\right)$
$\mathbf{C}_6$	$\frac{1}{2}\left(1-\frac{2}{3m}\right)$	$\mathbf{D}_6$	$\frac{1}{2}\left(1-\frac{1}{2m_1}-\frac{1}{2m_2}-\frac{1}{2m_3}-\frac{2}{3m_4}+\frac{4}{3m}\right)$

Here Rep(F) *denotes a representative of the equivalence class of* Aut F *under* $\mathrm{GL}_2(\mathbb{Q})$ *conjugation and* m, m_1, m_2, m_3, m_4 *are defined in (1.13),(1.14), (1.15), and (1.16).*

We remark, see Lemma 3.2, that if Aut F is equivalent to $\mathbf{D}_4$ then $m = \mathrm{lcm}(m_1, m_2, m_3)$, the least common multiple of m_1, m_2 and m_3, and if Aut F is equivalent to $\mathbf{D}_3$ or $\mathbf{D}_6$ then $m = \mathrm{lcm}(m_1, m_2, m_3, m_4)$.

Observe that if F is a binary form with $F(1,0) \neq 0$ and $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ is in Aut F then A acts on the roots of F by sending a root α to $\frac{a_1\alpha + a_2}{a_3\alpha + a_4}$. If A fixes a root α then

$$a_3\alpha^2 + (a_4 - a_1)\alpha + a_2 = 0.$$

If F is an irreducible cubic then α has degree 3 and so

$$a_3 = a_4 - a_1 = a_2 = 0,$$

hence

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

But since F has degree 3 we see that $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore the only element of Aut F which fixes a root of F is the identity matrix I.

If A in Aut F does not fix a root it must permute the roots cyclically and thus must have order 3. Further, since any element in Aut F of order 2 would fix a root of F, we find that Aut F is $\mathrm{GL}_2(\mathbb{Q})$-conjugate to $\mathbf{C}_3$, say Aut $F = T\mathbf{C}_3T^{-1}$ with T in $\mathrm{GL}_2(\mathbb{Q})$. Forms invariant under $\mathbf{C}_3$ are of the form

$$G(x,y) = ax^3 + bx^2y + (b-3a)xy^2 - ay^3$$

with a and b integers; see (74) of [34]. Notice that

$$\Delta(G) = (b^2 - 3ab + 9a^2)^2.$$

Then $F = G_T$ for some G invariant under $\mathbf{C}_3$ and so

$$\Delta(F) = (\det T)^6 \Delta(G).$$

We conclude that if F is an irreducible cubic form with discriminant not a square then $\operatorname{Aut} F$ is $\mathbf{C}_1$ and so $W_F = 1$; thus Hooley's result (1.4) follows from Theorems 1.1 and 1.2. When $\operatorname{Aut} F$ is equivalent to $\mathbf{C}_3$ then $W_F = 1 - \frac{2}{3m}$ where m is the determinant of the lattice consisting of (u, v) in $\mathbb{Z}^2$ for which $A\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$ for all A in $\operatorname{Aut} F$. By Lemma 3.2 it suffices to consider the lattice consisting of (u, v) in $\mathbb{Z}^2$ for which $A\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$ for a generator A of $\operatorname{Aut} F$. Hooley has shown in [23] that the determinant of the lattice is m and so (1.6) follows from Theorems 1.1 and 1.2.

Now if $F(x, y) = ax^4 + bx^2y^2 + cy^4$ and the discriminant of F is non-zero then $\operatorname{Aut} F$ is generated by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and so is equivalent to $\mathbf{D}_2$ unless $a/c = A^4/C^4$ with A and C coprime positive integers. In this case $\operatorname{Aut} F$ is generated by $\begin{pmatrix} 0 & C/A \\ A/C & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & C/A \\ -A/C & 0 \end{pmatrix}$ and so is equivalent to $\mathbf{D}_4$. In the first instance $m = 1$ and $W_F = \frac{1}{4}$ and we recover Hooley's estimate (1.7). In the second case $m_1 = 1$ and $m_2 = m_3 = m = AC$ and so

$$W_F = \frac{1}{4}\left(1 - \frac{1}{2AC}\right).$$

which gives (1.8).

If follows from the analysis on page 818 of [34] that when F is a binary cubic form with non-zero discriminant $\operatorname{Aut} F$ is equivalent to $\mathbf{C}_1, \mathbf{C}_3, \mathbf{D}_1$ or $\mathbf{D}_3$ whereas if F is a binary quartic form with non-zero discriminant $\operatorname{Aut} F$ is equivalent to $\mathbf{C}_2, \mathbf{C}_4, \mathbf{D}_2$ or $\mathbf{D}_4$. In [38] and [39] the second author gives a set of generators for $\operatorname{Aut} F$ in these cases and as a consequence it is possible to determine W_F explicitly in terms of the coefficients of F.

In the special case that F is a binomial form, so $F(x, y) = ax^d + by^d$, it is straightforward to determine $\operatorname{Aut} F$; see Lemma 3.3. Then, by Theorems 1.1 and 1.2, we have the following result.

Corollary 1.3. *Let a, b and d be non-zero integers with $d \geq 3$ and let*

$$F(x, y) = ax^d + by^d.$$

Then (1.12) holds with $C_F = W_F A_F$ and with β_F given by (1.11) when d is even and $ab > 0$ and given by (1.10) otherwise. If a/b is not the d-th power of a rational *number then*

$$W_F = \begin{cases} 1 & \text{if } d \text{ is odd,} \\ \frac{1}{4} & \text{if } d \text{ is even.} \end{cases}$$

If $\frac{a}{b} = \left(\frac{A}{B}\right)^d$ *with* A *and* B *coprime integers then*

$$W_F = \begin{cases} 1 - \frac{1}{2|AB|} & \text{if } d \text{ is odd,} \\ \frac{1}{4}\left(1 - \frac{1}{2|AB|}\right) & \text{if } d \text{ is even.} \end{cases}$$

Further if d *is odd then*

$$A_F = \frac{1}{d|ab|^{1/d}} \left(\frac{2\Gamma(1-2/d)\Gamma(1/d)}{\Gamma(1-1/d)} + \frac{\Gamma^2(1/d)}{\Gamma(2/d)} \right)$$

while if d *is even*

$$A_F = \frac{2}{d|ab|^{1/d}} \frac{\Gamma^2(1/d)}{\Gamma(2/d)} \qquad \text{if } ab > 0$$

and

$$A_F = \frac{4}{d|ab|^{1/d}} \frac{\Gamma(1/d)\Gamma(1-2/d)}{\Gamma(1-1/d)} \qquad \text{if } ab < 0.$$

Finally we mention that there are other families of forms where one may readily determine W_F. For instance let a, b and k be integers with $a \neq 0$, $2a \neq \pm b$ and $k \geq 2$ and put

$$F(x,y) = ax^{2k} + bx^k y^k + ay^{2k}. \tag{1.17}$$

The discriminant of F is non-zero since $a \neq 0$ and $2a \neq \pm b$. Further, $\mathbf{D}_4$ is plainly contained in Aut F and there is no larger group which is an automorphism group of a binary form which contains $\mathbf{D}_4$. Therefore $\mathbf{D}_4$ is Aut F. It now follows from Theorem 1.2 that $W_F = 1/8$ since $m_1 = m_2 = m_3 = m = 1$.

2. Preliminary lemmas

We shall require a result of Mahler [27] from 1933. For a positive number Z we put

$$\mathcal{N}_F(Z) = \{(x,y) \in \mathbb{Z}^2 : 0 < |F(x,y)| \leq Z\}$$

and

$$N_F(Z) = |\mathcal{N}_F(Z)|.$$

Lemma 2.1. *Let* F *be a binary form with integer coefficients, non-zero discriminant and degree* $d \geq 3$. *Then, with* A_F *defined by (1.3), we have*

$$N_F(Z) = A_F Z^{\frac{2}{d}} + O_F\left(Z^\theta\right) \tag{2.1}$$

where $\theta = 1/d$ *if* F *does not have a linear factor in* $\mathbb{R}[x,y]$ *and* $\theta = 1/(d-1)$ *otherwise.*

Proof. Mahler proved (2.1) with $\theta = 1/(d-1)$ under the assumption that F is irreducible. A special case of Theorem 3 in [35], due to Thunder, covers the more general situation where we suppose that F has non-zero discriminant.

If F has no linear factor in $\mathbb{R}[x, y]$ then the region $\{(x, y) \in \mathbb{R}^2 : |F(x, y)| \leq Z\}$ is closed and bounded with boundary length L say. Further if x and y are integers with $F(x, y) = 0$ then $(x, y) = (0, 0)$. Thus

$$|N_F(Z) - A_F Z^{\frac{2}{d}}| < 1 + 4(L + 1), \tag{2.2}$$

see for example [9], [27], and since $L = O_F(Z^{1/d})$ the result follows.

Lemma 2.2. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. Let Z be a positive real number and let γ be a real number larger than $1/d$. The number of pairs of integers (x, y) with*

$$0 < |F(x, y)| \leq Z \tag{2.3}$$

for which

$$\max\{|x|, |y|\} > Z^\gamma$$

is

$$O_F\left(Z^{\frac{1}{d}} \log Z + Z^{1-(d-2)\gamma}\right).$$

Proof. We shall follow Heath-Brown's proof of Theorem 8 in [17]. Accordingly put

$$S(Z; C) = |\{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z, C < \max\{|x|, |y|\} \leq 2C, \gcd(x, y) = 1\}|$$

and suppose that $C \geq Z^\gamma$. Heath-Brown observes that by Roth's theorem $S(Z; C) = 0$ unless $C \ll Z^2$. Further,

$$S(Z; C) \ll 1 + \frac{Z}{C^{d-2}}. \tag{2.4}$$

Put

$$S^{(1)}(Z; C) = |\{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z, C < \max\{|x|, |y|\}, \gcd(x, y) = 1\}|.$$

Therefore, on replacing C by $2^j C$ in (2.4) for $j = 1, 2, ...$ and summing we find that

$$S^{(1)}(Z; C) \ll \log Z + \frac{Z}{C^{d-2}}.$$

Next put

$$S^{(2)}(Z; C) = |\{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z, C < \max\{|x|, |y|\}|.$$

Then

$$\begin{aligned} S^{(2)}(Z; C) &\ll \sum_{h \leq Z^{1/d}} S^{(1)}\left(\frac{Z}{h^d}, \frac{C}{h}\right) \\ &\ll \sum_{h \leq Z^{1/d}} \left(\log Z + \frac{Z}{h^2 C^{d-2}}\right) \\ &\ll Z^{\frac{1}{d}} \log Z + \frac{Z}{C^{d-2}} \end{aligned}$$

and our result follows on taking $C = Z^\gamma$.

We note that instead of appealing to Roth's theorem it is possible to treat the large solutions of (2.3) by means of the Thue-Siegel principle; see [3] and [34]. As a consequence all constants in the proof are then effective. □

We say that an integer h is *essentially represented* by F if h is represented by F and whenever $(x_1, y_1), (x_2, y_2)$ are in $\mathbb{Z}^2$ and

$$F(x_1, y_1) = F(x_2, y_2) = h$$

then there exists A in $\operatorname{Aut} F$ such that

$$A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Observe that if there is only one integer pair (x_1, y_1) for which $F(x_1, y_1) = h$ then h is essentially represented since I is in $\operatorname{Aut} F$.

Put

$$\mathcal{N}_F^{(1)}(Z) = \{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z \text{ and } F(x, y) \text{ is essentially represented by } F\}$$

and

$$\mathcal{N}_F^{(2)}(Z) = \{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z \text{ and } F(x, y) \text{ is not essentially represented by } F\}.$$

Let $N_F^{(i)}(Z) = |\mathcal{N}_F^{(i)}(Z)|$ for $i = 1, 2$.

Let X be a smooth surface in $\mathbb{P}^3$ of degree d defined over $\mathbb{Q}$, and for a positive number B let $N_1(X; B)$ denote the number of integer points on X with height at most B which do not lie on any lines contained in X. Colliot-Thélène proved in the appendix of [17] that if X is a smooth projective surface of degree $d \geq 3$ then there are at most $O_d(1)$ curves of degree at most $d - 2$ contained in X. This, combined with Salberger's work in [31], implies that for any $\varepsilon > 0$, we have

$$N_1(X; B) = O_\varepsilon\left(B^{\frac{12}{7}+\varepsilon}\right) \text{ if } d = 3. \tag{2.5}$$

Heath-Brown [16] obtained a better estimate for $N_1(X; B)$ when $d = 3$ and the surface X contains three lines which are rational and co-planar. In particular, he proved that in this case we have

$$N_1(X; B) = O_{X,\varepsilon}\left(B^{\frac{4}{3}+\varepsilon}\right). \tag{2.6}$$

Further, by the main theorem of the global determinant method for projective surfaces of Salberger [30], which has been generalized to the case of weighted projective space in Theorem 3.1 of [37], and controlling the contribution from conics contained in a projective surface X, as was done by Salberger in [29], we obtain

$$N_1(X; B) = O_{d,\varepsilon}\left(B^{\frac{3}{\sqrt{d}}+\varepsilon} + B^{1+\varepsilon}\right) \text{ if } d \geq 4. \tag{2.7}$$

To make use of (2.6), we shall require the following lemma, which is a consequence of a result in [38], [39] characterizing lines on surfaces X of the shape

$$X : F(x_1, x_2) - F(x_3, x_4) = 0$$

when F is a binary form of degree either 3 or 4. In particular the degree three case allows us to deduce the following:

Lemma 2.3. *Let F be a binary cubic form with integer coefficients and non-zero discriminant. Let X be the surface in $\mathbb{P}^3$ given by the equation*

$$F(x_1, x_2) - F(x_3, x_4) = 0.$$

Then X contains three rational, co-planar lines if F is reducible over $\mathbb{Q}$.

Proof. We first show that X contains three rational, co-planar lines if F has a rational automorphism of order 2. Since all elements of order 2 in $\mathrm{GL}_2(\mathbb{Q})$ are $\mathrm{GL}_2(\mathbb{Q})$-conjugate to $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and the property of X having three rational, co-planar lines is preserved under $\mathrm{GL}_2(\mathbb{Q})$-transformations of F, we may assume that $T = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is in $\mathrm{Aut}\, F$. In particular, we assume that F is symmetric; an elementary calculation shows that F is divisible by the linear form $x + y$. By Lemma 5.2 in [38] we see that $X(\mathbb{R})$ contains the lines

$$\{[s,t,s,t] : s,t \in \mathbb{R}\}, \{[s,t,t,s] : s,t, \in \mathbb{R}\}, \{[s,-s,t,-t] : s,t \in \mathbb{R}\}$$

in $\mathbb{P}^3(\mathbb{R})$. These lines all lie in the plane given by the equation

$$x_1 + x_2 - x_3 - x_4 = 0.$$

Each of these three lines is rational, hence X contains three rational, co-planar lines. Now by Theorem 3.1 of [38] F is reducible over $\mathbb{Q}$ if and only if $\mathrm{Aut}\, F$ contains an element of order 2, which completes the proof. □

Lemma 2.4. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. Then, for each $\varepsilon > 0$,*

$$N_F^{(2)}(Z) = O_{F,\varepsilon}\left(Z^{\beta_F + \varepsilon}\right), \tag{2.8}$$

where β_F is given by (1.10) and (1.11).

Proof. By the work of Hooley [24], (2.8) holds with β_F given by 5/9 when the degree of F is 3 and F splits into linear factors over $\mathbb{Q}$ and so we shall assume in the balance of the proof that this is not the case. Let $\varepsilon > 0$. If F has a linear factor over $\mathbb{R}$ put

$$\eta = \begin{cases} \dfrac{7}{19} & \text{if } d = 3 \text{ and } F \text{ is irreducible over } \mathbb{Q}, \\[2ex] \dfrac{3}{7} & \text{if } d = 3 \text{ and } F \text{ is reducible over } \mathbb{Q}, \\[2ex] \dfrac{\sqrt{d}}{d\sqrt{d} - 2\sqrt{d} + 3} & \text{if } 4 \leq d \leq 8, \\[2ex] \dfrac{1}{d-1} & \text{if } d \geq 9. \end{cases}$$

If F does not have a linear factor over $\mathbb{R}$ put

$$\eta = \frac{1}{d} + \varepsilon.$$

We shall give an upper bound for $N_F^{(2)}(Z)$ by following the approach of Heath-Brown in his proof of Theorem 8 of [17]. We first split $\mathcal{N}_F^{(2)}(Z)$ into two sets:

(1) Those points $(x, y) \in \mathcal{N}_F^{(2)}(Z)$ which satisfy $\max\{|x|, |y|\} \leq Z^\eta$, and
(2) Those points $(x, y) \in \mathcal{N}_F^{(2)}(Z)$ which satisfy $\max\{|x|, |y|\} > Z^\eta$.

We will use (2.5), (2.6), and (2.7) to treat the points in category (1). Let us put

$$\mathcal{G}(\mathbf{x}) = F(x_1, x_2) - F(x_3, x_4).$$

We shall denote by X the surface defined by $\mathcal{G}(\mathbf{x}) = 0$. Notice that X is smooth since $\Delta(F) \neq 0$.

Let $N_2(X; B)$ be the number of integer points (r_1, r_2, r_3, r_4) in $\mathbb{R}^4$ with $\max\limits_{1 \leq i \leq 4} |r_i| \leq B$ for which (r_1, r_2, r_3, r_4), viewed as a point in $\mathbb{P}^3$, is on X but does not lie on a line in X; here we do not require $\gcd(r_1, r_2, r_3, r_4) = 1$. Then

$$N_2(X; B) \leq \sum_{t=1}^{B} N_1\left(X; \frac{B}{t}\right)$$

and so, by (2.5), (2.6), (2.7), and Lemma 2.3,

$$N_2(X; B) = O_\varepsilon\left(B^{\frac{12}{7}+\varepsilon}\right) \quad \text{if } d = 3 \text{ and } F \text{ is irreducible},$$

$$N_2(X; B) = O_{F,\varepsilon}\left(B^{\frac{4}{3}+\varepsilon}\right) \quad \text{if } d = 3 \text{ and } F \text{ is reducible},$$

and

$$N_2(X; B) = O_{d,\varepsilon}\left(B^{\frac{3}{\sqrt{d}}+\varepsilon} + B^{1+\varepsilon}\right) \quad \text{if } d \geq 4.$$

Therefore

$$N_2(X; Z^\eta) = O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right). \tag{2.9}$$

It remains to deal with integer points on X which lie on some line contained in X. Lines in $\mathbb{P}^3$ may be classified into two types. They are given by the pairs

$$u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 = 0, v_3x_3 + v_4x_4 = 0,$$

and by

$$x_1 = u_1x_3 + u_2x_4, x_2 = u_3x_3 + u_4x_4.$$

Suppose the first type of line is on X. Then one of v_3, v_4 is non-zero, and we may assume without loss of generality that $v_3 \neq 0$. We thus have

$$x_3 = \frac{-v_4}{v_3}x_4.$$

Substituting this back into the first equation yields

$$u_1x_1 + u_2x_2 = -u_3\frac{-v_4}{v_3}x_4 - u_4x_4 = \frac{u_3v_4 - v_3u_4}{v_3}x_4.$$

Substituting this back into $F(x_1, x_2) = F(x_3, x_4)$ and assuming that $u_3v_4 - v_3u_4 \neq 0$, we see that

$$\begin{aligned} F(x_1, x_2) &= F\left(\frac{-v_4}{v_3}x_4, x_4\right) = x_4^d F(-v_4/v_3, 1) \\ &= F\left(\frac{-v_4}{v_3}, 1\right)\left(\frac{v_3u_1}{u_3v_4 - v_3u_4}x_1 + \frac{u_2v_3}{u_3v_4 - u_4v_3}x_2\right)^d. \end{aligned}$$

If $F(-v_4/v_3, 1) \neq 0$, then we see that F is a perfect d-th power, which is not possible since $\Delta(F) \neq 0$. Therefore we must have $F(x_1, x_2) = 0$ which is a contradiction. Now suppose that $u_3v_4 = v_3u_4$. We see that u_1, u_2 cannot both be zero. Assume without loss of generality that $u_1 \neq 0$. Then

$$F(x_1, x_2) = x_2^d F(-u_2/u_1, 1),$$

which is not possible since $\Delta(F) \neq 0$. Therefore we must have $F(-u_2/u_1, 1) = 0$, so once again $F(x_1, x_2) = 0$.

Now suppose that X contains a line of the second type. Suppose that $u_1u_4 = u_2u_3$. Since at least one of u_1, u_2 and one of u_3, u_4 is non-zero, we may assume that u_1 and u_3 are non-zero. Then we have

$$u_3x_1 = u_1u_3x_3 + u_2u_3x_4 = u_1(u_3x_3 + u_4x_4),$$

hence

$$(u_3/u_1)x_1 = u_3x_3 + u_4x_4 = x_2.$$

Thus $F(x_1, x_2) = F(x_3, x_4)$ implies that

$$F(x_3, x_4) = x_1^d F(1, u_3/u_1) = (u_3x_3 + u_4x_4)^d (u_1/u_3)^d F(1, u_3/u_1).$$

As before we must have $F(x_3, x_4) = 0$.

The last case is a line of the second type and for which $u_1u_4 \neq u_2u_3$. Such a line yields the equation

$$F(x_3, x_4) = F(u_1x_3 + u_2x_4, u_3x_3 + u_4x_4).$$

If (r_1, r_2, r_3, r_4) is an integer point on X on such a line and there is no element A of $\operatorname{Aut} F$ which maps (r_1, r_2) to (r_3, r_4) then it follows that at least one of u_1, u_2, u_3 and u_4 is not rational. Therefore, (r_1, r_2, r_3, r_4) must lie on a line which is not defined over $\mathbb{Q}$ and hence has at most one primitive integer point on it. Thus there are at most $O(Z^\eta)$ integer points whose coordinates have absolute value at most Z^η which lie on it. Since X is smooth it follows from a classical result of Salmon and Clebsch, see p. 559 of [32] or [4], that there are at most $O_d(1)$ lines on X and so at most $O_d(Z^\eta)$ integer points whose coordinates have absolute value at most Z^η on lines on X which are not defined over $\mathbb{Q}$. This, together with (2.9), shows that the number of points in category (1) is at most

$$O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right).$$

When F has a linear factor over $\mathbb{R}$ we apply Lemma 2.2 with $\gamma = \eta$ to conclude that the number of points in category (2) is at most $O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right)$. Otherwise we may write

$$F(x, y) = \prod_{j=1}^{d} L_j(x, y)$$

with say $L_j(x, y) = \lambda_j x + \theta_j y$ where λ_j and θ_j are non-zero complex numbers whose ratio is not a real number. But then

$$|L_j(x, y)| \gg_{\lambda_j, \theta_j} \max(|x|, |y|)$$

and so

$$|F(x, y)| \gg_F \max(|x|, |y|)^d.$$

Therefore in this case the number of points in category (2) is at most $O_{F,\varepsilon}(1)$ and the result now follows. ☐

In [17] Heath-Brown proved that for each $\varepsilon > 0$ the number of integers h of absolute value at most Z which are represented by F but not essentially represented by F is

$$O_{F,\varepsilon}\left(Z^{\frac{12d+16}{9d^2-6d+16}+\varepsilon}\right), \tag{2.10}$$

whenever F is a binary form with integer coefficients and non-zero discriminant. This follows from the remark on page 559 of [17] on noting that the numerator of the exponent should be $12d + 16$ instead of $12d$. Observe that the exponent is less than $2/d$ for ε sufficiently small. It follows from (2.10) that Lemma 2.4 holds with β_F replaced by the larger quantity given by the exponent of Z in (2.10). To see this we denote, for any positive integer h, the number of prime factors of h by $\omega(h)$ and the number of positive integers which divide h by $\tau(h)$. By Bombieri and Schmidt [3] when F is irreducible and by Stewart [34] when F has non-zero discriminant, if h is a non-zero integer the Thue equation

$$F(x, y) = h, \tag{2.11}$$

has at most $2800d^{1+\omega(h)}$ solutions in coprime integers x and y. Therefore the number of solutions of (2.11) in integers x and y is at most

$$2800\tau(h)d^{1+\omega(h)}. \tag{2.12}$$

Our claim now follows from (2.10), (2.12) and Theorem 317 of [15].

Lemma 2.5. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. Then with A_F defined as in (1.3),*

$$N_F^{(1)}(Z) = A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right)$$

where β_F is given by (1.10) and (1.11).

Proof. This is an immediate consequence of Lemmas 2.1 and 2.4 since θ is less than or equal to β_F . ☐

3. The automorphism group of F and associated lattices

For any element A in $\mathrm{GL}_2(\mathbb{Q})$ we denote by $\Lambda(A)$ the lattice of (u, v) in $\mathbb{Z}^2$ for which $A\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$.

Lemma 3.1. *Let F be a binary form with integer coefficients and non-zero discriminant. Let A be in $\operatorname{Aut} F$. Then there exists a unique positive integer a and coprime integers a_1, a_2, a_3, a_4 such that*

$$A = \frac{1}{a}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \tag{3.1}$$

and

$$a = d(\Lambda(A)). \tag{3.2}$$

Proof. Let $A = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix}$ and write

$$\alpha_i = \frac{a_i}{a}$$

for $i = 1, 2, 3, 4$ where a is the least common denominator of the α_i's. Note that a_1, a_2, a_3, a_4 are coprime since A is in $\operatorname{Aut} F$ and so $|\det(A)| = 1$. This yields the form given in (3.1). Then $\Lambda(A)$ is the set of (u, v) in $\mathbb{Z}^2$ for which

$$a_1 u + a_2 v \equiv 0 \pmod{a}$$

and

$$a_3 u + a_4 v \equiv 0 \pmod{a}.$$

For each prime p let k be the largest power of p which divides a. We define the lattice $\Lambda^{(p)}(A)$ to be the set of (u, v) in $\mathbb{Z}^2$ for which

$$a_1 u + a_2 v \equiv 0 \pmod{p^k} \tag{3.3}$$

and

$$a_3 u + a_4 v \equiv 0 \pmod{p^k}. \tag{3.4}$$

Then

$$\Lambda(A) = \bigcap_p \Lambda^{(p)}(A), \tag{3.5}$$

where the intersection is taken over all primes p.

Since a_1, a_2, a_3 and a_4 are coprime at least one of them is not divisible by p. Suppose, without loss of generality, that p does not divide a_1. Suppose also that k is positive. Then a_1^{-1} exists modulo p^k. Thus if (3.3) holds then

$$u \equiv -a_1^{-1} a_2 v \pmod{p^k}$$

and (3.4) becomes

$$(a_1 a_4 - a_2 a_3) v \equiv 0 \pmod{p^k}. \tag{3.6}$$

But A is in $\operatorname{Aut} F$ and so $|\det(A)| = 1$. Thus

$$|a_1 a_4 - a_2 a_3| = a^2$$

and (3.6) holds regardless of the value of v. Therefore the elements of the lattice $\Lambda^{(p)}(A)$ are determined by the congruence relation (3.3). This is also true if k is 0. It follows that

$$d(\Lambda^{(p)}(A)) = p^k$$

and by (3.5) and the Chinese Remainder Theorem we obtain (3.2). □

Lemma 3.2. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. If A is an element of order 3 in $\operatorname{Aut} F$ then*

$$\Lambda(A) = \Lambda(A^2). \tag{3.7}$$

If $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3, \mathbf{D}_4$ or $\mathbf{D}_6$ then

$$\Lambda_i \cap \Lambda_j = \Lambda \textit{ for } i \neq j. \tag{3.8}$$

Further $m = \text{lcm}(m_1, m_2, m_3)$ *when* $\text{Aut}\, F$ *is equivalent to* $\mathbf{D}_4$ *and* $m = \text{lcm}(m_1, m_2, m_3, m_4)$ *when* $\text{Aut}\, F$ *is equivalent to* $\mathbf{D}_3$ *or* $\mathbf{D}_6$*.*

Proof. Let us first prove (3.7). Then either A or A^2 is conjugate in $\text{GL}_2(\mathbb{Q})$ to $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ and we may assume we are in the former case. Let T be an element of $\text{GL}_2(\mathbb{Q})$ with

$$T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}, \tag{3.9}$$

where t_1, t_2, t_3 and t_4 are coprime integers for which

$$A = T^{-1} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} T. \tag{3.10}$$

Put $t = t_1t_4 - t_2t_3$. Then

$$A = \frac{1}{t} \begin{pmatrix} t_1t_2 + t_2t_3 + t_3t_4 & t_2^2 + t_4^2 + t_2t_4 \\ -t_1t_3 - t_3^2 - t_1^2 & -t_1t_4 - t_3t_4 - t_1t_2 \end{pmatrix}$$

and

$$A^2 = \frac{1}{t} \begin{pmatrix} -t_1t_2 - t_3t_4 - t_1t_4 & -t_2^2 - t_4^2 - t_2t_4 \\ t_1^2 + t_3^2 + t_1t_3 & t_1t_2 + t_3t_4 + t_2t_3 \end{pmatrix},$$

hence $\Lambda(A)$ is the set of $(u, v) \in \mathbb{Z}^2$ for which

$$(t_1t_2 + t_2t_3 + t_3t_4)u + (t_2^2 + t_4^2 + t_2t_4)v \equiv 0 \pmod t \tag{3.11}$$

and

$$(t_1t_3 + t_3^2 + t_1^2)u + (t_1t_4 + t_3t_4 + t_1t_2)v \equiv 0 \pmod t. \tag{3.12}$$

Similarly, $\Lambda(A^2)$ is the set of $(u, v) \in \mathbb{Z}^2$ for which

$$(t_1t_2 + t_1t_4 + t_3t_4)u + (t_2^2 + t_4^2 + t_2t_4)v \equiv 0 \pmod t \tag{3.13}$$

and

$$(t_1^2 + t_3^2 + t_1t_3)u + (t_2t_3 + t_3t_4 + t_1t_2)v \equiv 0 \pmod t. \tag{3.14}$$

On noting that $t_1t_4 \equiv t_2t_3 \pmod t$ we see that the conditions (3.11) and (3.12) are the same as (3.13) and (3.14), hence

$$\Lambda(A) = \Lambda(A^2).$$

Suppose that $\text{Aut}\, F$ is equivalent to $\mathbf{D}_4$ under conjugation in $\text{GL}_2(\mathbb{Q})$. Then there exists an element T in $\text{GL}_2(\mathbb{Q})$ given by (3.9) with t_1, t_2, t_3 and t_4 coprime integers for which $\text{Aut}\, F = T^{-1}\mathbf{D}_4T$. Put $t = t_1t_4 - t_2t_3$ and note that $t \neq 0$. The lattices Λ_1, Λ_2 and Λ_3 may be taken to be the lattices of (u, v) in $\mathbb{Z}^2$ for which

$$T^{-1}A_iT \begin{pmatrix} u \\ v \end{pmatrix} \in \mathbb{Z}^2,$$

where

$$A_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Thus Λ_1 consists of integer pairs (u, v) for which

$$(t_1t_2 + t_3t_4)u + (t_2^2 + t_4^2)v \equiv 0 \pmod t \tag{3.15}$$

and

$$(t_1^2 + t_3^2)u + (t_1t_2 + t_3t_4)v \equiv 0 \pmod{t}. \tag{3.16}$$

Λ_2 consists of integer pairs (u, v) for which

$$(t_1t_2 - t_3t_4)u + (t_2^2 - t_4^2)v \equiv 0 \pmod{t} \tag{3.17}$$

and

$$(t_1^2 - t_3^2)u + (t_1t_2 - t_3t_4)v \equiv 0 \pmod{t} \tag{3.18}$$

and Λ_3 consists of integer pairs (u, v) for which

$$2t_2t_3u + 2t_2t_4v \equiv 0 \pmod{t} \tag{3.19}$$

and

$$2t_1t_3u + 2t_2t_3v \equiv 0 \pmod{t}, \tag{3.20}$$

where in (3.19) and (3.20) we have used the observation that

$$t_1t_4 \equiv t_2t_3 \pmod{t}.$$

For each prime p we put $h = \mathrm{ord}_p\, t$. Define $\Lambda_i^{(p)}$ for $i = 1, 2, 3$ to be the lattice of (u, v) in $\mathbb{Z}^2$ for which the congruences (3.15) and (3.16), (3.17) and (3.18), and (3.19) and (3.20) respectively hold with t replaced by p^h and define $\Lambda^{(p)}$ to be the lattice for which all of the congruences hold. We shall prove that for some reordering (i, j, k) of $(1, 2, 3)$ we have

$$\Lambda_i^{(p)} \supset \Lambda_j^{(p)} = \Lambda_k^{(p)}. \tag{3.21}$$

It then follows that

$$\Lambda_r^{(p)} \cap \Lambda_s^{(p)} = \Lambda_1^{(p)} \cap \Lambda_2^{(p)} \cap \Lambda_3^{(p)} = \Lambda^{(p)} \tag{3.22}$$

for any pair $\{r, s\}$ from $\{1, 2, 3\}$. But since

$$\bigcap_p \left(\Lambda_r^{(p)} \cap \Lambda_s^{(p)}\right) = \Lambda_r \cap \Lambda_s \text{ and } \bigcap_p \Lambda^{(p)} = \Lambda, \tag{3.23}$$

we see that (3.8) holds. Further

$$\max\left\{d\left(\Lambda_1^{(p)}\right), d\left(\Lambda_2^{(p)}\right), d\left(\Lambda_3^{(p)}\right)\right\} = d\left(\Lambda^{(p)}\right)$$

and so $d(\Lambda)$ is the least common multiple of $d(\Lambda_1), d(\Lambda_2)$ and $d(\Lambda_3)$.

It remains to prove (3.21). Put

$$g_1 = \gcd(t_1t_2 + t_3t_4, t_1^2 + t_3^2, t_2^2 + t_4^2, t),$$
$$g_2 = \gcd(t_1t_2 - t_3t_4, t_1^2 - t_3^2, t_2^2 - t_4^2, t)$$

and

$$g_3 = \gcd(2t_2t_3, 2t_2t_4, 2t_1t_3, t).$$

We shall show that $\gcd(g_1, g_2)$ is 1 or 2 and that

$$\gcd(g_1, g_2) = \gcd(g_1, g_3) = \gcd(g_2, g_3). \tag{3.24}$$

Notice that if p divides g_1 then $t_1^2 \equiv -t_3^2 \pmod{p}$ and $t_2^2 \equiv -t_4^2 \pmod{p}$ while if p divides g_2 then $t_1^2 \equiv t_3^2 \pmod{p}$ and $t_2^2 \equiv t_4^2 \pmod{p}$ and if p divides g_3 then p divides

$2t_2t_3, 2t_2t_4$ and $2t_1t_3$. Thus if p divides $\gcd(g_1, g_2)$ then p divides $2t_1^2, 2t_2^2, 2t_3^2$ and $2t_4^2$; whence $p = 2$ since $\gcd(t_1, t_2, t_3, t_4) = 1$. Next suppose that p divides $\gcd(g_1, g_3)$. Then p divides $2t_2t_4$ and $t_2^2 \equiv -t_4^2 \pmod{p}$ and p divides $2t_1t_3$ and $t_1^2 \equiv -t_3^2 \pmod{p}$. Since $\gcd(t_1, t_2, t_3, t_4) = 1$ we find that $p = 2$. Finally if p divides $\gcd(g_2, g_3)$ then, as in the previous case, $p = 2$. Observe that

$$0 = \operatorname{ord}_2 g_1 = \operatorname{ord}_2 g_2 \leq \operatorname{ord}_2 g_3 \tag{3.25}$$

unless (t_1, t_2, t_3, t_4) is congruent to $(1, 0, 1, 0), (0, 1, 0, 1)$ or $(1, 1, 1, 1)$ modulo 2 and in these cases

$$1 = \operatorname{ord}_2 g_1 = \operatorname{ord}_2 g_3 \leq \operatorname{ord}_2 g_2. \tag{3.26}$$

Thus (3.24) follows from (3.25) and (3.26).

For each prime p put $h_i = \operatorname{ord}_p g_i$ for $i = 1, 2, 3$. Then, by (3.24), for some rearrangement (i, j, k) of $(1, 2, 3)$ we have

$$h_i \geq h_j = h_k.$$

As in the proof of Lemma 3.1, $\Lambda_i^{(p)}$ is defined by a single congruence modulo p^{h-h_i} for $i = 1, 2, 3$. We check that t divides the determinant of any matrix whose rows are taken from the rows determined by the coefficients of the congruence relations (3.15), (3.16), (3.17), (3.18), (3.19), and (3.20). Furthermore $2t$ divides the determinant of such a matrix if (t_1, t_2, t_3, t_4) is congruent to $(1, 0, 1, 0), (0, 1, 0, 1)$ or $(1, 1, 1, 1)$ modulo 2. Since $h_j = h_k$ we see that the congruences modulo p^{h-h_j} define identical lattices $\Lambda_j^{(p)}$ and $\Lambda_k^{(p)}$. Further, since $h_i \geq h_j$, $\Lambda_j^{(p)}$ is a sublattice of $\Lambda_i^{(p)}$ and (3.8) follows when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_4$.

Suppose now that $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$ under conjugation in $\mathrm{GL}_2(\mathbb{Q})$. There exists an element T in $\mathrm{GL}_2(\mathbb{Q})$, as in (3.9), with t_1, t_2, t_3 and t_4 coprime integers for which

$$\operatorname{Aut} F = T^{-1}\mathbf{D}_3 T.$$

Define $t = t_1t_4 - t_2t_3$. The lattices $\Lambda_1, \Lambda_2, \Lambda_3$ and Λ_4 may be taken to be the lattices of integer pairs (u, v) for which

$$T^{-1}A_iT\begin{pmatrix} u \\ v \end{pmatrix} \in \mathbb{Z}^2$$

where

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, A_3 = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \text{ and } A_4 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Thus Λ_1 consists of integer pairs (u, v) for which

$$(t_1t_2 - t_3t_4)u + (t_2^2 - t_4^2)v \equiv 0 \pmod{t} \tag{3.27}$$

and

$$(t_1^2 - t_3^2)u + (t_1t_2 - t_3t_4)v \equiv 0 \pmod{t}. \tag{3.28}$$

Λ_2 consists of integer pairs (u, v) for which

$$(t_1t_2 + t_2t_3 + t_1t_4)u + (t_2^2 + 2t_2t_4)v \equiv 0 \pmod{t} \tag{3.29}$$

and

$$(t_1^2 + 2t_1t_3)u + (t_1t_2 + t_2t_3 + t_1t_4)v \equiv 0 \pmod{t}. \tag{3.30}$$

Λ_3 consists of integer pairs (u, v) for which

$$(t_1t_4 + t_2t_3 + t_3t_4)u + (2t_2t_4 + t_4^2)v \equiv 0 \pmod{t} \tag{3.31}$$

and

$$(2t_1t_3 + t_3^2)u + (t_1t_4 + t_2t_3 + t_3t_4)v \equiv 0 \pmod{t}. \tag{3.32}$$

Λ_4 consists of integer pairs (u, v) for which

$$(t_1t_2 + t_2t_3 + t_3t_4)u + (t_2^2 + t_2t_4 + t_4^2)v \equiv 0 \pmod{t} \tag{3.33}$$

and

$$(t_1^2 + t_1t_3 + t_3^2)u + (t_1t_2 + t_1t_4 + t_3t_4)v \equiv 0 \pmod{t}. \tag{3.34}$$

For each prime p we put $h = \text{ord}_p\, t$. Define $\Lambda_i^{(p)}$ for $i = 1, 2, 3, 4$ to be the lattice of (u, v) in $\mathbb{Z}^2$ for which the congruences (3.27) and (3.28), (3.29) and (3.30), (3.31) and (3.32), and (3.33) and (3.34) respectively hold with t replaced with p^h and define $\Lambda^{(p)}$ to be the lattice for which all the congruences hold. We shall prove that for some reordering (i, j, k, l) of $(1, 2, 3, 4)$ we have

$$\Lambda_i^{(p)} \supset \Lambda_j^{(p)} = \Lambda_k^{(p)} = \Lambda_l^{(p)}. \tag{3.35}$$

It then follows that

$$\Lambda_r^{(p)} \cap \Lambda_s^{(p)} = \Lambda_1^{(p)} \cap \Lambda_2^{(p)} \cap \Lambda_3^{(p)} \cap \Lambda_4^{(p)} = \Lambda^{(p)} \tag{3.36}$$

for any pair $\{r, s\}$ from $\{1, 2, 3, 4\}$. But since

$$\bigcap_p \left(\Lambda_r^{(p)} \cap \Lambda_s^{(p)}\right) = \Lambda_r \cap \Lambda_s \text{ and } \bigcap_p \Lambda^{(p)} = \Lambda, \tag{3.37}$$

we conclude that (3.8) holds. Further

$$\max\left\{d\left(\Lambda_1^{(p)}\right), d\left(\Lambda_2^{(p)}\right), d\left(\Lambda_3^{(p)}\right), d\left(\Lambda_4^{(p)}\right)\right\} = d\left(\Lambda^{(p)}\right)$$

and so $d(\Lambda)$ is the least common multiple of $d(\Lambda_1), d(\Lambda_2), d(\Lambda_3)$ and $d(\Lambda_4)$.

It remains to prove (3.35). Put

$$g_1 = \gcd(t_1t_2 - t_3t_4, t_1^2 - t_3^2, t_2^2 - t_4^2, t),$$
$$g_2 = \gcd(t_1t_2 + t_2t_3 + t_1t_4, t_1^2 + 2t_1t_3, t_2^2 + 2t_2t_4, t),$$
$$g_3 = \gcd(t_1t_4 + t_2t_3 + t_3t_4, 2t_1t_3 + t_3^2, 2t_2t_4 + t_4^2, t),$$

and

$$g_4 = \gcd(t_1t_2 + t_2t_3 + t_3t_4, t_1^2 + t_1t_3 + t_3^2, t_2^2 + t_2t_4 + t_4^2, t).$$

Suppose that p is a prime which divides $\gcd(g_1, g_2)$. If p divides t_1 then since p divides $t_1^2 - t_3^2$ we see that p divides t_3. Similarly if p divides t_2 then since p divides $t_2^2 - t_4^2$ we see that p divides t_4. Since t_1, t_2, t_3 and t_4 are coprime either p does not divide t_1 or p does not divide t_2. In the former case since p divides $t_1^2 + 2t_1t_3$ we find that p divides $t_1 + 2t_3$. Thus $t_1^2 \equiv 4t_3^2 \pmod{p}$ and since $t_1^2 \equiv t_3^2 \pmod{p}$ we conclude that $p = 3$. In the latter case since p divides $t_2^2 + 2t_2t_4$ we again find that $p = 3$. In a similar fashion we prove that if p is a prime which divides $\gcd(g_i, g_j)$ for any pair $\{i, j\}$ from

$\{1,2,3,4\}$ then $p = 3$.

Denote by E the set consisting of the 4-tuples $(1,1,1,1)$, $(-1,-1,-1,-1)$, $(1,-1,1,-1)$, $(-1,1,-1,1)$, $(1,0,1,0)$, $(-1,0,-1,0)$, $(0,1,0,1)$ and $(0,-1,0,-1)$. One may check that if (t_1,t_2,t_3,t_4) is not congruent modulo 3 to an element of E then for some reordering (i,j,k,l) of $(1,2,3,4)$ we have

$$0 = \operatorname{ord}_3 g_i = \operatorname{ord}_3 g_j = \operatorname{ord}_3 g_k \le \operatorname{ord}_3 g_l. \tag{3.38}$$

If (t_1,t_2,t_3,t_4) is congruent modulo 3 to an element of E then there is some reordering (i,j,k,l) of $(1,2,3,4)$ such that

$$1 = \operatorname{ord}_3 g_i = \operatorname{ord}_3 g_j = \operatorname{ord}_3 g_k \le \operatorname{ord}_3 g_l. \tag{3.39}$$

To see this we make use of the fact that

$$\operatorname{ord}_3 g_1 \le \operatorname{ord}_3(t_1^2 - t_3^2), \;\; \operatorname{ord}_3 g_2 \le \operatorname{ord}_3(t_1^2 + 2t_1t_3), \tag{3.40}$$
$$\operatorname{ord}_3 g_3 \le \operatorname{ord}_3(2t_1t_3 + t_3^2) \text{ and } \operatorname{ord}_3 g_4 \le \operatorname{ord}_3(t_1^2 + t_1t_3 + t_3^2),$$

to deal with the first six cases. To handle the remaining two cases, so when (t_1,t_2,t_3,t_4) is congruent modulo 3 to $(0,1,0,1)$ or $(0,-1,0,-1)$, we appeal to (3.40) but with t_1 and t_3 replaced by t_2 and t_4 respectively.

It now follows from (3.38) and (3.39) that $\gcd(g_1,g_2)$ is 1 or 3 and

$$\gcd(g_1,g_2) = \gcd(g_1,g_3) = \gcd(g_1,g_4) = \gcd(g_2,g_3) = \gcd(g_2,g_4) = \gcd(g_3,g_4). \tag{3.41}$$

For each prime p put $h_i = \operatorname{ord}_p g_i$ for $i = 1,2,3,4$. Then, by (3.41) for some reordering (i,j,k,l) of $(1,2,3,4)$ we have

$$h_i \ge h_j = h_k = h_l.$$

As in the proof of Lemma 3.1, $\Lambda_i^{(p)}$ is defined by a single congruence relation modulo p^{h-h_i} and $\Lambda_j^{(p)}, \Lambda_k^{(p)}$ and $\Lambda_l^{(p)}$ are defined by single congruences modulo p^{h-h_j}. We check that t divides the determinant of any matrix whose rows are taken from the rows determined by the coefficients of the congruence relations (3.27), (3.28), (3.29), (3.30), (3.31), (3.32), (3.33) and (3.34) and that $3t$ divides the determinant of such a matrix if (t_1,t_2,t_3,t_4) is congruent to an element of E. Then since $h_j = h_k = h_l$ we see that the congruences modulo p^{h-h_j} define identical lattices so

$$\Lambda_j^{(p)} = \Lambda_k^{(p)} = \Lambda_l^{(p)}.$$

Further, since $h_i \ge h_j$, $\Lambda_j^{(p)}$ is a sublattice of $\Lambda_i^{(p)}$ and thus (3.35) holds and (3.8) follows when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$.

Finally we remark that (3.8) holds when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_6$ by the same analysis we used when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$.

□

Lemma 3.3. *Let a and b be non-zero integers and let d be an integer with $d \ge 3$. Put*

$$F(x,y) = ax^d + by^d.$$

If a/b is not the d-th power of a rational number then when d is odd

$$\operatorname{Aut} F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

and when d is even

$$\operatorname{Aut} F = \left\{ \begin{pmatrix} w_1 & 0 \\ 0 & w_2 \end{pmatrix} ; w_i \in \{1, -1\}, i = 1, 2 \right\}.$$

If $\dfrac{a}{b} = \dfrac{A^d}{B^d}$ with A and B coprime integers then when d is odd

$$\operatorname{Aut} F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & B/A \\ A/B & 0 \end{pmatrix} \right\}$$

and when d is even

$$\operatorname{Aut} F = \left\{ \begin{pmatrix} w_1 & 0 \\ 0 & w_2 \end{pmatrix}, \begin{pmatrix} 0 & w_4 B/A \\ w_3 A/B & 0 \end{pmatrix} ; w_i \in \{1, -1\}, i = 1, 2, 3, 4 \right\}.$$

Proof. Let

$$U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}$$

be an element of $\operatorname{Aut} F$. Then u_1, u_2, u_3, u_4 are rational numbers with

$$u_1 u_4 - u_2 u_3 = \pm 1. \tag{3.42}$$

Since $F(u_1 x + u_2 y, u_3 x + u_4 y) = F(x, y)$ we see on comparing coefficients that

$$a u_1^d + b u_3^d = a, \ \ a u_2^d + b u_4^d = b \tag{3.43}$$

and

$$a u_1^j u_2^{d-j} = -b u_3^j u_4^{d-j} \tag{3.44}$$

for $j = 1, \cdots, d - 1$.

Suppose that $u_1 u_2 \neq 0$. Then by (3.44), we have $u_3 u_4 \neq 0$ as well. Therefore we may write

$$\left(\frac{u_3}{u_1} \right) \left(\frac{u_4}{u_2} \right)^{d-1} = \left(\frac{u_3}{u_1} \right)^2 \left(\frac{u_4}{u_2} \right)^{d-2},$$

which implies that $u_1 u_4 - u_2 u_3 = 0$, contradicting (3.42). Therefore, $u_1 u_2 = 0$ and similarly $u_3 u_4 = 0$. Further, by (3.42), either $u_1 u_4 = \pm 1$ and $u_2 = u_3 = 0$ or $u_2 u_3 = \pm 1$ and $u_1 = u_4 = 0$. In the first case, by (3.43), we have $u_1^d = 1$ and $u_4^d = 1$, hence if d is odd we have $u_1 = u_4 = 1$ while if d is even we have $u_1 = \pm 1$ and $u_4 = \pm 1$. In the other case, by (3.43), we have $u_3^d = \dfrac{a}{b}$ and this is only possible if there exist coprime integers A and B with

$$\frac{a}{b} = \frac{A^d}{B^d}.$$

In that case $u_3 = A/B$ if d is odd and $u_3 = \pm A/B$ if d is even. Thus, by (3.42), $u_2 = B/A$ if d is odd and $u_2 = \pm B/A$ if d is even. Our result now follows. ∎

4. Proof of Theorems 1.1 and 1.2

If $\mathrm{Aut}\, F$ is conjugate to $\mathbf{C}_1$ then every pair $(x,y) \in \mathbb{Z}^2$ for which $F(x,y)$ is essentially represented with $0 < |F(x,y)| \leq Z$ gives rise to a distinct integer h with $0 < |h| \leq Z$. It follows from Lemma 2.4 and Lemma 2.5 that

$$R_F(Z) = A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right),$$

and we see that W_F in this case is 1. In a similar way we see that if $\mathrm{Aut}\, F$ is conjugate to $\mathbf{C}_2$ then

$$R_F(Z) = \frac{A_F}{2} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right).$$

Next let us consider when $\mathrm{Aut}\, F$ is conjugate to $\mathbf{C}_3$. Then for A in $\mathrm{Aut}\, F$ with $A \neq I$ we have, by Lemma 3.2, $\Lambda(A) = \Lambda(A^2) = \Lambda$. Thus whenever $F(x,y) = h$ with (x,y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ there are two other elements $(x_1,y_1),(x_2,y_2)$ for which $F(x_i,y_i) = h$ for $i = 1,2$. When (x,y) is in $\mathbb{Z}^2$ but not in Λ and $F(x,y)$ is essentially represented then $F(x,y)$ has only one representation.

Let ω_1, ω_2 be a basis for Λ with $\omega_1 = (a_1,a_3)$ and $\omega_2 = (a_2,a_4)$. Put $F_\Lambda(x,y) = F(a_1x + a_2y, a_3x + a_4y)$ and notice that

$$|\mathcal{N}_F(Z) \cap \Lambda| = N_{F_\Lambda}(Z). \tag{4.1}$$

By Lemma 2.1

$$N_{F_\Lambda}(Z) = A_{F_\Lambda} Z^{\frac{2}{d}} + O_{F_\Lambda}\left(Z^{1/(d-1)}\right). \tag{4.2}$$

Since the quantity $|\Delta(F)|^{1/d(d-1)} A_F$ is invariant under $\mathrm{GL}_2(\mathbb{R})$

$$|\Delta(F)|^{1/d(d-1)} A_F = |\Delta(F_\Lambda)|^{1/d(d-1)} A_{F_\Lambda} \tag{4.3}$$

and we see that

$$A_{F_\Lambda} = \frac{1}{d(\Lambda)} A_F = \frac{A_F}{m}. \tag{4.4}$$

Therefore by (4.1), (4.2) and (4.4)

$$|\mathcal{N}_F(Z) \cap \Lambda| = \frac{A_F}{m} Z^{\frac{2}{d}} + O_F\left(Z^{\frac{1}{d-1}}\right). \tag{4.5}$$

Certainly $\mathcal{N}_F^{(2)}(Z) \cap \Lambda$ is contained in $\mathcal{N}_F^{(2)}(Z)$ and thus, by (4.5) and Lemma 2.4,

$$|\mathcal{N}_F^{(1)}(Z) \cap \Lambda| = \frac{A_F}{m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right). \tag{4.6}$$

Each pair (x,y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ is associated with two other pairs which represent the same integer. Thus the pairs (x,y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ yield

$$\frac{A_F}{3m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.7}$$

integers h with $0 < |h| \leq Z$. By Lemma 2.5 and (4.6) the number of pairs (x,y) in $\mathcal{N}_F^{(1)}(Z)$ which are not in Λ is

$$\left(1 - \frac{1}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.8}$$

and each pair gives rise to an integer h with $0 < |h| \leq Z$ which is uniquely represented by F. It follows from (4.7), (4.8) and Lemma 2.4 that when $\operatorname{Aut} F$ is equivalent to $\mathbf{C}_3$ we have

$$R_F(Z) = \left(1 - \frac{2}{3m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right).$$

A similar analysis applies in the case when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_1, \mathbf{D}_2, \mathbf{C}_4$ or $\mathbf{C}_6$. These groups are cyclic with the exception of $\mathbf{D}_2$ but $\mathbf{D}_2/\{\pm I\}$ is cyclic and that is sufficient for our purposes.

We are left with the possibility that $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_3, \mathbf{D}_4$ or $\mathbf{D}_6$. We first consider the case when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_4$. In this case, recall (4.6), we have

$$|\mathcal{N}_F^{(1)}(Z) \cap \Lambda| = \frac{A_F}{m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right)$$

and since each h for which $h = F(x,y)$ with (x,y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ is represented by 8 elements of $\mathcal{N}_F^{(1)}(Z)$ the pairs (x,y) of $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ yield

$$\frac{A_F}{8m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.9}$$

terms h in $\mathcal{R}_F(Z)$. By Lemma 3.2 we have $\Lambda_i \cap \Lambda_j = \Lambda$ for $1 \leq i < j \leq 3$; whence the terms (x,y) in Λ_1, Λ_2 or Λ_3 but not in Λ for which (x,y) is in $\mathcal{N}_F^{(1)}(Z)$ have cardinality

$$\left(\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} - \frac{3}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right).$$

If (x,y) is in Λ_1, Λ_2 or Λ_3 but not in Λ and $h = F(x,y)$ is essentially represented then h has precisely four representations. Accordingly the terms in

$$\mathcal{N}_F^{(1)}(Z) \cap \Lambda_i, 1 \leq i \leq 3$$

which are not in Λ contribute

$$\frac{1}{4}\left(\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} - \frac{3}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.10}$$

terms to $\mathcal{R}_F(Z)$. Finally the terms (x,y) in $\mathcal{N}_F^{(1)}(Z)$ but not in Λ_i for $i = 1,2,3$ have cardinality equal to

$$\left(1 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3} + \frac{2}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right).$$

Each integer h represented by such a term has 2 representations and therefore these terms (x,y) contribute

$$\frac{1}{2}\left(1 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3} + \frac{2}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.11}$$

terms to $\mathcal{R}_F(Z)$. It now follows from (4.9), (4.10), (4.11) and Lemma 2.4 that

$$R_F(Z) = \frac{1}{2}\left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} + \frac{3}{4m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right),$$

as required.

We now treat the case when $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_3$. As before the pairs (x,y) of $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ yield

$$\frac{A_F}{6m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.12}$$

terms in $\mathcal{R}_F(Z)$. Since $\Lambda_i \cap \Lambda_j = \Lambda$ for $1 \le i < j \le 3$ by Lemma 3.2, the pairs (x,y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda_i$ for $i = 1,2,3$ which are not in Λ contribute

$$\left(\frac{1}{2m_1} + \frac{1}{2m_2} + \frac{1}{2m_3} - \frac{3}{2m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.13}$$

to $\mathcal{R}_F(Z)$. Further, the pairs (x,y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda_4$ which are not in Λ contribute

$$\left(\frac{1}{3m_4} - \frac{1}{3m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.14}$$

terms to $\mathcal{R}_F(Z)$. Furthermore the pairs (x,y) in $\mathcal{N}_F^{(1)}(Z)$ which are not in Λ_i for $i = 1,2,3,4$ contribute, by Lemma 3.2,

$$\left(1 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3} - \frac{1}{m_4} + \frac{3}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right) \tag{4.15}$$

terms to $\mathcal{R}_F(Z)$. It then follows from (4.12), (4.13), (4.14), (4.15), and Lemma 2.4 that

$$R_F(Z) = \left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} - \frac{2}{3m_4} + \frac{4}{3m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_F+\varepsilon}\right)$$

as required.

When $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_6$ the analysis is the same as for $\mathbf{D}_3$ taking into account the fact that $\operatorname{Aut} F$ contains $-I$ and so the weighting factor W_F is one half of what it is when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$. This completes the proof of Theorems 1.1 and 1.2.

5. Proof of Corollary 1.3

We first determine W_F. By Lemma 3.3, if a/b is not the d-th power of a rational then when d is odd $\operatorname{Aut} F$ is equivalent to $\mathbf{C}_1$ and, by Theorem 1.2, $W_F = 1$ while when d is even we have $m = 1$ and $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_2$ and so by Theorem 1.2 we have $W_F = \dfrac{1}{4}$. Suppose that

$$\frac{a}{b} = \frac{A^d}{B^d}$$

with A and B coprime non-zero integers. If d is odd then $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_1$ by Lemma 3.3. Notice that

$$\begin{pmatrix} 0 & B/A \\ A/B & 0 \end{pmatrix} = \frac{1}{AB}\begin{pmatrix} 0 & B^2 \\ A^2 & 0 \end{pmatrix}$$

and that A^2 and B^2 are coprime integers. Therefore by Lemma 3.1 we have $m = |AB|$ and $W_F = 1 - \frac{1}{2|AB|}$ when d is odd. If d is even $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_4$ with $m_1 = 1, m_2 = m_3 = m = |AB|$ and by Theorem 1.2 we have

$$W_F = \frac{1}{4}\left(1 - \frac{1}{2|AB|}\right).$$

We now determine A_F. We first consider the case $F(x,y) = ax^{2k} + by^{2k}$, with a and b positive. Then

$$A_F = \iint_{ax^{2k}+by^{2k}\le 1} dxdy.$$

Note that A_F is four times the area of the region with $ax^{2k} + by^{2k} \le 1$ and with x and y non-negative. Make the substitution $ax^{2k} = u, by^{2k} = uv, u, v \ge 0$. Then we see that

$$\begin{aligned}\frac{1}{4}A_F &= \int_0^\infty \int_0^{\frac{1}{v+1}} \frac{1}{4k^2(ab)^{1/2k}} u^{\frac{1}{k}-1} v^{\frac{1}{2k}-1} dudv \\ &= \frac{1}{4k(ab)^{1/2k}} \int_0^\infty \frac{v^{1/2k-1}}{(1+v)^{1/k}} dv\end{aligned}$$

The above integral is $B(1/2k, 1/2k)$ where $B(z,w)$ denotes the Beta function and thus, see 6.2.1 of [10],

$$A_F = \frac{1}{k(ab)^{1/2k}} \frac{\Gamma^2(1/2k)}{\Gamma(1/k)}.$$

Next, we treat the case $F(x,y) = ax^{2k} - by^{2k}$ with a and b positive. The region $\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \le 1\}$ has equal area in each quadrant, so it suffices to estimate the area assuming $x, y \ge 0$. We further divide the region into two, depending on whether $ax^{2k} - by^{2k} \ge 0$ or not. Let $A_F^{(1)}$ denote the area of the region satisfying $x, y \ge 0, 0 \le F(x,y) \le 1$. We make the substitutions $ax^{2k} = u, by^{2k} = uv$ with $u, v \ge 0$. Then

$$\begin{aligned}\frac{1}{8}A_F = A_F^{(1)} &= \iint_{\substack{0\le ax^{2k}-by^{2k}\le 1\\ x,y\ge 0}} dxdy \\ &= \int_0^1 \int_0^{\frac{1}{1-v}} \frac{1}{4k^2(ab)^{1/2k}} u^{\frac{1}{k}-1} v^{\frac{1}{2k}-1} dudv \\ &= \frac{1}{4k(ab)^{1/2k}} \int_0^1 \frac{v^{1/2k-1}}{(1-v)^{1/k}} dv \\ &= \frac{1}{4k(ab)^{1/2k}} \frac{\Gamma(1/2k)\Gamma(1-1/k)}{\Gamma(1-1/2k)}.\end{aligned}$$

Next, we treat the case when $F(x,y) = ax^{2k+1} + by^{2k+1}$. We put $ax^{2k+1} = u$ and $by^{2k+1} = uv$. We thus obtain

$$\begin{aligned}\frac{A_F}{2}|ab|^{1/(2k+1)} &= \frac{1}{2(2k+1)}\int_{-\infty}^{\infty}\frac{|v|^{\frac{1}{2k+1}-1}dv}{|1+v|^{2/(2k+1)}} \\ &= \frac{1}{2(2k+1)}\left(\int_0^{\infty}\frac{v^{-2k/(2k+1)}dv}{(1+v)^{2/(2k+1)}} + \int_0^1 \frac{v^{-2k/(2k+1)}dv}{(1-v)^{2/(2k+1)}} + \int_1^{\infty}\frac{v^{-2k/(2k+1)}dv}{(1-v)^{2/(2k+1)}}\right) \\ &= \frac{1}{2(2k+1)}\left(\frac{\Gamma^2\left(\frac{1}{2k+1}\right)}{\Gamma\left(\frac{2}{2k+1}\right)} + \frac{\Gamma\left(\frac{1}{2k+1}\right)\Gamma\left(\frac{2k-1}{2k+1}\right)}{\Gamma\left(\frac{2k}{2k+1}\right)} + \frac{\Gamma\left(\frac{2k-1}{2k+1}\right)\Gamma\left(\frac{1}{2k+1}\right)}{\Gamma\left(\frac{2k}{2k+1}\right)}\right).\end{aligned}$$

References

[1] M. A. Bean, *The practical computation of areas associated with binary quartic forms*, Mathematics of Computation, (66) **219** (1997), 1269-1293.

[2] M. A. Bennett, N. P. Dummigan, T. D. Wooley, *The representation of integers by binary additive forms*, Compositio Mathematica **111** (1998), 15-33.

[3] E. Bombieri, W. Schmidt, *On Thue's equation*, Invent. Math. **88** (1987), 69-81.

[4] S. Boissire, A. Sarti, *Counting lines on surfaces*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5) **6** (2007), 39-52.

[5] T. D. Browning, *Equal sums of two kth powers*, J. Number Theory **96** (2002), 293-318.

[6] J. Buchmann, U. Vollmer, *Binary Quadratic Forms: An Algebraic Approach*, Springer-Verlag, New York, Berlin, 2007.

[7] D. A. Buell, *Binary Quadratic Forms: Classical Theory and Modern Computations*, Springer-Verlag, New York, Berlin, 1989.

[8] D. A. Cox, *Primes of the form x^2+ny^2: Fermat, Class Field Theory and Complex Multiplication*, John Wiley and Sons, Hoboken, 1989.

[9] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179-183.

[10] P. Davis, *Gamma function and related functions*, Handbook of Mathematical Functions (M. Abramowitz and I. Stegun, eds.), Dover Publications, New York, 1965.

[11] P. Erdős, K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc. **13** (1938), 134-139.

[12] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[13] G. Greaves, *Representation of a number by the sum of two fourth powers*, Mat. Zametki **55** (1994), 47-58.

[14] G. H. Hardy, *Ramanujan. Twelve lectures on subjects suggested by his life and work.* Cambridge Univ. Press, 1940.

[15] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford Univ. Press, 1979.

[16] D. R. Heath-Brown, *The density of rational points on cubic surfaces*, Acta Arith. **79** (1997), 17-30.

[17] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, Annals of Mathematics (2) **155** (2002), 553-598.

[18] C. Hooley, *On binary cubic forms*, J. reine angew. Math. **226** (1967), 30-87.

[19] C. Hooley, *On the numbers that are representable as the sum of two cubes*, J. reine angew. Math. **314** (1980), 146-173.

[20] C. Hooley, *On another sieve method and the numbers that are a sum of two h^{th} powers*, Proc. London Math. Soc. **43** (1981), 73-109.

[21] C. Hooley, *On another sieve method and the numbers that are a sum of two h^{th} powers. II*, J. reine angew. Math. **475** (1996), 55-75.

[22] C. Hooley, *On binary quartic forms*, J. reine angew. Math. **366** (1986), 32-52.

[23] C. Hooley, *On binary cubic forms: II*, J. reine angew. Math. **521** (2000), 185-240.

[24] C. Hooley, *On totally reducible binary forms: I*, Proc. Indian Acad. Sci. (Math. Sci.) **111** (2001), 249-262.
[25] C. Hooley, *On totally reducible binary forms: II*, Hardy-Ramanujan Journal **25** (2002), 22-49.
[26] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch.der Math. u. Phys. **13** (1908), 305-312.
[27] K. Mahler, *Zur Approximation algebraischer Zahlen. III. (Über die mittlere Anzahl der Darstellungen grosser Zahlen durch binäre Formen)*, Acta Math. **62** (1933), 91-166.
[28] M. Newman, *Integral matrices*, Pure and Appl. Math. (S. Eilenberg and P.A.Smith, eds.), vol.45, Academic Press, New York, 1972.
[29] P. Salberger, *Rational points of bounded height on projective surfaces*, Math.Z. **258** (2008), 805-826.
[30] P. Salberger, *Counting rational points on projective varieties*, Preprint, 2009.
[31] P. Salberger, *Uniform bounds for rational points on cubic hypersurfaces*, Arithmetic and Geometry, London Math. Soc. Lecture Note Ser.,**420**, Cambridge University Press, Cambridge (2015), 401-421.
[32] G. Salmon, *A treatise on the analytic geometry of three dimensions*, 4th ed., Hodges, Figgis, and Co., Dublin, 1882.
[33] C. Skinner, T. D. Wooley, *Sums of two k-th powers*, J. reine angew. Math. **462** (1995), 57-68.
[34] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, Journal of the American Mathematical Society, (4) **4** (1991), 793-835.
[35] J. L. Thunder, *Decomposable form inequalities*, Annals of Mathematics (3) **153** (2001), 767-804.
[36] T. D. Wooley, *Sums of two cubes*, Int. Math. Res. Notices. **4** (1995), 181-185.
[37] S. Y. Xiao, *Power-free values of binary forms and the global determinant method*, Int. Math. Res. Notices, Issue 16 Volume 2017, 5078-5135.
[38] S. Y. Xiao, *On binary cubic and quartic forms*, arXiv:1610.09208 [math.NT].
[39] S. Y. Xiao, *Some results on binary forms and counting rational points on algebraic varieties*, Ph.D. Thesis, University of Waterloo, 2016.

Department of Pure Mathematics, University of Waterloo, Waterloo, ON, N2L 3G1, Canada
E-mail address: cstewart@uwaterloo.ca

Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George Street, Room 6290, Toronto, Ontario, Canada, M5S 2E4
E-mail address: syxiao@math.toronto.edu