ON THE REPRESENTATION OF INTEGERS BY BINARY
QUADRATIC FORMS

STANLEY YAO XIAO

Abstract. In this note we show that for a given irreducible binary quadratic form
$f(x, y)$ with integer coefficients, whenever we have $f(x, y) = f(u, v)$ for integers
$x, y, u, v$, there exists a rational automorphism of $f$ which sends $(x, y)$ to $(u, v)$.

1. Introduction

Let $F$ be a binary form with integer coefficients, non-zero discriminant, and degree
d $\geq 2$. We say that an integer $h$ is representable by $F$ if there exist integers $x, y$ such
that $F(x, y) = h$. It is an old question, dating back to Diophantus in the case of sums
of two squares, to determine which integers $h$ are representable by a given form $F$.
While an exact description (for example, in terms of congruence conditions) remain
elusive for all but the simplest of cases, asymptotic results have now been established.
Define
\begin{equation}
R_F(Z) = \{h \in \mathbb{Z} : h \text{ is representable by } F, |h| \leq Z\}
\end{equation}
and $R_F(Z) = \#R_F(Z)$. Landau proved in 1908 that there exists a positive number
$C_1$ such that
\begin{equation}
R_{x^2+y^2}(Z) \sim C_1Z \sqrt{\log Z},
\end{equation}
and shortly after the result was established for all positive definite binary quadratic
forms.

In general, one expects that for a binary form $F$ with degree $d \geq 3$, integer coef-
ficients, and non-zero discriminant, that there exists a positive number $C(F)$ such
that the asymptotic relation
\begin{equation}
R_F(Z) \sim C(F)Z^{\frac{d}{2}}
\end{equation}
holds. It would take over half a century before the analogous asymptotic formula
would be established for non-abelian cubic forms, which was achieved by Hooley. He
proved in [3] that (1.3) holds whenever $F$ is a non-abelian binary cubic form. In
subsequent works [4], [5], he established (1.3) for bi-quadratic binary quartic forms
and abelian binary cubic forms, respectively. In [7], Stewart and Xiao established
(1.3) for all integral binary forms of degree $d \geq 3$ and non-zero discriminant.

For $F$ a binary form of degree $d \geq 2$, define
\[
\text{Aut}_Q F = \left\{ T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \in \text{GL}_2(\mathbb{Q}) : F(x, y) = F(t_1x + t_2y, t_3x + t_4y) \right\}.
\]
The absence of the logarithmic term in (1.3) as opposed to (1.2) is accounted for by
the fact that for a binary form $F$ of degree at least 3, Aut\_Q F is always finite. When
$F$ is a quadratic form, the group $\text{Aut}_Q F$ is infinite.

We say a representable integer $h$ is \textit{essentially represented} if whenever $(x, y), (u, v) \in \mathbb{Z}^2$ are such that $F(x, y) = F(u, v) = h$, there exists $T \in \text{Aut}_Q F$ such that $(x, y) = T(u, v)$. Note that if $F(x, y) = h$ has a unique solution, then $h$ is essentially represented since $(1, 0) \in \text{Aut}_Q F$. Put

$$R_F^{(1)}(Z) = \{ h \in R_F(Z) : h \text{ is essentially represented} \}$$

and $R_F(Z) = \#R_F^{(1)}(Z)$. In the $d \geq 3$ case Heath-Brown showed in [2] that there exists $\eta_d > 0$, depending only on the degree $d$, such that for all $\varepsilon > 0$

$$R_F(Z) = R_F^{(1)}(Z) \left( 1 + O_\varepsilon \left( Z^{-\eta_d + \varepsilon} \right) \right).$$

This is essentially reduces the question of enumerating $R_F(Z)$ to that of $R_F^{(1)}(Z)$, which is far simpler, and the key to our success in [7]. Heath-Brown’s theorem does not address the case of quadratic forms, which we do so now:

\textbf{Theorem 1.1.} Let $f$ be an irreducible and primitive binary quadratic form. Then every integer $h$ representable by $f$ is essentially represented.

Consider the quadric surface $X_f$ defined by

$$X_f : f(x_1, x_2) = f(x_3, x_4).$$

In [2], Heath-Brown showed that lines on $X_f$ correspond to automorphisms of $f$, possibly defined over a larger field. His result and our Theorem 1.1 has the following consequence:

\textbf{Corollary 1.2.} Let $X_f$ be the surfaced defined by $f(x_1, x_2) = f(x_3, x_4)$, with $f$ a binary quadratic form with integer coefficients and non-zero discriminant. Then every point in $X_f(\mathbb{Q})$ lies on a rational line contained in $X_f$.

It has been pointed out to the author that Theorem 1.1 essentially follows from Witt’s theorem (see Theorem 42.16 in [1]). Nevertheless, we feel that this result is of independent interest to number theorists and does not appear to be well-known.

\section{2. Preliminary lemmas}

The strategy is very simple: for a given pair of integers $(x, y), (u, v)$ such that $f(x, y) = f(u, v)$, we exhibit an explicit automorphism of $f$ which sends $(x, y)$ to $(u, v)$. In fact, we will draw such an automorphism from a proper subgroup of $\text{Aut}_Q f$. Put

$$f(x, y) = f_2 x^2 + f_1 xy + f_0 y^2,$$

and put

$$\delta = \left| \frac{f_1^2 - 4 f_2 f_0}{4} \right|.$$
2.1. **Positive definite binary quadratic forms.** In this case, we shall pick our $T$ from the group $\text{Aut}_\mathbb{Q} f \cap SO_f(\mathbb{R})$, where

$$SO_f(\mathbb{R}) = \{ T \in \text{GL}_2(\mathbb{R}) : \det T = 1, fT = f \}.$$ 

The group $SO_f(\mathbb{R})$ is conjugate to the special orthogonal group $SO_2(\mathbb{R})$ and its elements look like

$$T_f(t) = \left( \begin{array}{cc} \cos t + \frac{f_1 \sin t}{2\sqrt{\delta}} & \frac{f_0 \sin t}{\sqrt{\delta}} \\ \frac{-f_2 \sin t}{\sqrt{\delta}} & \cos t - \frac{f_1 \sin t}{2\sqrt{\delta}} \end{array} \right), t \in [0, 2\pi).$$

If we demand that $T_f(t) \in \text{GL}_2(\mathbb{Q})$, then it follows that $\cos t \in \mathbb{Q}$ and $\sqrt{\delta} \sin t \in \mathbb{Q}$. Put

$$u = \cos t, v = \frac{\sin t}{\sqrt{\delta}}.$$ 

Then $u, v$ satisfy the equation

$$u^2 + \delta v^2 = 1.$$ 

Put $E_\delta$ for the curve defined by

$$(2.1) \quad E_\delta : x^2 + \delta y^2 = 1.$$ 

We then see that there is a bijection between rational points on $E_\delta$ and rational elements $T \in \text{Aut}_\mathbb{Q} f$. We now characterize the set of rational points on $E_\delta$.

**Lemma 2.1.** Let $E_\delta$ be the curve given by (2.1), with $4\delta$ a positive integer. Then the set of rational points on $E_\delta$ is given by the parametrization

$$\left( \frac{\delta p^2 - q^2}{\delta p^2 + q^2}, \frac{2pq}{\delta p^2 + q^2} \right), p, q \in \mathbb{Z}, q > 0, \gcd(p, q) = 1.$$ 

**Proof.** Using the fact that $(1, 0)$ is a point on the curve $E_\delta$, we use the slope method to find all other rational points. Indeed, the intersection of the line given by

$$y = m(x - 1), m \in \mathbb{Q}$$

and the curve $E_\delta$ is another rational point on $E_\delta$, and all such points arise this way. Substituting, we find that

$$x^2 + \delta(m(x - 1))^2 = 1$$

is equivalent to

$$x = \frac{\delta m^2 \pm 1}{\delta m^2 + 1}.$$ 

The $+$ sign gives $x = 1$, and the $-$ sign gives

$$x = \frac{\delta m^2 - 1}{\delta m^2 + 1}$$

which corresponds to the point

$$(x, y) = \left( \frac{\delta m^2 - 1}{\delta m^2 + 1}, \frac{2m}{\delta m^2 + 1} \right).$$
If we write the slope $m$ as $m = p/q$, where $q > 0$ and $\gcd(p, q) = 1$, then the point can be given as

$$(x, y) = \left(\frac{\delta p^2 - q^2}{\delta p^2 + q^2}, \frac{2pq}{\delta p^2 + q^2}\right),$$
as desired. $\square$

2.2. **Indefinite binary quadratic forms.** In this case, the group $SO_f(\mathbb{R})$ is no longer connected, and we shall focus on the principal branch of $SO_f(\mathbb{R})$, which is the branch containing the identity matrix. This branch can be identified as the set of matrices of the form

$$T_f(t) = \begin{pmatrix}
\cosh t - \frac{f_1 \sinh t}{2\sqrt{\delta}} & -\frac{f_0 \sinh t}{\sqrt{\delta}} \\
\frac{f_2 \sinh t}{\sqrt{\delta}} & \cosh t + \frac{f_1 \sinh t}{2\sqrt{\delta}}
\end{pmatrix}, t \in \mathbb{R}.
$$

Again, if we demand that $T_f(t) \in \text{GL}_2(\mathbb{Q})$, then necessarily $\cosh t, \sqrt{\delta} \sinh t \in \mathbb{Q}$. Put $u = \cosh t, v = \frac{\sinh t}{\sqrt{\delta}}$.

Notice that $(u, v)$ lies on the curve

$$(2.2) \quad E_\delta : x^2 - \delta y^2 = 1.
$$

It is immediate that there is a bijection between the set of rational points $E_\delta(\mathbb{Q})$ and elements in $SO_f(\mathbb{Q})$. We have the following characterization of the rational points on $E_\delta$:

**Lemma 2.2.** Let $E_\delta$ be the curve given by (2.2). Then the set of rational points $E_\delta(\mathbb{Q})$ are given by the parametrization

$$(\delta p^2 + q^2, \frac{2pq}{\delta p^2 - q^2}; \frac{2pq}{\delta p^2 + q^2}), p, q \in \mathbb{Z}, q > 0, \gcd(p, q) = 1.
$$

**Proof.** Same as Lemma 2.1. $\square$

### 3. Proof of Theorem 1.1

We first address the case when $f$ is positive definite. Let $h$ be a representable integer of $f$. If there exists exactly one pair of integers $(x, y)$ such that $f(x, y) = h$, then $h$ is essentially represented. Now suppose there exist distinct representations $(x, y), (u, v)$ of $h$, so that

$$(3.1) \quad h = f(x, y) = f(u, v).
$$

Put

$$m = 2f_2ux + f_1(uy + vx) + 2f_0vy - 2h, n = 2\delta(uy - vx)
$$

and

$$T_f(m, n) = \frac{1}{\delta m^2 + n^2} \begin{pmatrix}
\delta m^2 - n^2 + f_1mn & \frac{2f_0mn}{\delta m^2 - n^2 - f_1mn} \\
-2f_2mn & \delta m^2 - n^2 - f_1mn
\end{pmatrix} \in \text{Aut}_\mathbb{Q} f.
$$

Observe that

$$(\delta m^2 - n^2 + f_1mn)x + 2f_0mny = hm\delta u$$
and

\[-2f_2mnx + (\delta m^2 - n^2 - f_1mn)y = hm\delta v.\]

Moreover, by expanding, we see that

\[\delta m^2 + n^2 = hm\delta.\]

It then follows that

\[T_f(m, n) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}.\]

The proof of the theorem when \( f \) is indefinite is similar, but we include the full argument for the sake of completeness. Suppose that (3.1) holds and put

\[m = 2f_2ux + f_1(uy + vx) + 2f_0vy - 2h, \quad n = 2\delta(vx - uy).\]

Then the associated \( T_f(m, n) \in \text{Aut}_\mathbb{Q} f \) is given by

\[T_f(m, n) = \frac{1}{\delta m^2 - n^2} \begin{pmatrix} \delta m^2 + n^2 - f_1mn & -2f_0mn \\ 2f_2mn & \delta m^2 + n^2 + f_1mn \end{pmatrix}.\]

A routine calculation then yields that

\[T_f(m, n) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix},\]

as desired.
References

[1] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, New York, 1978.
[2] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, Annals of Mathematics (2) **155** (2002), 553-598.
[3] C. Hooley, *On binary cubic forms*, J. reine angew. Math. **226** (1967), 30-87.
[4] C. Hooley, *On binary quartic forms*, J. reine angew. Math. **366** (1986), 32-52.
[5] C. Hooley, *On binary cubic forms: II*, J. reine angew. Math. **521** (2000), 185-240.
[6] C. L. Stewart, *On the number of solutions to polynomial congruences and Thue equations*, Journal of the American Mathematical Society, (4) **4** (1991), 793-835.
[7] C. L. Stewart, S. Y. Xiao, *On the representation of integers by binary forms*, arXiv:1605.03427 [math.NT].
[8] S. Y. Xiao, *On binary cubic and quartic forms*, arXiv:1610.09208 [math.NT].

Mathematical Institute, University of Oxford, Oxford, OX2 6GG, United Kingdom

*E-mail address*: stanley.xiao@maths.ox.ac.uk