Value sets of binary forms

Peter Koymans
Utrecht University

Debrecen Online Number Theory Seminar

11 October 2024

The value set

Definition (Value set)

Let $F \in \mathbb{Z}[X, Y]$ *be a binary form. Define*

$$\mathrm{Val}(F) := \{F(x, y) : (x, y) \in \mathbb{Z}^2\}.$$

For two forms $F, G \in \mathbb{Z}[X, Y]$*, we say* $F \sim_{\mathsf{val}} G$ *if* $\mathrm{Val}(F) = \mathrm{Val}(G)$.

The value set

Definition (Value set)

Let $F \in \mathbb{Z}[X, Y]$ *be a binary form. Define*

$$\mathrm{Val}(F) := \{F(x, y) : (x, y) \in \mathbb{Z}^2\}.$$

For two forms $F, G \in \mathbb{Z}[X, Y]$, *we say* $F \sim_{\mathsf{val}} G$ *if* $\mathrm{Val}(F) = \mathrm{Val}(G)$. *We denote by* $[F]_{\mathsf{val}}$ *the resulting equivalence class of* F.

The value set

Definition (Value set)

Let $F \in \mathbb{Z}[X, Y]$ *be a binary form. Define*

$$\mathrm{Val}(F) := \{F(x, y) : (x, y) \in \mathbb{Z}^2\}.$$

For two forms $F, G \in \mathbb{Z}[X, Y]$*, we say* $F \sim_{\mathsf{val}} G$ *if* $\mathrm{Val}(F) = \mathrm{Val}(G)$*. We denote by* $[F]_{\mathsf{val}}$ *the resulting equivalence class of* F*.*

Value sets of binary quadratic forms are classical topics of study.

The value set

Definition (Value set)

Let $F \in \mathbb{Z}[X, Y]$ *be a binary form. Define*

$$\mathrm{Val}(F) := \{F(x, y) : (x, y) \in \mathbb{Z}^2\}.$$

For two forms $F, G \in \mathbb{Z}[X, Y]$*, we say* $F \sim_{\mathrm{val}} G$ *if* $\mathrm{Val}(F) = \mathrm{Val}(G)$*. We denote by* $[F]_{\mathrm{val}}$ *the resulting equivalence class of* F*.*

Value sets of binary quadratic forms are classical topics of study.

Example (Fermat)

We have

$$\mathrm{Val}(X^2 + Y^2) = \{n \in \mathbb{Z}_{>0} : p \mid n \text{ and } p \equiv 3 \bmod 4 \Rightarrow v_p(n) \equiv 0 \bmod 2\}.$$

The value set

Definition (Value set)

Let $F \in \mathbb{Z}[X, Y]$ *be a binary form. Define*

$$\mathrm{Val}(F) := \{F(x, y) : (x, y) \in \mathbb{Z}^2\}.$$

For two forms $F, G \in \mathbb{Z}[X, Y]$, *we say* $F \sim_{\mathrm{val}} G$ *if* $\mathrm{Val}(F) = \mathrm{Val}(G)$. *We denote by* $[F]_{\mathrm{val}}$ *the resulting equivalence class of* F.

Value sets of binary quadratic forms are classical topics of study.

Example (Fermat)

We have

$$\mathrm{Val}(X^2 + Y^2) = \{n \in \mathbb{Z}_{>0} : p \mid n \text{ and } p \equiv 3 \bmod 4 \Rightarrow v_p(n) \equiv 0 \bmod 2\}.$$

Class field theory gives an explicit description of $\mathrm{Val}(F)$ for F binary quadratic. However, much less is known if $\deg(F) \geq 3$.

Equivalence of forms

Recall that two binary forms $F, G \in \mathbb{Z}[X, Y]$ are $GL_2(\mathbb{Z})$–equivalent, written $F \sim_{GL_2(\mathbb{Z})} G$, if there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ with

$$F(\gamma(X, Y)) = F(aX + bY, cX + dY) = G(X, Y).$$

Equivalence of forms

Recall that two binary forms $F, G \in \mathbb{Z}[X, Y]$ are $GL_2(\mathbb{Z})$–equivalent, written $F \sim_{GL_2(\mathbb{Z})} G$, if there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ with

$$F(\gamma(X, Y)) = F(aX + bY, cX + dY) = G(X, Y).$$

Lemma

If $F \sim_{GL_2(\mathbb{Z})} G$, then $F \sim_{\mathrm{val}} G$. Hence

$$[F]_{GL_2(\mathbb{Z})} \subseteq [F]_{\mathrm{val}}. \tag{1}$$

Equivalence of forms

Recall that two binary forms $F, G \in \mathbb{Z}[X, Y]$ are $GL_2(\mathbb{Z})$–equivalent, written $F \sim_{GL_2(\mathbb{Z})} G$, if there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ with

$$F(\gamma(X, Y)) = F(aX + bY, cX + dY) = G(X, Y).$$

Lemma

If $F \sim_{GL_2(\mathbb{Z})} G$, then $F \sim_{\mathrm{val}} G$. Hence

$$[F]_{GL_2(\mathbb{Z})} \subseteq [F]_{\mathrm{val}}. \tag{1}$$

Proof.

This follows from the fact that all $\gamma \in GL_2(\mathbb{Z})$ permute $\mathbb{Z}^2$. □

Equivalence of forms

Recall that two binary forms $F, G \in \mathbb{Z}[X, Y]$ are $GL_2(\mathbb{Z})$–equivalent, written $F \sim_{GL_2(\mathbb{Z})} G$, if there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ with

$$F(\gamma(X, Y)) = F(aX + bY, cX + dY) = G(X, Y).$$

Lemma

If $F \sim_{GL_2(\mathbb{Z})} G$, then $F \sim_{\text{val}} G$. Hence

$$[F]_{GL_2(\mathbb{Z})} \subseteq [F]_{\text{val}}. \tag{1}$$

Proof.

This follows from the fact that all $\gamma \in GL_2(\mathbb{Z})$ permute $\mathbb{Z}^2$. □

The main question of today is: when is the inclusion (1) strict?

An example

Example

Take $F(X,Y) = X^3 - 3XY^2 - Y^3$ *and* $R := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. *One checks*

An example

Example

Take $F(X, Y) = X^3 - 3XY^2 - Y^3$ *and* $R := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. *One checks*

- *we have* $F \circ R = F$,

An example

Example

Take $F(X,Y) = X^3 - 3XY^2 - Y^3$ *and* $R := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. *One checks*

- *we have* $F \circ R = F$,
- *we have* $R^3 = \mathrm{id}$.

An example

Example

Take $F(X,Y) = X^3 - 3XY^2 - Y^3$ *and* $R := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. *One checks*

- *we have* $F \circ R = F$,
- *we have* $R^3 = \mathrm{id}$.

Let $G(X,Y) := F(2X, Y)$.

An example

Example

Take $F(X,Y) = X^3 - 3XY^2 - Y^3$ *and* $R := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. *One checks*

- *we have* $F \circ R = F$,
- *we have* $R^3 = \mathrm{id}$.

Let $G(X,Y) := F(2X, Y)$.

Lemma

We have $\mathrm{Val}(F) = \mathrm{Val}(G)$, *but* $F \not\sim_{GL_2(\mathbb{Z})} G$ *by looking at discriminants. In particular,* $[F]_{GL_2(\mathbb{Z})} \subsetneq [F]_{\mathrm{val}}$.

Proof of lemma

Recall $F(X,Y) = X^3 - 3XY^2 - Y^3$, $R := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $F \circ R = F$ and $G(X,Y) := F(2X,Y)$. We must prove $\mathrm{Val}(F) = \mathrm{Val}(G)$.

Proof.

Clearly, $\mathrm{Val}(G) \subseteq \mathrm{Val}(F)$, so suffices to show $\mathrm{Val}(F) \subseteq \mathrm{Val}(G)$.

Proof of lemma

Recall $F(X, Y) = X^3 - 3XY^2 - Y^3$, $R := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $F \circ R = F$ and $G(X, Y) := F(2X, Y)$. We must prove $\mathrm{Val}(F) = \mathrm{Val}(G)$.

Proof.

Clearly, $\mathrm{Val}(G) \subseteq \mathrm{Val}(F)$, so suffices to show $\mathrm{Val}(F) \subseteq \mathrm{Val}(G)$. Take $z \in \mathrm{Val}(F)$, so $z = F(x, y)$ for some $x, y \in \mathbb{Z}$. Exploiting $F = F \circ R = F \circ R^2$, we get

$$z = F(x, y) = F(y, -x - y) = F(-x - y, x).$$

Proof of lemma

Recall $F(X, Y) = X^3 - 3XY^2 - Y^3$, $R := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $F \circ R = F$ and $G(X, Y) := F(2X, Y)$. We must prove $\mathrm{Val}(F) = \mathrm{Val}(G)$.

Proof.

Clearly, $\mathrm{Val}(G) \subseteq \mathrm{Val}(F)$, so suffices to show $\mathrm{Val}(F) \subseteq \mathrm{Val}(G)$. Take $z \in \mathrm{Val}(F)$, so $z = F(x, y)$ for some $x, y \in \mathbb{Z}$. Exploiting $F = F \circ R = F \circ R^2$, we get

$$z = F(x, y) = F(y, -x - y) = F(-x - y, x).$$

Now at least one of $x, y, -x - y$ is even, say $x = 2m$. Then

$$z = F(x, y) = F(2m, y) = G(m, y),$$

so $z \in \mathrm{Val}(G)$, as desired. □

Our main result

Theorem (K.–Fouvry)

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $d \geq 3$, and assume $\mathrm{disc}(F) \neq 0$. Then $[F]_{\mathsf{val}}$ consists of one or two $GL_2(\mathbb{Z})$–equivalence classes.

Our main result

Theorem (K.–Fouvry)

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $d \geq 3$, and assume $\mathrm{disc}(F) \neq 0$. Then $[F]_{\mathrm{val}}$ consists of one or two $GL_2(\mathbb{Z})$–equivalence classes. It consists of two classes if and only if there exists $G \in [F]_{\mathrm{val}}$ and $\sigma \in \mathrm{Aut}(G) := \{\gamma \in GL_2(\mathbb{Q}) : G \circ \gamma = G\}$ satisfying:

- *σ has order exactly 3,*
- *$\sigma \in GL_2(\mathbb{Z})$.*

Our main result

Theorem (K.–Fouvry)

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $d \geq 3$, and assume $\mathrm{disc}(F) \neq 0$. Then $[F]_{\mathrm{val}}$ consists of one or two $GL_2(\mathbb{Z})$–equivalence classes. It consists of two classes if and only if there exists $G \in [F]_{\mathrm{val}}$ and $\sigma \in \mathrm{Aut}(G) := \{\gamma \in GL_2(\mathbb{Q}) : G \circ \gamma = G\}$ satisfying:

- *σ has order exactly 3,*
- *$\sigma \in GL_2(\mathbb{Z})$.*

Furthermore, in this case

$$[F]_{\mathrm{val}} = [G(X, Y)]_{GL_2(\mathbb{Z})} \cup [G(2X, Y)]_{GL_2(\mathbb{Z})}.$$

Remark.

- We prove a similar result if $d = 2$.

Our main result

Theorem (K.–Fouvry)

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $d \geq 3$, and assume $\mathrm{disc}(F) \neq 0$. Then $[F]_{\mathrm{val}}$ consists of one or two $GL_2(\mathbb{Z})$–equivalence classes. It consists of two classes if and only if there exists $G \in [F]_{\mathrm{val}}$ and $\sigma \in \mathrm{Aut}(G) := \{\gamma \in GL_2(\mathbb{Q}) : G \circ \gamma = G\}$ satisfying:

- *σ has order exactly 3,*
- *$\sigma \in GL_2(\mathbb{Z})$.*

Furthermore, in this case

$$[F]_{\mathrm{val}} = [G(X, Y)]_{GL_2(\mathbb{Z})} \cup [G(2X, Y)]_{GL_2(\mathbb{Z})}.$$

Remark.

- We prove a similar result if $d = 2$.
- The possibilities for $\mathrm{Aut}(G)$ have been classified (as an abstract group). In particular, $|\mathrm{Aut}(G)| \leq 12$.

Our main result

Theorem (K.–Fouvry)

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $d \geq 3$, and assume $\mathrm{disc}(F) \neq 0$. Then $[F]_{\mathrm{val}}$ consists of one or two $GL_2(\mathbb{Z})$–equivalence classes. It consists of two classes if and only if there exists $G \in [F]_{\mathrm{val}}$ and $\sigma \in \mathrm{Aut}(G) := \{\gamma \in GL_2(\mathbb{Q}) : G \circ \gamma = G\}$ satisfying:

- *σ has order exactly 3,*
- *$\sigma \in GL_2(\mathbb{Z})$.*

Furthermore, in this case

$$[F]_{\mathrm{val}} = [G(X, Y)]_{GL_2(\mathbb{Z})} \cup [G(2X, Y)]_{GL_2(\mathbb{Z})}.$$

Remark.

- We prove a similar result if $d = 2$.
- The possibilities for $\mathrm{Aut}(G)$ have been classified (as an abstract group). In particular, $|\mathrm{Aut}(G)| \leq 12$.
- Generically, we have $\mathrm{Aut}(F) = \{\mathrm{id}\}$ for d odd, $\mathrm{Aut}(F) = \{\mathrm{id}, -\mathrm{id}\}$ for d even. In particular, we generically have $[F]_{GL_2(\mathbb{Z})} = [F]_{\mathrm{val}}$.

Counting value sets

Theorem (Stewart–Xiao, "Asymptotic density of value sets")

Let F be a binary form with non-zero discriminant of degree $d \geq 3$. Then there exists $C > 0$ such that

$$|\{|h| \leq Z : h = F(x, y) \text{ for some } (x, y) \in \mathbb{Z}^2\}| \sim CZ^{2/d}.$$

Counting value sets

Theorem (Stewart–Xiao, "Asymptotic density of value sets")

Let F be a binary form with non-zero discriminant of degree $d \geq 3$. Then there exists $C > 0$ such that

$$|\{|h| \leq Z : h = F(x, y) \text{ for some } (x, y) \in \mathbb{Z}^2\}| \sim CZ^{2/d}.$$

Although we shall not directly use the full strength of this result, we use many classical techniques for counting asymptotic densities of value sets.

Counting value sets

Theorem (Stewart–Xiao, "Asymptotic density of value sets")

Let F be a binary form with non-zero discriminant of degree $d \geq 3$. Then there exists $C > 0$ such that

$$|\{|h| \leq Z : h = F(x, y) \text{ for some } (x, y) \in \mathbb{Z}^2\}| \sim CZ^{2/d}.$$

Although we shall not directly use the full strength of this result, we use many classical techniques for counting asymptotic densities of value sets.

Of particular importance for us is the determinant method developed by Heath-Brown, Salberger etc.

High level proof strategy

Consider the surface $S \subseteq \mathbb{P}^3$ defined by

$$F(X, Y) = G(Z, W).$$

High level proof strategy

Consider the surface $S \subseteq \mathbb{P}^3$ defined by

$$F(X, Y) = G(Z, W).$$

The key proof idea is that $\mathrm{Val}(F) = \mathrm{Val}(G)$ gives an abundance of rational points on S.

High level proof strategy

Consider the surface $S \subseteq \mathbb{P}^3$ defined by

$$F(X, Y) = G(Z, W).$$

The key proof idea is that $\mathrm{Val}(F) = \mathrm{Val}(G)$ gives an abundance of rational points on S.

However, the determinant method shows that the rational points can only come in a rather structured way, namely from the lines on the surface.

High level proof strategy

Consider the surface $S \subseteq \mathbb{P}^3$ defined by

$$F(X, Y) = G(Z, W).$$

The key proof idea is that $\mathrm{Val}(F) = \mathrm{Val}(G)$ gives an abundance of rational points on S.

However, the determinant method shows that the rational points can only come in a rather structured way, namely from the lines on the surface.

The lines on the surface have been classified, which will then turn our problem into a question of lattice coverings.

Detailed proof strategy

Step 1: use the determinant method to show that almost all points on S come from the lines lying on the surface.

Detailed proof strategy

Step 1: use the determinant method to show that almost all points on S come from the lines lying on the surface.

Step 2: classify the complex lines $L \subseteq \mathbb{P}^3(\mathbb{C})$ on S.

Proposition (Boissière–Sarti)

The lines $L \subseteq \mathbb{P}^3(\mathbb{C})$ *on* S *are:*

Detailed proof strategy

Step 1: use the determinant method to show that almost all points on S come from the lines lying on the surface.

Step 2: classify the complex lines $L \subseteq \mathbb{P}^3(\mathbb{C})$ on S.

Proposition (Boissière–Sarti)

The lines $L \subseteq \mathbb{P}^3(\mathbb{C})$ on S are:

- *There exists $(x_1 : x_2)$ with $F(x_1, x_2) = 0$ and $(x_3 : x_4)$ with $G(x_3 : x_4) = 0$, and L is the unique line going through $(x_1 : x_2 : 0 : 0)$ and $(0 : 0 : x_3 : x_4)$.*

Detailed proof strategy

Step 1: use the determinant method to show that almost all points on S come from the lines lying on the surface.

Step 2: classify the complex lines $L \subseteq \mathbb{P}^3(\mathbb{C})$ on S.

Proposition (Boissière–Sarti)

The lines $L \subseteq \mathbb{P}^3(\mathbb{C})$ on S are:

- *There exists $(x_1 : x_2)$ with $F(x_1, x_2) = 0$ and $(x_3 : x_4)$ with $G(x_3 : x_4) = 0$, and L is the unique line going through $(x_1 : x_2 : 0 : 0)$ and $(0 : 0 : x_3 : x_4)$.*
- *There exists $\rho \in GL_2(\mathbb{C})$ with $G \circ \rho = F$ such that the line L_ρ has the parametric equation $L_\rho : (u, v) \in \mathbb{C}^2 \mapsto (u, v, \rho(u, v))$.*

Detailed proof strategy

Step 1: use the determinant method to show that almost all points on S come from the lines lying on the surface.

Step 2: classify the complex lines $L \subseteq \mathbb{P}^3(\mathbb{C})$ on S.

Proposition (Boissière–Sarti)

The lines $L \subseteq \mathbb{P}^3(\mathbb{C})$ on S are:

- *There exists $(x_1 : x_2)$ with $F(x_1, x_2) = 0$ and $(x_3 : x_4)$ with $G(x_3 : x_4) = 0$, and L is the unique line going through $(x_1 : x_2 : 0 : 0)$ and $(0 : 0 : x_3 : x_4)$.*
- *There exists $\rho \in GL_2(\mathbb{C})$ with $G \circ \rho = F$ such that the line L_ρ has the parametric equation $L_\rho : (u, v) \in \mathbb{C}^2 \mapsto (u, v, \rho(u, v))$.*

Note: if $(z_1 : z_2 : z_3 : z_4)$ is a point on a line of type 1, then $F(z_1, z_2) = G(z_3, z_4) = 0$. Lines of type 1 will contribute negligibly to the total point count.

Detailed proof strategy II

Step 3: show that the lines L_ρ with $\rho \in GL_2(\mathbb{C}) - GL_2(\mathbb{Q})$ contribute negligibly to the number of rational points. From Step 1, 2, 3, we will deduce the key claim:

Detailed proof strategy II

Step 3: show that the lines L_ρ with $\rho \in GL_2(\mathbb{C}) - GL_2(\mathbb{Q})$ contribute negligibly to the number of rational points. From Step 1, 2, 3, we will deduce the key claim:

Theorem (K.–Fouvry, "The lattice theorem")

Let F, G with $\mathrm{Val}(F) = \mathrm{Val}(G)$, and let $\rho \in GL_2(\mathbb{Q})$ satisfy $F = G \circ \rho$.

Detailed proof strategy II

Step 3: show that the lines L_ρ with $\rho \in GL_2(\mathbb{C}) - GL_2(\mathbb{Q})$ contribute negligibly to the number of rational points. From Step 1, 2, 3, we will deduce the key claim:

Theorem (K.–Fouvry, "The lattice theorem")

Let F, G with $\mathrm{Val}(F) = \mathrm{Val}(G)$, and let $\rho \in GL_2(\mathbb{Q})$ satisfy $F = G \circ \rho$. Then

$$\mathbb{Z}^2 = \bigcup_{\sigma_1 \in \mathrm{Aut}(F)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma_1 \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

and

$$\mathbb{Z}^2 = \bigcup_{\sigma_2 \in \mathrm{Aut}(G)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \sigma_2\rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

Detailed proof strategy II

Step 3: show that the lines L_ρ with $\rho \in GL_2(\mathbb{C}) - GL_2(\mathbb{Q})$ contribute negligibly to the number of rational points. From Step 1, 2, 3, we will deduce the key claim:

Theorem (K.–Fouvry, "The lattice theorem")

Let F, G with $\mathrm{Val}(F) = \mathrm{Val}(G)$, and let $\rho \in GL_2(\mathbb{Q})$ satisfy $F = G \circ \rho$. Then

$$\mathbb{Z}^2 = \bigcup_{\sigma_1 \in \mathrm{Aut}(F)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma_1 \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

and

$$\mathbb{Z}^2 = \bigcup_{\sigma_2 \in \mathrm{Aut}(G)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \sigma_2\rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

Remark. The first and second equality mean that $\mathbb{Z}^2$ is the union of sublattices of $\mathbb{Z}^2$ indexed by $\mathrm{Aut}(F)$ respectively $\mathrm{Aut}(G)$.

Detailed proof strategy II

Step 3: show that the lines L_ρ with $\rho \in GL_2(\mathbb{C}) - GL_2(\mathbb{Q})$ contribute negligibly to the number of rational points. From Step 1, 2, 3, we will deduce the key claim:

Theorem (K.–Fouvry, "The lattice theorem")

Let F, G with $\mathrm{Val}(F) = \mathrm{Val}(G)$, and let $\rho \in GL_2(\mathbb{Q})$ satisfy $F = G \circ \rho$. Then

$$\mathbb{Z}^2 = \bigcup_{\sigma_1 \in \mathrm{Aut}(F)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma_1 \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

and

$$\mathbb{Z}^2 = \bigcup_{\sigma_2 \in \mathrm{Aut}(G)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \sigma_2\rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

Remark. The first and second equality mean that $\mathbb{Z}^2$ is the union of sublattices of $\mathbb{Z}^2$ indexed by $\mathrm{Aut}(F)$ respectively $\mathrm{Aut}(G)$.
Remark. Such a ρ must exist, since $\mathrm{Val}(F) = \mathrm{Val}(G)$ implies that S has many rational points, so by Step 1, 2, 3, there must be such a ρ.

Proof of lattice theorem assuming Step 1, 2, 3

We show

$$\mathbb{Z}^2 = \bigcup_{\sigma_1 \in \mathrm{Aut}(F)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma_1 \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} =: U.$$

Proof of lattice theorem assuming Step 1, 2, 3

We show

$$\mathbb{Z}^2 = \bigcup_{\sigma_1 \in \mathrm{Aut}(F)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma_1 \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} =: U.$$

The inclusion $\supseteq$ is obvious, so we prove $\subseteq$. Suppose not. Then there exists $M > 1$, c_1, c_2 such that

$$\mathcal{E} := \{(u, v) \in \mathbb{Z}^2 : u \equiv c_1 \bmod M, v \equiv c_2 \bmod M\}$$

is disjoint from U.

Proof of lattice theorem assuming Step 1, 2, 3

We show

$$\mathbb{Z}^2 = \bigcup_{\sigma_1 \in \mathrm{Aut}(F)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma_1 \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} =: U.$$

The inclusion $\supseteq$ is obvious, so we prove $\subseteq$. Suppose not. Then there exists $M > 1$, c_1, c_2 such that

$$\mathcal{E} := \{(u, v) \in \mathbb{Z}^2 : u \equiv c_1 \bmod M, v \equiv c_2 \bmod M\}$$

is disjoint from U. Using that $\mathrm{Val}(F) = \mathrm{Val}(G)$, we get for $(u, v) \in \mathcal{E}$ that there exists (m, n) with $F(u, v) = G(m, n)$. We get many rational points on S in this way.

Proof of lattice theorem assuming Step 1, 2, 3

We show

$$\mathbb{Z}^2 = \bigcup_{\sigma_1 \in \mathrm{Aut}(F)} \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma_1 \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} =: U.$$

The inclusion $\supseteq$ is obvious, so we prove $\subseteq$. Suppose not. Then there exists $M > 1$, c_1, c_2 such that

$$\mathcal{E} := \{(u, v) \in \mathbb{Z}^2 : u \equiv c_1 \bmod M, v \equiv c_2 \bmod M\}$$

is disjoint from U. Using that $\mathrm{Val}(F) = \mathrm{Val}(G)$, we get for $(u, v) \in \mathcal{E}$ that there exists (m, n) with $F(u, v) = G(m, n)$. We get many rational points on S in this way.

By Step 1, 2, 3, such rational points must lie on the rational lines of S, which are $\{\rho\sigma_1 : \sigma_1 \in \mathrm{Aut}(F)\}$. But the points on $\mathcal{E}$ are not on such lines, contradiction.

The main result for trivial automorphism group

The "lattice theorem" is extremely useful. For example, if $\mathrm{Aut}(F) = \mathrm{id}$, we get

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

The main result for trivial automorphism group

The "lattice theorem" is extremely useful. For example, if $\mathrm{Aut}(F) = \mathrm{id}$, we get

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

and

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

The main result for trivial automorphism group

The "lattice theorem" is extremely useful. For example, if $\mathrm{Aut}(F) = \mathrm{id}$, we get

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

and

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

This implies that $\rho(\mathbb{Z}^2) \subseteq \mathbb{Z}^2$ and $\rho^{-1}(\mathbb{Z}^2) \subseteq \mathbb{Z}^2$. So ρ and ρ^{-1} have integer coefficients.

The main result for trivial automorphism group

The "lattice theorem" is extremely useful. For example, if $\mathrm{Aut}(F) = \text{id}$, we get

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

and

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

This implies that $\rho(\mathbb{Z}^2) \subseteq \mathbb{Z}^2$ and $\rho^{-1}(\mathbb{Z}^2) \subseteq \mathbb{Z}^2$. So ρ and ρ^{-1} have integer coefficients.

This means precisely that $\rho \in GL_2(\mathbb{Z})$, so F and G are $GL_2(\mathbb{Z})$–equivalent.

The main result for automorphism group C_2

This argument also works if

$$\mathrm{Aut}(F) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} =: \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma \right\},$$

i.e. $F(X, Y) = F(Y, X)$.

The main result for automorphism group C_2

This argument also works if

$$\mathrm{Aut}(F) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} =: \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma \right\},$$

i.e. $F(X, Y) = F(Y, X)$. In this case

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

The main result for automorphism group C_2

This argument also works if

$$\mathrm{Aut}(F) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} =: \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma \right\},$$

i.e. $F(X, Y) = F(Y, X)$. In this case

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

and

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \sigma\rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

The main result for automorphism group C_2

This argument also works if

$$\mathrm{Aut}(F) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} =: \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma \right\},$$

i.e. $F(X, Y) = F(Y, X)$. In this case

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho\sigma \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}$$

and

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : \sigma\rho^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

However, if lattices $L_1, L_2 \subseteq \mathbb{Z}^2$ satisfy $L_1 \cup L_2 = \mathbb{Z}^2$, then $L_1 = \mathbb{Z}^2$ or $L_2 = \mathbb{Z}^2$. This still implies that F, G are $GL_2(\mathbb{Z})$–equivalent.

The general case

In general, we are led to the question: let $L_1, \ldots, L_6 \subseteq \mathbb{Z}^2$ be lattices. Suppose that $\mathbb{Z}^2 = L_1 \cup \cdots \cup L_6$. What can $L_1, \ldots, L_6$ be?

The general case

In general, we are led to the question: let $L_1, \ldots, L_6 \subseteq \mathbb{Z}^2$ be lattices. Suppose that $\mathbb{Z}^2 = L_1 \cup \cdots \cup L_6$. What can $L_1, \ldots, L_6$ be?

Remark. The number 6 comes from the largest possible automorphism group, which is D_6.

The general case

In general, we are led to the question: let $L_1, \ldots, L_6 \subseteq \mathbb{Z}^2$ be lattices. Suppose that $\mathbb{Z}^2 = L_1 \cup \cdots \cup L_6$. What can $L_1, \ldots, L_6$ be?

Remark. The number 6 comes from the largest possible automorphism group, which is D_6.

Theorem (K.–Fouvry, "Lattice covering classification")

- *There is exactly* 1 *(i.e. up to permutation and inclusion) covering with* 3 *lattices.*

The general case

In general, we are led to the question: let $L_1, \ldots, L_6 \subseteq \mathbb{Z}^2$ be lattices. Suppose that $\mathbb{Z}^2 = L_1 \cup \cdots \cup L_6$. What can $L_1, \ldots, L_6$ be?

Remark. The number 6 comes from the largest possible automorphism group, which is D_6.

Theorem (K.–Fouvry, "Lattice covering classification")

- *There is exactly* 1 *(i.e. up to permutation and inclusion) covering with* 3 *lattices.*
- *There are exactly* 4 *coverings with* 4 *lattices.*

The general case

In general, we are led to the question: let $L_1, \ldots, L_6 \subseteq \mathbb{Z}^2$ be lattices. Suppose that $\mathbb{Z}^2 = L_1 \cup \cdots \cup L_6$. What can $L_1, \ldots, L_6$ be?

Remark. The number 6 comes from the largest possible automorphism group, which is D_6.

Theorem (K.–Fouvry, "Lattice covering classification")

- *There is exactly* 1 *(i.e. up to permutation and inclusion) covering with* 3 *lattices.*
- *There are exactly* 4 *coverings with* 4 *lattices.*
- *There are exactly* 9 *coverings with* 5 *lattices.*

The general case

In general, we are led to the question: let $L_1, \ldots, L_6 \subseteq \mathbb{Z}^2$ be lattices. Suppose that $\mathbb{Z}^2 = L_1 \cup \cdots \cup L_6$. What can $L_1, \ldots, L_6$ be?

Remark. The number 6 comes from the largest possible automorphism group, which is D_6.

Theorem (K.–Fouvry, "Lattice covering classification")

- *There is exactly* 1 *(i.e. up to permutation and inclusion) covering with* 3 *lattices.*
- *There are exactly* 4 *coverings with* 4 *lattices.*
- *There are exactly* 9 *coverings with* 5 *lattices.*
- *There are exactly* 40 *coverings with* 6 *lattices.*

The cover with 3 lattices

The unique cover with 3 lattices is

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x \equiv 0 \bmod 2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : y \equiv 0 \bmod 2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x + y \equiv 0 \bmod 2 \right\}.$$

The cover with 3 lattices

The unique cover with 3 lattices is

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x \equiv 0 \bmod 2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : y \equiv 0 \bmod 2 \right\}$$
$$\cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x + y \equiv 0 \bmod 2 \right\}.$$

This covering can actually arise from binary forms!

The cover with 3 lattices

The unique cover with 3 lattices is

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x \equiv 0 \bmod 2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : y \equiv 0 \bmod 2 \right\}$$
$$\cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x + y \equiv 0 \bmod 2 \right\}.$$

This covering can actually arise from binary forms!

Indeed, these are exactly the cases where $[F]_{\mathrm{val}}$ consists of two classes: in particular, this is the covering one would get from our first example.

The cover with 3 lattices

The unique cover with 3 lattices is

$$\mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x \equiv 0 \bmod 2 \right\} \cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : y \equiv 0 \bmod 2 \right\}$$
$$\cup \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x + y \equiv 0 \bmod 2 \right\}.$$

This covering can actually arise from binary forms!

Indeed, these are exactly the cases where $[F]_{\text{val}}$ consists of two classes: in particular, this is the covering one would get from our first example.

The other cases do not arise.

Ruling out all other coverings

Ruling out the remaining coverings is the hardest part of our papers, although completely elementary. We use:

Ruling out all other coverings

Ruling out the remaining coverings is the hardest part of our papers, although completely elementary. We use:

- Many case distinctions...

Ruling out all other coverings

Ruling out the remaining coverings is the hardest part of our papers, although completely elementary. We use:

- Many case distinctions...
- Some Gröbner basis computations...

Ruling out all other coverings

Ruling out the remaining coverings is the hardest part of our papers, although completely elementary. We use:

- Many case distinctions...
- Some Gröbner basis computations...
- Many brute force searches with the computer...

Summary

We classify precisely when $[F]_{GL_2(\mathbb{Z})} = [F]_{\mathrm{val}}$.

Summary

We classify precisely when $[F]_{GL_2(\mathbb{Z})} = [F]_{\text{val}}$.

We reduce this problem to a lattice covering problem by the determinant method and a classification of lines on the surface $F(X, Y) = G(Z, W)$.

Summary

We classify precisely when $[F]_{GL_2(\mathbb{Z})} = [F]_{\text{val}}$.

We reduce this problem to a lattice covering problem by the determinant method and a classification of lines on the surface $F(X, Y) = G(Z, W)$.

We completely solve this lattice covering problem with a computer algorithm.

Summary

We classify precisely when $[F]_{GL_2(\mathbb{Z})} = [F]_{\text{val}}$.

We reduce this problem to a lattice covering problem by the determinant method and a classification of lines on the surface $F(X, Y) = G(Z, W)$.

We completely solve this lattice covering problem with a computer algorithm.

We then rule out almost all of these coverings (except for 1) with a long elementary argument with many cases and also some further computer assistance.

Summary

We classify precisely when $[F]_{GL_2(\mathbb{Z})} = [F]_{\text{val}}$.

We reduce this problem to a lattice covering problem by the determinant method and a classification of lines on the surface $F(X, Y) = G(Z, W)$.

We completely solve this lattice covering problem with a computer algorithm.

We then rule out almost all of these coverings (except for 1) with a long elementary argument with many cases and also some further computer assistance.

Thank you for your attention!