A New Parametrization for Ideal Classes in Rings Cut Out by Binary Forms

Ashvin A. Swaminathan
in joint work with Manjul Bhargava and Arul Shankar

University of Debrecen
Online Number Theory Seminar

June 17th, 2022

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute⋆ average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute⋆ average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute⋆ average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute⋆ second moment of 2-Selmer group of elliptic curves
  - Compute⋆ second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Roadmap

- Background on the ring R_f associated to a binary form f
- Parametrization of square roots of class of inverse different of R_f
- Applications to forms $f \in \mathbb{Z}[x, y]$ with fixed leading coefficient:
  - Compute* average 2-torsion in $\mathrm{Cl}(R_f)$
  - $\deg f$ odd: Prove that most "superelliptic equations" $z^2 = f(x, y)$ have no primitive integer solutions
  - $\deg f$ even: Compute* average size of the 2-Selmer group of the Jacobian of hyperelliptic curve $z^2 = f(x, y)$
- Applications to quartic $f \in \mathbb{Z}[x, y]$ with varying leading coefficient:
  - Compute* average size of the 2-Selmer group of the Jacobians of loc. sol. genus-1 curves $z^2 = f(x, y)$
  - Compute* second moment of 2-Selmer group of elliptic curves
  - Compute* second moment of 2-torsion in class groups of monogenic cubic fields

Rings Associated to Binary Forms

- Let R be a PID, let K be fraction field of R
- Let $f(x,y) = \sum_{i=0} f_i x^{n-i} y^i \in R[x,y]$ separable over K, $f_0 \neq 0$
- Let $K_f := K[x]/(f(x,1))$ (étale K-algebra); let $\theta = \text{image}(x) \in K_f$
- For each $i \in \{1, \ldots, n-1\}$, let p_i be the polynomial defined by

$$p_i(t) := \sum_{j=0}^{i-1} f_j t^{i-j}$$

- Let $\zeta_i := p_i(\theta) \in K_f$ for each i

Definition

To the binary form f, there is a naturally associated free R-submodule $R_f \subset K_f$ having rank n and R-basis

$$R_f := R\langle 1, \zeta_1, \zeta_2, \ldots, \zeta_{n-1} \rangle.$$

The Definition of R_f

- Let R be a PID, let K be fraction field of R
- Let $f(x, y) = \sum_{i=0} f_i x^{n-i} y^i \in R[x, y]$ separable over K, $f_0 \neq 0$
- Let $K_f := K[x]/(f(x, 1))$ (étale K-algebra); let $\theta = \text{image}(x) \in K_f$
- For each $i \in \{1, \dots, n-1\}$, let p_i be the polynomial defined by

$$p_i(t) := \sum_{j=0}^{i-1} f_j t^{i-j}$$

- Let $\zeta_i := p_i(\theta) \in K_f$ for each i

Definition

To the binary form f, there is a naturally associated free R-submodule $R_f \subset K_f$ having rank n and R-basis

$$R_f := R\langle 1, \zeta_1, \zeta_2, \dots, \zeta_{n-1} \rangle.$$

The Definition of R_f

- Let R be a PID, let K be fraction field of R
- Let $f(x,y) = \sum_{i=0} f_i x^{n-i} y^i \in R[x,y]$ separable over K, $f_0 \neq 0$
- Let $K_f := K[x]/(f(x,1))$ (étale K-algebra); let $\theta = \text{image}(x) \in K_f$
- For each $i \in \{1, \ldots, n-1\}$, let p_i be the polynomial defined by

$$p_i(t) := \sum_{j=0}^{i-1} f_j t^{i-j}$$

- Let $\zeta_i := p_i(\theta) \in K_f$ for each i

Definition

To the binary form f, there is a naturally associated free R-submodule $R_f \subset K_f$ having rank n and R-basis

$$R_f := R\langle 1, \zeta_1, \zeta_2, \ldots, \zeta_{n-1} \rangle.$$

The Definition of R_f

- Let R be a PID, let K be fraction field of R
- Let $f(x,y) = \sum_{i=0} f_i x^{n-i} y^i \in R[x,y]$ separable over K, $f_0 \neq 0$
- Let $K_f := K[x]/(f(x,1))$ (étale K-algebra); let $\theta = \text{image}(x) \in K_f$
- For each $i \in \{1, \ldots, n-1\}$, let p_i be the polynomial defined by

$$p_i(t) := \sum_{j=0}^{i-1} f_j t^{i-j}$$

- Let $\zeta_i := p_i(\theta) \in K_f$ for each i

Definition

To the binary form f, there is a naturally associated free R-submodule $R_f \subset K_f$ having rank n and R-basis

$$R_f := R\langle 1, \zeta_1, \zeta_2, \ldots, \zeta_{n-1} \rangle.$$

The Definition of R_f

- Let R be a PID, let K be fraction field of R
- Let $f(x, y) = \sum_{i=0} f_i x^{n-i} y^i \in R[x, y]$ separable over K, $f_0 \neq 0$
- Let $K_f := K[x]/(f(x, 1))$ (étale K-algebra); let $\theta = \text{image}(x) \in K_f$
- For each $i \in \{1, \ldots, n-1\}$, let p_i be the polynomial defined by

$$p_i(t) := \sum_{j=0}^{i-1} f_j t^{i-j}$$

- Let $\zeta_i := p_i(\theta) \in K_f$ for each i

Definition

To the binary form f, there is a naturally associated free R-submodule $R_f \subset K_f$ having rank n and R-basis

$$R_f := R\langle 1, \zeta_1, \zeta_2, \ldots, \zeta_{n-1} \rangle.$$

The Definition of R_f

- Let R be a PID, let K be fraction field of R
- Let $f(x,y) = \sum_{i=0} f_i x^{n-i} y^i \in R[x,y]$ separable over K, $f_0 \neq 0$
- Let $K_f := K[x]/(f(x,1))$ (étale K-algebra); let $\theta = \text{image}(x) \in K_f$
- For each $i \in \{1, \ldots, n-1\}$, let p_i be the polynomial defined by

$$p_i(t) := \sum_{j=0}^{i-1} f_j t^{i-j}$$

- Let $\zeta_i := p_i(\theta) \in K_f$ for each i

Definition

To the binary form f, there is a naturally associated free R-submodule $R_f \subset K_f$ having rank n and R-basis

$$R_f := R\langle 1, \zeta_1, \zeta_2, \ldots, \zeta_{n-1} \rangle.$$

Properties of R_f

- The module R_f has been studied extensively in the literature
  - $\mathrm{Disc}(f) = \mathrm{Disc}(R_f)$ (Birch & Merriman, 1972)
  - R_f is actually a ring (hence an order in K_f) with multiplication table

$$\zeta_i\zeta_j = \sum_{k=j+1}^{\min\{i+j,n\}} f_{i+j-k}\zeta_k - \sum_{k=\max\{i+j-n,1\}}^{i} f_{i+j-k}\zeta_k,$$

    where $1 \le i \le j \le n-1$ and $\zeta_0 = 1$ and $\zeta_n = -f_n$ (Nakagawa, 1989)
- When $n = 3$, $f \mapsto R_f$ agrees with Delone-Faddeev correspondence between GL_2-equivalence classes of binary cubic forms and isomorphism classes of cubic rings

Properties of R_f

- The module R_f has been studied extensively in the literature
  - $\mathrm{Disc}(f) = \mathrm{Disc}(R_f)$ (Birch & Merriman, 1972)
  - R_f is actually a ring (hence an order in K_f) with multiplication table

$$\zeta_i\zeta_j = \sum_{k=j+1}^{\min\{i+j,n\}} f_{i+j-k}\zeta_k - \sum_{k=\max\{i+j-n,1\}}^{i} f_{i+j-k}\zeta_k,$$

    where $1 \le i \le j \le n-1$ and $\zeta_0 = 1$ and $\zeta_n = -f_n$ (Nakagawa, 1989)
- When $n = 3$, $f \mapsto R_f$ agrees with Delone-Faddeev correspondence between GL_2-equivalence classes of binary cubic forms and isomorphism classes of cubic rings

Properties of R_f

- The module R_f has been studied extensively in the literature
  - $\mathrm{Disc}(f) = \mathrm{Disc}(R_f)$ (Birch & Merriman, 1972)
  - R_f is actually a ring (hence an order in K_f) with multiplication table

$$\zeta_i\zeta_j = \sum_{k=j+1}^{\min\{i+j,n\}} f_{i+j-k}\zeta_k - \sum_{k=\max\{i+j-n,1\}}^{i} f_{i+j-k}\zeta_k,$$

  where $1 \le i \le j \le n-1$ and $\zeta_0 = 1$ and $\zeta_n = -f_n$ (Nakagawa, 1989)

- When $n = 3$, $f \mapsto R_f$ agrees with Delone-Faddeev correspondence between GL_2-equivalence classes of binary cubic forms and isomorphism classes of cubic rings

Properties of R_f

- The module R_f has been studied extensively in the literature
  - $\mathrm{Disc}(f) = \mathrm{Disc}(R_f)$ (Birch & Merriman, 1972)
  - R_f is actually a ring (hence an order in K_f) with multiplication table

$$\zeta_i\zeta_j = \sum_{k=j+1}^{\min\{i+j,n\}} f_{i+j-k}\zeta_k - \sum_{k=\max\{i+j-n,1\}}^{i} f_{i+j-k}\zeta_k,$$

where $1 \le i \le j \le n-1$ and $\zeta_0 = 1$ and $\zeta_n = -f_n$ (Nakagawa, 1989)

- When $n = 3$, $f \mapsto R_f$ agrees with Delone-Faddeev correspondence between GL_2-equivalence classes of binary cubic forms and isomorphism classes of cubic rings

Properties of R_f

- The module R_f has been studied extensively in the literature
  - $\mathrm{Disc}(f) = \mathrm{Disc}(R_f)$ (Birch & Merriman, 1972)
  - R_f is actually a ring (hence an order in K_f) with multiplication table

$$\zeta_i\zeta_j = \sum_{k=j+1}^{\min\{i+j,n\}} f_{i+j-k}\zeta_k - \sum_{k=\max\{i+j-n,1\}}^{i} f_{i+j-k}\zeta_k,$$

    where $1 \leq i \leq j \leq n-1$ and $\zeta_0 = 1$ and $\zeta_n = -f_n$ (Nakagawa, 1989)

- When $n = 3$, $f \mapsto R_f$ agrees with Delone-Faddeev correspondence between GL_2-equivalence classes of binary cubic forms and isomorphism classes of cubic rings

Fractional Ideals of R_f

- Consider free rank-n R-submodule $I_f^k \subset K_f$ with R-basis

$$I_f^k := R\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1} \rangle, \quad k \in \{0, \ldots, n-1\}$$

- Properties of I_f^k:
  - I_f^k is R_f-module and hence fractional ideal of R_f, and $I_f^k = (I_f^1)^k$
  - I_f^k invertible $\iff$ f is primitive (i.e., $\gcd(f_0, \ldots, f_n) = 1$)
- For a *based* fractional ideal I of R_f, the *norm* $\mathrm{N}(I) =$ det. of the K-linear map taking basis of I to basis of R_f; we have

$$\mathrm{N}(I_f^k) = f_0^{-k}$$

- When $n = 2$, $f \mapsto [I_f^1]$ agrees well-known bijection between $\mathrm{SL}_2(\mathbb{Z})$-classes of b. q. f.'s of disc. D and elements of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$
- Class of I_f^{n-2} is class of inverse different of R_f; i.e.,

$$[I_f^{n-2}] = \left[\mathrm{Hom}_R(R_f, R)\right] \in \mathrm{Cl}(R_f)$$

Fractional Ideals of R_f

- Consider free rank-n R-submodule $I_f^k \subset K_f$ with R-basis

$$I_f^k := R\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\rangle, \quad k \in \{0, \ldots, n-1\}$$

- Properties of I_f^k:
  - I_f^k is R_f-module and hence fractional ideal of R_f, and $I_f^k = (I_f^1)^k$
  - I_f^k invertible $\Longleftrightarrow$ f is primitive (i.e., $\gcd(f_0, \ldots, f_n) = 1$)
- For a *based* fractional ideal I of R_f, the *norm* $\mathrm{N}(I) =$ det. of the K-linear map taking basis of I to basis of R_f; we have

$$\mathrm{N}(I_f^k) = f_0^{-k}$$

- When $n = 2$, $f \mapsto [I_f^1]$ agrees well-known bijection between $\mathrm{SL}_2(\mathbb{Z})$-classes of b. q. f.'s of disc. D and elements of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$
- Class of I_f^{n-2} is class of inverse different of R_f; i.e.,

$$[I_f^{n-2}] = \left[\mathrm{Hom}_R(R_f, R)\right] \in \mathrm{Cl}(R_f)$$

Fractional Ideals of R_f

- Consider free rank-n R-submodule $I_f^k \subset K_f$ with R-basis

$$I_f^k := R\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\rangle, \quad k \in \{0, \ldots, n-1\}$$

- Properties of I_f^k:
  - I_f^k is R_f-module and hence fractional ideal of R_f, and $I_f^k = (I_f^1)^k$
  - I_f^k invertible $\Longleftrightarrow$ f is primitive (i.e., $\gcd(f_0, \ldots, f_n) = 1$)
- For a *based* fractional ideal I of R_f, the *norm* $\mathrm{N}(I) =$ det. of the K-linear map taking basis of I to basis of R_f; we have

$$\mathrm{N}(I_f^k) = f_0^{-k}$$

- When $n = 2$, $f \mapsto [I_f^1]$ agrees well-known bijection between $\mathrm{SL}_2(\mathbb{Z})$-classes of b. q. f.'s of disc. D and elements of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$
- Class of I_f^{n-2} is class of inverse different of R_f; i.e.,

$$[I_f^{n-2}] = \left[\mathrm{Hom}_R(R_f, R)\right] \in \mathrm{Cl}(R_f)$$

Fractional Ideals of R_f

- Consider free rank-n R-submodule $I_f^k \subset K_f$ with R-basis

$$I_f^k := R\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\rangle, \quad k \in \{0, \ldots, n-1\}$$

- Properties of I_f^k:
  - I_f^k is R_f-module and hence fractional ideal of R_f, and $I_f^k = (I_f^1)^k$
  - I_f^k invertible $\Longleftrightarrow$ f is primitive (i.e., $\gcd(f_0, \ldots, f_n) = 1$)
- For a *based* fractional ideal I of R_f, the *norm* $\mathrm{N}(I) =$ det. of the K-linear map taking basis of I to basis of R_f; we have

$$\mathrm{N}(I_f^k) = f_0^{-k}$$

- When $n = 2$, $f \mapsto [I_f^1]$ agrees well-known bijection between $\mathrm{SL}_2(\mathbb{Z})$-classes of b. q. f.'s of disc. D and elements of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$
- Class of I_f^{n-2} is class of inverse different of R_f; i.e.,

$$[I_f^{n-2}] = \left[\mathrm{Hom}_R(R_f, R)\right] \in \mathrm{Cl}(R_f)$$

Fractional Ideals of R_f

- Consider free rank-n R-submodule $I_f^k \subset K_f$ with R-basis

$$I_f^k := R\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\rangle, \quad k \in \{0, \ldots, n-1\}$$

- Properties of I_f^k:
  - I_f^k is R_f-module and hence fractional ideal of R_f, and $I_f^k = (I_f^1)^k$
  - I_f^k invertible $\iff$ f is primitive (i.e., $\gcd(f_0, \ldots, f_n) = 1$)
- For a *based* fractional ideal I of R_f, the *norm* $\mathrm{N}(I)$ = det. of the K-linear map taking basis of I to basis of R_f; we have

$$\mathrm{N}(I_f^k) = f_0^{-k}$$

- When $n = 2$, $f \mapsto [I_f^1]$ agrees well-known bijection between $\mathrm{SL}_2(\mathbb{Z})$-classes of b. q. f.'s of disc. D and elements of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$
- Class of I_f^{n-2} is class of inverse different of R_f; i.e.,

$$[I_f^{n-2}] = \big[\mathrm{Hom}_R(R_f, R)\big] \in \mathrm{Cl}(R_f)$$

Fractional Ideals of R_f

- Consider free rank-n R-submodule $I_f^k \subset K_f$ with R-basis

$$I_f^k := R\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\rangle, \quad k \in \{0, \ldots, n-1\}$$

- Properties of I_f^k:
  - I_f^k is R_f-module and hence fractional ideal of R_f, and $I_f^k = (I_f^1)^k$
  - I_f^k invertible $\iff$ f is primitive (i.e., $\gcd(f_0, \ldots, f_n) = 1$)
- For a *based* fractional ideal I of R_f, the *norm* $\mathrm{N}(I) =$ det. of the K-linear map taking basis of I to basis of R_f; we have

$$\mathrm{N}(I_f^k) = f_0^{-k}$$

- When $n = 2$, $f \mapsto [I_f^1]$ agrees well-known bijection between $\mathrm{SL}_2(\mathbb{Z})$-classes of b. q. f.'s of disc. D and elements of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$
- Class of I_f^{n-2} is class of inverse different of R_f; i.e.,

$$[I_f^{n-2}] = \left[\mathrm{Hom}_R(R_f, R)\right] \in \mathrm{Cl}(R_f)$$

Fractional Ideals of R_f

- Consider free rank-n R-submodule $I_f^k \subset K_f$ with R-basis

$$I_f^k := R\langle 1, \theta, \dots, \theta^k, \zeta_{k+1}, \dots, \zeta_{n-1}\rangle, \quad k \in \{0, \dots, n-1\}$$

- Properties of I_f^k:
  - I_f^k is R_f-module and hence fractional ideal of R_f, and $I_f^k = (I_f^1)^k$
  - I_f^k invertible $\iff$ f is primitive (i.e., $\gcd(f_0, \dots, f_n) = 1$)
- For a *based* fractional ideal I of R_f, the *norm* $\mathrm{N}(I) =$ det. of the K-linear map taking basis of I to basis of R_f; we have

$$\mathrm{N}(I_f^k) = f_0^{-k}$$

- When $n = 2$, $f \mapsto [I_f^1]$ agrees well-known bijection between $\mathrm{SL}_2(\mathbb{Z})$-classes of b. q. f.'s of disc. D and elements of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$
- Class of I_f^{n-2} is class of inverse different of R_f; i.e.,

$$[I_f^{n-2}] = \left[\mathrm{Hom}_R(R_f, R)\right] \in \mathrm{Cl}(R_f)$$

Fractional Ideals of R_f

- Consider free rank-n R-submodule $I_f^k \subset K_f$ with R-basis

$$I_f^k := R\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\rangle, \quad k \in \{0, \ldots, n-1\}$$

- Properties of I_f^k:
  - I_f^k is R_f-module and hence fractional ideal of R_f, and $I_f^k = (I_f^1)^k$
  - I_f^k invertible $\iff$ f is primitive (i.e., $\gcd(f_0, \ldots, f_n) = 1$)
- For a *based* fractional ideal I of R_f, the *norm* $\mathrm{N}(I) =$ det. of the K-linear map taking basis of I to basis of R_f; we have

$$\mathrm{N}(I_f^k) = f_0^{-k}$$

- When $n = 2$, $f \mapsto [I_f^1]$ agrees well-known bijection between $\mathrm{SL}_2(\mathbb{Z})$-classes of b. q. f.'s of disc. D and elements of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$
- Class of I_f^{n-2} is class of inverse different of R_f; i.e.,

$$[I_f^{n-2}] = \left[\mathrm{Hom}_R(R_f, R)\right] \in \mathrm{Cl}(R_f)$$

A New Parametrization

A Theorem of Hecke

- Let K be a number field with ring of integers $\mathcal{O}_K$

Theorem (Hecke)

The class of the different in $\mathrm{Cl}(\mathcal{O}_K)$ *is a perfect square.*

- Hecke's theorem has received no shortage of admiration:
  - In *Basic Number Theory*, Weil placed Hecke's result in a section entitled "*Coronodis loco*" (i.e., crowning moment)
  - Patterson and Armitage agreed with Weil's characterization
- But the proof is not constructive!

A Theorem of Hecke

- Let K be a number field with ring of integers $\mathcal{O}_K$

Theorem (Hecke)

The class of the different in $\mathrm{Cl}(\mathcal{O}_K)$ *is a perfect square.*

- Hecke's theorem has received no shortage of admiration:
  - In *Basic Number Theory*, Weil placed Hecke's result in a section entitled "*Coronodis loco*" (i.e., crowning moment)
  - Patterson and Armitage agreed with Weil's characterization
- But the proof is not constructive!

A Theorem of Hecke

- Let K be a number field with ring of integers $\mathcal{O}_K$

Theorem (Hecke)

The class of the different in $\mathrm{Cl}(\mathcal{O}_K)$ *is a perfect square.*

- Hecke's theorem has received no shortage of admiration:
  - In *Basic Number Theory*, Weil placed Hecke's result in a section entitled "*Coronodis loco*" (i.e., crowning moment)
  - Patterson and Armitage agreed with Weil's characterization
- But the proof is not constructive!

A Theorem of Hecke

- Let K be a number field with ring of integers $\mathcal{O}_K$

Theorem (Hecke)

The class of the different in $\mathrm{Cl}(\mathcal{O}_K)$ *is a perfect square.*

- Hecke's theorem has received no shortage of admiration:
  - In *Basic Number Theory*, Weil placed Hecke's result in a section entitled "*Coronodis loco*" (i.e., crowning moment)
  - Patterson and Armitage agreed with Weil's characterization
- But the proof is not constructive!

A Theorem of Hecke

- Let K be a number field with ring of integers $\mathcal{O}_K$

Theorem (Hecke)

The class of the different in $\mathrm{Cl}(\mathcal{O}_K)$ *is a perfect square.*

- Hecke's theorem has received no shortage of admiration:
  - In *Basic Number Theory*, Weil placed Hecke's result in a section entitled "*Coronodis loco*" (i.e., crowning moment)
  - Patterson and Armitage agreed with Weil's characterization
- But the proof is not constructive!

Questions

Question (Emerton, *MathOverflow* 2010)

Does the ideal class of the different of K have a canonical square root?

- **Answer:** When $K = K_f$ for an even-degree binary form f, yes (consider $\left[I_f^{\frac{2-n}{2}}\right]$); otherwise, we have no idea
- Even if we cannot always construct it, can we still use it?

Question (Ellenberg, *MathOverflow* 2010)

Is there a “parametrization” à la Bhargava for cubic rings together with a square root of the class of the different?

- We answer generalization of Ellenberg's question to rings of any degree $n \geq 3$ defined by integral binary n-ic forms
- Note: all cubic rings are of this form (Delone-Faddeev)

Questions

Question (Emerton, *MathOverflow* 2010)

Does the ideal class of the different of K have a canonical square root?

- **Answer:** When $K = K_f$ for an even-degree binary form f, yes (consider $\left[I_f^{\frac{2-n}{2}}\right]$); otherwise, we have no idea
- Even if we cannot always construct it, can we still use it?

Question (Ellenberg, *MathOverflow* 2010)

Is there a "parametrization" à la Bhargava for cubic rings together with a square root of the class of the different?

- We answer generalization of Ellenberg's question to rings of any degree $n \geq 3$ defined by integral binary n-ic forms
- Note: all cubic rings are of this form (Delone-Faddeev)

Questions

Question (Emerton, *MathOverflow* 2010)

Does the ideal class of the different of K have a canonical square root?

- **Answer:** When $K = K_f$ for an even-degree binary form f, yes (consider $\left[I_f^{\frac{2-n}{2}}\right]$); otherwise, we have no idea
- Even if we cannot always construct it, can we still use it?

Question (Ellenberg, *MathOverflow* 2010)

Is there a "parametrization" à la Bhargava for cubic rings together with a square root of the class of the different?

- We answer generalization of Ellenberg's question to rings of any degree $n \geq 3$ defined by integral binary n-ic forms
- Note: all cubic rings are of this form (Delone-Faddeev)

Questions

Question (Emerton, *MathOverflow* 2010)

Does the ideal class of the different of K have a canonical square root?

- **Answer:** When $K = K_f$ for an even-degree binary form f, yes (consider $\left[I_f^{\frac{2-n}{2}}\right]$); otherwise, we have no idea
- Even if we cannot always construct it, can we still use it?

Question (Ellenberg, *MathOverflow* 2010)

Is there a "parametrization" à la Bhargava for cubic rings together with a square root of the class of the different?

- We answer generalization of Ellenberg's question to rings of any degree $n \geq 3$ defined by integral binary n-ic forms
- Note: all cubic rings are of this form (Delone-Faddeev)

Questions

Question (Emerton, *MathOverflow* 2010)

Does the ideal class of the different of K have a canonical square root?

- **Answer:** When $K = K_f$ for an even-degree binary form f, yes (consider $\left[I_f^{\frac{2-n}{2}}\right]$); otherwise, we have no idea
- Even if we cannot always construct it, can we still use it?

Question (Ellenberg, *MathOverflow* 2010)

Is there a "parametrization" à la Bhargava for cubic rings together with a square root of the class of the different?

- We answer generalization of Ellenberg's question to rings of any degree $n \geq 3$ defined by integral binary n-ic forms
- Note: all cubic rings are of this form (Delone-Faddeev)

Questions

Question (Emerton, *MathOverflow* 2010)

Does the ideal class of the different of K have a canonical square root?

- **Answer:** When $K = K_f$ for an even-degree binary form f, yes (consider $\left[I_f^{\frac{2-n}{2}}\right]$); otherwise, we have no idea
- Even if we cannot always construct it, can we still use it?

Question (Ellenberg, *MathOverflow* 2010)

Is there a "parametrization" à la Bhargava for cubic rings together with a square root of the class of the different?

- We answer generalization of Ellenberg's question to rings of any degree $n \geq 3$ defined by integral binary n-ic forms
- Note: all cubic rings are of this form (Delone-Faddeev)

Orbit Parametrization

Theorem (S., 2020)

- *Let $f \in \mathbb{Z}[x, y]$ be a form of degree $n \geq 3$, leading coeff. $f_0 \neq 0$; and*
- *Let $G = \mathrm{SL}_n$ if n is odd and $G = \mathrm{SL}_n^{\pm}$ if n is even.*

Square roots of the class of the $(\text{different})^{-1}$ of R_f give rise to $G(\mathbb{Z})$-orbits of certain pairs $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\, \mathbb{Z}^n$ of $n \times n$ symmetric integer matrices satisfying

$$\det(xA + yB) = f_0^{-1} \times f(x, f_0 y),$$

where $g \in G(\mathbb{Z})$ acts on (A, B) by $g \cdot (A, B) = (gAg^T, gBg^T)$.

- We call $f_0^{-1} \times f(x, f_0 y)$ the *monicized form* of f and denote it f^{mon}

Orbit Parametrization

Theorem (S., 2020)

- *Let* $f \in \mathbb{Z}[x, y]$ *be a form of degree* $n \geq 3$, *leading coeff.* $f_0 \neq 0$; *and*
- *Let* $G = \mathrm{SL}_n$ *if* n *is odd and* $G = \mathrm{SL}_n^{\pm}$ *if* n *is even.*

Square roots of the class of the $(\text{different})^{-1}$ *of* R_f *give rise to* $G(\mathbb{Z})$*-orbits of certain pairs* $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ *of* $n \times n$ *symmetric integer matrices satisfying*

$$\det(xA + yB) = f_0^{-1} \times f(x, f_0 y),$$

where $g \in G(\mathbb{Z})$ *acts on* (A, B) *by* $g \cdot (A, B) = (gAg^T, gBg^T)$.

- We call $f_0^{-1} \times f(x, f_0 y)$ the *monicized form* of f and denote it f^{mon}

Orbit Parametrization

Theorem (S., 2020)

- *Let $f \in \mathbb{Z}[x, y]$ be a form of degree $n \geq 3$, leading coeff. $f_0 \neq 0$; and*
- *Let $G = \mathrm{SL}_n$ if n is odd and $G = \mathrm{SL}_n^{\pm}$ if n is even.*

Square roots of the class of the $(\text{different})^{-1}$ of R_f give rise to $G(\mathbb{Z})$-orbits of certain pairs $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ of $n \times n$ symmetric integer matrices satisfying

$$\det(xA + yB) = f_0^{-1} \times f(x, f_0 y),$$

where $g \in G(\mathbb{Z})$ acts on (A, B) by $g \cdot (A, B) = (gAg^T, gBg^T)$.

- We call $f_0^{-1} \times f(x, f_0 y)$ the *monicized form* of f and denote it f^{mon}

Orbit Parametrization

Theorem (S., 2020)

- *Let* $f \in \mathbb{Z}[x, y]$ *be a form of degree* $n \geq 3$, *leading coeff.* $f_0 \neq 0$; *and*
- *Let* $G = \mathrm{SL}_n$ *if* n *is odd and* $G = \mathrm{SL}_n^{\pm}$ *if* n *is even.*

Square roots of the class of the $(\textit{different})^{-1}$ *of* R_f *give rise to* $G(\mathbb{Z})$*-orbits of certain pairs* $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ *of* $n \times n$ *symmetric integer matrices satisfying*

$$\det(xA + yB) = f_0^{-1} \times f(x, f_0 y),$$

where $g \in G(\mathbb{Z})$ *acts on* (A, B) *by* $g \cdot (A, B) = (gAg^T, gBg^T)$.

- We call $f_0^{-1} \times f(x, f_0 y)$ the *monicized form* of f and denote it f^{mon}

Construction of An Integral Orbit

- Let I be a fractional ideal of R_f; suppose $\exists\, \alpha \in K_f^\times$ such that

$$I^2 \subset \alpha \cdot I_f^{n-2} \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \cdot \mathrm{N}(I_f^{n-2})$$

- Consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to I_f^{n-2}, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \cdot \beta\gamma$$

- Define functionals $\psi_{n-2}, \psi_{n-1} \in \mathrm{Hom}_R(I_f^{n-2}, R)$ by

$$\psi_{n-2} = \text{projection onto } \theta^{n-2}, \quad \psi_{n-1} = -(\text{projection onto } \zeta_{n-1})$$

- Let A and B be symmetric $n \times n$ matrices over R representing

$$\psi_{n-1} \circ \langle -, - \rangle \colon I \times I \to R \quad \text{and} \quad \psi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$$

w.r.t. chosen R-basis of I

- $G(R)$ acts via change-of-basis on I, induces action

$$g \cdot (A, B) = (gAg^T, gBg^T) \text{ for } g \in G(R)$$

Construction of An Integral Orbit

- Let I be a fractional ideal of R_f; suppose $\exists\, \alpha \in K_f^\times$ such that

$$I^2 \subset \alpha \cdot I_f^{n-2} \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \cdot \mathrm{N}(I_f^{n-2})$$

- Consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to I_f^{n-2}, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \cdot \beta\gamma$$

- Define functionals $\psi_{n-2}, \psi_{n-1} \in \mathrm{Hom}_R(I_f^{n-2}, R)$ by

$$\psi_{n-2} = \text{projection onto } \theta^{n-2}, \quad \psi_{n-1} = -(\text{projection onto } \zeta_{n-1})$$

- Let A and B be symmetric $n \times n$ matrices over R representing

$$\psi_{n-1} \circ \langle -, - \rangle \colon I \times I \to R \quad \text{and} \quad \psi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$$

  w.r.t. chosen R-basis of I

- $G(R)$ acts via change-of-basis on I, induces action

$$g \cdot (A, B) = (gAg^T, gBg^T) \text{ for } g \in G(R)$$

Construction of An Integral Orbit

- Let I be a fractional ideal of R_f; suppose $\exists\, \alpha \in K_f^\times$ such that

$$I^2 \subset \alpha \cdot I_f^{n-2} \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \cdot \mathrm{N}(I_f^{n-2})$$

- Consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to I_f^{n-2}, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \cdot \beta\gamma$$

- Define functionals $\psi_{n-2}, \psi_{n-1} \in \mathrm{Hom}_R(I_f^{n-2}, R)$ by

$$\psi_{n-2} = \text{projection onto } \theta^{n-2}, \quad \psi_{n-1} = -(\text{projection onto } \zeta_{n-1})$$

- Let A and B be symmetric $n \times n$ matrices over R representing

$$\psi_{n-1} \circ \langle -, - \rangle \colon I \times I \to R \quad \text{and} \quad \psi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$$

w.r.t. chosen R-basis of I

- $G(R)$ acts via change-of-basis on I, induces action

$$g \cdot (A, B) = (gAg^T, gBg^T) \text{ for } g \in G(R)$$

Construction of An Integral Orbit

- Let I be a fractional ideal of R_f; suppose $\exists\, \alpha \in K_f^\times$ such that

$$I^2 \subset \alpha \cdot I_f^{n-2} \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \cdot \mathrm{N}(I_f^{n-2})$$

- Consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to I_f^{n-2}, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \cdot \beta\gamma$$

- Define functionals $\psi_{n-2}, \psi_{n-1} \in \mathrm{Hom}_R(I_f^{n-2}, R)$ by

$$\psi_{n-2} = \text{projection onto } \theta^{n-2}, \quad \psi_{n-1} = -(\text{projection onto } \zeta_{n-1})$$

- Let A and B be symmetric $n \times n$ matrices over R representing

$$\psi_{n-1} \circ \langle -, - \rangle \colon I \times I \to R \quad \text{and} \quad \psi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$$

  w.r.t. chosen R-basis of I

- $G(R)$ acts via change-of-basis on I, induces action

$$g \cdot (A, B) = (gAg^T, gBg^T) \text{ for } g \in G(R)$$

Construction of An Integral Orbit

- Let I be a fractional ideal of R_f; suppose $\exists\, \alpha \in K_f^\times$ such that

$$I^2 \subset \alpha \cdot I_f^{n-2} \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \cdot \mathrm{N}(I_f^{n-2})$$

- Consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to I_f^{n-2}, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \cdot \beta\gamma$$

- Define functionals $\psi_{n-2}, \psi_{n-1} \in \mathrm{Hom}_R(I_f^{n-2}, R)$ by

$$\psi_{n-2} = \text{projection onto } \theta^{n-2}, \quad \psi_{n-1} = -(\text{projection onto } \zeta_{n-1})$$

- Let A and B be symmetric $n \times n$ matrices over R representing

$$\psi_{n-1} \circ \langle -, - \rangle \colon I \times I \to R \quad \text{and} \quad \psi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$$

  w.r.t. chosen R-basis of I

- $G(R)$ acts via change-of-basis on I, induces action

$$g \cdot (A, B) = (gAg^T, gBg^T) \text{ for } g \in G(R)$$

Construction of An Integral Orbit

- Let I be a fractional ideal of R_f; suppose $\exists\, \alpha \in K_f^\times$ such that
$$I^2 \subset \alpha \cdot I_f^{n-2} \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \cdot \mathrm{N}(I_f^{n-2})$$
- Consider the symmetric bilinear form
$$\langle -, - \rangle \colon I \times I \to I_f^{n-2}, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \cdot \beta\gamma$$
- Define functionals $\psi_{n-2}, \psi_{n-1} \in \mathrm{Hom}_R(I_f^{n-2}, R)$ by
$$\psi_{n-2} = \text{projection onto } \theta^{n-2}, \quad \psi_{n-1} = -(\text{projection onto } \zeta_{n-1})$$
- Let A and B be symmetric $n \times n$ matrices over R representing
$$\psi_{n-1} \circ \langle -, - \rangle \colon I \times I \to R \quad \text{and} \quad \psi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$$
w.r.t. chosen R-basis of I
- $G(R)$ acts via change-of-basis on I, induces action
$$g \cdot (A, B) = (gAg^T, gBg^T) \text{ for } g \in G(R)$$

Construction of An Integral Orbit

- Let I be a fractional ideal of R_f; suppose $\exists\, \alpha \in K_f^\times$ such that

$$I^2 \subset \alpha \cdot I_f^{n-2} \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \cdot \mathrm{N}(I_f^{n-2})$$

- Consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to I_f^{n-2}, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \cdot \beta\gamma$$

- Define functionals $\psi_{n-2}, \psi_{n-1} \in \mathrm{Hom}_R(I_f^{n-2}, R)$ by

$$\psi_{n-2} = \text{projection onto } \theta^{n-2}, \quad \psi_{n-1} = -(\text{projection onto } \zeta_{n-1})$$

- Let A and B be symmetric $n \times n$ matrices over R representing

$$\psi_{n-1} \circ \langle -, - \rangle \colon I \times I \to R \quad \text{and} \quad \psi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$$

  w.r.t. chosen R-basis of I
- $G(R)$ acts via change-of-basis on I, induces action

$$g \cdot (A, B) = (gAg^T, gBg^T) \text{ for } g \in G(R)$$

Image of the Parametrization

Theorem (S., 2020)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ *be such that* $\det(xA + yB) = f^{\mathrm{mon}}(x, y)$*.* *The* $(G(R)$*-orbit) of* (A, B) *arises from parametrization if and only if*

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(R) \quad \text{for each} \quad i \in \{1, \dots, n-1\}.$$

- Image cut out by congruence conditions mod f_0^{n-1}
- For applications to forms with varying leading coefficient, helpful if image is defined mod f_0, rather than a higher power

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$*. If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto (\text{linear form})^2$*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$*. Converse holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$*.*

Image of the Parametrization

Theorem (S., 2020)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ *be such that* $\det(xA + yB) = f^{\mathrm{mon}}(x, y)$*. The* $(G(R)$*-orbit) of* (A, B) *arises from parametrization if and only if*

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(R) \quad \textit{for each} \quad i \in \{1, \ldots, n-1\}.$$

- Image cut out by congruence conditions mod f_0^{n-1}
- For applications to forms with varying leading coefficient, helpful if image is defined mod f_0, rather than a higher power

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$*. If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto (\textit{linear form})^2$*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$*. Converse holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$*.*

Image of the Parametrization

Theorem (S., 2020)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ *be such that* $\det(xA + yB) = f^{\mathrm{mon}}(x, y)$*. The* $(G(R)$*-orbit) of* (A, B) *arises from parametrization if and only if*

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(R) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

- Image cut out by congruence conditions mod f_0^{n-1}
- For applications to forms with varying leading coefficient, helpful if image is defined mod f_0, rather than a higher power

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$*. If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto (\text{linear form})^2$*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$*. Converse holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$*.*

Image of the Parametrization

Theorem (S., 2020)

Let $(A, B) \in R^2 \otimes_R \operatorname{Sym}_2 R^n$ be such that $\det(xA + yB) = f^{\text{mon}}(x, y)$. The $(G(R)$-orbit$)$ of (A, B) arises from parametrization if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \operatorname{Mat}_{n\times n}(R) \quad \textit{for each} \quad i \in \{1, \ldots, n-1\}.$$

- Image cut out by congruence conditions mod f_0^{n-1}
- For applications to forms with varying leading coefficient, helpful if image is defined mod f_0, rather than a higher power

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \operatorname{Sym}_2 R^n$. If $\det A = 1$ and B has $\operatorname{rk} \leq 1$ mod f_0 (i.e., $B \propto (\text{linear form})^2$), then (A, B) arises for some integral binary n-ic form f with $f(1, 0) = f_0$. Converse holds when $R_f = \mathcal{O}_{K_f}$ or $\gcd(f_0, f_1) = 1$.

Image of the Parametrization

Theorem (S., 2020)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ be such that $\det(xA + yB) = f^{\mathrm{mon}}(x, y)$. The $(G(R)$-orbit$)$ of (A, B) arises from parametrization if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(R) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

- Image cut out by congruence conditions mod f_0^{n-1}
- For applications to forms with varying leading coefficient, helpful if image is defined mod f_0, rather than a higher power

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$. If $\det A = 1$ and B has rk ≤ 1 mod f_0 (i.e., $B \propto$ (linear form)^2), then (A, B) arises for some integral binary n-ic form f with $f(1, 0) = f_0$. Converse holds when $R_f = \mathcal{O}_{K_f}$ or $\gcd(f_0, f_1) = 1$.

Image of the Parametrization

Theorem (S., 2020)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ *be such that* $\det(xA + yB) = f^{\mathrm{mon}}(x, y)$*. The* $(G(R)$*-orbit) of* (A, B) *arises from parametrization if and only if*

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(R) \quad \textit{for each} \quad i \in \{1, \ldots, n-1\}.$$

- Image cut out by congruence conditions mod f_0^{n-1}
- For applications to forms with varying leading coefficient, helpful if image is defined mod f_0, rather than a higher power

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$*. If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto$ *(linear form)*^{2}*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$*. Converse holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$*.*

Statistical Applications to Forms with Fixed Leading Coefficient

Primer on Parametrize-and-Count Strategy

- **Step 1** (algebraic): Parametrize arithmetic objects of interest in terms of integral/rational orbits of a coregular representation $G \curvearrowright V$; if rational, check that these orbits have integral representatives
- E.g., let $V = \{\text{binary quartic forms}\}$ and $G = \mathrm{PGL}_2$; $\mathrm{PGL}_2 \curvearrowright V$, with ring of invariants $= \mathbb{Z}\langle I, J\rangle$
- **Step 2** (analytic): Use geometry-of-numbers methods and sieve techniques to count integral representatives

Primer on Parametrize-and-Count Strategy

- **Step 1** (algebraic): Parametrize arithmetic objects of interest in terms of integral/rational orbits of a coregular representation $G \curvearrowright V$; if rational, check that these orbits have integral representatives
- E.g., let $V = \{\text{binary quartic forms}\}$ and $G = \mathrm{PGL}_2$; $\mathrm{PGL}_2 \curvearrowright V$, with ring of invariants $= \mathbb{Z}\langle I, J\rangle$
- **Step 2** (analytic): Use geometry-of-numbers methods and sieve techniques to count integral representatives

Primer on Parametrize-and-Count Strategy

- **Step 1** (algebraic): Parametrize arithmetic objects of interest in terms of integral/rational orbits of a coregular representation $G \curvearrowright V$; if rational, check that these orbits have integral representatives
- E.g., let $V = \{\text{binary quartic forms}\}$ and $G = \mathrm{PGL}_2$; $\mathrm{PGL}_2 \curvearrowright V$, with ring of invariants $= \mathbb{Z}\langle I, J \rangle$
- **Step 2** (analytic): Use geometry-of-numbers methods and sieve techniques to count integral representatives

Primer on Parametrize-and-Count Strategy

- **Step 1** (algebraic): Parametrize arithmetic objects of interest in terms of integral/rational orbits of a coregular representation $G \curvearrowright V$; if rational, check that these orbits have integral representatives
- E.g., let $V = \{\text{binary quartic forms}\}$ and $G = \mathrm{PGL}_2$; $\mathrm{PGL}_2 \curvearrowright V$, with ring of invariants $= \mathbb{Z}\langle I, J\rangle$
- **Step 2** (analytic): Use geometry-of-numbers methods and sieve techniques to count integral representatives

2-Torsion in the Class Group of R_f

- If $R_f = \mathcal{O}_{K_f}$, then
$$\# \operatorname{Cl}(R_f)[2] = \#\{\text{square roots of class of (different)}^{-1}\}$$

Theorem (S., 2020)

Let n be odd, let $f_0 \in \mathbb{Z} \setminus \{0\}$, and let $|f_0| = m^2 k$, where k is square-free. When fields defined by integral binary n-ic forms f with $f(1,0) = f_0$, r_1 real roots, and $r_2 = \frac{n-r_1}{2}$ pairs of complex roots are ordered by height,

$$\operatorname{Avg}_f(\# \operatorname{Cl}(R_f)[2]) \leq^{\star} 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \frac{1}{\sigma(k) \cdot k^{\frac{n-3}{2}}}$$

- Generalizes results of Bhargava-Hanke-Shankar (2019) in the case $n = 3$ and Siad (2020) in the case $f_0 = 1$ (monogenic)

2-Torsion in the Class Group of R_f

- If $R_f = \mathcal{O}_{K_f}$, then

$$\#\,\mathrm{Cl}(R_f)[2] = \#\{\text{square roots of class of (different)}^{-1}\}$$

Theorem (S., 2020)

Let n be odd, let $f_0 \in \mathbb{Z} \setminus \{0\}$, and let $|f_0| = m^2 k$, where k is square-free. When fields defined by integral binary n-ic forms f with $f(1,0) = f_0$, r_1 real roots, and $r_2 = \frac{n-r_1}{2}$ pairs of complex roots are ordered by height,

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^\star 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \frac{1}{\sigma(k) \cdot k^{\frac{n-3}{2}}}$$

- Generalizes results of Bhargava-Hanke-Shankar (2019) in the case $n = 3$ and Siad (2020) in the case $f_0 = 1$ (monogenic)

2-Torsion in the Class Group of R_f

- If $R_f = \mathcal{O}_{K_f}$, then
$$\#\,\mathrm{Cl}(R_f)[2] = \#\{\text{square roots of class of (different)}^{-1}\}$$

Theorem (S., 2020)

Let n be odd, let $f_0 \in \mathbb{Z} \setminus \{0\}$, and let $|f_0| = m^2 k$, where k is square-free. When fields defined by integral binary n-ic forms f with $f(1,0) = f_0$, r_1 real roots, and $r_2 = \frac{n-r_1}{2}$ pairs of complex roots are ordered by height,

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^{\star} 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \frac{1}{\sigma(k) \cdot k^{\frac{n-3}{2}}}$$

- Generalizes results of Bhargava-Hanke-Shankar (2019) in the case $n = 3$ and Siad (2020) in the case $f_0 = 1$ (monogenic)

2-Torsion in the Class Group of R_f

- If $R_f = \mathcal{O}_{K_f}$, then
$$\#\,\mathrm{Cl}(R_f)[2] = \#\{\text{square roots of class of (different)}^{-1}\}$$

Theorem (S., 2020)

Let n be odd, let $f_0 \in \mathbb{Z} \setminus \{0\}$, and let $|f_0| = m^2 k$, where k is square-free. When fields defined by integral binary n-ic forms f with $f(1,0) = f_0$, r_1 real roots, and $r_2 = \frac{n-r_1}{2}$ pairs of complex roots are ordered by height,

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^\star 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \frac{1}{\sigma(k)\cdot k^{\frac{n-3}{2}}}$$

- Generalizes results of Bhargava-Hanke-Shankar (2019) in the case $n = 3$ and Siad (2020) in the case $f_0 = 1$ (monogenic)

2-Torsion in the Class Group of R_f (cont'd.)

Theorem (S., 2020)

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^\star 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \left(\sigma(k) \cdot k^{\frac{n-3}{2}}\right)^{-1}$$

- Cohen-Lenstra-Martinet-Malle $\Longrightarrow \mathrm{Avg}_K(\#\,\mathrm{Cl}(K)[2]) = 1 + 2^{1-r_1-r_2}$ over *all* degree-n S_n number fields K with signature (r_1, r_2)
- Deviation from conjecture vanishes upon averaging over all f_0
- Note: the family of number fields K_f defined by binary n-ic forms with leading coefficient f_0 is a *multiset*, as distinct binary forms (e.g., $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms) can define the same field!

Theorem (Győry, Bennett, Evertse–Győry, Evertse, Akhtari–Bhargava)

An order in a number field has finitely many monogenizations (i.e., choice of monogenizer up to $\mathbb{Z}$-translate). When $n = 2$, exactly 1; when $n = 3$, at most 10; when $n = 4$, at most 2760; when $n \geq 4$, at most $2^{4(n+5)(n-2)}$.

2-Torsion in the Class Group of R_f (cont'd.)

Theorem (S., 2020)

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^{\star} 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \left(\sigma(k) \cdot k^{\frac{n-3}{2}}\right)^{-1}$$

- Cohen-Lenstra-Martinet-Malle $\Longrightarrow \mathrm{Avg}_K(\#\,\mathrm{Cl}(K)[2]) = 1 + 2^{1-r_1-r_2}$ over *all* degree-n S_n number fields K with signature (r_1, r_2)
- Deviation from conjecture vanishes upon averaging over all f_0
- Note: the family of number fields K_f defined by binary n-ic forms with leading coefficient f_0 is a *multiset*, as distinct binary forms (e.g., $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms) can define the same field!

Theorem (Győry, Bennett, Evertse–Győry, Evertse, Akhtari–Bhargava)

An order in a number field has finitely many monogenizations (i.e., choice of monogenizer up to $\mathbb{Z}$-translate). When $n = 2$, exactly 1; when $n = 3$, at most 10; when $n = 4$, at most 2760; when $n \geq 4$, at most $2^{4(n+5)(n-2)}$.

2-Torsion in the Class Group of R_f (cont'd.)

Theorem (S., 2020)

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^\star 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \left(\sigma(k) \cdot k^{\frac{n-3}{2}}\right)^{-1}$$

- Cohen-Lenstra-Martinet-Malle $\Longrightarrow$ $\mathrm{Avg}_K(\#\,\mathrm{Cl}(K)[2]) = 1 + 2^{1-r_1-r_2}$ over *all* degree-n S_n number fields K with signature (r_1, r_2)
- Deviation from conjecture vanishes upon averaging over all f_0
- Note: the family of number fields K_f defined by binary n-ic forms with leading coefficient f_0 is a *multiset*, as distinct binary forms (e.g., $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms) can define the same field!

Theorem (Győry, Bennett, Evertse–Győry, Evertse, Akhtari–Bhargava)

An order in a number field has finitely many monogenizations (i.e., choice of monogenizer up to $\mathbb{Z}$-translate). When $n = 2$, exactly 1; when $n = 3$, at most 10; when $n = 4$, at most 2760; when $n \geq 4$, at most $2^{4(n+5)(n-2)}$.

2-Torsion in the Class Group of R_f (cont'd.)

Theorem (S., 2020)

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^{\star} 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \left(\sigma(k) \cdot k^{\frac{n-3}{2}}\right)^{-1}$$

- Cohen-Lenstra-Martinet-Malle $\Longrightarrow \mathrm{Avg}_K(\#\,\mathrm{Cl}(K)[2]) = 1 + 2^{1-r_1-r_2}$ over *all* degree-n S_n number fields K with signature (r_1, r_2)
- Deviation from conjecture vanishes upon averaging over all f_0
- Note: the family of number fields K_f defined by binary n-ic forms with leading coefficient f_0 is a *multiset*, as distinct binary forms (e.g., $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms) can define the same field!

Theorem (Győry, Bennett, Evertse–Győry, Evertse, Akhtari–Bhargava)

An order in a number field has finitely many monogenizations (i.e., choice of monogenizer up to $\mathbb{Z}$-translate). When $n = 2$, exactly 1; when $n = 3$, at most 10; when $n = 4$, at most 2760; when $n \geq 4$, at most $2^{4(n+5)(n-2)}$.

2-Torsion in the Class Group of R_f (cont'd.)

Theorem (S., 2020)

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^{\star} 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \left(\sigma(k) \cdot k^{\frac{n-3}{2}}\right)^{-1}$$

- Cohen-Lenstra-Martinet-Malle $\Longrightarrow$ $\mathrm{Avg}_K(\#\,\mathrm{Cl}(K)[2]) = 1 + 2^{1-r_1-r_2}$ over *all* degree-n S_n number fields K with signature (r_1, r_2)
- Deviation from conjecture vanishes upon averaging over all f_0
- Note: the family of number fields K_f defined by binary n-ic forms with leading coefficient f_0 is a *multiset*, as distinct binary forms (e.g., $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms) can define the same field!

Theorem (Győry, Bennett, Evertse–Győry, Evertse, Akhtari–Bhargava)

An order in a number field has finitely many monogenizations (i.e., choice of monogenizer up to $\mathbb{Z}$-translate). When $n = 2$, exactly 1; when $n = 3$, at most 10; when $n = 4$, at most 2760; when $n \geq 4$, at most $2^{4(n+5)(n-2)}$.

2-Torsion in the Class Group of R_f (cont'd.)

Theorem (S., 2020)

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^\star 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \left(\sigma(k) \cdot k^{\frac{n-3}{2}}\right)^{-1}$$

- Cohen-Lenstra-Martinet-Malle $\Longrightarrow$ $\mathrm{Avg}_K(\#\,\mathrm{Cl}(K)[2]) = 1 + 2^{1-r_1-r_2}$ over *all* degree-n S_n number fields K with signature (r_1, r_2)
- Deviation from conjecture vanishes upon averaging over all f_0
- Note: the family of number fields K_f defined by binary n-ic forms with leading coefficient f_0 is a *multiset*, as distinct binary forms (e.g., $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms) can define the same field!

Theorem (Győry, Bennett, Evertse–Győry, Evertse, Akhtari–Bhargava)

An order in a number field has finitely many monogenizations (i.e., choice of monogenizer up to $\mathbb{Z}$-translate). When $n = 2$, exactly 1; when $n = 3$, at most 10; when $n = 4$, at most 2760; when $n \geq 4$, at most $2^{4(n+5)(n-2)}$.

2-Torsion in the Class Group of R_f (cont'd.)

Theorem (S., 2020)

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^\star 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \left(\sigma(k) \cdot k^{\frac{n-3}{2}}\right)^{-1}$$

- Cohen-Lenstra-Martinet-Malle $\Longrightarrow \mathrm{Avg}_K(\#\,\mathrm{Cl}(K)[2]) = 1 + 2^{1-r_1-r_2}$ over *all* degree-n S_n number fields K with signature (r_1, r_2)
- Deviation from conjecture vanishes upon averaging over all f_0
- Note: the family of number fields K_f defined by binary n-ic forms with leading coefficient f_0 is a *multiset*, as distinct binary forms (e.g., $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms) can define the same field!

Theorem (Győry, Bennett, Evertse–Győry, Evertse, Akhtari–Bhargava)

An order in a number field has finitely many monogenizations (i.e., choice of monogenizer up to $\mathbb{Z}$-translate). When $n = 2$, exactly 1; when $n = 3$, at most 10; when $n = 4$, at most 2760; when $n \geq 4$, at most $2^{4(n+5)(n-2)}$.

2-Torsion in the Class Group of R_f (cont'd.)

Theorem (S., 2020)

$$\mathrm{Avg}_f(\#\,\mathrm{Cl}(R_f)[2]) \leq^{\star} 1 + 2^{1-r_1-r_2} + 2^{1-r_1-r_2} \cdot \left(\sigma(k) \cdot k^{\frac{n-3}{2}}\right)^{-1}$$

- Cohen-Lenstra-Martinet-Malle $\Longrightarrow$ $\mathrm{Avg}_K(\#\,\mathrm{Cl}(K)[2]) = 1 + 2^{1-r_1-r_2}$ over *all* degree-n S_n number fields K with signature (r_1, r_2)
- Deviation from conjecture vanishes upon averaging over all f_0
- Note: the family of number fields K_f defined by binary n-ic forms with leading coefficient f_0 is a *multiset*, as distinct binary forms (e.g., $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms) can define the same field!

Theorem (Győry, Bennett, Evertse–Győry, Evertse, Akhtari–Bhargava)

An order in a number field has finitely many monogenizations (i.e., choice of monogenizer up to $\mathbb{Z}$-translate). When $n = 2$, exactly 1; when $n = 3$, at most 10; when $n = 4$, at most 2760; when $n \geq 4$, at most $2^{4(n+5)(n-2)}$.

- Let $f \in \mathbb{Z}[x, y]$ a separable form of degree $n = 2N + 1 \geq 5$
- Rational solutions to $z^2 = f(x, y)$ are not interesting:
  - For any $(x_0, y_0) \in \mathbb{Q}^2$, let $z_0 = f(x_0, y_0)$; then $(z_0^{N+1})^2 = f(x_0 z_0, y_0 z_0)$
  - Geometrically:

$$V(z^2 - f(x,y)) \hookrightarrow \mathbb{P}^2_{\mathbb{Q}}(2, 2, 2N+1)$$

$$V(z^2 - f(x,y)) \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{Q}}, \qquad \mathbb{P}^2_{\mathbb{Q}}(2, 2, 2N+1) \dashrightarrow \mathbb{P}^1_{\mathbb{Q}} \text{ (forget } z\text{)}$$

- Consider primitive solutions: $(x_0, y_0) \in \mathbb{Z}^2$ s.t. $\gcd(x_0, y_0) = 1$

Theorem ("Faltings $+\varepsilon$," Darmon-Granville, 1995)

$z^2 = f(x, y)$ has finitely many primitive integer solutions.

Integral Solutions to Superelliptic Equations

- Let $f \in \mathbb{Z}[x, y]$ a separable form of degree $n = 2N + 1 \geq 5$
- Rational solutions to $z^2 = f(x, y)$ are not interesting:
  - For any $(x_0, y_0) \in \mathbb{Q}^2$, let $z_0 = f(x_0, y_0)$; then $(z_0^{N+1})^2 = f(x_0 z_0, y_0 z_0)$
  - Geometrically:

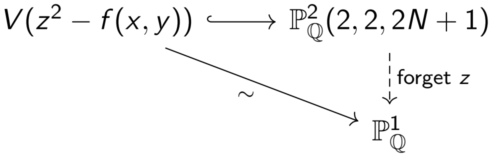
$$\begin{array}{ccc} V(z^2 - f(x,y)) & \hookrightarrow & \mathbb{P}^2_{\mathbb{Q}}(2, 2, 2N+1) \\ & \searrow^{\sim} & \downarrow \text{forget } z \\ & & \mathbb{P}^1_{\mathbb{Q}} \end{array}$$

- Consider primitive solutions: $(x_0, y_0) \in \mathbb{Z}^2$ s.t. $\gcd(x_0, y_0) = 1$

Theorem ("Faltings $+\varepsilon$," Darmon-Granville, 1995)

$z^2 = f(x, y)$ has finitely many primitive integer solutions.

- Let $f \in \mathbb{Z}[x, y]$ a separable form of degree $n = 2N + 1 \geq 5$
- Rational solutions to $z^2 = f(x, y)$ are not interesting:
  - For any $(x_0, y_0) \in \mathbb{Q}^2$, let $z_0 = f(x_0, y_0)$; then $(z_0^{N+1})^2 = f(x_0 z_0, y_0 z_0)$
  - Geometrically:



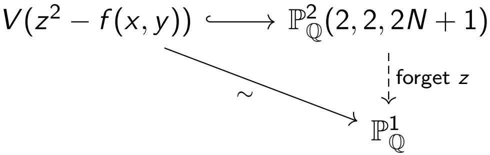
- Consider primitive solutions: $(x_0, y_0) \in \mathbb{Z}^2$ s.t. $\gcd(x_0, y_0) = 1$

Theorem (“Faltings $+\varepsilon$,” Darmon-Granville, 1995)

$z^2 = f(x, y)$ has finitely many primitive integer solutions.

Integral Solutions to Superelliptic Equations

- Let $f \in \mathbb{Z}[x, y]$ a separable form of degree $n = 2N + 1 \geq 5$
- Rational solutions to $z^2 = f(x, y)$ are not interesting:
  - For any $(x_0, y_0) \in \mathbb{Q}^2$, let $z_0 = f(x_0, y_0)$; then $(z_0^{N+1})^2 = f(x_0 z_0, y_0 z_0)$
  - Geometrically:



- Consider primitive solutions: $(x_0, y_0) \in \mathbb{Z}^2$ s.t. $\gcd(x_0, y_0) = 1$

Theorem (“Faltings $+\varepsilon$,” Darmon-Granville, 1995)

$z^2 = f(x, y)$ has finitely many primitive integer solutions.

Integral Solutions to Superelliptic Equations

- Let $f \in \mathbb{Z}[x, y]$ a separable form of degree $n = 2N + 1 \geq 5$
- Rational solutions to $z^2 = f(x, y)$ are not interesting:
  - For any $(x_0, y_0) \in \mathbb{Q}^2$, let $z_0 = f(x_0, y_0)$; then $(z_0^{N+1})^2 = f(x_0 z_0, y_0 z_0)$
  - Geometrically:

$$\begin{array}{ccc} V(z^2 - f(x,y)) & \hookrightarrow & \mathbb{P}^2_{\mathbb{Q}}(2, 2, 2N+1) \\ & \searrow^{\sim} & \downarrow \text{forget } z \\ & & \mathbb{P}^1_{\mathbb{Q}} \end{array}$$

- Consider primitive solutions: $(x_0, y_0) \in \mathbb{Z}^2$ s.t. $\gcd(x_0, y_0) = 1$

Theorem ("Faltings $+\varepsilon$," Darmon-Granville, 1995)

$z^2 = f(x, y)$ *has finitely many primitive integer solutions.*

Integral Solutions to Superelliptic Equations (cont'd.)

- Given a primitive integer solution to $z^2 = f(x,y)$, can construct fractional ideal of R_f whose class is a square root of class of $(\text{different})^{-1}$

Theorem (S., 2019)

Fix odd $f_0 \in \mathbb{Z}$ such that $f_0 \neq \square$, let $|f_0| = m^2 k$. Then for all sufficiently large odd integers n:

- *A positive proportion of degree-n forms f with leading coefficient f_0 are such that $z^2 = f(x,y)$ has no primitive integer solutions.*
- *More specifically, let $\mu_{f_0} = \prod_{p \mid k} (p^{-2} + (p-1)p^{-N-1})$. The density of f such that $z^2 = f(x,y)$ is soluble is $\leq \mu_{f_0} + o(2^{-N})$.*
- *Furthermore, a positive proportion of degree-n forms f are such that $z^2 = f(x,y)$ fails Hasse principle due to Brauer-Manin obstruction.*

- E.g.: $\{p \mid k\} \supset \{2,3,7\} \implies \lim_{n\to\infty} 1 - \mu_{f_0} + o(2^{-N}) \geq 99.9\%$

Integral Solutions to Superelliptic Equations (cont'd.)

- Given a primitive integer solution to $z^2 = f(x,y)$, can construct fractional ideal of R_f whose class is a square root of class of (different)$^{-1}$

Theorem (S., 2019)

Fix odd $f_0 \in \mathbb{Z}$ such that $f_0 \neq \square$, let $|f_0| = m^2 k$. Then for all sufficiently large odd integers n:

- *A positive proportion of degree-n forms f with leading coefficient f_0 are such that $z^2 = f(x,y)$ has no primitive integer solutions.*
- *More specifically, let $\mu_{f_0} = \prod_{p \mid k}(p^{-2} + (p-1)p^{-N-1})$. The density of f such that $z^2 = f(x,y)$ is soluble is $\leq \mu_{f_0} + o(2^{-N})$.*
- *Furthermore, a positive proportion of degree-n forms f are such that $z^2 = f(x,y)$ fails Hasse principle due to Brauer-Manin obstruction.*

- E.g.: $\{p \mid k\} \supset \{2,3,7\} \Longrightarrow \lim_{n\to\infty} 1 - \mu_{f_0} + o(2^{-N}) \geq 99.9\%$

Integral Solutions to Superelliptic Equations (cont'd.)

- Given a primitive integer solution to $z^2 = f(x, y)$, can construct fractional ideal of R_f whose class is a square root of class of $(\text{different})^{-1}$

Theorem (S., 2019)

Fix odd $f_0 \in \mathbb{Z}$ such that $f_0 \neq \square$, let $|f_0| = m^2 k$. Then for all sufficiently large odd integers n:

- *A positive proportion of degree-n forms f with leading coefficient f_0 are such that $z^2 = f(x, y)$ has no primitive integer solutions.*
- *More specifically, let $\mu_{f_0} = \prod_{p \mid k}(p^{-2} + (p-1)p^{-N-1})$. The density of f such that $z^2 = f(x, y)$ is soluble is $\leq \mu_{f_0} + o(2^{-N})$.*
- *Furthermore, a positive proportion of degree-n forms f are such that $z^2 = f(x, y)$ fails Hasse principle due to Brauer-Manin obstruction.*

- E.g.: $\{p \mid k\} \supset \{2, 3, 7\} \implies \lim_{n \to \infty} 1 - \mu_{f_0} + o(2^{-N}) \geq 99.9\%$

Integral Solutions to Superelliptic Equations (cont'd.)

- Given a primitive integer solution to $z^2 = f(x,y)$, can construct fractional ideal of R_f whose class is a square root of class of $(\text{different})^{-1}$

Theorem (S., 2019)

Fix odd $f_0 \in \mathbb{Z}$ such that $f_0 \neq \square$, let $|f_0| = m^2k$. Then for all sufficiently large odd integers n:

- *A positive proportion of degree-n forms f with leading coefficient f_0 are such that $z^2 = f(x,y)$ has no primitive integer solutions.*
- *More specifically, let $\mu_{f_0} = \prod_{p|k}(p^{-2} + (p-1)p^{-N-1})$. The density of f such that $z^2 = f(x,y)$ is soluble is $\leq \mu_{f_0} + o(2^{-N})$.*
- *Furthermore, a positive proportion of degree-n forms f are such that $z^2 = f(x,y)$ fails Hasse principle due to Brauer-Manin obstruction.*

- E.g.: $\{p \mid k\} \supset \{2,3,7\} \implies \lim_{n\to\infty} 1 - \mu_{f_0} + o(2^{-N}) \geq 99.9\%$

Integral Solutions to Superelliptic Equations (cont'd.)

- Given a primitive integer solution to $z^2 = f(x, y)$, can construct fractional ideal of R_f whose class is a square root of class of $(\text{different})^{-1}$

Theorem (S., 2019)

Fix odd $f_0 \in \mathbb{Z}$ such that $f_0 \neq \square$, let $|f_0| = m^2 k$. Then for all sufficiently large odd integers n:

- *A positive proportion of degree-n forms f with leading coefficient f_0 are such that $z^2 = f(x, y)$ has no primitive integer solutions.*
- *More specifically, let $\mu_{f_0} = \prod_{p \mid k}(p^{-2} + (p-1)p^{-N-1})$. The density of f such that $z^2 = f(x, y)$ is soluble is $\leq \mu_{f_0} + o(2^{-N})$.*
- *Furthermore, a positive proportion of degree-n forms f are such that $z^2 = f(x, y)$ fails Hasse principle due to Brauer-Manin obstruction.*

- E.g.: $\{p \mid k\} \supset \{2, 3, 7\} \implies \lim_{n \to \infty} 1 - \mu_{f_0} + o(2^{-N}) \geq 99.9\%$

Integral Solutions to Superelliptic Equations (cont'd.)

- Given a primitive integer solution to $z^2 = f(x, y)$, can construct fractional ideal of R_f whose class is a square root of class of $(\text{different})^{-1}$

Theorem (S., 2019)

Fix odd $f_0 \in \mathbb{Z}$ such that $f_0 \neq \square$, let $|f_0| = m^2 k$. Then for all sufficiently large odd integers n:

- *A positive proportion of degree-n forms f with leading coefficient f_0 are such that $z^2 = f(x, y)$ has no primitive integer solutions.*
- *More specifically, let $\mu_{f_0} = \prod_{p \mid k}(p^{-2} + (p-1)p^{-N-1})$. The density of f such that $z^2 = f(x, y)$ is soluble is $\leq \mu_{f_0} + o(2^{-N})$.*
- *Furthermore, a positive proportion of degree-n forms f are such that $z^2 = f(x, y)$ fails Hasse principle due to Brauer-Manin obstruction.*

- E.g.: $\{p \mid k\} \supset \{2, 3, 7\} \implies \lim_{n \to \infty} 1 - \mu_{f_0} + o(2^{-N}) \geq 99.9\%$

- Let $f(x,y) \in \mathbb{Z}[x,y]$ be a separable form of even degree $n \geq 4$; consider hyperelliptic curve $C_f : z^2 = f(x,y)$ with Jacobian $\mathrm{J}(C_f)$

Definition

- 2-*cover* of C_f (resp., $\mathrm{J}(C_f)$) := cover of C_f (resp., $\mathrm{J}(C_f)$) with automorphism group isomorphic to $\mathrm{J}(C_f)[2]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
- Variety $X/\mathbb{Q}$ is *soluble* if $X(\mathbb{Q}) \neq \varnothing$, *locally soluble* if $X(\mathbb{Q}_v) \neq \varnothing \; \forall v$
- 2-*Selmer group* $\mathrm{Sel}_2(\mathrm{J}(C_f)) := \{$loc. sol. 2-covers of $\mathrm{J}(C_f)\}$

- Motivation: rank of the 2-Selmer group $\geq$ rank of $\mathrm{J}(C_f)$
- Objective: apply parametrize-and-count strategy to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as f varies

- Let $f(x,y) \in \mathbb{Z}[x,y]$ be a separable form of even degree $n \geq 4$; consider hyperelliptic curve $C_f \colon z^2 = f(x,y)$ with Jacobian $\mathrm{J}(C_f)$

Definition

- 2-*cover* of C_f (resp., $\mathrm{J}(C_f)$) := cover of C_f (resp., $\mathrm{J}(C_f)$) with automorphism group isomorphic to $\mathrm{J}(C_f)[2]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
- Variety $X/\mathbb{Q}$ is *soluble* if $X(\mathbb{Q}) \neq \varnothing$, *locally soluble* if $X(\mathbb{Q}_v) \neq \varnothing \ \forall v$
- 2-*Selmer group* $\mathrm{Sel}_2(\mathrm{J}(C_f)) := \{$loc. sol. 2-covers of $\mathrm{J}(C_f)\}$

- Motivation: rank of the 2-Selmer group $\geq$ rank of $\mathrm{J}(C_f)$
- Objective: apply parametrize-and-count strategy to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as f varies

2-Selmer Groups of Hyperelliptic Jacobians

- Let $f(x,y) \in \mathbb{Z}[x,y]$ be a separable form of even degree $n \geq 4$; consider hyperelliptic curve $C_f : z^2 = f(x,y)$ with Jacobian $\mathrm{J}(C_f)$

Definition

- 2-*cover* of C_f (resp., $\mathrm{J}(C_f)$) := cover of C_f (resp., $\mathrm{J}(C_f)$) with automorphism group isomorphic to $\mathrm{J}(C_f)[2]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
- Variety $X/\mathbb{Q}$ is *soluble* if $X(\mathbb{Q}) \neq \varnothing$, *locally soluble* if $X(\mathbb{Q}_v) \neq \varnothing \; \forall v$
- 2-*Selmer group* $\mathrm{Sel}_2(\mathrm{J}(C_f)) := \{$loc. sol. 2-covers of $\mathrm{J}(C_f)\}$

- Motivation: rank of the 2-Selmer group $\geq$ rank of $\mathrm{J}(C_f)$
- Objective: apply parametrize-and-count strategy to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as f varies

2-Selmer Groups of Hyperelliptic Jacobians

- Let $f(x,y) \in \mathbb{Z}[x,y]$ be a separable form of even degree $n \geq 4$; consider hyperelliptic curve $C_f : z^2 = f(x,y)$ with Jacobian $\mathrm{J}(C_f)$

Definition

- 2-*cover* of C_f (resp., $\mathrm{J}(C_f)$) := cover of C_f (resp., $\mathrm{J}(C_f)$) with automorphism group isomorphic to $\mathrm{J}(C_f)[2]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
- Variety $X/\mathbb{Q}$ is *soluble* if $X(\mathbb{Q}) \neq \varnothing$, *locally soluble* if $X(\mathbb{Q}_v) \neq \varnothing\ \forall v$
- 2-*Selmer group* $\mathrm{Sel}_2(\mathrm{J}(C_f)) :=$ {loc. sol. 2-covers of $\mathrm{J}(C_f)$}

- Motivation: rank of the 2-Selmer group $\geq$ rank of $\mathrm{J}(C_f)$
- Objective: apply parametrize-and-count strategy to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as f varies

2-Selmer Groups of Hyperelliptic Jacobians

- Let $f(x,y) \in \mathbb{Z}[x,y]$ be a separable form of even degree $n \geq 4$; consider hyperelliptic curve $C_f : z^2 = f(x,y)$ with Jacobian $\mathrm{J}(C_f)$

Definition

- *2-cover* of C_f (resp., $\mathrm{J}(C_f)$) := cover of C_f (resp., $\mathrm{J}(C_f)$) with automorphism group isomorphic to $\mathrm{J}(C_f)[2]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
- Variety $X/\mathbb{Q}$ is *soluble* if $X(\mathbb{Q}) \neq \varnothing$, *locally soluble* if $X(\mathbb{Q}_v) \neq \varnothing\ \forall v$
- *2-Selmer group* $\mathrm{Sel}_2(\mathrm{J}(C_f)) := \{$loc. sol. 2-covers of $\mathrm{J}(C_f)\}$

- Motivation: rank of the 2-Selmer group $\geq$ rank of $\mathrm{J}(C_f)$
- Objective: apply parametrize-and-count strategy to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as f varies

2-Selmer Groups of Hyperelliptic Jacobians

- Let $f(x,y) \in \mathbb{Z}[x,y]$ be a separable form of even degree $n \geq 4$; consider hyperelliptic curve $C_f \colon z^2 = f(x,y)$ with Jacobian $\mathrm{J}(C_f)$

Definition

- 2-*cover* of C_f (resp., $\mathrm{J}(C_f)$) := cover of C_f (resp., $\mathrm{J}(C_f)$) with automorphism group isomorphic to $\mathrm{J}(C_f)[2]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
- Variety $X/\mathbb{Q}$ is *soluble* if $X(\mathbb{Q}) \neq \varnothing$, *locally soluble* if $X(\mathbb{Q}_v) \neq \varnothing \ \forall v$
- 2-*Selmer group* $\mathrm{Sel}_2(\mathrm{J}(C_f)) := \{$loc. sol. 2-covers of $\mathrm{J}(C_f)\}$

- Motivation: rank of the 2-Selmer group $\geq$ rank of $\mathrm{J}(C_f)$
- Objective: apply parametrize-and-count strategy to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as f varies

2-Selmer Groups of Hyperelliptic Jacobians

- Let $f(x,y) \in \mathbb{Z}[x,y]$ be a separable form of even degree $n \geq 4$; consider hyperelliptic curve $C_f \colon z^2 = f(x,y)$ with Jacobian $\mathrm{J}(C_f)$

Definition

- 2-*cover* of C_f (resp., $\mathrm{J}(C_f)$) := cover of C_f (resp., $\mathrm{J}(C_f)$) with automorphism group isomorphic to $\mathrm{J}(C_f)[2]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
- Variety $X/\mathbb{Q}$ is *soluble* if $X(\mathbb{Q}) \neq \varnothing$, *locally soluble* if $X(\mathbb{Q}_v) \neq \varnothing \ \forall v$
- 2-*Selmer group* $\mathrm{Sel}_2(\mathrm{J}(C_f)) := \{$loc. sol. 2-covers of $\mathrm{J}(C_f)\}$

- Motivation: rank of the 2-Selmer group $\geq$ rank of $\mathrm{J}(C_f)$
- Objective: apply parametrize-and-count strategy to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as f varies

2-Selmer Groups of Hyperelliptic Jacobians

- Let $f(x, y) \in \mathbb{Z}[x, y]$ be a separable form of even degree $n \geq 4$; consider hyperelliptic curve $C_f \colon z^2 = f(x, y)$ with Jacobian $\mathrm{J}(C_f)$

Definition

- 2-*cover* of C_f (resp., $\mathrm{J}(C_f)$) := cover of C_f (resp., $\mathrm{J}(C_f)$) with automorphism group isomorphic to $\mathrm{J}(C_f)[2]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
- Variety $X/\mathbb{Q}$ is *soluble* if $X(\mathbb{Q}) \neq \varnothing$, *locally soluble* if $X(\mathbb{Q}_v) \neq \varnothing \ \forall v$
- 2-*Selmer group* $\mathrm{Sel}_2(\mathrm{J}(C_f)) := \{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\}$

- Motivation: rank of the 2-Selmer group $\geq$ rank of $\mathrm{J}(C_f)$
- Objective: apply parametrize-and-count strategy to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as f varies

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } J(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\text{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $J(C_f)[2] \simeq J(C_{f^{\text{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(J(C_f))$ with certain 2-covers of $J(C_{f^{\text{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\text{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\text{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\text{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^n \ \textit{s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\text{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $J(C_f)[2] \simeq J(C_{f^{\text{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(J(C_f))$ with certain 2-covers of $J(C_{f^{\text{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\, \mathbb{Z}^n \ \textit{s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\, \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $J(C_f)[2] \simeq J(C_{f^{\mathrm{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(J(C_f))$ with certain 2-covers of $J(C_{f^{\mathrm{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via $C_f \hookrightarrow J(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } C_f\}$$

Theorem (Bhargava, 2013 (via Wood, 2010))

$$\{\textit{loc. sol. 2-cover of } C_f\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Simple solution: Create a $\mathbb{Q}$-rational point by replacing f with f^{mon}
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of C_f by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Suppose C_f is loc. sol. if $4 \mid n$. Given element of $\mathrm{Sel}_2(\mathrm{J}(C_f))$, can construct square root of class of $(\text{different})^{-1}$ of R_f
- Combining with parametrization yields:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\, \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

Theorem (Bhargava, Shankar, and S., 2021)

Consider forms $f \in \mathbb{Z}[x,y]$ of even degree $n \geq 4$ with fixed $f_0 \neq 0$ such that C_f is loc. sol. if $4 \mid n$. Then $\mathrm{Avg}\, \#\, \mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^* 6$.

- Robust under imposition of any finite set, and even very general infinite sets, of congruence conditions
- Confirms Poonen–Rains conjecture for even genus curves

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Suppose C_f is loc. sol. if $4 \mid n$. Given element of $\mathrm{Sel}_2(\mathrm{J}(C_f))$, can construct square root of class of $(\text{different})^{-1}$ of R_f
- Combining with parametrization yields:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

Theorem (Bhargava, Shankar, and S., 2021)

Consider forms $f \in \mathbb{Z}[x,y]$ of even degree $n \geq 4$ with fixed $f_0 \neq 0$ such that C_f is loc. sol. if $4 \mid n$. Then $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Robust under imposition of any finite set, and even very general infinite sets, of congruence conditions
- Confirms Poonen–Rains conjecture for even genus curves

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Suppose C_f is loc. sol. if $4 \mid n$. Given element of $\mathrm{Sel}_2(\mathrm{J}(C_f))$, can construct square root of class of $(\text{different})^{-1}$ of R_f
- Combining with parametrization yields:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\,\mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

Theorem (Bhargava, Shankar, and S., 2021)

Consider forms $f \in \mathbb{Z}[x,y]$ of even degree $n \geq 4$ with fixed $f_0 \neq 0$ such that C_f is loc. sol. if $4 \mid n$. Then $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Robust under imposition of any finite set, and even very general infinite sets, of congruence conditions
- Confirms Poonen–Rains conjecture for even genus curves

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Suppose C_f is loc. sol. if $4 \mid n$. Given element of $\mathrm{Sel}_2(\mathrm{J}(C_f))$, can construct square root of class of $(\text{different})^{-1}$ of R_f
- Combining with parametrization yields:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

Theorem (Bhargava, Shankar, and S., 2021)

Consider forms $f \in \mathbb{Z}[x,y]$ of even degree $n \geq 4$ with fixed $f_0 \neq 0$ such that C_f is loc. sol. if $4 \mid n$. Then $\mathrm{Avg}\, \#\, \mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Robust under imposition of any finite set, and even very general infinite sets, of congruence conditions
- Confirms Poonen–Rains conjecture for even genus curves

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Suppose C_f is loc. sol. if $4 \mid n$. Given element of $\mathrm{Sel}_2(\mathrm{J}(C_f))$, can construct square root of class of $(\text{different})^{-1}$ of R_f
- Combining with parametrization yields:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

Theorem (Bhargava, Shankar, and S., 2021)

Consider forms $f \in \mathbb{Z}[x,y]$ of even degree $n \geq 4$ with fixed $f_0 \neq 0$ such that C_f is loc. sol. if $4 \mid n$. Then $\mathrm{Avg}\, \# \mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Robust under imposition of any finite set, and even very general infinite sets, of congruence conditions
- Confirms Poonen–Rains conjecture for even genus curves

2-Selmer Groups of Hyperelliptic Jacobians (cont'd.)

- Suppose C_f is loc. sol. if $4 \mid n$. Given element of $\mathrm{Sel}_2(\mathrm{J}(C_f))$, can construct square root of class of $(\text{different})^{-1}$ of R_f
- Combining with parametrization yields:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\,\mathbb{Z}^n \text{ s.t.} \\ \det(xA+yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

Theorem (Bhargava, Shankar, and S., 2021)

Consider forms $f \in \mathbb{Z}[x,y]$ of even degree $n \geq 4$ with fixed $f_0 \neq 0$ such that C_f is loc. sol. if $4 \mid n$. Then $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^\star 6$.

- Robust under imposition of any finite set, and even very general infinite sets, of congruence conditions
- Confirms Poonen–Rains conjecture for even genus curves

Statistical Applications to Forms with Varying Leading Coefficient

Varying the Leading Coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all f (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed f_0, and then simply sum over all possible values of f_0
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

Varying the Leading Coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all f (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed f_0, and then simply sum over all possible values of f_0
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

Varying the Leading Coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all f (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed f_0, and then simply sum over all possible values of f_0
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

Varying the Leading Coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all f (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed f_0, and then simply sum over all possible values of f_0
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i\{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

Varying the Leading Coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all f (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed f_0, and then simply sum over all possible values of f_0
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

Varying the Leading Coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all f (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed f_0, and then simply sum over all possible values of f_0
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

Varying the Leading Coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all f (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed f_0, and then simply sum over all possible values of f_0
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i\{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

Varying the Leading Coefficient (cont'd.)

- Summing bound over $f_0 \asymp X$ and ignoring error term, we find that $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll$

$$\frac{1}{\#\{f : \mathrm{H}(f) < X\}} \sum_{f_0 \asymp X} f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} \ll \frac{1}{X^{n+1}} \times X^{n+1} = 1$$

- Problem: Error term overtakes main term for f_0 close to X
- Multiple sources of error; worst is application of Davenport's Lemma: # of lattice points satisfying congruence conditions in a "round" region $\approx$ the volume of the region times the probability that the congruence conditions are satisfied

Varying the Leading Coefficient (cont'd.)

- Summing bound over $f_0 \asymp X$ and ignoring error term, we find that $\operatorname{Avg}\#\operatorname{Sel}_2(\mathrm{J}(C_f)) \ll$

$$\frac{1}{\#\{f : \mathrm{H}(f) < X\}} \sum_{f_0 \asymp X} f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} \ll \frac{1}{X^{n+1}} \times X^{n+1} = 1$$

- Problem: Error term overtakes main term for f_0 close to X
- Multiple sources of error; worst is application of Davenport's Lemma: # of lattice points satisfying congruence conditions in a "round" region $\approx$ the volume of the region times the probability that the congruence conditions are satisfied

Varying the Leading Coefficient (cont'd.)

- Summing bound over $f_0 \asymp X$ and ignoring error term, we find that $\text{Avg}\,\#\,\text{Sel}_2(\text{J}(C_f)) \ll$

$$\frac{1}{\#\{f : \text{H}(f) < X\}} \sum_{f_0 \asymp X} f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} \ll \frac{1}{X^{n+1}} \times X^{n+1} = 1$$

- Problem: Error term overtakes main term for f_0 close to X
- Multiple sources of error; worst is application of Davenport's Lemma: # of lattice points satisfying congruence conditions in a "round" region $\approx$ the volume of the region times the probability that the congruence conditions are satisfied

Varying the Leading Coefficient (cont'd.)

- Summing bound over $f_0 \asymp X$ and ignoring error term, we find that $\operatorname{Avg} \# \operatorname{Sel}_2(\mathrm{J}(C_f)) \ll$

$$\frac{1}{\#\{f : \mathrm{H}(f) < X\}} \sum_{f_0 \asymp X} f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} \ll \frac{1}{X^{n+1}} \times X^{n+1} = 1$$

- Problem: Error term overtakes main term for f_0 close to X
- Multiple sources of error; worst is application of Davenport's Lemma: # of lattice points satisfying congruence conditions in a "round" region $\approx$ the volume of the region times the probability that the congruence conditions are satisfied

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}: (A, B) with $\det(xA + yB) = f^{\text{mon}}(x, y)$ arises if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \text{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \text{Sym}_2 R^n$.

1. *If $\det A = 1$ and B has rk ≤ 1 mod f_0 (i.e., $B \propto (\text{linear form})^2$), then (A, B) arises for some integral binary n-ic form f with $f(1, 0) = f_0$.*
2. *Converse of (1) holds when $R_f = \mathcal{O}_{K_f}$ or $\gcd(f_0, f_1) = 1$.*
3. *If $\det A = 1$ and $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ for each $i \in \{2, \ldots, n\}$, then (A, B) arises for some integral binary n-ic form f with $f(1, 0) = f_0$.*
4. *Let $n = 4$. $\exists$ $(\text{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \text{Sym}_2 \mathbb{Z}^4$ such that $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ for each $i \in \{2, 3, 4\}$*

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}:
  (A, B) with $\det(xA + yB) = f^{\text{mon}}(x, y)$ arises if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$.

1. *If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto$ *(linear form)*^{2}*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
2. *Converse of* (1) *holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$.
3. *If* $\det A = 1$ *and* $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, \ldots, n\}$*, then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
4. *Let* $n = 4$. $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$*-translate* $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ *such that* $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, 3, 4\}$

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}: (A, B) with $\det(xA + yB) = f^{\text{mon}}(x, y)$ arises if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$.

1. *If $\det A = 1$ and B has rk ≤ 1 mod f_0 (i.e., $B \propto$ (linear form)^2), then (A, B) arises for some integral binary n-ic form f with $f(1, 0) = f_0$.*
2. *Converse of (1) holds when $R_f = \mathcal{O}_{K_f}$ or $\gcd(f_0, f_1) = 1$.*
3. *If $\det A = 1$ and $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ for each $i \in \{2, \ldots, n\}$, then (A, B) arises for some integral binary n-ic form f with $f(1, 0) = f_0$.*
4. *Let $n = 4$. $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ such that $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ for each $i \in \{2, 3, 4\}$*

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}: (A, B) with $\det(xA + yB) = f^{\mathrm{mon}}(x, y)$ arises if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$.

1. *If* $\det A = 1$ *and* B *has* rk ≤ 1 *mod* f_0 *(i.e.,* $B \propto (\text{linear form})^2$*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
2. *Converse of* (1) *holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$.
3. *If* $\det A = 1$ *and* $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, \ldots, n\}$*, then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
4. *Let* $n = 4$. $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$*-translate* $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ *such that* $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, 3, 4\}$

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}: (A, B) with $\det(xA + yB) = f^{\text{mon}}(x, y)$ arises if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$.

1. *If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 (*i.e.,* $B \propto (\textit{linear form})^2$), *then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1,0) = f_0$.
2. *Converse of* (1) *holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$.
3. *If* $\det A = 1$ *and* $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, \ldots, n\}$, *then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1,0) = f_0$.
4. *Let* $n = 4$. $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$*-translate* $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ *such that* $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, 3, 4\}$

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}: (A, B) with $\det(xA + yB) = f^{\text{mon}}(x, y)$ arises if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$.

1. *If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto$ *(linear form)*^{2}*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
2. *Converse of* (1) *holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$.
3. *If* $\det A = 1$ *and* $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, \ldots, n\}$*, then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
4. *Let* $n = 4$. $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$*-translate* $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ *such that* $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, 3, 4\}$

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}: (A, B) with $\det(xA + yB) = f^{\text{mon}}(x, y)$ arises if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \text{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \dots, n-1\}.$$

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \text{Sym}_2 R^n$.

1. *If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto$ *(linear form)*^{2}*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
2. *Converse of* (1) *holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$.
3. *If* $\det A = 1$ *and* $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, \dots, n\}$*, then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
4. *Let* $n = 4$. $\exists$ $(\text{SL}_4/\mu_2)(\mathbb{Q})$*-translate* $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \text{Sym}_2 \mathbb{Z}^4$ *such that* $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, 3, 4\}$

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}: (A, B) with $\det(xA + yB) = f^{\text{mon}}(x, y)$ arises if and only if

$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \ldots, n-1\}.$$

Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$.

1. *If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto$ *(linear form)*^{2}*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
2. *Converse of* (1) *holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$.
3. *If* $\det A = 1$ *and* $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, \ldots, n\}$*, then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
4. *Let* $n = 4$. $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$*-translate* $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ *such that* $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, 3, 4\}$

Orbits of rk ≤ 1 mod f_0

- To control error, need to understand image of parametrization better
- Recall image is *a priori* defined by congruence conditions mod f_0^{n-1}: (A, B) with $\det(xA + yB) = f^{\mathrm{mon}}(x, y)$ arises if and only if

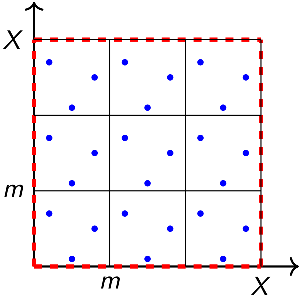
$$p_i\left(\tfrac{1}{f_0} \cdot -BA^{-1}\right) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \quad \text{for each} \quad i \in \{1, \dots, n-1\}.$$

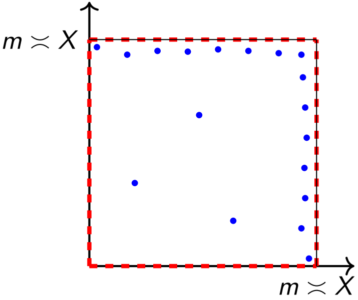
Theorem (Bhargava, Shankar, S., 2021)

Let $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$.

1. *If* $\det A = 1$ *and* B *has rk* ≤ 1 *mod* f_0 *(i.e.,* $B \propto$ *(linear form)*^{2}*), then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
2. *Converse of* (1) *holds when* $R_f = \mathcal{O}_{K_f}$ *or* $\gcd(f_0, f_1) = 1$.
3. *If* $\det A = 1$ *and* $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, \dots, n\}$*, then* (A, B) *arises for some integral binary n-ic form* f *with* $f(1, 0) = f_0$.
4. *Let* $n = 4$. $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$*-translate* $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ *such that* $\wedge^i B' \equiv 0 \pmod{f_0^{i-1}}$ *for each* $i \in \{2, 3, 4\}$

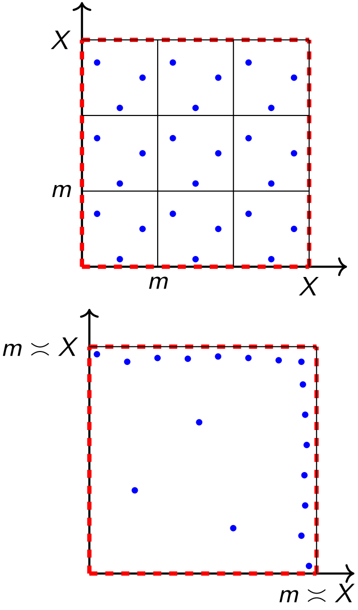
Error from Davenport's Lemma





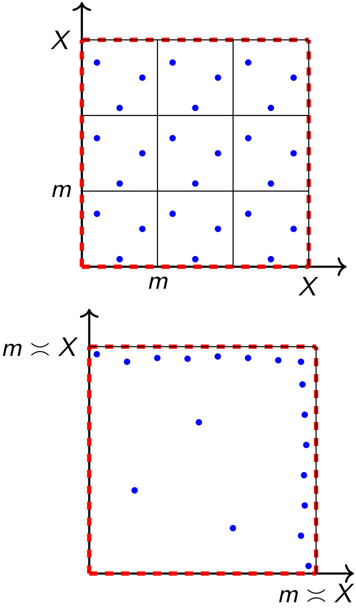
- Want to count lattice pts cut out by congruence conditions mod m in box of sidelength X
- If m/X is tiny, Davenport's lemma gives good estimate
- But orbits we want to count are defined by conditions mod f_0, and $f_0 \asymp X$
- If $m \asymp X$ and pts are sparse or concentrated near edges of box, error in Davenport's lemma will be huge

Error from Davenport's Lemma



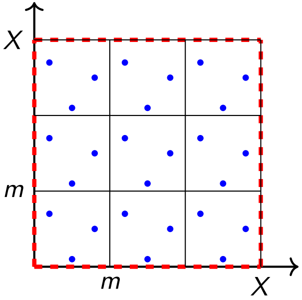
- Want to count lattice pts cut out by congruence conditions mod m in box of sidelength X
- If m/X is tiny, Davenport's lemma gives good estimate
- But orbits we want to count are defined by conditions mod f_0, and $f_0 \asymp X$
- If $m \asymp X$ and pts are sparse or concentrated near edges of box, error in Davenport's lemma will be huge

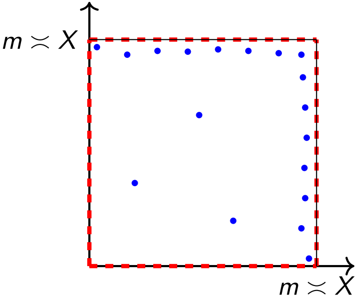
Error from Davenport's Lemma



- Want to count lattice pts cut out by congruence conditions mod m in box of sidelength X
- If m/X is tiny, Davenport's lemma gives good estimate
- But orbits we want to count are defined by conditions mod f_0, and $f_0 \asymp X$
- If $m \asymp X$ and pts are sparse or concentrated near edges of box, error in Davenport's lemma will be huge

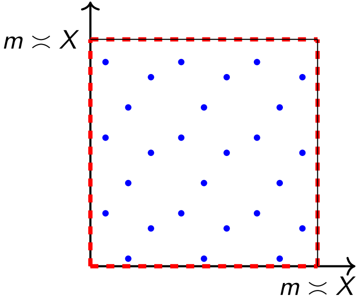
Error from Davenport's Lemma





- Want to count lattice pts cut out by congruence conditions mod m in box of sidelength X
- If m/X is tiny, Davenport's lemma gives good estimate
- But orbits we want to count are defined by conditions mod f_0, and $f_0 \asymp X$
- If $m \asymp X$ and pts are sparse or concentrated near edges of box, error in Davenport's lemma will be huge

Error from Davenport's Lemma (cont'd.)

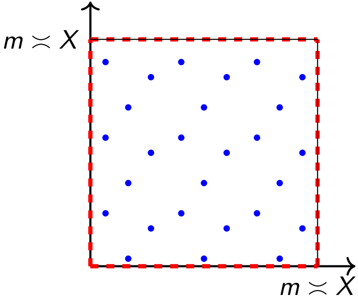


- Want to prove that orbits arising from parametrization are somewhat equidistributed in box, even when $m = f_0 \asymp X$
- Let $\chi =$ indicator function mod f_0 of image of parametrization

$$\text{proving pts somewhat equidistributed} \iff \text{bounding} \sum_{B \neq 0} |\widehat{\chi}(B)|$$

- Easy to show that if $f_0 =$ prime p, e.g., we have $|\widehat{\chi}(B)| \ll p^{4-\frac{\operatorname{rk} B}{2}}$

Error from Davenport's Lemma (cont'd.)

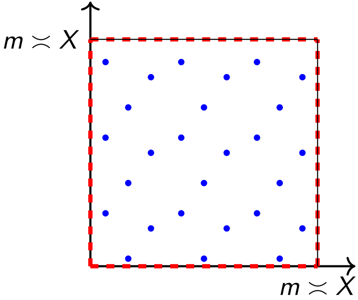


- Want to prove that orbits arising from parametrization are somewhat equidistributed in box, even when $m = f_0 \asymp X$
- Let $\chi =$ indicator function mod f_0 of image of parametrization

  proving pts somewhat equidistributed $\Longleftrightarrow$ bounding $\sum_{B \neq 0} |\widehat{\chi}(B)|$

- Easy to show that if $f_0 =$ prime p, e.g., we have $|\widehat{\chi}(B)| \ll p^{4 - \frac{\mathrm{rk}\, B}{2}}$

Error from Davenport's Lemma (cont'd.)

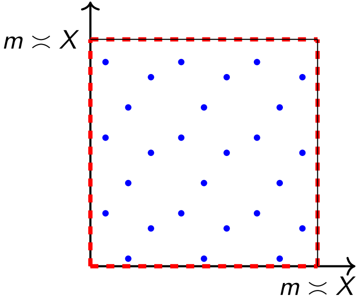


- Want to prove that orbits arising from parametrization are somewhat equidistributed in box, even when $m = f_0 \asymp X$
- Let $\chi =$ indicator function mod f_0 of image of parametrization

$$\text{proving pts somewhat equidistributed} \iff \text{bounding} \sum_{B \neq 0} |\widehat{\chi}(B)|$$

- Easy to show that if $f_0 =$ prime p, e.g., we have $|\widehat{\chi}(B)| \ll p^{4-\frac{\text{rk}\, B}{2}}$

Error from Davenport's Lemma (cont'd.)



- Want to prove that orbits arising from parametrization are somewhat equidistributed in box, even when $m = f_0 \asymp X$
- Let $\chi =$ indicator function mod f_0 of image of parametrization

$$\text{proving pts somewhat equidistributed} \iff \text{bounding} \sum_{B \neq 0} |\widehat{\chi}(B)|$$

- Easy to show that if $f_0 =$ prime p, e.g., we have $|\widehat{\chi}(B)| \ll p^{4-\frac{\mathrm{rk}\,B}{2}}$

2-Selmer Groups of Genus-1 Curves

Theorem (Bhargava, Shankar, and S., 2021)

When integral binary quartic forms f such that C_f is loc. sol. are ordered by the max norm on their coefficients, we have $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^\star 6$.

- Family of curves C_f, where f ranges over all binary quartic forms, has redundancies: If f, f' are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Crucially, average remains $\leq^\star 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$

2-Selmer Groups of Genus-1 Curves

Theorem (Bhargava, Shankar, and S., 2021)

When integral binary quartic forms f such that C_f is loc. sol. are ordered by the max norm on their coefficients, we have $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^\star 6$.

- Family of curves C_f, where f ranges over all binary quartic forms, has redundancies: If f, f' are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Crucially, average remains $\leq^\star 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$

2-Selmer Groups of Genus-1 Curves

Theorem (Bhargava, Shankar, and S., 2021)

When integral binary quartic forms f such that C_f is loc. sol. are ordered by the max norm on their coefficients, we have $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^\star 6$.

- Family of curves C_f, where f ranges over all binary quartic forms, has redundancies: If f, f' are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Crucially, average remains $\leq^\star 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$

2-Selmer Groups of Genus-1 Curves

Theorem (Bhargava, Shankar, and S., 2021)

When integral binary quartic forms f such that C_f is loc. sol. are ordered by the max norm on their coefficients, we have $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Family of curves C_f, where f ranges over all binary quartic forms, has redundancies: If f, f' are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Crucially, average remains $\leq^{\star} 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$

The Second Moment of the Size of the 2-Selmer Group of Elliptic Curves

Background on Elliptic Curves and their Selmer groups

- Every elliptic curve $E/\mathbb{Q}$ is iso. to unique curve of the form

$$E = E_{I,J}\colon y^2 = x^3 + Ix + J,$$

where $I, J \in \mathbb{Z}$ such that $p^4 \mid I \implies p^6 \nmid J$

- Order elliptic curves by height: $H(E_{I,J}) = \max\{4|I|^3, 27J^2\}$

Question

What is the distribution of $\mathrm{Sel}_2(E)$ as E ranges through all elliptic curves ordered by height?

Conjecture (Poonen and Rains, 2010)

$\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^m = \prod_{i=1}^{m}(2^i + 1)$

- E.g., $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E) = 3$, and $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^2 = 15$

Background on Elliptic Curves and their Selmer groups

- Every elliptic curve $E/\mathbb{Q}$ is iso. to unique curve of the form

$$E = E_{I,J}\colon\ y^2 = x^3 + Ix + J,$$

where $I, J \in \mathbb{Z}$ such that $p^4 \mid I \implies p^6 \nmid J$

- Order elliptic curves by height: $H(E_{I,J}) = \max\{4|I|^3, 27J^2\}$

Question

What is the distribution of $\mathrm{Sel}_2(E)$ as E ranges through all elliptic curves ordered by height?

Conjecture (Poonen and Rains, 2010)

$\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^m = \prod_{i=1}^{m}(2^i + 1)$

- E.g., $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E) = 3$, and $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^2 = 15$

Background on Elliptic Curves and their Selmer groups

- Every elliptic curve $E/\mathbb{Q}$ is iso. to unique curve of the form

$$E = E_{I,J}\colon y^2 = x^3 + Ix + J,$$

where $I, J \in \mathbb{Z}$ such that $p^4 \mid I \implies p^6 \nmid J$

- Order elliptic curves by height: $H(E_{I,J}) = \max\{4|I|^3, 27J^2\}$

Question

What is the distribution of $\mathrm{Sel}_2(E)$ as E ranges through all elliptic curves ordered by height?

Conjecture (Poonen and Rains, 2010)

$\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^m = \prod_{i=1}^{m}(2^i + 1)$

- E.g., $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E) = 3$, and $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^2 = 15$

Background on Elliptic Curves and their Selmer groups

- Every elliptic curve $E/\mathbb{Q}$ is iso. to unique curve of the form

$$E = E_{I,J} \colon y^2 = x^3 + Ix + J,$$

where $I, J \in \mathbb{Z}$ such that $p^4 \mid I \implies p^6 \nmid J$

- Order elliptic curves by height: $H(E_{I,J}) = \max\{4|I|^3, 27J^2\}$

Question

What is the distribution of $\mathrm{Sel}_2(E)$ as E ranges through all elliptic curves ordered by height?

Conjecture (Poonen and Rains, 2010)

$\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^m = \prod_{i=1}^{m}(2^i + 1)$

- E.g., $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E) = 3$, and $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^2 = 15$

Background on Elliptic Curves and their Selmer groups

- Every elliptic curve $E/\mathbb{Q}$ is iso. to unique curve of the form

$$E = E_{I,J} \colon y^2 = x^3 + Ix + J,$$

where $I, J \in \mathbb{Z}$ such that $p^4 \mid I \implies p^6 \nmid J$

- Order elliptic curves by height: $H(E_{I,J}) = \max\{4|I|^3, 27J^2\}$

Question

What is the distribution of $\mathrm{Sel}_2(E)$ as E ranges through all elliptic curves ordered by height?

Conjecture (Poonen and Rains, 2010)

$\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^m = \prod_{i=1}^{m}(2^i + 1)$

- E.g., $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E) = 3$, and $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^2 = 15$

Background on Elliptic Curves and their Selmer groups

- Every elliptic curve $E/\mathbb{Q}$ is iso. to unique curve of the form

$$E = E_{I,J}\colon\, y^2 = x^3 + Ix + J,$$

  where $I, J \in \mathbb{Z}$ such that $p^4 \mid I \Longrightarrow p^6 \nmid J$
- Order elliptic curves by height: $H(E_{I,J}) = \max\{4|I|^3, 27J^2\}$

Question

What is the distribution of $\mathrm{Sel}_2(E)$ as E ranges through all elliptic curves ordered by height?

Conjecture (Poonen and Rains, 2010)

$\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^m = \prod_{i=1}^{m}(2^i + 1)$

- E.g., $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E) = 3$, and $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^2 = 15$

Progress toward the Conjecture

Theorem (Bhargava and Shankar, 2010)

Avg $\# \operatorname{Sel}_2(E) = 3$.

- Proof proceeds by means of parametrize-and-count strategy
- Let $V = \{\text{binary quartic forms}\}$; $\mathrm{PGL}_2 \curvearrowright V$, with invts. $= \mathbb{Z}\langle I, J\rangle$

Theorem (Birch and Swinnerton-Dyer, 1963)

The map $f \mapsto C_f$ defines a bijection between the set of $\mathrm{PGL}_2(\mathbb{Q})$-orbits of forms $f \in V(\mathbb{Z})$ with PGL_2-invariants I, J such that C_f is (loc.) sol. and the set of isomorphism classes of (loc.) sol. 2-covers of $E_{I,J}$.

- By abuse of notation, write $f \in \operatorname{Sel}_2(E)$ to denote corresponding ($\mathrm{PGL}_2(\mathbb{Q})$-orbit of) integral binary quartic form

Progress toward the Conjecture

Theorem (Bhargava and Shankar, 2010)

Avg $\# \operatorname{Sel}_2(E) = 3$.

- Proof proceeds by means of parametrize-and-count strategy
- Let $V = \{\text{binary quartic forms}\}$; $\mathrm{PGL}_2 \curvearrowright V$, with invts. $= \mathbb{Z}\langle I, J\rangle$

Theorem (Birch and Swinnerton-Dyer, 1963)

The map $f \mapsto C_f$ defines a bijection between the set of $\mathrm{PGL}_2(\mathbb{Q})$-orbits of forms $f \in V(\mathbb{Z})$ with PGL_2-invariants I, J such that C_f is (loc.) sol. and the set of isomorphism classes of (loc.) sol. 2-covers of $E_{I,J}$.

- By abuse of notation, write $f \in \operatorname{Sel}_2(E)$ to denote corresponding ($\mathrm{PGL}_2(\mathbb{Q})$-orbit of) integral binary quartic form

Theorem (Bhargava and Shankar, 2010)

$\text{Avg}\,\#\,\text{Sel}_2(E) = 3.$

- Proof proceeds by means of parametrize-and-count strategy
- Let $V = \{\text{binary quartic forms}\}$; $\text{PGL}_2 \curvearrowright V$, with invts. $= \mathbb{Z}\langle I, J\rangle$

Theorem (Birch and Swinnerton-Dyer, 1963)

The map $f \mapsto C_f$ defines a bijection between the set of $\text{PGL}_2(\mathbb{Q})$-orbits of forms $f \in V(\mathbb{Z})$ with PGL_2-invariants I, J such that C_f is (loc.) sol. and the set of isomorphism classes of (loc.) sol. 2-covers of $E_{I,J}$.

- By abuse of notation, write $f \in \text{Sel}_2(E)$ to denote corresponding ($\text{PGL}_2(\mathbb{Q})$-orbit of) integral binary quartic form

Progress toward the Conjecture

Theorem (Bhargava and Shankar, 2010)

Avg $\#\,\mathrm{Sel}_2(E) = 3$.

- Proof proceeds by means of parametrize-and-count strategy
- Let $V = \{\text{binary quartic forms}\}$; $\mathrm{PGL}_2 \curvearrowright V$, with invts. $= \mathbb{Z}\langle I, J\rangle$

Theorem (Birch and Swinnerton-Dyer, 1963)

The map $f \mapsto C_f$ defines a bijection between the set of $\mathrm{PGL}_2(\mathbb{Q})$-orbits of forms $f \in V(\mathbb{Z})$ with PGL_2-invariants I, J such that C_f is (loc.) sol. and the set of isomorphism classes of (loc.) sol. 2-covers of $E_{I,J}$.

- By abuse of notation, write $f \in \mathrm{Sel}_2(E)$ to denote corresponding ($\mathrm{PGL}_2(\mathbb{Q})$-orbit of) integral binary quartic form

Progress toward the Conjecture

Theorem (Bhargava and Shankar, 2010)

Avg $\# \operatorname{Sel}_2(E) = 3$.

- Proof proceeds by means of parametrize-and-count strategy
- Let $V = \{\text{binary quartic forms}\}$; $\mathrm{PGL}_2 \curvearrowright V$, with invts. $= \mathbb{Z}\langle I, J \rangle$

Theorem (Birch and Swinnerton-Dyer, 1963)

The map $f \mapsto C_f$ defines a bijection between the set of $\mathrm{PGL}_2(\mathbb{Q})$-orbits of forms $f \in V(\mathbb{Z})$ with PGL_2-invariants I, J such that C_f is (loc.) sol. and the set of isomorphism classes of (loc.) sol. 2-covers of $E_{I,J}$.

- By abuse of notation, write $f \in \operatorname{Sel}_2(E)$ to denote corresponding ($\mathrm{PGL}_2(\mathbb{Q})$-orbit of) integral binary quartic form

Progress toward the Conjecture

Theorem (Bhargava and Shankar, 2010)

Avg $\#\,\mathrm{Sel}_2(E) = 3$.

- Proof proceeds by means of parametrize-and-count strategy
- Let $V = \{\text{binary quartic forms}\}$; $\mathrm{PGL}_2 \curvearrowright V$, with invts. $= \mathbb{Z}\langle I, J\rangle$

Theorem (Birch and Swinnerton-Dyer, 1963)

The map $f \mapsto C_f$ defines a bijection between the set of $\mathrm{PGL}_2(\mathbb{Q})$-orbits of forms $f \in V(\mathbb{Z})$ with PGL_2-invariants I, J such that C_f is $($loc.$)$ sol. and the set of isomorphism classes of $($loc.$)$ sol. 2-covers of $E_{I,J}$.

- By abuse of notation, write $f \in \mathrm{Sel}_2(E)$ to denote corresponding ($\mathrm{PGL}_2(\mathbb{Q})$-orbit of) integral binary quartic form

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

Avg $\# \mathrm{Sel}_2(E)^2 \leq^\star 15$.

Idea of the Proof:

- Want to count pairs $(f, f') \in \mathrm{Sel}_2(E)^2$
- Fix $f \in \mathrm{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\Longrightarrow 2 \times 3 = 6$ choices for f' on avg
    - $\mathrm{Sel}_2(E) \simeq \mathrm{Sel}_2(\mathrm{J}(C_f))$, so Avg $\#\{\text{choices for f'}\} =$ Avg $\# \mathrm{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \Longrightarrow 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

Avg $\# \mathrm{Sel}_2(E)^2 \leq^\star 15$.

Idea of the Proof:

- Want to count pairs $(f, f') \in \mathrm{Sel}_2(E)^2$
- Fix $f \in \mathrm{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\implies 2 \times 3 = 6$ choices for f' on avg
    - $\mathrm{Sel}_2(E) \simeq \mathrm{Sel}_2(\mathrm{J}(C_f))$, so Avg $\#\{\text{choices for f'}\} =$ Avg $\# \mathrm{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \implies 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

Avg $\# \mathrm{Sel}_2(E)^2 \leq^\star 15$.

Idea of the Proof:

- Want to count pairs $(f, f') \in \mathrm{Sel}_2(E)^2$
- Fix $f \in \mathrm{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\Longrightarrow 2 \times 3 = 6$ choices for f' on avg
    - $\mathrm{Sel}_2(E) \simeq \mathrm{Sel}_2(\mathrm{J}(C_f))$, so Avg $\#\{\text{choices for f'}\} = $ Avg $\# \mathrm{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \Longrightarrow 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

$\text{Avg}\,\#\,\text{Sel}_2(E)^2 \leq^{\star} 15.$

Idea of the Proof:

- Want to count pairs $(f, f') \in \text{Sel}_2(E)^2$
- Fix $f \in \text{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \text{id} \in \text{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \text{id} \in \text{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\implies 2 \times 3 = 6$ choices for f' on avg
    - $\text{Sel}_2(E) \simeq \text{Sel}_2(\text{J}(C_f))$, so $\text{Avg}\,\#\{\text{choices for f'}\} = \text{Avg}\,\#\,\text{Sel}_2(\text{J}(C_f))$, where we work with binary quartic forms f up to $\text{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \implies 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

Avg $\# \,\mathrm{Sel}_2(E)^2 \leq^\star 15$.

Idea of the Proof:

- Want to count pairs $(f, f') \in \mathrm{Sel}_2(E)^2$
- Fix $f \in \mathrm{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\implies 2 \times 3 = 6$ choices for f' on avg
    - $\mathrm{Sel}_2(E) \simeq \mathrm{Sel}_2(\mathrm{J}(C_f))$, so Avg $\#\{\text{choices for f'}\} = $ Avg $\# \,\mathrm{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \implies 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

Avg $\# \mathrm{Sel}_2(E)^2 \leq^{\star} 15$.

Idea of the Proof:

- Want to count pairs $(f, f') \in \mathrm{Sel}_2(E)^2$
- Fix $f \in \mathrm{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\Longrightarrow 2 \times 3 = 6$ choices for f' on avg
    - $\mathrm{Sel}_2(E) \simeq \mathrm{Sel}_2(\mathrm{J}(C_f))$, so Avg $\#\{\text{choices for f'}\} = \text{Avg}\, \# \mathrm{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \Longrightarrow 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

$\mathrm{Avg}\,\#\,\mathrm{Sel}_2(E)^2 \leq^\star 15.$

Idea of the Proof:

- Want to count pairs $(f, f') \in \mathrm{Sel}_2(E)^2$
- Fix $f \in \mathrm{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\implies 2 \times 3 = 6$ choices for f' on avg
    - $\mathrm{Sel}_2(E) \simeq \mathrm{Sel}_2(\mathrm{J}(C_f))$, so $\mathrm{Avg}\,\#\{\text{choices for f'}\} = \mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \implies 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

Avg $\#\,\mathrm{Sel}_2(E)^2 \leq^\star 15$.

Idea of the Proof:

- Want to count pairs $(f, f') \in \mathrm{Sel}_2(E)^2$
- Fix $f \in \mathrm{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\implies 2 \times 3 = 6$ choices for f' on avg
    - $\mathrm{Sel}_2(E) \simeq \mathrm{Sel}_2(\mathrm{J}(C_f))$, so Avg $\#\{\text{choices for f'}\} =$ Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \implies 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

Avg $\# \operatorname{Sel}_2(E)^2 \leq^\star 15$.

Idea of the Proof:

- Want to count pairs $(f, f') \in \operatorname{Sel}_2(E)^2$
- Fix $f \in \operatorname{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \operatorname{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \operatorname{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\implies 2 \times 3 = 6$ choices for f' on avg
    - $\operatorname{Sel}_2(E) \simeq \operatorname{Sel}_2(\mathrm{J}(C_f))$, so Avg $\#\{\text{choices for f'}\} =$ Avg $\# \operatorname{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases 1, 2 $\implies 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

The Second Moment

Theorem (Bhargava, Shankar, and S., 2021)

Avg $\#\,\mathrm{Sel}_2(E)^2 \leq^\star 15$.

Idea of the Proof:

- Want to count pairs $(f, f') \in \mathrm{Sel}_2(E)^2$
- Fix $f \in \mathrm{Sel}_2(E)$, and consider 2 cases:
  - Case 1: $f = \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 3 choices for f' on avg
    - Proven by Bhargava–Shankar (2010)
  - Case 2: $f \neq \mathrm{id} \in \mathrm{Sel}_2(E)$
    - Heuristic: 2 choices for f on avg, and notice E has marked non-trivial 2-Selmer element $\implies 2 \times 3 = 6$ choices for f' on avg
    - $\mathrm{Sel}_2(E) \simeq \mathrm{Sel}_2(\mathrm{J}(C_f))$, so Avg $\#\{\text{choices for f'}\} =$ Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$, where we work with binary quartic forms f up to $\mathrm{PGL}_2(\mathbb{Q})$ action
- Combining Cases $1, 2 \implies 1 \times 3 + 2 \times 6 = 15$ choices for (f, f') on avg

Class Group Application

- Let $f \in \mathbb{Z}[x, y]$ be monic integral binary cubic form such that $R_f = \mathcal{O}_{K_f}$ (so that K_f is a monogenic cubic field)
- Class field theory $\Longrightarrow \mathrm{Cl}(R_f)[2]^* \hookrightarrow \mathrm{Sel}_2(y^2 = f(x, 1))$

Theorem (Bhargava, Shankar, and S., 2021)

When fields arising from monic integral binary cubic forms f with 3 (resp., 1) real roots are ordered by height, $\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2]^2 \leq^\star 3$ (*resp.*, 6).

# real roots	$\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2] =$	$\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2]^2 \leq^\star$
3	3/2 (5/4)	3 (15/8)
1	2 (3/2)	6 (3)

Class Group Application

- Let $f \in \mathbb{Z}[x,y]$ be monic integral binary cubic form such that $R_f = \mathcal{O}_{K_f}$ (so that K_f is a monogenic cubic field)
- Class field theory $\implies \mathrm{Cl}(R_f)[2]^* \hookrightarrow \mathrm{Sel}_2(y^2 = f(x,1))$

Theorem (Bhargava, Shankar, and S., 2021)

When fields arising from monic integral binary cubic forms f with 3 (resp., 1) real roots are ordered by height, $\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2]^2 \leq^* 3$ (*resp.*, 6).

# real roots	$\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2] =$	$\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2]^2 \leq^\star$
3	3/2 (5/4)	3 (15/8)
1	2 (3/2)	6 (3)

Class Group Application

- Let $f \in \mathbb{Z}[x, y]$ be monic integral binary cubic form such that $R_f = \mathcal{O}_{K_f}$ (so that K_f is a monogenic cubic field)
- Class field theory $\Longrightarrow \mathrm{Cl}(R_f)[2]^* \hookrightarrow \mathrm{Sel}_2(y^2 = f(x, 1))$

Theorem (Bhargava, Shankar, and S., 2021)

When fields arising from monic integral binary cubic forms f with 3 (*resp.,* 1) *real roots are ordered by height,* $\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2]^2 \leq^\star 3$ (*resp.,* 6).

# real roots	$\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2] =$	$\mathrm{Avg}_f \# \mathrm{Cl}(R_f)[2]^2 \leq^\star$
3	3/2 (5/4)	3 (15/8)
1	2 (3/2)	6 (3)

Class Group Application

- Let $f \in \mathbb{Z}[x, y]$ be monic integral binary cubic form such that $R_f = \mathcal{O}_{K_f}$ (so that K_f is a monogenic cubic field)
- Class field theory $\implies \mathrm{Cl}(R_f)[2]^* \hookrightarrow \mathrm{Sel}_2(y^2 = f(x, 1))$

Theorem (Bhargava, Shankar, and S., 2021)

When fields arising from monic integral binary cubic forms f with 3 (*resp.,* 1) *real roots are ordered by height,* $\mathrm{Avg}_f \, \# \, \mathrm{Cl}(R_f)[2]^2 \leq^{\star} 3$ (*resp.,* 6).

# real roots	$\mathrm{Avg}_f \, \# \, \mathrm{Cl}(R_f)[2] =$	$\mathrm{Avg}_f \, \# \, \mathrm{Cl}(R_f)[2]^2 \leq^{\star}$
3	3/2 (5/4)	3 (15/8)
1	2 (3/2)	6 (3)

Thank You!!