Growth of rational points on curves

Robert J. Lemke Oliver
Tufts University

(Actual theorems joint with Frank Thorne)

Diophantine stability

Let $C/\mathbb{Q}$ be a curve,

Diophantine stability

Let $C/\mathbb{Q}$ be a curve, and let

$$\mathcal{F}^C := \{K : K = \mathbb{Q}(P) \text{ for some } P \in C(\bar{\mathbb{Q}})\}$$

be the set of fields over which C gains a point.

Diophantine stability

Let $C/\mathbb{Q}$ be a curve, and let

$$\mathcal{F}^C := \{K : K = \mathbb{Q}(P) \text{ for some } P \in C(\bar{\mathbb{Q}})\}$$

be the set of fields over which C gains a point.

Question (Mazur–Rubin)

What does $\mathcal{F}^C$ look like?

Diophantine stability

Let $C/\mathbb{Q}$ be a curve, and let

$$\mathcal{F}^C := \{K : K = \mathbb{Q}(P) \text{ for some } P \in C(\bar{\mathbb{Q}})\}$$

be the set of fields over which C gains a point.

Question (Mazur–Rubin)

What does $\mathcal{F}^C$ look like? To what extent does it determine C?

Diophantine stability

Let $C/\mathbb{Q}$ be a curve, and let

$$\mathcal{F}^C := \{K : K = \mathbb{Q}(P) \text{ for some } P \in C(\bar{\mathbb{Q}})\}$$

be the set of fields over which C gains a point.

Question (Mazur–Rubin)

What does $\mathcal{F}^C$ look like? To what extent does it determine C?

Today: How does

$$\mathcal{F}_n^C(X; G) := \{K \in \mathcal{F}^C : [K : \mathbb{Q}] = n, \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G, |\mathrm{Disc}(K)| \leq X\}$$

behave?

Diophantine stability

Let $C/\mathbb{Q}$ be a curve, and let

$$\mathcal{F}^C := \{K : K = \mathbb{Q}(P) \text{ for some } P \in C(\bar{\mathbb{Q}})\}$$

be the set of fields over which C gains a point.

Question (Mazur–Rubin)

What does $\mathcal{F}^C$ look like? To what extent does it determine C?

Today: How does

$$\mathcal{F}_n^C(X; G) := \{K \in \mathcal{F}^C : [K : \mathbb{Q}] = n, \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G, |\mathrm{Disc}(K)| \leq X\}$$

behave?

Notation: When $C = \mathbb{P}^1_{\mathbb{Q}}$, we simply write $\mathcal{F}_n(X; G)$ instead.

Elliptic curves

Suppose $E/\mathbb{Q}$ is an elliptic curve.

Elliptic curves

Suppose $E/\mathbb{Q}$ is an elliptic curve. For a number field $K/\mathbb{Q}$, let

$$w(E_K) := (-1)^{\mathrm{rk}_{\mathrm{an}}(E_K)},$$

Elliptic curves

Suppose $E/\mathbb{Q}$ is an elliptic curve. For a number field $K/\mathbb{Q}$, let

$$w(E_K) := (-1)^{\mathrm{rk}_{\mathrm{an}}(E_K)},$$

and set $w(E, \rho_K) = w(E_K)/w(E_{\mathbb{Q}})$.

Elliptic curves

Suppose $E/\mathbb{Q}$ is an elliptic curve. For a number field $K/\mathbb{Q}$, let

$$w(E_K) := (-1)^{\mathrm{rk}_{\mathrm{an}}(E_K)},$$

and set $w(E, \rho_K) = w(E_K)/w(E_{\mathbb{Q}})$.

Philosophy ("Minimalist philosophy")

Suppose G is *primitive*,

Elliptic curves

Suppose $E/\mathbb{Q}$ is an elliptic curve. For a number field $K/\mathbb{Q}$, let

$$w(E_K) := (-1)^{\mathrm{rk}_{\mathrm{an}}(E_K)},$$

and set $w(E, \rho_K) = w(E_K)/w(E_{\mathbb{Q}})$.

Philosophy ("Minimalist philosophy")

Suppose G is *primitive*, i.e. $K \in \mathcal{F}_n(X; G)$ has no subfields.

Elliptic curves

Suppose $E/\mathbb{Q}$ is an elliptic curve. For a number field $K/\mathbb{Q}$, let

$$w(E_K) := (-1)^{\mathrm{rk}_{\mathrm{an}}(E_K)},$$

and set $w(E, \rho_K) = w(E_K)/w(E_{\mathbb{Q}})$.

Philosophy ("Minimalist philosophy")

Suppose G is *primitive*, i.e. $K \in \mathcal{F}_n(X; G)$ has no subfields. Then

- $K \in \mathcal{F}_n^E(X; G)$ for all $K \in \mathcal{F}_n(X; G)$ with $w(E, \rho_K) = -1$,

Elliptic curves

Suppose $E/\mathbb{Q}$ is an elliptic curve. For a number field $K/\mathbb{Q}$, let

$$w(E_K) := (-1)^{\mathrm{rk}_{\mathrm{an}}(E_K)},$$

and set $w(E, \rho_K) = w(E_K)/w(E_{\mathbb{Q}})$.

Philosophy ("Minimalist philosophy")

Suppose G is *primitive*, i.e. $K \in \mathcal{F}_n(X; G)$ has no subfields. Then

- $K \in \mathcal{F}_n^E(X; G)$ for all $K \in \mathcal{F}_n(X; G)$ with $w(E, \rho_K) = -1$,
- $K \in \mathcal{F}_n^E(X; G)$ for 0% of $K \in \mathcal{F}_n(X; G)$ with $w(E, \rho_K) = 1$.

Elliptic curves

Suppose $E/\mathbb{Q}$ is an elliptic curve. For a number field $K/\mathbb{Q}$, let

$$w(E_K) := (-1)^{\mathrm{rk}_{\mathrm{an}}(E_K)},$$

and set $w(E, \rho_K) = w(E_K)/w(E_{\mathbb{Q}})$.

Philosophy ("Minimalist philosophy")

Suppose G is *primitive*, i.e. $K \in \mathcal{F}_n(X; G)$ has no subfields. Then

- $K \in \mathcal{F}_n^E(X; G)$ for all $K \in \mathcal{F}_n(X; G)$ with $w(E, \rho_K) = -1$,
- $K \in \mathcal{F}_n^E(X; G)$ for 0% of $K \in \mathcal{F}_n(X; G)$ with $w(E, \rho_K) = 1$.

V. Dokchitser: Computes $w(E, \rho)$ for any Artin representation ρ.

Goldfeld's conjecture

Conjecture (Goldfeld; proved up to $\epsilon + \sqrt{\epsilon}$ by A. Smith, 2019)

If $E/\mathbb{Q}$ is an elliptic curve,

Goldfeld's conjecture

Conjecture (Goldfeld; proved up to $\epsilon + \sqrt{\epsilon}$ by A. Smith, 2019)

If $E/\mathbb{Q}$ is an elliptic curve, then:

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $\mathbb{Q}(\sqrt{d})$,

Goldfeld's conjecture

Conjecture (Goldfeld; proved up to $\epsilon + \sqrt{\epsilon}$ by A. Smith, 2019)

If $E/\mathbb{Q}$ is an elliptic curve, then:

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $\mathbb{Q}(\sqrt{d})$,
- $\mathrm{rk}(E)$ *grows by* 1 *for* 50% *of* $\mathbb{Q}(\sqrt{d})$,

Goldfeld's conjecture

Conjecture (Goldfeld; proved up to $\epsilon + \sqrt{\epsilon}$ by A. Smith, 2019)

If $E/\mathbb{Q}$ is an elliptic curve, then:

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $\mathbb{Q}(\sqrt{d})$,
- $\mathrm{rk}(E)$ *grows by* 1 *for* 50% *of* $\mathbb{Q}(\sqrt{d})$, *and*
- $\mathrm{rk}(E)$ *grows by* ≥ 2 *for* 0% *of* $\mathbb{Q}(\sqrt{d})$.

Goldfeld's conjecture

Conjecture (Goldfeld; proved up to $\epsilon + \sqrt{\epsilon}$ by A. Smith, 2019)

If $E/\mathbb{Q}$ is an elliptic curve, then:

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $\mathbb{Q}(\sqrt{d})$,
- $\mathrm{rk}(E)$ *grows by* 1 *for* 50% *of* $\mathbb{Q}(\sqrt{d})$, *and*
- $\mathrm{rk}(E)$ *grows by* ≥ 2 *for* 0% *of* $\mathbb{Q}(\sqrt{d})$.

Theorem (Gouvêa–Mazur)

$$\#\{K \in \mathcal{F}_2^E(X) : w(E, \rho_K) = +1\} \gg X^{1/2-\epsilon}.$$

Goldfeld's conjecture

Conjecture (Goldfeld; proved up to $\epsilon + \sqrt{\epsilon}$ by A. Smith, 2019)

If $E/\mathbb{Q}$ is an elliptic curve, then:

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $\mathbb{Q}(\sqrt{d})$,
- $\mathrm{rk}(E)$ *grows by* 1 *for* 50% *of* $\mathbb{Q}(\sqrt{d})$, *and*
- $\mathrm{rk}(E)$ *grows by* ≥ 2 *for* 0% *of* $\mathbb{Q}(\sqrt{d})$.

Theorem (Gouvêa–Mazur)

$$\#\{K \in \mathcal{F}_2^E(X) : w(E, \rho_K) = +1\} \gg X^{1/2-\epsilon}.$$

In particular, $\mathrm{rk}_{\mathrm{an}}(E)$ *grows by (at least)* 2 *in* $X^{1/2-\epsilon}$ *fields.*

Nonabelian twists

Nonabelian twists

Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve.

Nonabelian twists

Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$, as $X \to \infty$,

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $K \in \mathcal{F}_n(X; S_n)$,

Nonabelian twists

Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$, as $X \to \infty$,

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $K \in \mathcal{F}_n(X; S_n)$,
- $\mathrm{rk}(E)$ *grows by* 1 *in* 50% *of* $K \in \mathcal{F}_n(X; S_n)$,

Nonabelian twists

Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$, as $X \to \infty$,

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $K \in \mathcal{F}_n(X; S_n)$,
- $\mathrm{rk}(E)$ *grows by* 1 *in* 50% *of* $K \in \mathcal{F}_n(X; S_n)$, *and*
- $\mathrm{rk}(E)$ *grows by* ≥ 2 *in* 0% *of* $K \in \mathcal{F}_n(X; S_n)$.

Nonabelian twists

Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$, as $X \to \infty$,

- $\mathrm{rk}(E)$ *doesn't grow in* 50% *of* $K \in \mathcal{F}_n(X; S_n)$,
- $\mathrm{rk}(E)$ *grows by* 1 *in* 50% *of* $K \in \mathcal{F}_n(X; S_n)$, *and*
- $\mathrm{rk}(E)$ *grows by* ≥ 2 *in* 0% *of* $K \in \mathcal{F}_n(X; S_n)$.

"Theorem" (LO–Thorne)

There's an analogue of Gouvêa–Mazur for twists by $K \in \mathcal{F}_n(X; S_n)$.

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\#\mathcal{F}_n^E(X; S_n)$$

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\#\mathcal{F}_n^E(X; S_n) \quad = \quad \#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))\}$$

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\begin{aligned} \#\mathcal{F}_n^E(X; S_n) &= \#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))\} \\ &\gg X^{c_n - \epsilon}, \end{aligned}$$

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\begin{aligned} \#\mathcal{F}_n^E(X; S_n) &= \#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))\} \\ &\gg X^{c_n - \epsilon}, \end{aligned}$$

where

$$c_n = \begin{cases} 1/n & n \leq 5 \\ & \\ & \end{cases}$$

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\begin{aligned} \#\mathcal{F}_n^E(X; S_n) &= \#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))\} \\ &\gg X^{c_n - \epsilon}, \end{aligned}$$

where

$$c_n = \begin{cases} 1/n & n \leq 5 \\ 1/5 & n = 6 \\ \\ \\ \end{cases}$$

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\begin{aligned}\#\mathcal{F}_n^E(X; S_n) &= \#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))\} \\ &\gg X^{c_n - \epsilon},\end{aligned}$$

where

$$c_n = \begin{cases} 1/n & n \leq 5 \\ 1/5 & n = 6 \\ 1/6 & n = 7, 8 \\ & \end{cases}$$

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\begin{aligned} \#\mathcal{F}_n^E(X; S_n) &= \#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))\} \\ &\gg X^{c_n - \epsilon}, \end{aligned}$$

where

$$c_n = \begin{cases} 1/n & n \leq 5 \\ 1/5 & n = 6 \\ 1/6 & n = 7, 8 \\ \frac{1}{4} - \frac{n^2+4n-2}{2n^2(n-1)} & n \geq 9. \end{cases}$$

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\begin{aligned} \#\mathcal{F}_n^E(X; S_n) &= \#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))\} \\ &\gg X^{c_n - \epsilon}, \end{aligned}$$

where

$$c_n = \begin{cases} 1/n & n \leq 5 \\ 1/5 & n = 6 \\ 1/6 & n = 7, 8 \\ \frac{1}{4} - \frac{n^2+4n-2}{2n^2(n-1)} & n \geq 9. \end{cases}$$

Same bound when $w(E, \rho_K) = 1$ and when $w(E, \rho_K) = -1$.

Rank growth of nonabelian twists

Theorem (LO–Thorne)

Let $E/\mathbb{Q}$ be an elliptic curve. For any $n \geq 2$,

$$\begin{aligned} \#\mathcal{F}_n^E(X; S_n) &= \#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))\} \\ &\gg X^{c_n - \epsilon}, \end{aligned}$$

where

$$c_n = \begin{cases} 1/n & n \leq 5 \\ 1/5 & n = 6 \\ 1/6 & n = 7, 8 \\ \frac{1}{4} - \frac{n^2+4n-2}{2n^2(n-1)} & n \geq 9. \end{cases}$$

Same bound when $w(E, \rho_K) = 1$ and when $w(E, \rho_K) = -1$.

Corollary

$\mathrm{rk}_{\mathrm{an}}(E)$ *grows by ≥ 2 in at least $X^{1/3-\epsilon}$ fields $K \in \mathcal{F}_3(X; S_3)$.*

Rank two quadratic twists

Theorem (Gouvêa–Mazur)

$\mathrm{rk}_{\mathrm{an}}(E)$ *grows by* ≥ 2 *in* $\gg X^{1/2-\epsilon}$ *fields* $\mathbb{Q}(\sqrt{d})$ *with* $|d| \leq X$*.*

Rank two quadratic twists

Theorem (Gouvêa–Mazur)

$\mathrm{rk}_{\mathrm{an}}(E)$ *grows by* ≥ 2 *in* $\gg X^{1/2-\epsilon}$ *fields* $\mathbb{Q}(\sqrt{d})$ *with* $|d| \leq X$.

Idea: If $E\colon y^2 = x^3 + Ax + B$,

Rank two quadratic twists

Theorem (Gouvêa–Mazur)

$\mathrm{rk}_{\mathrm{an}}(E)$ *grows by* ≥ 2 *in* $\gg X^{1/2-\epsilon}$ *fields* $\mathbb{Q}(\sqrt{d})$ *with* $|d| \leq X$.

Idea: If $E\colon y^2 = x^3 + Ax + B$, choose any $x \in \mathbb{Q}$.

Rank two quadratic twists

Theorem (Gouvêa–Mazur)

$\mathrm{rk}_{\mathrm{an}}(E)$ grows by ≥ 2 in $\gg X^{1/2-\epsilon}$ fields $\mathbb{Q}(\sqrt{d})$ with $|d| \leq X$.

Idea: If $E\colon y^2 = x^3 + Ax + B$, choose any $x \in \mathbb{Q}$.

If $x = u/v$ for coprime u, v,

Rank two quadratic twists

Theorem (Gouvêa–Mazur)

$\mathrm{rk}_{\mathrm{an}}(E)$ grows by ≥ 2 in $\gg X^{1/2-\epsilon}$ fields $\mathbb{Q}(\sqrt{d})$ with $|d| \leq X$.

Idea: If $E\colon y^2 = x^3 + Ax + B$, choose any $x \in \mathbb{Q}$.

If $x = u/v$ for coprime u, v, then

$$v^4 y^2 = v(u^3 + Auv^2 + Bv^3).$$

Rank two quadratic twists

Theorem (Gouvêa–Mazur)

$\mathrm{rk}_{\mathrm{an}}(E)$ *grows by* ≥ 2 *in* $\gg X^{1/2-\epsilon}$ *fields* $\mathbb{Q}(\sqrt{d})$ *with* $|d| \leq X$.

Idea: If $E\colon y^2 = x^3 + Ax + B$, choose any $x \in \mathbb{Q}$.

If $x = u/v$ for coprime u, v, then

$$v^4 y^2 = v(u^3 + Auv^2 + Bv^3).$$

Choosing $|u|, |v| \leq X^{1/4}$

Rank two quadratic twists

Theorem (Gouvêa–Mazur)

$\mathrm{rk}_{\mathrm{an}}(E)$ grows by ≥ 2 in $\gg X^{1/2-\epsilon}$ fields $\mathbb{Q}(\sqrt{d})$ with $|d| \leq X$.

Idea: If $E\colon y^2 = x^3 + Ax + B$, choose any $x \in \mathbb{Q}$.

If $x = u/v$ for coprime u, v, then

$$v^4 y^2 = v(u^3 + Auv^2 + Bv^3).$$

Choosing $|u|, |v| \leq X^{1/4} \Longrightarrow |\mathrm{RHS}| \leq X$.

Rank two quadratic twists

Theorem (Gouvêa–Mazur)

$\mathrm{rk}_{\mathrm{an}}(E)$ grows by ≥ 2 in $\gg X^{1/2-\epsilon}$ fields $\mathbb{Q}(\sqrt{d})$ with $|d| \leq X$.

Idea: If $E\colon y^2 = x^3 + Ax + B$, choose any $x \in \mathbb{Q}$.

If $x = u/v$ for coprime u, v, then

$$v^4 y^2 = v(u^3 + Auv^2 + Bv^3).$$

Choosing $|u|, |v| \leq X^{1/4} \Longrightarrow |\mathrm{RHS}| \leq X$.

Problem

How do we distinguish the fields $\mathbb{Q}(\sqrt{v(u^3 + Auv^2 + Bv^3)})$?

Distinguishing quadratic fields

Problem

How do we distinguish the fields $\mathbb{Q}(\sqrt{v(u^3 + Auv^2 + Bv^3)})$*?*

Distinguishing quadratic fields

Problem

How do we distinguish the fields $\mathbb{Q}(\sqrt{v(u^3 + Auv^2 + Bv^3)})$*?*

Gouvêa and Mazur show that:

1. $v(u^3 + Auv^2 + Bv^3)$ assumes $\gg X^{1/2}$ *squarefree* values $\leq X$,

Distinguishing quadratic fields

Problem

How do we distinguish the fields $\mathbb{Q}(\sqrt{v(u^3 + Auv^2 + Bv^3)})$*?*

Gouvêa and Mazur show that:

1. $v(u^3 + Auv^2 + Bv^3)$ assumes $\gg X^{1/2}$ *squarefree* values $\leq X$,
2. any particular value arises $\ll X^{\epsilon}$ times.

Distinguishing quadratic fields

Problem

How do we distinguish the fields $\mathbb{Q}(\sqrt{v(u^3 + Auv^2 + Bv^3)})$*?*

Gouvêa and Mazur show that:

1. $v(u^3 + Auv^2 + Bv^3)$ assumes $\gg X^{1/2}$ *squarefree* values $\leq X$,
2. any particular value arises $\ll X^{\epsilon}$ times.

$\Longrightarrow \mathrm{rk}(E)$ grows in at least $X^{1/2-\epsilon}$ fields $K \in \mathcal{F}_2(X)$.

Distinguishing quadratic fields

Problem

How do we distinguish the fields $\mathbb{Q}(\sqrt{v(u^3 + Auv^2 + Bv^3)})$*?*

Gouvêa and Mazur show that:

1. $v(u^3 + Auv^2 + Bv^3)$ assumes $\gg X^{1/2}$ *squarefree* values $\leq X$,
2. any particular value arises $\ll X^{\epsilon}$ times.

$\Longrightarrow \mathrm{rk}(E)$ grows in at least $X^{1/2-\epsilon}$ fields $K \in \mathcal{F}_2(X)$.

Get growth ≥ 2 of $\mathrm{rk}_{\mathrm{an}}(E)$ by controlling the root number.

First parametrization in higher degree fields

First parametrization in higher degree fields

If $E\colon y^2 = f(x)$ and n is even,

First parametrization in higher degree fields

If $E\colon y^2 = f(x)$ and n is even, then $(x, tx^{n/2})$ is a point on $E(K_t)$,

First parametrization in higher degree fields

If $E\colon y^2 = f(x)$ and n is even, then $(x, tx^{n/2})$ is a point on $E(K_t)$, where

$$K_t := \mathbb{Q}(t)[x]/P_f(x,t), \quad P_f(x,t) := t^2x^n - f(x).$$

First parametrization in higher degree fields

If $E\colon y^2 = f(x)$ and n is even, then $(x, tx^{n/2})$ is a point on $E(K_t)$, where

$$K_t := \mathbb{Q}(t)[x]/P_f(x,t), \quad P_f(x,t) := t^2x^n - f(x).$$

Proposition

There is a model $E\colon y^2 = f(x)$ s.t. $\mathrm{Gal}(\widetilde{K_t}/\mathbb{Q}(t)) \simeq S_n$.

First parametrization in higher degree fields

If $E\colon y^2 = f(x)$ and n is even, then $(x, tx^{n/2})$ is a point on $E(K_t)$, where

$$K_t := \mathbb{Q}(t)[x]/P_f(x,t), \quad P_f(x,t) := t^2x^n - f(x).$$

Proposition

There is a model $E\colon y^2 = f(x)$ s.t. $\mathrm{Gal}(\widetilde{K_t}/\mathbb{Q}(t)) \simeq S_n$.

Get many $K \in \mathcal{F}_n(X; S_n)$ in which $\mathrm{rk}(E)$ grows by specializing t

First parametrization in higher degree fields

If $E\colon y^2 = f(x)$ and n is even, then $(x, tx^{n/2})$ is a point on $E(K_t)$, where

$$K_t := \mathbb{Q}(t)[x]/P_f(x,t), \quad P_f(x,t) := t^2x^n - f(x).$$

Proposition

There is a model $E\colon y^2 = f(x)$ s.t. $\mathrm{Gal}(\widetilde{K_t}/\mathbb{Q}(t)) \simeq S_n$.

Get many $K \in \mathcal{F}_n(X; S_n)$ in which $\mathrm{rk}(E)$ grows by specializing t, provided we can control multiplicities!

First parametrization: Controlling multiplicities

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

First parametrization: Controlling multiplicities

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma

If $t = u/v$, then $\mathrm{Disc}_x(P_f(x, u/v)) = u^{2n-4} v^{4-2n} H(u,v)$ for a not-squarefull sextic form $H(u,v)$.

First parametrization: Controlling multiplicities

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma

If $t = u/v$, then $\mathrm{Disc}_x(P_f(x, u/v)) = u^{2n-4} v^{4-2n} H(u,v)$ for a not-squarefull sextic form $H(u,v)$.

Theorem (Greaves)

Any "not obstructed" form $H(u,v)$ of degree ≤ 6 assumes $\gg T^2$ squarefree values with $|u|, |v| \leq T$.

First parametrization: Controlling multiplicities

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma

If $t = u/v$, then $\mathrm{Disc}_x(P_f(x,u/v)) = u^{2n-4} v^{4-2n} H(u,v)$ for a not-squarefull sextic form $H(u,v)$.

Theorem (Greaves)

Any "not obstructed" form $H(u,v)$ of degree ≤ 6 assumes $\gg T^2$ squarefree values with $|u|,|v| \leq T$.

Each value occurs $\ll X^\epsilon$ times

First parametrization: Controlling multiplicities

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma

If $t = u/v$, then $\mathrm{Disc}_x(P_f(x,u/v)) = u^{2n-4} v^{4-2n} H(u,v)$ for a not-squarefull sextic form $H(u,v)$.

Theorem (Greaves)

Any "not obstructed" form $H(u,v)$ of degree ≤ 6 assumes $\gg T^2$ squarefree values with $|u|,|v| \leq T$.

Each value occurs $\ll X^{\epsilon}$ times $\Longrightarrow$ there are $\gg X^{2/(n+4)-\epsilon}$ fields K_t with $|\mathrm{Disc}(K_t)| \leq X$.

How do we control root numbers?

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

How do we control root numbers?

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma (V. Dokchitser)

If K and $K' \in \mathcal{F}_n(X; S_n)$ are such that

How do we control root numbers?

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma (V. Dokchitser)

If K and $K' \in \mathcal{F}_n(X; S_n)$ are such that

- $K \otimes \mathbb{Q}_p \simeq K' \otimes \mathbb{Q}_p$ *for each* $p \mid N_E$,

How do we control root numbers?

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma (V. Dokchitser)

If K and $K' \in \mathcal{F}_n(X; S_n)$ are such that

- $K \otimes \mathbb{Q}_p \simeq K' \otimes \mathbb{Q}_p$ *for each* $p \mid N_E$, *and*
- $\mathrm{sgn}(\mathrm{Disc}(K)) = -\mathrm{sgn}(\mathrm{Disc}(K'))$,

How do we control root numbers?

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma (V. Dokchitser)

If K and $K' \in \mathcal{F}_n(X; S_n)$ are such that

- $K \otimes \mathbb{Q}_p \simeq K' \otimes \mathbb{Q}_p$ *for each* $p \mid N_E$, *and*
- $\mathrm{sgn}(\mathrm{Disc}(K)) = -\mathrm{sgn}(\mathrm{Disc}(K'))$,

then $w(E, \rho_K) = -w(E, \rho_{K'})$.

How do we control root numbers?

(**Recall:** $P_f(x,t) = x^n t^2 - f(x)$ and $K_t = \mathbb{Q}(t)[x]/P_f(x,t)$.)

Lemma (V. Dokchitser)

If K and $K' \in \mathcal{F}_n(X; S_n)$ are such that

- $K \otimes \mathbb{Q}_p \simeq K' \otimes \mathbb{Q}_p$ *for each* $p \mid N_E$*, and*
- $\mathrm{sgn}(\mathrm{Disc}(K)) = -\mathrm{sgn}(\mathrm{Disc}(K'))$*,*

then $w(E, \rho_K) = -w(E, \rho_{K'})$*.*

Theorem

The number of $K \in \mathcal{F}_n(X; S_n)$ s.t. $\mathrm{rk}(E(K)) > \mathrm{rk}(E(\mathbb{Q}))$ and $w(E, \rho_K) = +1$ is $\gg X^{1/(\lceil \frac{n}{2} \rceil + 2) - \epsilon}$*.*

Second Parametrization

If n is even,

Second Parametrization

If n is even, let $F, G \in \mathbb{Z}[x]$ have degree $n/2$ and $n/2 - 2$, resp.

Second Parametrization

If n is even, let $F, G \in \mathbb{Z}[x]$ have degree $n/2$ and $n/2 - 2$, resp. Then $(x, \frac{F(x)}{G(x)})$ is on $E(K_{F,G})$,

Second Parametrization

If n is even, let $F, G \in \mathbb{Z}[x]$ have degree $n/2$ and $n/2-2$, resp. Then $(x, \frac{F(x)}{G(x)})$ is on $E(K_{F,G})$, where

$$K_{F,G} = \mathbb{Q}[x]/(F^2 - fG^2).$$

Second Parametrization

If n is even, let $F, G \in \mathbb{Z}[x]$ have degree $n/2$ and $n/2-2$, resp. Then $(x, \frac{F(x)}{G(x)})$ is on $E(K_{F,G})$, where

$$K_{F,G} = \mathbb{Q}[x]/(F^2 - fG^2).$$

Lemma

$\mathrm{Gal}(\widetilde{K_{F,G}}/\mathbb{Q}) \simeq S_n$ *for almost all* F, G*.*

Second Parametrization

If n is even, let $F, G \in \mathbb{Z}[x]$ have degree $n/2$ and $n/2-2$, resp. Then $(x, \frac{F(x)}{G(x)})$ is on $E(K_{F,G})$, where

$$K_{F,G} = \mathbb{Q}[x]/(F^2 - fG^2).$$

Lemma

$\mathrm{Gal}(\widetilde{K_{F,G}}/\mathbb{Q}) \simeq S_n$ *for almost all* F, G.

Proof.

If $F(x) = tx^{n/2}$ and $G(x) = 1$,

Second Parametrization

If n is even, let $F, G \in \mathbb{Z}[x]$ have degree $n/2$ and $n/2 - 2$, resp. Then $(x, \frac{F(x)}{G(x)})$ is on $E(K_{F,G})$, where

$$K_{F,G} = \mathbb{Q}[x]/(F^2 - fG^2).$$

Lemma
$\mathrm{Gal}(\widetilde{K_{F,G}}/\mathbb{Q}) \simeq S_n$ *for almost all* F, G.

Proof.
If $F(x) = tx^{n/2}$ and $G(x) = 1$, then $K_{F,G} = K_t$.

Second Parametrization

If n is even, let $F, G \in \mathbb{Z}[x]$ have degree $n/2$ and $n/2 - 2$, resp. Then $(x, \frac{F(x)}{G(x)})$ is on $E(K_{F,G})$, where

$$K_{F,G} = \mathbb{Q}[x]/(F^2 - fG^2).$$

Lemma

$\mathrm{Gal}(\widetilde{K_{F,G}}/\mathbb{Q}) \simeq S_n$ for almost all F, G.

Proof.

If $F(x) = tx^{n/2}$ and $G(x) = 1$, then $K_{F,G} = K_t$. Now use Hilbert Irreducibility. □

Second Parametrization: Controlling Multiplicities

Question

How do we control the multiplicity of $K_{F,G} = \mathbb{Q}[x]/(F^2 - fG^2)$?

Second Parametrization: Controlling Multiplicities

Question

How do we control the multiplicity of $K_{F,G} = \mathbb{Q}[x]/(F^2 - fG^2)$?

Lemma

Given $f, H \in \mathbb{Z}[x]$, there are $O_n(1)$ solutions F, G to $H = F^2 - fG^2$.

Second Parametrization: Controlling Multiplicities

Question

How do we control the multiplicity of $K_{F,G} = \mathbb{Q}[x]/(F^2 - fG^2)$?

Lemma

Given $f, H \in \mathbb{Z}[x]$, there are $O_n(1)$ solutions F, G to $H = F^2 - fG^2$.

Question

How do we make sure the same field isn't cut out by lots of polynomials?

Multiplicities of fields

Let

$$\mathcal{S}_n(Y) := \{g(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x] : |a_i| \le Y^i\}.$$

Multiplicities of fields

Let

$$\mathcal{S}_n(Y) := \{g(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x] : |a_i| \leq Y^i\}.$$

(**Note:** If $g \in \mathcal{S}_n(Y)$, then $|\mathrm{Disc}(g)| \ll Y^{n(n-1)}$.)

Multiplicities of fields

Let

$$\mathcal{S}_n(Y) := \{g(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x] : |a_i| \le Y^i\}.$$

(**Note:** If $g \in \mathcal{S}_n(Y)$, then $|\mathrm{Disc}(g)| \ll Y^{n(n-1)}$.)

Lemma (Ellenberg–Venkatesh + $\epsilon\cdot$(LO–Thorne))

If $K \in \mathcal{F}_n(X)$, then

$\#\{g \in \mathcal{S}_n(Y) : \mathbb{Q}[x]/g \simeq K\}$

Multiplicities of fields

Let

$$\mathcal{S}_n(Y) := \{g(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x] : |a_i| \leq Y^i\}.$$

(**Note:** If $g \in \mathcal{S}_n(Y)$, then $|\mathrm{Disc}(g)| \ll Y^{n(n-1)}$.)

Lemma (Ellenberg–Venkatesh + $\epsilon \cdot$(LO–Thorne))

If $K \in \mathcal{F}_n(X)$, then

$\#\{g \in \mathcal{S}_n(Y) : \mathbb{Q}[x]/g \simeq K\} \ll \max\left\{ Y^n \mathrm{Disc}(K)^{-1/2}, Y^{n/2} \right\}.$

Multiplicities of fields

Let

$$\mathcal{S}_n(Y) := \{g(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x] : |a_i| \le Y^i\}.$$

(**Note:** If $g \in \mathcal{S}_n(Y)$, then $|\mathrm{Disc}(g)| \ll Y^{n(n-1)}$.)

Lemma (Ellenberg–Venkatesh + $\epsilon\cdot$(LO–Thorne))

If $K \in \mathcal{F}_n(X)$, then
$\#\{g \in \mathcal{S}_n(Y) : \mathbb{Q}[x]/g \simeq K\} \ll \max\left\{Y^n \mathrm{Disc}(K)^{-1/2}, Y^{n/2}\right\}$.

$\Longrightarrow \#\{|\mathrm{Disc}(K_{F,G})| \le X\}/\mathrm{iso.}$

Multiplicities of fields

Let

$$\mathcal{S}_n(Y) := \{g(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x] : |a_i| \leq Y^i\}.$$

(**Note:** If $g \in \mathcal{S}_n(Y)$, then $|\mathrm{Disc}(g)| \ll Y^{n(n-1)}$.)

Lemma (Ellenberg–Venkatesh + $\epsilon\cdot$(LO–Thorne))

If $K \in \mathcal{F}_n(X)$, then
$\#\{g \in \mathcal{S}_n(Y) : \mathbb{Q}[x]/g \simeq K\} \ll \max\left\{Y^n \mathrm{Disc}(K)^{-1/2}, Y^{n/2}\right\}.$

$$\implies \#\{|\mathrm{Disc}(K_{F,G})| \leq X\}/\mathrm{iso.} \gg X^{\frac{1}{4} - \frac{n^2+4n-2}{2n^2(n-1)}}.$$

The limit of the method

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve.

The limit of the method

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. If for each $K \in \mathcal{F}_n(X; S_n)$,

- *$L(s, E_K)$ is automorphic,*

The limit of the method

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. If for each $K \in \mathcal{F}_n(X; S_n)$,

- *$L(s, E_K)$ is automorphic,*
- *$L(s, E_K)$ satisfies GRH,*

The limit of the method

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. If for each $K \in \mathcal{F}_n(X; S_n)$,

- $L(s, E_K)$ *is automorphic,*
- $L(s, E_K)$ *satisfies GRH, and*
- $L(s, E_K)$ *satisfies BSD,*

The limit of the method

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. If for each $K \in \mathcal{F}_n(X; S_n)$,

- $L(s, E_K)$ *is automorphic,*
- $L(s, E_K)$ *satisfies GRH, and*
- $L(s, E_K)$ *satisfies BSD,*

then

$$\#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) \geq 2 + \mathrm{rk}(E(\mathbb{Q}))\}$$

The limit of the method

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. If for each $K \in \mathcal{F}_n(X; S_n)$,

- *$L(s, E_K)$ is automorphic,*
- *$L(s, E_K)$ satisfies GRH, and*
- *$L(s, E_K)$ satisfies BSD,*

then

$$\#\{K \in \mathcal{F}_n(X; S_n) : \mathrm{rk}(E(K)) \geq 2 + \mathrm{rk}(E(\mathbb{Q}))\} \gg X^{\frac{1}{4} + \frac{1}{2(n^2 - n)}}.$$

But what's the truth?

But what's the truth?

Conjecture (Birch–Swinnerton-Dyer)

If $r = \mathrm{rk}(E)$, then $r = \mathrm{ord}_{s=1} L(s, E)$ and

$$\frac{L^{(r)}(1, E)}{r!} = \frac{|\text{Ш}(E)| \mathrm{Reg}(E) \mathrm{Tam}(E) \Omega_{\mathbb{R}}(E)}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

But what's the truth?

Conjecture (Birch–Swinnerton-Dyer)

If $r = \mathrm{rk}(E)$*, then* $r = \mathrm{ord}_{s=1} L(s, E)$ *and*

$$\frac{L^{(r)}(1, E)}{r!} = \frac{|Ш(E)|\mathrm{Reg}(E)\mathrm{Tam}(E)\Omega_{\mathbb{R}}(E)}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

Conjecture (Tate's Séminaire Bourbaki)

If $K/\mathbb{Q}$ *has sig.* (r_1, r_2) *and* $r = \mathrm{rk}(E_K)$*,*

But what's the truth?

Conjecture (Birch–Swinnerton-Dyer)

If $r = \mathrm{rk}(E)$, *then* $r = \mathrm{ord}_{s=1} L(s, E)$ *and*

$$\frac{L^{(r)}(1, E)}{r!} = \frac{|\text{Ш}(E)|\mathrm{Reg}(E)\mathrm{Tam}(E)\Omega_{\mathbb{R}}(E)}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

Conjecture (Tate's Séminaire Bourbaki)

If $K/\mathbb{Q}$ *has sig.* (r_1, r_2) *and* $r = \mathrm{rk}(E_K)$, *then* $r = \mathrm{ord}_{s=1} L(s, E_K)$ *and*

$$\frac{L^{(r)}(1, E_K)}{r!} = \frac{|\text{Ш}(E_K)|\mathrm{Reg}(E_K)\mathrm{Tam}(E_K)\Omega_{\mathbb{R}}(E)^{r_1}\Omega_{\mathbb{C}}(E)^{r_2}}{|\mathrm{Disc}(K)|^{1/2}|E(K)_{\mathrm{tors}}|^2}.$$

But what's the truth?

Conjecture (Birch–Swinnerton-Dyer)

If $r = \mathrm{rk}(E)$*, then* $r = \mathrm{ord}_{s=1} L(s, E)$ *and*

$$\frac{L^{(r)}(1, E)}{r!} = \frac{|\text{Ш}(E)|\mathrm{Reg}(E)\mathrm{Tam}(E)\Omega_{\mathbb{R}}(E)}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

Conjecture (Tate's Séminaire Bourbaki)

If $K/\mathbb{Q}$ *has sig.* (r_1, r_2) *and* $r = \mathrm{rk}(E_K)$*, then* $r = \mathrm{ord}_{s=1} L(s, E_K)$ *and*

$$\frac{L^{(r)}(1, E_K)}{r!} = \frac{|\text{Ш}(E_K)|\mathrm{Reg}(E_K)\mathrm{Tam}(E_K)\Omega_{\mathbb{R}}(E)^{r_1}\Omega_{\mathbb{C}}(E)^{r_2}}{|\mathrm{Disc}(K)|^{1/2}|E(K)_{\mathrm{tors}}|^2}.$$

Idea: Pay attention to the case when $\mathrm{rk}(E_{\mathbb{Q}}) = \mathrm{rk}(E_K)$.

Relative rank zero BSD

Conjecture

Let $L(s, E, \rho_K) = L(s, E_K)/L(s, E)$.

Relative rank zero BSD

Conjecture

Let $L(s, E, \rho_K) = L(s, E_K)/L(s, E)$*. If* $E(K) = E(\mathbb{Q})$*, then*

$$L(1, E, \rho_K) = \frac{|\text{Ш}(E_K)|}{|\text{Ш}(E)|} \frac{\mathrm{Tam}(E_K)}{\mathrm{Tam}(E)} \frac{\Omega_{\mathbb{R}}(E)^{r_1 - 1}\Omega_{\mathbb{C}}(E)^{r_2}}{|\mathrm{Disc}(K)|^{1/2}}.$$

Relative rank zero BSD

Conjecture

Let $L(s, E, \rho_K) = L(s, E_K)/L(s, E)$. If $E(K) = E(\mathbb{Q})$, then

$$L(1, E, \rho_K) = \frac{|\text{Ш}(E_K)|}{|\text{Ш}(E)|} \frac{\mathrm{Tam}(E_K)}{\mathrm{Tam}(E)} \frac{\Omega_{\mathbb{R}}(E)^{r_1 - 1}\Omega_{\mathbb{C}}(E)^{r_2}}{|\mathrm{Disc}(K)|^{1/2}}.$$

Expect: $L(1, E, \rho_K), \mathrm{Tam}(E_K) \ll (\mathrm{ht}(E)|\mathrm{Disc}(K)|)^{\epsilon} =: Q^{\epsilon}$,

Relative rank zero BSD

Conjecture

Let $L(s, E, \rho_K) = L(s, E_K)/L(s, E)$. If $E(K) = E(\mathbb{Q})$, then

$$L(1, E, \rho_K) = \frac{|\text{Ш}(E_K)|}{|\text{Ш}(E)|} \frac{\mathrm{Tam}(E_K)}{\mathrm{Tam}(E)} \frac{\Omega_{\mathbb{R}}(E)^{r_1 - 1}\Omega_{\mathbb{C}}(E)^{r_2}}{|\mathrm{Disc}(K)|^{1/2}}.$$

Expect: $L(1, E, \rho_K), \mathrm{Tam}(E_K) \ll (\mathrm{ht}(E)|\mathrm{Disc}(K)|)^{\epsilon} =: Q^{\epsilon}$, so

$$\frac{|\text{Ш}(E_K)|}{|\text{Ш}(E)|} \ll \frac{|\mathrm{Disc}(K)|^{1/2}}{\Omega_{\mathbb{R}}(E)^{r_1 - 1}\Omega_{\mathbb{C}}(E)^{r_2}} Q^{\epsilon}.$$

Relative rank zero BSD

Conjecture

Let $L(s, E, \rho_K) = L(s, E_K)/L(s, E)$. If $E(K) = E(\mathbb{Q})$, then

$$L(1, E, \rho_K) = \frac{|\text{Ш}(E_K)|}{|\text{Ш}(E)|}\frac{\mathrm{Tam}(E_K)}{\mathrm{Tam}(E)}\frac{\Omega_{\mathbb{R}}(E)^{r_1-1}\Omega_{\mathbb{C}}(E)^{r_2}}{|\mathrm{Disc}(K)|^{1/2}}.$$

Expect: $L(1, E, \rho_K), \mathrm{Tam}(E_K) \ll (\mathrm{ht}(E)|\mathrm{Disc}(K)|)^{\epsilon} =: Q^{\epsilon}$, so

$$\frac{|\text{Ш}(E_K)|}{|\text{Ш}(E)|} \ll \frac{|\mathrm{Disc}(K)|^{1/2}}{\Omega_{\mathbb{R}}(E)^{r_1-1}\Omega_{\mathbb{C}}(E)^{r_2}}Q^{\epsilon}.$$

Crude model: $|\text{Ш}(E_K)/\text{Ш}(E)| = m^2$ uniformly with

$$m \ll \frac{|\mathrm{Disc}(K)|^{1/4}Q^{\epsilon}}{\Omega_{\mathbb{R}}(E)^{\frac{r_1-1}{2}}\Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}.$$

An embarrassingly crude model

We thus expect

$$L(1, E, \rho_K) = m^2 \cdot (\text{Invariants of } E)$$

with

$$m \ll \frac{|\mathrm{Disc}(K)|^{1/4} Q^{\epsilon}}{\Omega_{\mathbb{R}}(E)^{\frac{r_1 - 1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}.$$

An embarrassingly crude model

We thus expect

$$L(1, E, \rho_K) = m^2 \cdot (\text{Invariants of } E)$$

with

$$m \ll \frac{|\mathrm{Disc}(K)|^{1/4} Q^{\epsilon}}{\Omega_{\mathbb{R}}(E)^{\frac{r_1-1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}.$$

Very crude model: $L(1, E, \rho_K) = 0$ if m "accidentally" equals 0,

An embarrassingly crude model

We thus expect

$$L(1, E, \rho_K) = m^2 \cdot (\text{Invariants of } E)$$

with

$$m \ll \frac{|\mathrm{Disc}(K)|^{1/4} Q^{\epsilon}}{\Omega_{\mathbb{R}}(E)^{\frac{r_1-1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}.$$

Very crude model: $L(1, E, \rho_K) = 0$ if m "accidentally" equals 0, which happens with probability about

$$\frac{\Omega_{\mathbb{R}}(E)^{\frac{r_1-1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}{|\mathrm{Disc}(K)|^{1/4}}.$$

A prediction for rank 2 twists

For fixed E, if $K \in \mathcal{F}_n(X; S_n)$ with $w(E, \rho_K) = +1$, we thus expect

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{1}{|\mathrm{Disc}(K)|^{1/4}}.$$

A prediction for rank 2 twists

For fixed E, if $K \in \mathcal{F}_n(X; S_n)$ with $w(E, \rho_K) = +1$, we thus expect

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{1}{|\mathrm{Disc}(K)|^{1/4}}.$$

Conjecture

If $E/\mathbb{Q}$ is an elliptic curve, then for each n

$$X^{3/4-\epsilon} \ll \#\{K \in \mathcal{F}_n^E(X; S_n) : w(E, \rho_K) = +1\} \ll X^{3/4+\epsilon}.$$

A prediction for rank 2 twists

For fixed E, if $K \in \mathcal{F}_n(X; S_n)$ with $w(E, \rho_K) = +1$, we thus expect

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{1}{|\mathrm{Disc}(K)|^{1/4}}.$$

Conjecture

If $E/\mathbb{Q}$ is an elliptic curve, then for each n

$$X^{3/4-\epsilon} \ll \#\{K \in \mathcal{F}_n^E(X; S_n) : w(E, \rho_K) = +1\} \ll X^{3/4+\epsilon}.$$

More generally, if $G \subseteq S_n$ is primitive, then

$$\#\{K \in \mathcal{F}_n^E(X; G) : w(E, \rho_K) = +1\}$$

A prediction for rank 2 twists

For fixed E, if $K \in \mathcal{F}_n(X; S_n)$ with $w(E, \rho_K) = +1$, we thus expect

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{1}{|\mathrm{Disc}(K)|^{1/4}}.$$

Conjecture

If $E/\mathbb{Q}$ is an elliptic curve, then for each n

$$X^{3/4-\epsilon} \ll \#\{K \in \mathcal{F}_n^E(X; S_n) : w(E, \rho_K) = +1\} \ll X^{3/4+\epsilon}.$$

More generally, if $G \subseteq S_n$ is primitive, then

$$X^{\frac{1}{a(G)}-\frac{1}{4}-\epsilon} \ll \#\{K \in \mathcal{F}_n^E(X; G) : w(E, \rho_K) = +1\} \ll X^{\frac{1}{a(G)}-\frac{1}{4}+\epsilon}.$$

A prediction for rank 2 twists

For fixed E, if $K \in \mathcal{F}_n(X; S_n)$ with $w(E, \rho_K) = +1$, we thus expect

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{1}{|\mathrm{Disc}(K)|^{1/4}}.$$

Conjecture

If $E/\mathbb{Q}$ is an elliptic curve, then for each n

$$X^{3/4-\epsilon} \ll \#\{K \in \mathcal{F}_n^E(X; S_n) : w(E, \rho_K) = +1\} \ll X^{3/4+\epsilon}.$$

More generally, if $G \subseteq S_n$ is primitive, then

$$X^{\frac{1}{a(G)} - \frac{1}{4} - \epsilon} \ll \#\{K \in \mathcal{F}_n^E(X; G) : w(E, \rho_K) = +1\} \ll X^{\frac{1}{a(G)} - \frac{1}{4} + \epsilon}.$$

Take note: What if $1/a(G) < 1/4$?

A prediction for rank 2 twists

For fixed E, if $K \in \mathcal{F}_n(X; S_n)$ with $w(E, \rho_K) = +1$, we thus expect

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{1}{|\mathrm{Disc}(K)|^{1/4}}.$$

Conjecture

If $E/\mathbb{Q}$ is an elliptic curve, then for each n

$$X^{3/4-\epsilon} \ll \#\{K \in \mathcal{F}_n^E(X; S_n) : w(E, \rho_K) = +1\} \ll X^{3/4+\epsilon}.$$

More generally, if $G \subseteq S_n$ is primitive, then

$$X^{\frac{1}{a(G)} - \frac{1}{4} - \epsilon} \ll \#\{K \in \mathcal{F}_n^E(X; G) : w(E, \rho_K) = +1\} \ll X^{\frac{1}{a(G)} - \frac{1}{4} + \epsilon}.$$

Take note: What if $1/a(G) < 1/4$? Predicts finiteness/emptiness.

Example: Prime degree cyclic fields

Let $K \in \mathcal{F}_p(X; C_p)$.

Example: Prime degree cyclic fields

Let $K \in \mathcal{F}_p(X; C_p)$. Then

$$L(s, E, \rho_K) = \prod_{\chi \neq \chi_0} L(s, E, \chi),$$

Example: Prime degree cyclic fields

Let $K \in \mathcal{F}_p(X; C_p)$. Then

$$L(s, E, \rho_K) = \prod_{\chi \neq \chi_0} L(s, E, \chi),$$

and since each χ is complex, no $L(s, E, \chi)$ is self-dual

Example: Prime degree cyclic fields

Let $K \in \mathcal{F}_p(X; C_p)$. Then

$$L(s, E, \rho_K) = \prod_{\chi \neq \chi_0} L(s, E, \chi),$$

and since each χ is complex, no $L(s, E, \chi)$ is self-dual and $w(E, \rho_K) = +1$ always.

Example: Prime degree cyclic fields

Let $K \in \mathcal{F}_p(X; C_p)$. Then

$$L(s, E, \rho_K) = \prod_{\chi \neq \chi_0} L(s, E, \chi),$$

and since each χ is complex, no $L(s, E, \chi)$ is self-dual and $w(E, \rho_K) = +1$ always.

Moreover, $\#\mathcal{F}_p(X; C_p) \ll X^{1/(p-1)+\epsilon}$,

Example: Prime degree cyclic fields

Let $K \in \mathcal{F}_p(X; C_p)$. Then

$$L(s, E, \rho_K) = \prod_{\chi \neq \chi_0} L(s, E, \chi),$$

and since each χ is complex, no $L(s, E, \chi)$ is self-dual and $w(E, \rho_K) = +1$ always.

Moreover, $\#\mathcal{F}_p(X; C_p) \ll X^{1/(p-1)+\epsilon}$, so we obtain:

Conjecture (David–Fearnley–Kisilevsky)

$\lim_{X\to\infty} \mathcal{F}_p^E(X; C_p)$ is finite if $p \geq 7$.

Example: Prime degree cyclic fields

Let $K \in \mathcal{F}_p(X; C_p)$. Then

$$L(s, E, \rho_K) = \prod_{\chi \neq \chi_0} L(s, E, \chi),$$

and since each χ is complex, no $L(s, E, \chi)$ is self-dual and $w(E, \rho_K) = +1$ always.

Moreover, $\#\mathcal{F}_p(X; C_p) \ll X^{1/(p-1)+\epsilon}$, so we obtain:

Conjecture (David–Fearnley–Kisilevsky)

$\lim_{X \to \infty} \mathcal{F}_p^E(X; C_p)$ *is finite if* $p \geq 7$.

Example: Prime degree cyclic fields, cont.

Variant: Fix $K \in \mathcal{F}_p(X; C_p)$ and vary E.

Example: Prime degree cyclic fields, cont.

Variant: Fix $K \in \mathcal{F}_p(X; C_p)$ and vary E. Model had

$$\text{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{\Omega_{\mathbb{R}}(E)^{\frac{r_1 - 1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}{|\text{Disc}(K)|^{1/4}}.$$

Example: Prime degree cyclic fields, cont.

Variant: Fix $K \in \mathcal{F}_p(X; C_p)$ and vary E. Model had

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{\Omega_{\mathbb{R}}(E)^{\frac{r_1 - 1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}{|\mathrm{Disc}(K)|^{1/4}}.$$

K has signature $(p, 0)$ and $\Omega_{\mathbb{R}}(E) \approx \mathrm{ht}(E)^{-1/12}$,

Example: Prime degree cyclic fields, cont.

Variant: Fix $K \in \mathcal{F}_p(X; C_p)$ and vary E. Model had

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{\Omega_{\mathbb{R}}(E)^{\frac{r_1 - 1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}{|\mathrm{Disc}(K)|^{1/4}}.$$

K has signature $(p, 0)$ and $\Omega_{\mathbb{R}}(E) \approx \mathrm{ht}(E)^{-1/12}$,
$\Rightarrow \mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \mathrm{ht}(E)^{-\frac{p-1}{24}}$.

Conjecture

If $p \leq 19$, there exist infinitely many E for which $K \in \mathcal{F}_p^E(X; C_p)$.

Example: Prime degree cyclic fields, cont.

Variant: Fix $K \in \mathcal{F}_p(X; C_p)$ and vary E. Model had

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{\Omega_{\mathbb{R}}(E)^{\frac{r_1-1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}{|\mathrm{Disc}(K)|^{1/4}}.$$

K has signature $(p, 0)$ and $\Omega_{\mathbb{R}}(E) \approx \mathrm{ht}(E)^{-1/12}$,
$\Rightarrow \mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \mathrm{ht}(E)^{-\frac{p-1}{24}}$.

Conjecture

If $p \leq 19$, there exist infinitely many E for which $K \in \mathcal{F}_p^E(X; C_p)$.
If $p \geq 23$, then there are only finitely many.

Example: Prime degree cyclic fields, cont.

Variant: Fix $K \in \mathcal{F}_p(X; C_p)$ and vary E. Model had

$$\mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \frac{\Omega_{\mathbb{R}}(E)^{\frac{r_1 - 1}{2}} \Omega_{\mathbb{C}}(E)^{\frac{r_2}{2}}}{|\mathrm{Disc}(K)|^{1/4}}.$$

K has signature $(p, 0)$ and $\Omega_{\mathbb{R}}(E) \approx \mathrm{ht}(E)^{-1/12}$,
$\Rightarrow \mathrm{Prob.}(L(1, E, \rho_K) = 0) \approx \mathrm{ht}(E)^{-\frac{p-1}{24}}$.

Conjecture

If $p \leq 19$, there exist infinitely many E for which $K \in \mathcal{F}_p^E(X; C_p)$.
If $p \geq 23$, then there are only finitely many.

Hybrid: Is there no $E/\mathbb{Q}$ and no $K \in \mathcal{F}_p(X; C_p)$ with $p \geq 23$ for which $E(K) \neq E(\mathbb{Q})$?

Higher genus curves

Theorem (Keyes)

Let $C/\mathbb{Q}$ be hyperelliptic of genus g.

Higher genus curves

Theorem (Keyes)

Let $C/\mathbb{Q}$ be hyperelliptic of genus g. If $\deg(C)$ is odd, then

$$\#\mathcal{F}_n^C(X; S_n) \gg X^{\frac{1}{4} - c_{g,n} - \epsilon}$$

for each $n \geq g$, where $c_{g,n}$ is explicit and $\to 0$ as $n \to \infty$.

Higher genus curves

Theorem (Keyes)

Let $C/\mathbb{Q}$ be hyperelliptic of genus g. If $\deg(C)$ is odd, then

$$\#\mathcal{F}_n^C(X; S_n) \gg X^{\frac{1}{4} - c_{g,n} - \epsilon}$$

for each $n \geq g$, where $c_{g,n}$ is explicit and $\to 0$ as $n \to \infty$.

Question

What's the truth?

Higher genus curves

Theorem (Keyes)

Let $C/\mathbb{Q}$ be hyperelliptic of genus g. If $\deg(C)$ is odd, then

$$\#\mathcal{F}_n^C(X; S_n) \gg X^{\frac{1}{4} - c_{g,n} - \epsilon}$$

for each $n \geq g$, where $c_{g,n}$ is explicit and $\to 0$ as $n \to \infty$.

Question

What's the truth? How does $\#\mathcal{F}_n^C(X; G)$ behave for other G?

Higher genus curves

Theorem (Keyes)

Let $C/\mathbb{Q}$ be hyperelliptic of genus g. If $\deg(C)$ is odd, then

$$\#\mathcal{F}_n^C(X; S_n) \gg X^{\frac{1}{4} - c_{g,n} - \epsilon}$$

for each $n \geq g$, where $c_{g,n}$ is explicit and $\to 0$ as $n \to \infty$.

Question

What's the truth? How does $\#\mathcal{F}_n^C(X; G)$ behave for other G? For other C?

Higher genus curves

Theorem (Keyes)

Let $C/\mathbb{Q}$ be hyperelliptic of genus g. If $\deg(C)$ is odd, then

$$\#\mathcal{F}_n^C(X; S_n) \gg X^{\frac{1}{4} - c_{g,n} - \epsilon}$$

for each $n \geq g$, where $c_{g,n}$ is explicit and $\to 0$ as $n \to \infty$.

Question

What's the truth? How does $\#\mathcal{F}_n^C(X; G)$ behave for other G? For other C? What does this reveal about the geometry of C?