Quadratic twists of elliptic curves with 3-torsion

Robert J. Lemke Oliver [1]
Tufts University

(Joint with M. Bhargava, Z. Klagsbrun, and A. Shnidman)

[1] Partially supported by NSF grant DMS-1601398

Ranks of elliptic curves

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve.

Ranks of elliptic curves

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve.

Theorem (Mordell-Weil)

The rational points $E(\mathbb{Q})$ are a finitely generated abelian group,

Ranks of elliptic curves

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve.

Theorem (Mordell-Weil)

The rational points $E(\mathbb{Q})$ are a finitely generated abelian group, i.e.

$$E(\mathbb{Q}) = \mathbb{Z}^{r(E)} \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

Ranks of elliptic curves

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve.

Theorem (Mordell-Weil)

The rational points $E(\mathbb{Q})$ are a finitely generated abelian group, i.e.

$$E(\mathbb{Q}) = \mathbb{Z}^{r(E)} \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

where $E(\mathbb{Q})_{\mathrm{tors}}$ is finite.

Ranks of elliptic curves

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve.

Theorem (Mordell-Weil)

The rational points $E(\mathbb{Q})$ are a finitely generated abelian group, i.e.

$$E(\mathbb{Q}) = \mathbb{Z}^{r(E)} \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

where $E(\mathbb{Q})_{\mathrm{tors}}$ is finite.

Theorem (Mazur)

$E(\mathbb{Q})_{\mathrm{tors}}$ is one of:

- $\mathbb{Z}/N\mathbb{Z}$ *for* $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$,

Ranks of elliptic curves

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve.

Theorem (Mordell-Weil)

The rational points $E(\mathbb{Q})$ are a finitely generated abelian group, i.e.

$$E(\mathbb{Q}) = \mathbb{Z}^{r(E)} \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

where $E(\mathbb{Q})_{\mathrm{tors}}$ is finite.

Theorem (Mazur)

$E(\mathbb{Q})_{\mathrm{tors}}$ is one of:

- *$\mathbb{Z}/N\mathbb{Z}$ for $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$, or*
- *$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ for $N \in \{2, 4, 6, 8\}$.*

Examples

Example

Let $E\colon y^2 = x^3 - x$.

Examples

Example

Let $E\colon y^2 = x^3 - x$. Then

$$E(\mathbb{Q}) \quad = \quad \{(0,0),(\pm 1,0),\infty\}$$

Examples

Example

Let $E\colon y^2 = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \{(0,0),(\pm 1,0),\infty\} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Examples

Example

Let $E\colon y^2 = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \{(0,0), (\pm 1, 0), \infty\} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Thus, $r(E) = 0$.

Examples

Example

Let $E\colon y^2 = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \{(0,0), (\pm 1, 0), \infty\} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Thus, $r(E) = 0$.

Example

Let $E\colon y^2 + y = x^3 - x$.

Examples

Example

Let $E\colon y^2 = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \{(0,0),(\pm 1,0),\infty\} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Thus, $r(E) = 0$.

Example

Let $E\colon y^2 + y = x^3 - x$. Then

$$E(\mathbb{Q}) \ni (0,0)$$

Examples

Example

Let $E\colon y^2 = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \{(0,0), (\pm 1, 0), \infty\} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Thus, $r(E) = 0$.

Example

Let $E\colon y^2 + y = x^3 - x$. Then

$$E(\mathbb{Q}) = \langle (0,0) \rangle$$

Examples

Example

Let $E\colon y^2 = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \{(0,0),(\pm 1,0),\infty\} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Thus, $r(E) = 0$.

Example

Let $E\colon y^2 + y = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \langle (0,0) \rangle \\ &\simeq \mathbb{Z}, \end{aligned}$$

Examples

Example

Let $E\colon y^2 = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \{(0,0), (\pm 1, 0), \infty\} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Thus, $r(E) = 0$.

Example

Let $E\colon y^2 + y = x^3 - x$. Then

$$\begin{aligned} E(\mathbb{Q}) &= \langle (0,0) \rangle \\ &\simeq \mathbb{Z}, \end{aligned}$$

so $r(E) = 1$.

Ranks of elliptic curves

For any given $E/\mathbb{Q}$, computing $r(E)$ can be hard,

Ranks of elliptic curves

For any given $E/\mathbb{Q}$, computing $r(E)$ can be hard, but:

Theorem

Assuming BSD + GRH, $\exists$ algorithm to compute $r(E)$.

Ranks of elliptic curves

For any given $E/\mathbb{Q}$, computing $r(E)$ can be hard, but:

Theorem

Assuming BSD + GRH, $\exists$ algorithm to compute $r(E)$.

Question

How does $r(E)$ behave for “typical” E?

Ranks of elliptic curves

For any given $E/\mathbb{Q}$, computing $r(E)$ can be hard, but:

Theorem

Assuming BSD + GRH, $\exists$ algorithm to compute $r(E)$.

Question

How does $r(E)$ behave for "typical" E? e.g.

- What is $\mathrm{Prob.}(r(E) = m)$ for given $m \geq 0$?

Ranks of elliptic curves

For any given $E/\mathbb{Q}$, computing $r(E)$ can be hard, but:

Theorem

Assuming BSD + GRH, $\exists$ algorithm to compute $r(E)$.

Question

How does $r(E)$ behave for "typical" E? e.g.

- What is $\mathrm{Prob.}(r(E) = m)$ for given $m \geq 0$?
- What is $\mathrm{Avg.}(r(E))$?

Parity

The L-function of $E/\mathbb{Q}$ satisfies

$$L(s, E) \doteq \qquad L(2 - s, E),$$

Parity

The L-function of $E/\mathbb{Q}$ satisfies

$$L(s,E) \doteq w(E) \cdot L(2-s,E),$$

Parity

The L-function of $E/\mathbb{Q}$ satisfies

$$L(s, E) \doteq w(E) \cdot L(2 - s, E), \quad w(E) = \pm 1.$$

Parity

The L-function of $E/\mathbb{Q}$ satisfies

$$L(s,E) \doteq w(E) \cdot L(2-s,E), \quad w(E) = \pm 1.$$

Conjecture (Birch and Swinnerton-Dyer)

For any $E/\mathbb{Q}$, $r(E) = \mathrm{ord}_{s=1} L(s,E)$.

Parity

The L-function of $E/\mathbb{Q}$ satisfies

$$L(s,E) \doteq w(E)\cdot L(2-s,E), \quad w(E)=\pm 1.$$

Conjecture (Birch and Swinnerton-Dyer)

For any $E/\mathbb{Q}$, $r(E) = \mathrm{ord}_{s=1} L(s,E)$.

Corollary (Parity conjecture)

Assuming BSD, for any $E/\mathbb{Q}$,

$$(-1)^{r(E)} = w(E).$$

Expectations via root numbers

Conjecture

$w(E) = 1$ for 50% of $E/\mathbb{Q}$ and $w(E) = -1$ for 50% of $E/\mathbb{Q}$.

Expectations via root numbers

Conjecture

$w(E) = 1$ for 50% of $E/\mathbb{Q}$ and $w(E) = -1$ for 50% of $E/\mathbb{Q}$.

Parity + minimality hypothesis leads to:

Expectations via root numbers

Conjecture

$w(E) = 1$ *for* 50% *of* $E/\mathbb{Q}$ *and* $w(E) = -1$ *for* 50% *of* $E/\mathbb{Q}$.

Parity + minimality hypothesis leads to:

Conjecture (Katz-Sarnak)

$r(E) = 0$ *for* 50% *of* $E/\mathbb{Q}$, *and* $r(E) = 1$ *for* 50% *of* $E/\mathbb{Q}$.

Expectations via root numbers

Conjecture

$w(E) = 1$ for 50% of $E/\mathbb{Q}$ and $w(E) = -1$ for 50% of $E/\mathbb{Q}$.

Parity + minimality hypothesis leads to:

Conjecture (Katz-Sarnak)

$r(E) = 0$ for 50% of $E/\mathbb{Q}$, and $r(E) = 1$ for 50% of $E/\mathbb{Q}$.

Theorem (Bhargava-Shankar, Bhargava-Skinner-Zhang)

At least 20% of $E/\mathbb{Q}$ have rank 0, and at least 20% have rank 1.

Quadratic Twists

Definition
Given $E\colon y^2 = x^3 + Ax + B$, the quadratic twist by d

Quadratic Twists

Definition

Given $E\colon y^2 = x^3 + Ax + B$, the quadratic twist by d is
$E_d\colon dy^2 = x^3 + Ax + B$

Quadratic Twists

Definition

Given $E\colon y^2 = x^3 + Ax + B$, the quadratic twist by d is
$E_d\colon dy^2 = x^3 + Ax + B \quad \longleftrightarrow \quad y^2 = x^3 + d^2AX + d^3B$.

Quadratic Twists

Definition
Given $E\colon y^2 = x^3 + Ax + B$, the quadratic twist by d is
$E_d\colon dy^2 = x^3 + Ax + B \quad \longleftrightarrow \quad y^2 = x^3 + d^2AX + d^3B$.

Theorem
Given E, $w(E_d) = 1$ for 50% of d, and $w(E_d) = -1$ for 50% of d.

Quadratic Twists

Definition

Given $E\colon y^2 = x^3 + Ax + B$, the quadratic twist by d is
$E_d\colon dy^2 = x^3 + Ax + B \quad \longleftrightarrow \quad y^2 = x^3 + d^2AX + d^3B.$

Theorem

Given E, $w(E_d) = 1$ for 50% of d, and $w(E_d) = -1$ for 50% of d.

Conjecture (Goldfeld)

Given E, $r(E_d) = 0$ for 50% of d, and $r(E_d) = 1$ for 50% of d.

Quadratic Twists

Definition

Given $E\colon y^2 = x^3 + Ax + B$, the quadratic twist by d is
$E_d\colon dy^2 = x^3 + Ax + B \quad \longleftrightarrow \quad y^2 = x^3 + d^2AX + d^3B$.

Theorem

Given E, $w(E_d) = 1$ for 50% of d, and $w(E_d) = -1$ for 50% of d.

Conjecture (Goldfeld)

Given E, $r(E_d) = 0$ for 50% of d, and $r(E_d) = 1$ for 50% of d.

Question (Weak Goldfeld)

Do $r(E_d) = 0$ and $r(E_d) = 1$ hold for a positive proportion of d?

The congruent number curve

Theorem (Heath-Brown)

Let $E\colon y^2 = x^3 - x$.

The congruent number curve

Theorem (Heath-Brown)

Let $E\colon y^2 = x^3 - x$. *Then:*

- *the average rank of* $E_d/\mathbb{Q}$ *is at most* $3/2$,

The congruent number curve

Theorem (Heath-Brown)

Let $E: y^2 = x^3 - x$. *Then:*

- *the average rank of* $E_d/\mathbb{Q}$ *is at most* $3/2$,
- $r(E_d) = 0$ *for at least* 20.9% *of* d,

The congruent number curve

Theorem (Heath-Brown)

Let $E\colon y^2 = x^3 - x$. *Then:*

- *the average rank of* $E_d/\mathbb{Q}$ *is at most* $3/2$,
- $r(E_d) = 0$ *for at least* 20.9% *of* d, *and*
- $r(E_d) = 1$ *for at least* 41.9% *of* d,

The congruent number curve

Theorem (Heath-Brown)

Let $E\colon y^2 = x^3 - x$. *Then:*

- *the average rank of* $E_d/\mathbb{Q}$ *is at most* $3/2$,
- $r(E_d) = 0$ *for at least* 20.9% *of* d, *and*
- $r(E_d) = 1$ *for at least* 41.9% *of* d, *assuming finiteness of Sha.*

The congruent number curve

Theorem (Heath-Brown)
Let $E\colon y^2 = x^3 - x$. Then:

- *the average rank of $E_d/\mathbb{Q}$ is at most $3/2$,*
- *$r(E_d) = 0$ for at least 20.9% of d, and*
- *$r(E_d) = 1$ for at least 41.9% of d, assuming finiteness of Sha.*

Theorem (Smith)
$r(E_d) = 1$ for at least 27.9% of d unconditionally.

Idea of the proof of Heath-Brown

Use 2-Selmer groups,

Idea of the proof of Heath-Brown

Use 2-Selmer groups,

$$0 \to E_d(\mathbb{Q})/2E_d(\mathbb{Q}) \to \mathrm{Sel}_2(E_d/\mathbb{Q})$$

Idea of the proof of Heath-Brown

Use 2-Selmer groups,

$$0 \to E_d(\mathbb{Q})/2E_d(\mathbb{Q}) \to \mathrm{Sel}_2(E_d/\mathbb{Q}) \to Ш(E_d/\mathbb{Q})[2] \to 0.$$

Idea of the proof of Heath-Brown

Use 2-Selmer groups,

$$0 \to E_d(\mathbb{Q})/2E_d(\mathbb{Q}) \to \mathrm{Sel}_2(E_d/\mathbb{Q}) \to Ш(E_d/\mathbb{Q})[2] \to 0.$$

Point

The 2-Selmer group is an algebraic proxy for $E_d(\mathbb{Q})$,

Idea of the proof of Heath-Brown

Use 2-Selmer groups,

$$0 \to E_d(\mathbb{Q})/2E_d(\mathbb{Q}) \to \mathrm{Sel}_2(E_d/\mathbb{Q}) \to Ш(E_d/\mathbb{Q})[2] \to 0.$$

Point

The 2-Selmer group is an algebraic proxy for $E_d(\mathbb{Q})$, and satisfies

$$|\mathrm{Sel}_2(E_d/\mathbb{Q})| = 2^{s_2(E_d)}$$

Idea of the proof of Heath-Brown

Use 2-Selmer groups,

$$0 \to E_d(\mathbb{Q})/2E_d(\mathbb{Q}) \to \mathrm{Sel}_2(E_d/\mathbb{Q}) \to Ш(E_d/\mathbb{Q})[2] \to 0.$$

Point

The 2-Selmer group is an algebraic proxy for $E_d(\mathbb{Q})$, and satisfies

$$|\mathrm{Sel}_2(E_d/\mathbb{Q})| = 2^{s_2(E_d)} \geq 2^{r(E_d)+2}$$

since $E_d(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Idea of the proof of Heath-Brown

Use 2-Selmer groups,

$$0 \to E_d(\mathbb{Q})/2E_d(\mathbb{Q}) \to \mathrm{Sel}_2(E_d/\mathbb{Q}) \to Ш(E_d/\mathbb{Q})[2] \to 0.$$

Point

The 2-Selmer group is an algebraic proxy for $E_d(\mathbb{Q})$, and satisfies

$$|\mathrm{Sel}_2(E_d/\mathbb{Q})| = 2^{s_2(E_d)} \geq 2^{r(E_d)+2}$$

since $E_d(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Idea (Heath-Brown)

Study the distribution of $s_2(E_d)$.

Explicitly accessing the 2-Selmer group

Explicitly accessing the 2-Selmer group

Elements of $\mathrm{Sel}_2(E_d/\mathbb{Q})$ correspond to

Explicitly accessing the 2-Selmer group

Elements of $\mathrm{Sel}_2(E_d/\mathbb{Q})$ correspond to

- biquadratic fields $\mathbb{Q}(\sqrt{m_1}, \sqrt{m_2})$

Explicitly accessing the 2-Selmer group

Elements of $\mathrm{Sel}_2(E_d/\mathbb{Q})$ correspond to

- biquadratic fields $\mathbb{Q}(\sqrt{m_1}, \sqrt{m_2})$
- that are unramified away from $2d$,

Explicitly accessing the 2-Selmer group

Elements of $\mathrm{Sel}_2(E_d/\mathbb{Q})$ correspond to

- biquadratic fields $\mathbb{Q}(\sqrt{m_1}, \sqrt{m_2})$
- that are unramified away from $2d$, and
- which satisfy nested local conditions at primes dividing $2d$.

Explicitly accessing the 2-Selmer group

Elements of $\mathrm{Sel}_2(E_d/\mathbb{Q})$ correspond to

- biquadratic fields $\mathbb{Q}(\sqrt{m_1}, \sqrt{m_2})$
- that are unramified away from $2d$, and
- which satisfy nested local conditions at primes dividing $2d$.

We (=Heath-Brown) can count these things!

Explicitly accessing the 2-Selmer group

Elements of $\mathrm{Sel}_2(E_d/\mathbb{Q})$ correspond to

- biquadratic fields $\mathbb{Q}(\sqrt{m_1}, \sqrt{m_2})$
- that are unramified away from $2d$, and
- which satisfy nested local conditions at primes dividing $2d$.

We (=Heath-Brown) can count these things!

(Secretly, what's going on is that

$$\begin{aligned} \mathrm{Sel}_2(E_d/\mathbb{Q}) &\subseteq H^1(\mathbb{Q}, E_d[2]) \\ &\simeq H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \\ &\leftrightarrow \text{biquadratic fields.} \end{aligned}$$

But let's agree to mostly ignore this picture!)

Curves with full two-torsion

This works for any elliptic curve with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$:

Curves with full two-torsion

This works for any elliptic curve with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$:

Theorem (Kane, Swinnerton-Dyer)

If $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then:

- *the average rank of $E_d/\mathbb{Q}$ is at most $3/2$,*
- *$r(E_d) = 0$ for at least 20.9% of d, and*
- *$r(E_d) = 1$ for at least 41.9% of d, assuming finiteness of Sha.*

Curves with full two-torsion

This works for any elliptic curve with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$:

Theorem (Kane, Swinnerton-Dyer)

If $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then:

- *the average rank of $E_d/\mathbb{Q}$ is at most $3/2$,*
- *$r(E_d) = 0$ for at least 20.9% of d, and*
- *$r(E_d) = 1$ for at least 41.9% of d, assuming finiteness of Sha.*

Question

How common are curves with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$?

Counting curves by height

Definition
Given $E\colon y^2 = x^3 + Ax + B$, let $Ht(E) := \max(|A|^3, B^2)$.

Counting curves by height

Definition

Given $E\colon y^2 = x^3 + Ax + B$, let $Ht(E) := \max(|A|^3, B^2)$.

Fact

There are $\sim \frac{4}{\zeta(10)} X^{5/6}$ *non-isomorphic* $E/\mathbb{Q}$ *with* $Ht(E) \leq X$.

Counting curves by height

Definition

Given $E\colon y^2 = x^3 + Ax + B$, let $Ht(E) := \max(|A|^3, B^2)$.

Fact

There are $\sim \frac{4}{\zeta(10)} X^{5/6}$ *non-isomorphic* $E/\mathbb{Q}$ *with* $Ht(E) \leq X$.

Theorem (Harron-Snowden)

There are $\asymp X^{1/3}$ *non-isomorphic curves with* $Ht(E) \leq X$ *and* $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Counting curves by height

Definition

Given $E\colon y^2 = x^3 + Ax + B$, let $Ht(E) := \max(|A|^3, B^2)$.

Fact

There are $\sim \frac{4}{\zeta(10)} X^{5/6}$ *non-isomorphic* $E/\mathbb{Q}$ *with* $Ht(E) \leq X$.

Theorem (Harron-Snowden)

There are $\asymp X^{1/3}$ *non-isomorphic curves with* $Ht(E) \leq X$ *and* $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Question

Are there bigger families for which we can prove weak Goldfeld?

Elliptic curves with 3-isogenies

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny[1]*.*

[1] More on this in a second.

Elliptic curves with 3-isogenies

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny[1]*. Then:*

- *the average rank of $E_d/\mathbb{Q}$ is bounded,*

[1] More on this in a second.

Elliptic curves with 3-isogenies

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny[1]*. Then:*

- *the average rank of $E_d/\mathbb{Q}$ is bounded,*
- *$r(E_d) = 0$ for a positive proportion of d,*

[1] More on this in a second.

Elliptic curves with 3-isogenies

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny[1]*. Then:*

- *the average rank of $E_d/\mathbb{Q}$ is bounded,*
- *$r(E_d) = 0$ for a positive proportion of d, and*
- *$r(E_d) = 1$ for a positive proportion of d,*

---

[1] More on this in a second.

Elliptic curves with 3-isogenies

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny[1]*. Then:*

- *the average rank of $E_d/\mathbb{Q}$ is bounded,*
- *$r(E_d) = 0$ for a positive proportion of d, and*
- *$r(E_d) = 1$ for a positive proportion of d, assuming finiteness of Sha.*

[1] More on this in a second.

Elliptic curves with 3-isogenies

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny[1]*. Then:*

- *the average rank of $E_d/\mathbb{Q}$ is bounded,*
- *$r(E_d) = 0$ for a positive proportion of d, and*
- *$r(E_d) = 1$ for a positive proportion of d, assuming finiteness of Sha.*

Remark

Kriz and Li recently obtained $r(E_d) = 0$ and $r(E_d) = 1$ unconditionally,

[1] More on this in a second.

Elliptic curves with 3-isogenies

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny[1]*. Then:*

- *the average rank of $E_d/\mathbb{Q}$ is bounded,*
- *$r(E_d) = 0$ for a positive proportion of d, and*
- *$r(E_d) = 1$ for a positive proportion of d, assuming finiteness of Sha.*

Remark

Kriz and Li recently obtained $r(E_d) = 0$ and $r(E_d) = 1$ unconditionally, but with weaker proportions.

[1] More on this in a second.

Elliptic curves with 3-isogenies

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny[1]*. Then:*

- *the average rank of $E_d/\mathbb{Q}$ is bounded,*
- *$r(E_d) = 0$ for a positive proportion of d, and*
- *$r(E_d) = 1$ for a positive proportion of d, assuming finiteness of Sha.*

Remark

Kriz and Li recently obtained $r(E_d) = 0$ and $r(E_d) = 1$ unconditionally, but with weaker proportions.

Remark

It follows from Harron and Snowden that there are $\asymp X^{1/2}$ such curves.

---

[1] More on this in a second.

Explicit Examples

Corollary

Let $E\colon y^2 + y = x^3 + x^2 + x$*.*

Explicit Examples

Corollary

Let $E\colon y^2 + y = x^3 + x^2 + x$. *Then* E *has a* 3*-isogeny,*

Explicit Examples

Corollary

Let $E\colon y^2 + y = x^3 + x^2 + x$. *Then* E *has a* 3*-isogeny, and*

- *the average rank of* $E_d/\mathbb{Q}$ *is at most* $7/6$*,*

Explicit Examples

Corollary

Let $E\colon y^2 + y = x^3 + x^2 + x$. *Then* E *has a 3-isogeny, and*

- *the average rank of* $E_d/\mathbb{Q}$ *is at most* $7/6$,
- $r(E_d) = 0$ *for at least* 25% *of* d,

Explicit Examples

Corollary

Let $E\colon y^2 + y = x^3 + x^2 + x$. *Then* E *has a 3-isogeny, and*

- *the average rank of* $E_d/\mathbb{Q}$ *is at most* $7/6$,
- $r(E_d) = 0$ *for at least* 25% *of* d, *and*
- $r(E_d) = 1$ *for at least* $5/12 \approx 41.6\%$ *of* d, *assuming finiteness of Sha.*

Corollary

Let $E\colon y^2 + y = x^3 + x^2 + x$. *Then* E *has a 3-isogeny, and*

- *the average rank of* $E_d/\mathbb{Q}$ *is at most* $7/6$,
- $r(E_d) = 0$ *for at least* 25% *of* d, *and*
- $r(E_d) = 1$ *for at least* $5/12 \approx 41.6\%$ *of* d, *assuming finiteness of Sha.*

Remark

The above corollary also holds for $E\colon y^2 = x^3 + 208$ and $E\colon y^2 + y = x^3 + x^2 - 3x + 1$, among others.

Isogenies

Definition

An m-isogeny is a degree m rational function $\phi\colon E \to E'$ that is also a group homomorphism.

Isogenies

Definition

An m-isogeny is a degree m rational function $\phi \colon E \to E'$ that is also a group homomorphism.

Example

Multiplication-by-m is an m^2-isogeny.

Isogenies

Definition

An m-isogeny is a degree m rational function $\phi\colon E \to E'$ that is also a group homomorphism.

Example

Multiplication-by-m is an m^2-isogeny.

Fact

E has a 3-isogeny iff there exists d such that $E_d(\mathbb{Q})[3] \simeq \mathbb{Z}/3\mathbb{Z}$.

Examples of isogenies

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$.

Examples of isogenies

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$,

Examples of isogenies

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, so E has a 3-isogeny.

Examples of isogenies

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, so E has a 3-isogeny.

In fact, let $E'\colon y^2 + y = x^3 + x^2 - 9x - 15$,

Examples of isogenies

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, so E has a 3-isogeny.

In fact, let $E'\colon y^2 + y = x^3 + x^2 - 9x - 15$, and define

$$\phi((x, y)) = \left(\frac{x^3 + 2x + 1}{x^2}, \frac{x^3 - 2xy - x - 2y - 1}{x^3}\right).$$

Examples of isogenies

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, so E has a 3-isogeny.

In fact, let $E'\colon y^2 + y = x^3 + x^2 - 9x - 15$, and define

$$\phi((x,y)) = \left(\frac{x^3 + 2x + 1}{x^2}, \frac{x^3 - 2xy - x - 2y - 1}{x^3} \right).$$

Then $\phi\colon E \to E'$ is a 3-isogeny.

Examples of isogenies

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, so E has a 3-isogeny.

In fact, let $E'\colon y^2 + y = x^3 + x^2 - 9x - 15$, and define

$$\phi((x,y)) = \left(\frac{x^3 + 2x + 1}{x^2}, \frac{x^3 - 2xy - x - 2y - 1}{x^3}\right).$$

Then $\phi\colon E \to E'$ is a 3-isogeny.

Point

If $\phi\colon E \to E'$ is an isogeny, then $r(E) = r(E')$.

Examples of isogenies

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, so E has a 3-isogeny.

In fact, let $E'\colon y^2 + y = x^3 + x^2 - 9x - 15$, and define

$$\phi((x, y)) = \left(\frac{x^3 + 2x + 1}{x^2}, \frac{x^3 - 2xy - x - 2y - 1}{x^3} \right).$$

Then $\phi\colon E \to E'$ is a 3-isogeny.

Point

If $\phi\colon E \to E'$ is an isogeny, then $r(E) = r(E')$. We will use the ϕ-Selmer group to access the rank.

ϕ-Selmer groups

Let $\phi\colon E \to E'$ be an isogeny.

ϕ-Selmer groups

Let $\phi\colon E \to E'$ be an isogeny. Then

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathrm{Sel}_\phi(E/\mathbb{Q})$$

ϕ-Selmer groups

Let $\phi\colon E \to E'$ be an isogeny. Then

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathrm{Sel}_\phi(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0.$$

ϕ-Selmer groups

Let $\phi\colon E \to E'$ be an isogeny. Then

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathrm{Sel}_\phi(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0.$$

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $\phi\colon E \to E'$ be a 3-isogeny.

ϕ-Selmer groups

Let $\phi\colon E \to E'$ be an isogeny. Then

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathrm{Sel}_\phi(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[\phi] \to 0.$$

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $\phi\colon E \to E'$ be a 3-isogeny. The average size of $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ is exactly

$$1 + \frac{2}{3}\prod_{p \mid N_E} \mathrm{Avg.}(c_p(\phi_d)),$$

ϕ-Selmer groups

Let $\phi\colon E \to E'$ be an isogeny. Then

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathrm{Sel}_\phi(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0.$$

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $\phi\colon E \to E'$ be a 3-isogeny. The average size of $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ is exactly

$$1 + \frac{2}{3}\prod_{p \mid N_E} \mathrm{Avg.}(c_p(\phi_d)),$$

where

$$c_p(\phi_d) = \frac{|E'_d(\mathbb{Q}_p)/\phi(E_d(\mathbb{Q}_p))|}{|E_d[\phi](\mathbb{Q}_p)|}.$$

A more refined average

Let
$$c(\phi_d) = \prod_{p \leq \infty} c_p(\phi_d)$$

A more refined average

Let

$$c(\phi_d) = \prod_{p \leq \infty} c_p(\phi_d)$$

and $T_m = \{d : c(\phi_d) = 3^m\}$.

A more refined average

Let

$$c(\phi_d) = \prod_{p \leq \infty} c_p(\phi_d)$$

and $T_m = \{d : c(\phi_d) = 3^m\}$.

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

- *T_m is empty for all but finitely many m*

A more refined average

Let

$$c(\phi_d) = \prod_{p \le \infty} c_p(\phi_d)$$

and $T_m = \{d : c(\phi_d) = 3^m\}$.

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

- *T_m is empty for all but finitely many m*
- *Each non-empty T_m has positive density*

A more refined average

Let

$$c(\phi_d) = \prod_{p \leq \infty} c_p(\phi_d)$$

and $T_m = \{d : c(\phi_d) = 3^m\}$.

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

- *T_m is empty for all but finitely many m*
- *Each non-empty T_m has positive density*
- *For $d \in T_m$, $\mathrm{Avg.}|\mathrm{Sel}_\phi(E_d/\mathbb{Q})| = 1 + 3^m$*

A more refined average

Let

$$c(\phi_d) = \prod_{p \leq \infty} c_p(\phi_d)$$

and $T_m = \{d : c(\phi_d) = 3^m\}$.

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

- *T_m is empty for all but finitely many m*
- *Each non-empty T_m has positive density*
- *For $d \in T_m$, $\mathrm{Avg.}|\mathrm{Sel}_\phi(E_d/\mathbb{Q})| = 1 + 3^m$*
- *For $d \in T_m$, the average rank of $E_d/\mathbb{Q}$ is at most $|m| + 3^{-|m|}$*

A more refined average

Let

$$c(\phi_d) = \prod_{p \leq \infty} c_p(\phi_d)$$

and $T_m = \{d : c(\phi_d) = 3^m\}$.

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

- *T_m is empty for all but finitely many m*
- *Each non-empty T_m has positive density*
- *For $d \in T_m$, $\mathrm{Avg.}|\mathrm{Sel}_\phi(E_d/\mathbb{Q})| = 1 + 3^m$*
- *For $d \in T_m$, the average rank of $E_d/\mathbb{Q}$ is at most $|m| + 3^{-|m|}$*
- *For at least $1/2$ of $d \in T_0$, $r(E_d) = 0$*

A more refined average

Let

$$c(\phi_d) = \prod_{p \leq \infty} c_p(\phi_d)$$

and $T_m = \{d : c(\phi_d) = 3^m\}$.

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

- *T_m is empty for all but finitely many m*
- *Each non-empty T_m has positive density*
- *For $d \in T_m$, $\mathrm{Avg.}|\mathrm{Sel}_\phi(E_d/\mathbb{Q})| = 1 + 3^m$*
- *For $d \in T_m$, the average rank of $E_d/\mathbb{Q}$ is at most $|m| + 3^{-|m|}$*
- *For at least $1/2$ of $d \in T_0$, $r(E_d) = 0$*
- *For at least $5/6$ of $d \in T_1 \cup T_{-1}$, $r(E_d) = 1$, assuming Sha is finite*

Returning to the example

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$.

Returning to the example

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $c(\phi_d) = c_{19}(\phi_d) c_\infty(\phi_d)$,

Returning to the example

Example

Let $E\colon y^2+y=x^3+x^2+x$. Then $c(\phi_d)=c_{19}(\phi_d)c_\infty(\phi_d)$, where

$$c_\infty(\phi_d)=\begin{cases}1, & d>0\\ 1/3, & d<0\end{cases}$$

Returning to the example

Example

Let $E\colon y^2+y=x^3+x^2+x$. Then $c(\phi_d)=c_{19}(\phi_d)c_\infty(\phi_d)$, where

$$c_\infty(\phi_d)=\begin{cases} 1, & d>0 \\ 1/3, & d<0 \end{cases}$$

and

$$c_{19}(\phi_d)=\begin{cases} 3, & \text{if } 19\nmid d \text{ and } \left(\frac{d}{19}\right)=+1, \\ 1, & \text{otherwise.} \end{cases}$$

Returning to the example

Example

Let $E\colon y^2+y=x^3+x^2+x$. Then $c(\phi_d)=c_{19}(\phi_d)c_\infty(\phi_d)$, where

$$c_\infty(\phi_d)=\begin{cases}1, & d>0\\ 1/3, & d<0\end{cases}$$

and

$$c_{19}(\phi_d)=\begin{cases}3, & \text{if } 19\nmid d \text{ and } \left(\frac{d}{19}\right)=+1,\\ 1, & \text{otherwise.}\end{cases}$$

Thus, T_m is empty unless $m\in\{-1,0,1\}$.

Returning to the example

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $c(\phi_d) = c_{19}(\phi_d)c_\infty(\phi_d)$, where

$$c_\infty(\phi_d) = \begin{cases} 1, & d > 0 \\ 1/3, & d < 0 \end{cases}$$

and

$$c_{19}(\phi_d) = \begin{cases} 3, & \text{if } 19 \nmid d \text{ and } \left(\frac{d}{19}\right) = +1, \\ 1, & \text{otherwise.} \end{cases}$$

Thus, T_m is empty unless $m \in \{-1, 0, 1\}$.

Moreover, $\mathrm{dens}(T_0) = 1/2$,

Returning to the example

Example

Let $E\colon y^2 + y = x^3 + x^2 + x$. Then $c(\phi_d) = c_{19}(\phi_d)c_\infty(\phi_d)$, where

$$c_\infty(\phi_d) = \begin{cases} 1, & d > 0 \\ 1/3, & d < 0 \end{cases}$$

and

$$c_{19}(\phi_d) = \begin{cases} 3, & \text{if } 19 \nmid d \text{ and } \left(\frac{d}{19}\right) = +1, \\ 1, & \text{otherwise.} \end{cases}$$

Thus, T_m is empty unless $m \in \{-1, 0, 1\}$.

Moreover, $\mathrm{dens}(T_0) = 1/2$, so $r(E_d) = 0$ for $1/4$ of d.

Idea of the proof

Any $E/\mathbb{Q}$ with a 3-isogeny can be written as

$$E\colon y^2 = x^3 + D(ax+b)^2.$$

Idea of the proof

Any $E/\mathbb{Q}$ with a 3-isogeny can be written as

$$E\colon y^2 = x^3 + D(ax+b)^2.$$

Very loosely, elements of $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ correspond to

- cubic fields,

Idea of the proof

Any $E/\mathbb{Q}$ with a 3-isogeny can be written as

$$E\colon y^2 = x^3 + D(ax+b)^2.$$

Very loosely, elements of $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ correspond to

- cubic fields,
- that are unramified away from $6dD$,

Idea of the proof

Any $E/\mathbb{Q}$ with a 3-isogeny can be written as

$$E\colon y^2 = x^3 + D(ax+b)^2.$$

Very loosely, elements of $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ correspond to

- cubic fields,
- that are unramified away from $6dD$, and
- which satisfy local conditions at primes dividing $6dD$.

Idea of the proof

Any $E/\mathbb{Q}$ with a 3-isogeny can be written as

$$E\colon y^2 = x^3 + D(ax+b)^2.$$

Very loosely, elements of $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ correspond to

- cubic fields,
- that are unramified away from $6dD$, and
- which satisfy local conditions at primes dividing $6dD$.

Better: Elements of $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ correspond to binary cubic forms.

Binary cubic forms

Theorem (Delone-Fadeev)

Cubic fields $\longleftrightarrow \mathrm{GL}_2(\mathbb{Z})$*-classes of binary cubic forms*

Binary cubic forms

Theorem (Delone-Fadeev)

Cubic fields $\longleftrightarrow \mathrm{GL}_2(\mathbb{Z})$*-classes of binary cubic forms that are irreducible and maximal.*

Binary cubic forms

Theorem (Delone-Fadeev)

Cubic fields $\longleftrightarrow \mathrm{GL}_2(\mathbb{Z})$*-classes of binary cubic forms that are irreducible and maximal.*

Theorem (Davenport-Heilbronn)

The number of cubic fields of discriminant up to X *is* $\sim \frac{1}{3\zeta(3)}X$.

Binary cubic forms

Theorem (Delone-Fadeev)

Cubic fields $\longleftrightarrow \mathrm{GL}_2(\mathbb{Z})$*-classes of binary cubic forms that are irreducible and maximal.*

Theorem (Davenport-Heilbronn)

The number of cubic fields of discriminant up to X *is* $\sim \frac{1}{3\zeta(3)}X$.

Proof.

Use Delone-Fadeev and geometry of numbers. □

Binary cubic forms and ϕ-Selmer elements

Let $E\colon y^2 = x^3 + D(ax+b)^2$.

Binary cubic forms and ϕ-Selmer elements

Let $E\colon y^2 = x^3 + D(ax+b)^2$.

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

There is a bijection between $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ and the $\mathrm{SL}_2(\mathbb{Q})$-orbits of locally E-soluble integral binary cubic forms of discriminant $-12dDM^2$, where M is an integer depending only on E.

Binary cubic forms and ϕ-Selmer elements

Let $E\colon y^2 = x^3 + D(ax+b)^2$.

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

There is a bijection between $\mathrm{Sel}_\phi(E_d/\mathbb{Q})$ and the $\mathrm{SL}_2(\mathbb{Q})$-orbits of locally E-soluble integral binary cubic forms of discriminant $-12dDM^2$, where M is an integer depending only on E.

Idea

Use geometry of numbers + theorem to count ϕ-Selmer elements.

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny.

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum(|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum(|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,
- $r(E_d) = 0$ *for at least* $\frac{1}{2}\mathrm{dens}(T_0)$ *of* d,

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum (|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,
- $r(E_d) = 0$ *for at least* $\frac{1}{2}\mathrm{dens}(T_0)$ *of* d*, and*
- $r(E_d) = 1$ *for at least* $\frac{5}{6}\mathrm{dens}(T_{-1} \cup T_1)$ *of* d*, assuming Sha is finite.*

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum(|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,
- $r(E_d) = 0$ *for at least* $\frac{1}{2}\mathrm{dens}(T_0)$ *of* d*, and*
- $r(E_d) = 1$ *for at least* $\frac{5}{6}\mathrm{dens}(T_{-1} \cup T_1)$ *of* d*, assuming Sha is finite.*

Question

How do these results depend on E?

Typical behavior

Our results are sensitive to the number of bad primes,

Typical behavior

Our results are sensitive to the number of bad primes, but for "typical" curves E:

Typical behavior

Our results are sensitive to the number of bad primes, but for "typical" curves E:

- the average rank of $E_d/\mathbb{Q}$ is $O(\sqrt{\log\log N_E})$,

Typical behavior

Our results are sensitive to the number of bad primes, but for "typical" curves E:

- the average rank of $E_d/\mathbb{Q}$ is $O(\sqrt{\log\log N_E})$,
- the proportion of d with $r(E_d) = 0$ is $\gg 1/\sqrt{\log\log N_E}$,

Typical behavior

Our results are sensitive to the number of bad primes, but for "typical" curves E:

- the average rank of $E_d/\mathbb{Q}$ is $O(\sqrt{\log\log N_E})$,
- the proportion of d with $r(E_d) = 0$ is $\gg 1/\sqrt{\log\log N_E}$, and
- the same holds for the proportion of d with $r(E_d) = 1$, assuming Sha is finite.

Typical behavior

Our results are sensitive to the number of bad primes, but for "typical" curves E:

- the average rank of $E_d/\mathbb{Q}$ is $O(\sqrt{\log\log N_E})$,
- the proportion of d with $r(E_d) = 0$ is $\gg 1/\sqrt{\log\log N_E}$, and
- the same holds for the proportion of d with $r(E_d) = 1$, assuming Sha is finite.

However, there exist "extreme" curves

Typical behavior

Our results are sensitive to the number of bad primes, but for "typical" curves E:

- the average rank of $E_d/\mathbb{Q}$ is $O(\sqrt{\log\log N_E})$,
- the proportion of d with $r(E_d) = 0$ is $\gg 1/\sqrt{\log\log N_E}$, and
- the same holds for the proportion of d with $r(E_d) = 1$, assuming Sha is finite.

However, there exist "extreme" curves for which we can show only:

- $\mathrm{Avg.}(r(E_d)) \ll \log N_E / \log\log N_E$,

Typical behavior

Our results are sensitive to the number of bad primes, but for "typical" curves E:

- the average rank of $E_d/\mathbb{Q}$ is $O(\sqrt{\log\log N_E})$,
- the proportion of d with $r(E_d) = 0$ is $\gg 1/\sqrt{\log\log N_E}$, and
- the same holds for the proportion of d with $r(E_d) = 1$, assuming Sha is finite.

However, there exist "extreme" curves for which we can show only:

- $\mathrm{Avg.}(r(E_d)) \ll \log N_E / \log\log N_E$, and
- $r(E_d) = 0$ for $\gg \exp(-\log N_E / \log\log N_E)$ of d.

Typical behavior

Our results are sensitive to the number of bad primes, but for "typical" curves E:

- the average rank of $E_d/\mathbb{Q}$ is $O(\sqrt{\log\log N_E})$,
- the proportion of d with $r(E_d) = 0$ is $\gg 1/\sqrt{\log\log N_E}$, and
- the same holds for the proportion of d with $r(E_d) = 1$, assuming Sha is finite.

However, there exist "extreme" curves for which we can show only:

- $\mathrm{Avg.}(r(E_d)) \ll \log N_E / \log\log N_E$, and
- $r(E_d) = 0$ for $\gg \exp(-\log N_E / \log\log N_E)$ of d.

Question

Are we just inefficient, or is there something weird with ϕ-Selmer?

Averages in big families

Theorem (Bhargava-Shankar)

Let $m \in \{2, 3, 4, 5\}$. *Then* $\mathrm{Avg.}|\mathrm{Sel}_m(E/\mathbb{Q})| = \sigma(m)$,

Averages in big families

Theorem (Bhargava-Shankar)

Let $m \in \{2,3,4,5\}$*. Then* $\mathrm{Avg.}|\mathrm{Sel}_m(E/\mathbb{Q})| = \sigma(m)$*, where the average is over all elliptic curves.*

Averages in big families

Theorem (Bhargava-Shankar)

Let $m \in \{2, 3, 4, 5\}$*. Then* $\mathrm{Avg.}|\mathrm{Sel}_m(E/\mathbb{Q})| = \sigma(m)$*, where the average is over all elliptic curves.*

Theorem (Klagsbrun-LO)

Let $p \in \{3, 5, 7, 13\}$*, and let* E *range over all elliptic curves with a* p*-isogeny and* $Ht^*(E) \leq X$*.*

Averages in big families

Theorem (Bhargava-Shankar)

Let $m \in \{2, 3, 4, 5\}$. *Then* $\mathrm{Avg.}|\mathrm{Sel}_m(E/\mathbb{Q})| = \sigma(m)$, *where the average is over all elliptic curves.*

Theorem (Klagsbrun-LO)

Let $p \in \{3, 5, 7, 13\}$, *and let* E *range over all elliptic curves with a* p*-isogeny and* $Ht^*(E) \leq X$. *Then*

$$\mathrm{Avg.}|\mathrm{Sel}_\phi(E/\mathbb{Q})|$$

Averages in big families

Theorem (Bhargava-Shankar)

Let $m \in \{2, 3, 4, 5\}$*. Then* $\mathrm{Avg.}|\mathrm{Sel}_m(E/\mathbb{Q})| = \sigma(m)$*, where the average is over all elliptic curves.*

Theorem (Klagsbrun-LO)

Let $p \in \{3, 5, 7, 13\}$*, and let* E *range over all elliptic curves with a* p*-isogeny and* $Ht^*(E) \leq X$*. Then*

$$\mathrm{Avg.}|\mathrm{Sel}_\phi(E/\mathbb{Q})| \gg (\log X)^{(p-1)^2/2p}.$$

Averages in big families

Theorem (Bhargava-Shankar)

Let $m \in \{2,3,4,5\}$*. Then* $\mathrm{Avg.}|\mathrm{Sel}_m(E/\mathbb{Q})| = \sigma(m)$*, where the average is over all elliptic curves.*

Theorem (Klagsbrun-LO)

Let $p \in \{3,5,7,13\}$*, and let* E *range over all elliptic curves with a* p*-isogeny and* $Ht^*(E) \leq X$*. Then*

$$\mathrm{Avg.}|\mathrm{Sel}_\phi(E/\mathbb{Q})| \gg (\log X)^{(p-1)^2/2p}.$$

Corollary

For $E/\mathbb{Q}$ *with a 3-isogeny,* $\mathrm{Avg.}|\mathrm{Sel}_\phi(E/\mathbb{Q})| \gg (\log X)^{2/3}$*.*

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny.

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum(|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum (|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,
- $r(E_d) = 0$ *for at least* $\frac{1}{2}\mathrm{dens}(T_0)$ *of* d,

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum(|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,
- $r(E_d) = 0$ *for at least* $\frac{1}{2}\mathrm{dens}(T_0)$ *of* d*, and*
- $r(E_d) = 1$ *for at least* $\frac{5}{6}\mathrm{dens}(T_{-1} \cup T_1)$ *of* d*, assuming Sha is finite.*

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum(|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,
- $r(E_d) = 0$ *for at least* $\frac{1}{2}\mathrm{dens}(T_0)$ *of* d*, and*
- $r(E_d) = 1$ *for at least* $\frac{5}{6}\mathrm{dens}(T_{-1} \cup T_1)$ *of* d*, assuming Sha is finite.*

Remark

Also works over number fields.

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\mathrm{Avg.}(r(E_d)) \leq \sum(|m| + 3^{-|m|}) \cdot \mathrm{dens}(T_m)$,
- $r(E_d) = 0$ *for at least* $\frac{1}{2}\mathrm{dens}(T_0)$ *of* d*, and*
- $r(E_d) = 1$ *for at least* $\frac{5}{6}\mathrm{dens}(T_{-1} \cup T_1)$ *of* d*, assuming Sha is finite.*

Remark

Also works over number fields. There are examples with $r(E_d/K) = 0$ for 50% of d,

A more explicit result

Theorem (Bhargava-Klagsbrun-LO-Shnidman)

Let $E/\mathbb{Q}$ have a 3-isogeny. Then

- $\text{Avg.}(r(E_d)) \leq \sum (|m| + 3^{-|m|}) \cdot \text{dens}(T_m)$,
- $r(E_d) = 0$ *for at least* $\frac{1}{2}\text{dens}(T_0)$ *of* d, *and*
- $r(E_d) = 1$ *for at least* $\frac{5}{6}\text{dens}(T_{-1} \cup T_1)$ *of* d, *assuming Sha is finite.*

Remark

Also works over number fields. There are examples with $r(E_d/K) = 0$ for 50% of d, but all have $w(E_d) = +1$.