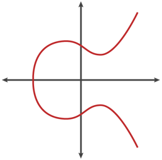
# On ranks of quadratic twists of a Mordell curve

Bidisha Roy
Scuola Normale Superiore di Pisa
Pisa, Italy
bidisha.roy@sns.it

Journées Arithmétiques 2023
Nancy, France

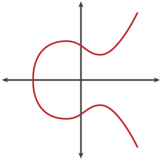
this is a joint work with A. Jyual and D. Moody

# Elliptic curve defined over number fields (Overview)



- Let $K$ be a number field and $E$ be an elliptic curve defined over $K$.

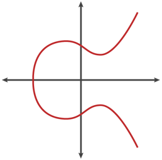
# Elliptic curve defined over number fields (Overview)



• Let $K$ be a number field and $E$ be an elliptic curve defined over $K$.

• We can take $E$ in Weierstrass form: $y^2 = x^3 + ax^2 + bx + c$.

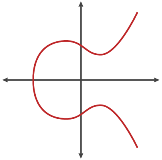
# Elliptic curve defined over number fields (Overview)



- Let $K$ be a number field and $E$ be an elliptic curve defined over $K$.

- We can take $E$ in Weierstrass form: $y^2 = x^3 + ax^2 + bx + c$.

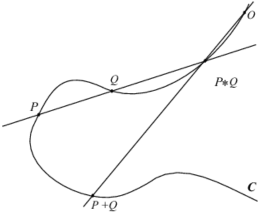
- We know $E(K) := \{P = (x, y) : x, y \in K \text{ and } E(x, y) = \mathcal{O}\} \cup \{\mathcal{O}\}$ is called the set of $K$-rational points of $E$.



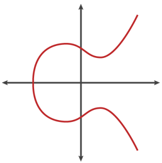
• Let $K$ be a number field and $E$ be an elliptic curve defined over $K$.

• We can take $E$ in Weierstrass form: $y^2 = x^3 + ax^2 + bx + c$.

• We know $E(K) := \{P = (x, y) : x, y \in K \text{ and } E(x, y) = \mathcal{O}\} \cup \{\mathcal{O}\}$ is called the set of $K$-rational points of $E$.



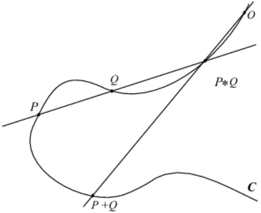

• The set, $E(K)$, has a group structure under addition with the identity element, $\mathcal{O}$.



• Let $K$ be a number field and $E$ be an elliptic curve defined over $K$.

• We can take $E$ in Weierstrass form: $y^2 = x^3 + ax^2 + bx + c$.

• We know $E(K) := \{P = (x, y) : x, y \in K \text{ and } E(x, y) = \mathcal{O}\} \cup \{\mathcal{O}\}$ is called the set of $K$-rational points of $E$.




• The set, $E(K)$, has a group structure under addition with the identity element, $\mathcal{O}$.

• We also know that the group $E(K)$ is a finitely generated abelian group by Mordell-Weil theorem.

# Elliptic curve defined over number fields (Overview)...

- By structure theorem, the *Mordell-Weil group*, $E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$.

- By structure theorem, the *Mordell-Weil group*, $E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$.

It is well known that the possible torsion groups are of the form $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for two positive integers $n$ and $m$.

- By structure theorem, the *Mordell-Weil group*, $E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$.

It is well known that the possible torsion groups are of the form $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for two positive integers $n$ and $m$.

Focus on rationals ($\mathbb{Q}$)

- By structure theorem, the *Mordell-Weil group*, $E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$.

It is well known that the possible torsion groups are of the form $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for two positive integers $n$ and $m$.

Focus on rationals ($\mathbb{Q}$)

- $r$ is called the rank(E).

- By structure theorem, the *Mordell-Weil group*, $E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$.

It is well known that the possible torsion groups are of the form $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for two positive integers $n$ and $m$.

Focus on rationals ($\mathbb{Q}$)

- $r$ is called the rank(E).

⇢ The rank is related to several outstanding problems in number theory, most notably the Birch–Swinnerton-Dyer conjecture.

- By structure theorem, the *Mordell-Weil group*, $E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$.

It is well known that the possible torsion groups are of the form $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for two positive integers $n$ and $m$.

Focus on rationals ($\mathbb{Q}$)

- $r$ is called the rank(E).

--→ The rank is related to several outstanding problems in number theory, most notably the Birch–Swinnerton-Dyer conjecture.

--→ It is widely believed that there is no maximum rank for an elliptic curve.

• By structure theorem, the *Mordell-Weil group*, $E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$.

It is well known that the possible torsion groups are of the form $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for two positive integers $n$ and $m$.

Focus on rationals ($\mathbb{Q}$)

• $r$ is called the rank(E).

--→ The rank is related to several outstanding problems in number theory, most notably the Birch–Swinnerton-Dyer conjecture.

--→ It is widely believed that there is no maximum rank for an elliptic curve.

**Known records:**

• By structure theorem, the *Mordell-Weil group*, $E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$.

It is well known that the possible torsion groups are of the form $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for two positive integers $n$ and $m$.

Focus on rationals ($\mathbb{Q}$)

• $r$ is called the rank(E).

--→ The rank is related to several outstanding problems in number theory, most notably the Birch–Swinnerton-Dyer conjecture.

--→ It is widely believed that there is no maximum rank for an elliptic curve.

**Known records:**

- There exist elliptic curves with rank as large as 28.

# Quadratic twist:

A general elliptic curve $E/\mathbb{Q}$ given by the weierstrass equation

$$E : y^2 = x^3 + ax^2 + bx + c, \qquad a, b, c \in \mathbb{Z}$$

# Quadratic twist:

A general elliptic curve $E/\mathbb{Q}$ given by the weierstrass equation

$$E : y^2 = x^3 + ax^2 + bx + c, \qquad a, b, c \in \mathbb{Z}$$

A twist of $E/\mathbb{Q}$ is another elliptic curve which is isomorphic to E over $\overline{\mathbb{Q}}$.

# Quadratic twist:

A general elliptic curve $E/\mathbb{Q}$ given by the weierstrass equation

$$E : y^2 = x^3 + ax^2 + bx + c, \qquad a, b, c \in \mathbb{Z}$$

A twist of $E/\mathbb{Q}$ is another elliptic curve which is isomorphic to E over $\overline{\mathbb{Q}}$.

For a square free integer $d$,

$$\text{Quadratic Twist (E)}: y^2 = x^3 + dax^2 + d^2bx + d^3c$$

# Quadratic twist:

A general elliptic curve $E/\mathbb{Q}$ given by the weierstrass equation

$$E : y^2 = x^3 + ax^2 + bx + c, \qquad a, b, c \in \mathbb{Z}$$

A twist of $E/\mathbb{Q}$ is another elliptic curve which is isomorphic to E over $\overline{\mathbb{Q}}$.

For a square free integer $d$,

$$\text{Quadratic Twist (E)}: y^2 = x^3 + dax^2 + d^2bx + d^3c$$

$$E \simeq \text{Quadratic Twist (E)}$$

$$(x, y) \mapsto \left(\frac{x}{d}, \frac{y}{d\sqrt{d}}\right)$$

# Quadratic twist:

A general elliptic curve $E/\mathbb{Q}$ given by the weierstrass equation

$$E : y^2 = x^3 + ax^2 + bx + c, \qquad a, b, c \in \mathbb{Z}$$

A twist of $E/\mathbb{Q}$ is another elliptic curve which is isomorphic to E over $\overline{\mathbb{Q}}$.

For a square free integer $d$,

$$\text{Quadratic Twist (E)}: y^2 = x^3 + dax^2 + d^2bx + d^3c$$

$$E \simeq \text{Quadratic Twist (E)}$$

$$(x, y) \mapsto \left(\frac{x}{d}, \frac{y}{d\sqrt{d}}\right)$$

$\rightsquigarrow$ Twists has importance in multiple directions like cryptography, understanding 'positive-ranks' etc .

# Goal

For today's discussion:

# Goal

For today's discussion:

Mordell Curve: $y^2 = x^3 - c$

# Goal

For today's discussion:

Mordell Curve: $y^2 = x^3 - c$

Our sample:

$$E^0 : y^2 = x^3 - 1$$

$$\downarrow$$

Quadratic twist $(E^0)$ is $E_d^0 : y^2 = x^3 - d^3$

# Goal

For today's discussion:

Mordell Curve: $y^2 = x^3 - c$

Our sample:

$$E^0 : y^2 = x^3 - 1$$

$$\downarrow$$

Quadratic twist $(E^0)$ is $E_d^0 : y^2 = x^3 - d^3$

Understand Ranks of $E_d^0$, while varying $d$!

# Historical Remarks

**Goldfeld, Katz-Sarnark**

Almost all elliptic curves have rank 0 or 1.

# Historical Remarks

**Goldfeld, Katz-Sarnark**

Almost all elliptic curves have rank 0 or 1.

In particular:

**Goldfeld**: Average ranks of quadratic twists of a specific curve $= \frac{1}{2}$

**Goldfeld, Katz-Sarnark**

Almost all elliptic curves have rank 0 or 1.

In particular:

**Goldfeld**: Average ranks of quadratic twists of a specific curve $= \frac{1}{2}$

In technical terms:

$$\lim_{X\to\infty} \frac{\sum_{|d|<X} rank(E_d)}{\#\{d : |d| < X\}} = \frac{1}{2},$$

**Goldfeld, Katz-Sarnark**

Almost all elliptic curves have rank 0 or 1.

In particular:

**Goldfeld**: Average ranks of quadratic twists of a specific curve $= \frac{1}{2}$

In technical terms:

$$\lim_{X \to \infty} \frac{\sum_{|d|<X} rank(E_d)}{\#\{d : |d| < X\}} = \frac{1}{2},$$

**Known records:**

# Historical Remarks

**Goldfeld, Katz-Sarnark**

Almost all elliptic curves have rank 0 or 1.

In particular:

**Goldfeld**: Average ranks of quadratic twists of a specific curve $= \frac{1}{2}$

In technical terms:

$$\lim_{X\to\infty} \frac{\sum_{|d|<X} rank(E_d)}{\#\{d : |d| < X\}} = \frac{1}{2},$$

**Known records:**

- Hofstein & Luo: for any fixed $E$, there exists infinitley many odd square free $d$ with $\omega(d) \leq 3$, we have $\text{rank}(E_d) = 0$.

# Historical Remarks

**Goldfeld, Katz-Sarnark**

Almost all elliptic curves have rank 0 or 1.

In particular:

**Goldfeld**: Average ranks of quadratic twists of a specific curve $= \frac{1}{2}$

In technical terms:

$$\lim_{X\to\infty} \frac{\sum_{|d|<X} rank(E_d)}{\#\{d : |d| < X\}} = \frac{1}{2},$$

**Known records:**

- Hofstein & Luo: for any fixed $E$, there exists infinitley many odd square free $d$ with $\omega(d) \leq 3$, we have $\text{rank}(E_d) = 0$.
- Ono & Skinner: $\#\{|d| \leq X : rank(E_d) = 0\} >> X/\log X$

**Goldfeld, Katz-Sarnark**

Almost all elliptic curves have rank 0 or 1.

In particular:

**Goldfeld**: Average ranks of quadratic twists of a specific curve $= \frac{1}{2}$

In technical terms:

$$\lim_{X\to\infty} \frac{\sum_{|d|<X} rank(E_d)}{\#\{d : |d| < X\}} = \frac{1}{2},$$

**Known records:**

- Hofstein & Luo: for any fixed $E$, there exists infinitley many odd square free $d$ with $\omega(d) \leq 3$, we have $\text{rank}(E_d) = 0$.
- Ono & Skinner: $\#\{|d| \leq X : rank(E_d) = 0\} >> X/\log X$
- K. James: $y^2 = x^3 - x^2 - 72x + 368$

**Goldfeld, Katz-Sarnark**

Almost all elliptic curves have rank 0 or 1.

In particular:

**Goldfeld**: Average ranks of quadratic twists of a specific curve $= \frac{1}{2}$

In technical terms:

$$\lim_{X\to\infty} \frac{\sum_{|d|<X} rank(E_d)}{\#\{d : |d| < X\}} = \frac{1}{2},$$

**Known records:**

- Hofstein & Luo: for any fixed $E$, there exists infinitley many odd square free $d$ with $\omega(d) \leq 3$, we have $\text{rank}(E_d) = 0$.
- Ono & Skinner: $\#\{|d| \leq X : rank(E_d) = 0\} >> X/\log X$
- K. James: $y^2 = x^3 - x^2 - 72x + 368$
- Kohen: 19.B of Cremona Level $\dashrightarrow$ Rank 1

--→ Most of these types of results have taken the approach of utilizing the non-vanishing of $L$ - functions.

⇢ Most of these types of results have taken the approach of utilizing the non-vanishing of $L$ - functions.

In general, Goldfeld's conjecture is very much open.

⇢ Most of these types of results have taken the approach of utilizing the non-vanishing of $L$ - functions.

In general, Goldfeld's conjecture is very much open. [A. Smith made remarkable progress towards a Selmer-counterpart of Goldfeld's conjecture]

⇢ Most of these types of results have taken the approach of utilizing the non-vanishing of $L$ - functions.

In general, Goldfeld's conjecture is very much open. [A. Smith made remarkable progress towards a Selmer-counterpart of Goldfeld's conjecture]

<u>Application of decent methods:</u>

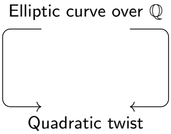
⇢ Most of these types of results have taken the approach of utilizing the non-vanishing of $L$ - functions.

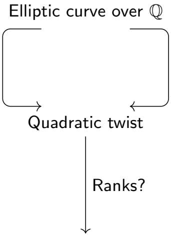
In general, Goldfeld's conjecture is very much open. [A. Smith made remarkable progress towards a Selmer-counterpart of Goldfeld's conjecture]

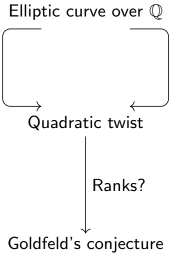
Application of decent methods:

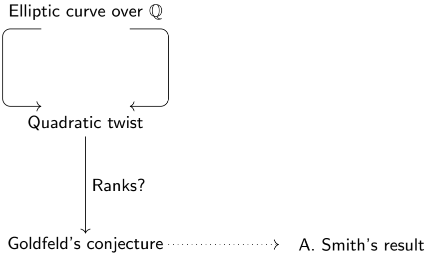
⇢ Dabrowski: For any positive integer $k$, there exits pairwise non-isogenous elliptic curves $E^1, \ldots, E^k$ such that $rank(E_p^1) = \cdots = rank(E_p^k) = 0$, for positive proposition of primes.

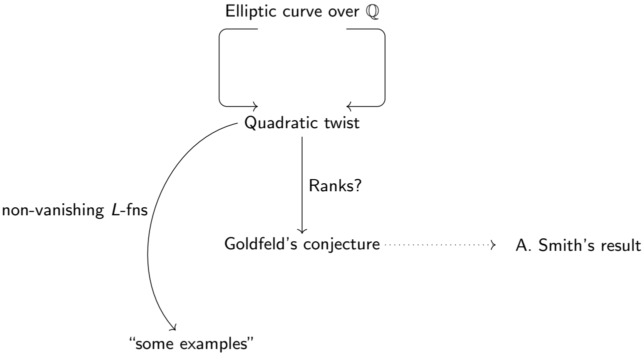
Elliptic curve over $\mathbb{Q}$

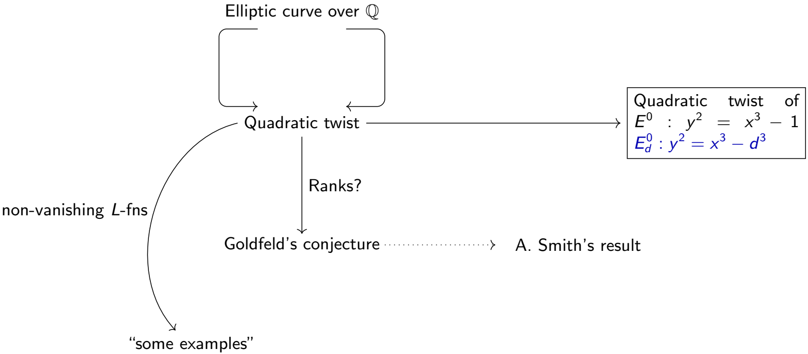

Elliptic curve over $\mathbb{Q}$
Quadratic twist

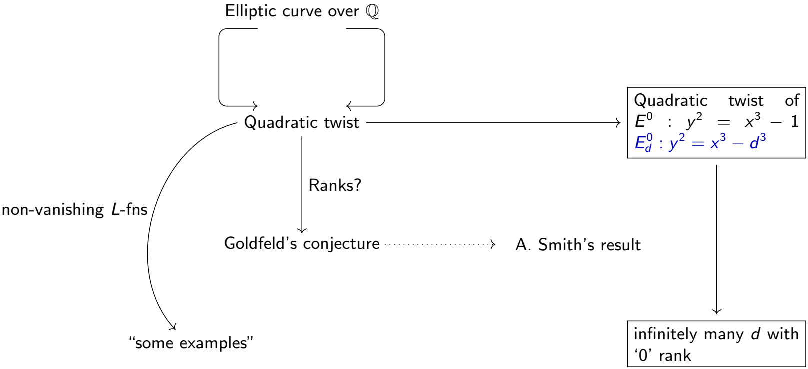

Elliptic curve over $\mathbb{Q}$
Quadratic twist
Ranks?


Elliptic curve over $\mathbb{Q}$
Quadratic twist
Ranks?
Goldfeld's conjecture


Elliptic curve over $\mathbb{Q}$
Quadratic twist
Ranks?
Goldfeld's conjecture
A. Smith's result

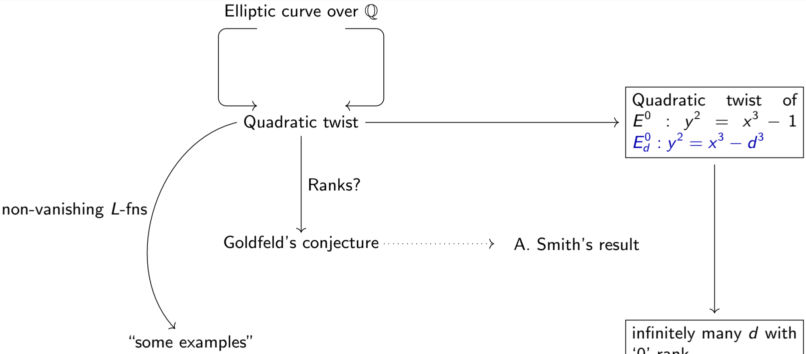

Elliptic curve over $\mathbb{Q}$
Quadratic twist
Ranks?
non-vanishing $L$-fns
Goldfeld's conjecture
A. Smith's result
"some examples"

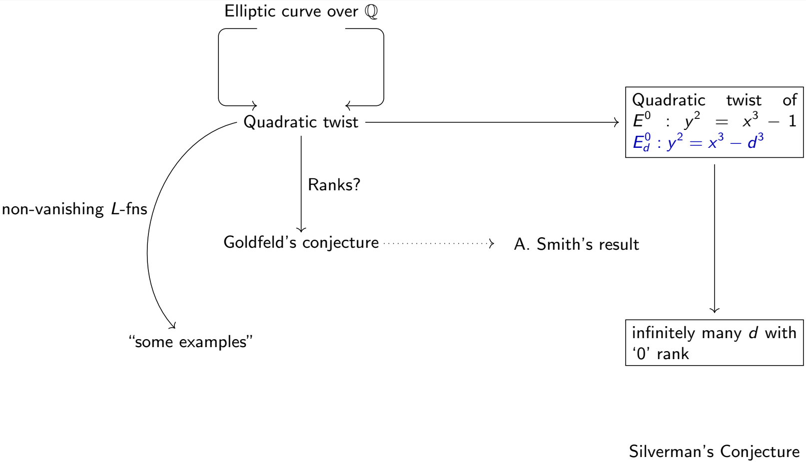

Elliptic curve over ℚ
Quadratic twist
Quadratic twist of
$E^0 : y^2 = x^3 - 1$
$E^0_d : y^2 = x^3 - d^3$
Ranks?
non-vanishing $L$-fns
Goldfeld's conjecture
A. Smith's result
"some examples"

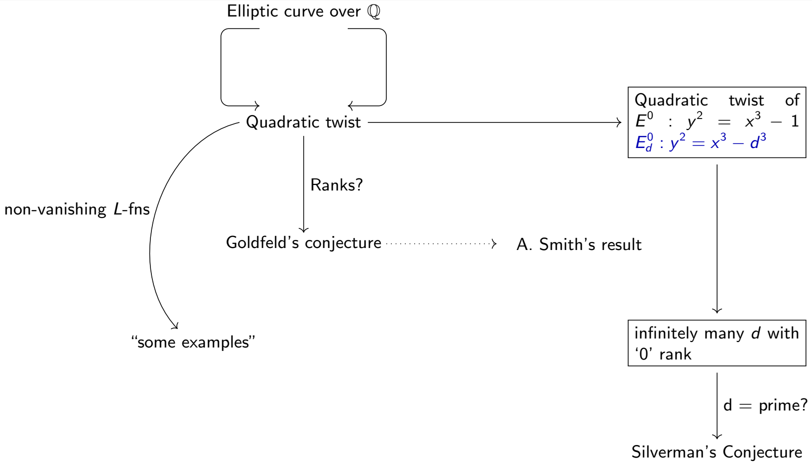



**Theorem: (2022)**

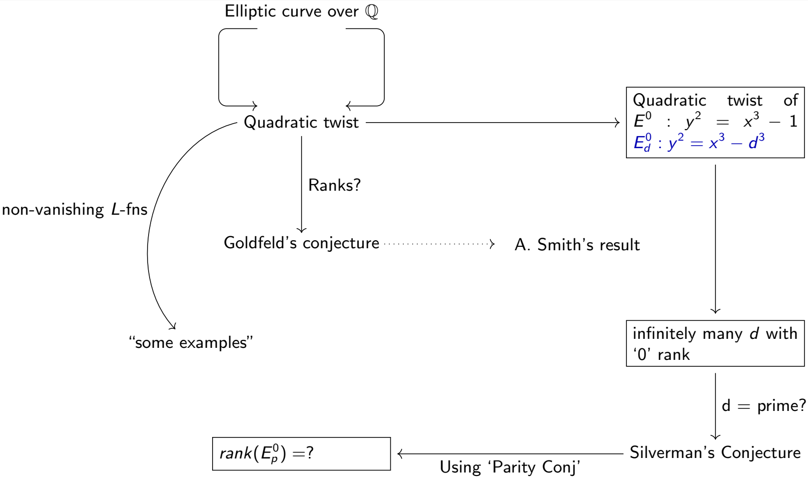
For any square-free integer $d$, we have the quadratic twist $E_d^0 : y^2 = x^3 - d^3$. Let $\omega(d)$ be the number of distinct prime divisors of $d$. Then there exist infinitely many square-free integers $d$, with $\omega(d) > 1$, such that $rank(E_d^0) = 0$.


Elliptic curve over $\mathbb{Q}$
Quadratic twist
Quadratic twist of $E^0: y^2 = x^3 - 1$ $E^0_d: y^2 = x^3 - d^3$
Ranks?
non-vanishing $L$-fns
Goldfeld's conjecture
A. Smith's result
"some examples"
infinitely many $d$ with '0' rank


Elliptic curve over $\mathbb{Q}$
Quadratic twist
Quadratic twist of $E^0 : y^2 = x^3 - 1$
$E^0_d : y^2 = x^3 - d^3$
Ranks?
non-vanishing $L$-fns
Goldfeld's conjecture
A. Smith's result
"some examples"
infinitely many $d$ with '0' rank
Silverman's Conjecture



Elliptic curve over $\mathbb{Q}$
Quadratic twist
Quadratic twist of $E^0 : y^2 = x^3 - 1$
$E_d^0 : y^2 = x^3 - d^3$
Ranks?
non-vanishing $L$-fns
Goldfeld's conjecture
A. Smith's result
"some examples"
infinitely many $d$ with '0' rank
d = prime?
Silverman's Conjecture




**Conj: Parity**

Let $E$ be an elliptic curve defined over a number field $K$. Then

$$(-1)^{rank(E/K)} = w(E/K)$$

where $w(E/K)$ is the *global root number*.

**Conj:(Silverman)**

If $E$ is an elliptic curve, then there are infinitely many primes $p$ for which $E_p(\mathbb{Q})$ has positive ranks, and there are infinitely many primes $q$ for which $E_q(\mathbb{Q})$ has rank 0.

**Conj:(Silverman)**

If $E$ is an elliptic curve, then there are infinitely many primes $p$ for which $E_p(\mathbb{Q})$ has positive ranks, and there are infinitely many primes $q$ for which $E_q(\mathbb{Q})$ has rank 0.

$$\updownarrow$$

### Conj:(Silverman)

If $E$ is an elliptic curve, then there are infinitely many primes $p$ for which $E_p(\mathbb{Q})$ has positive ranks, and there are infinitely many primes $q$ for which $E_q(\mathbb{Q})$ has rank 0.

$$\updownarrow$$

### Theorem: (2022)

For the elliptic curve $E_p^0 : y^2 = x^3 - p^3$, we have

$$rank(E_p^0) = \begin{cases} 0 & \text{if } p \equiv 5 \pmod{12}, \\ 1 & \text{if } p \equiv 11 \pmod{12} \text{ (assuming the Parity Conjecture).} \end{cases} \quad (1)$$

♦ quadratic twist of the Mordell curve $E^0 : y^2 = x^3 - 1$:

$$E^0_d : y^2 = x^3 - d^3$$

♦ quadratic twist of the Mordell curve $E^0 : y^2 = x^3 - 1$:

$$E_d^0 : y^2 = x^3 - d^3$$

♦ It is easy to check that $E_d^0$ has a 2- torsion point, namely $(d, 0)$.

♦ quadratic twist of the Mordell curve $E^0 : y^2 = x^3 - 1$:

$$E_d^0 : y^2 = x^3 - d^3$$

♦ It is easy to check that $E_d^0$ has a 2- torsion point, namely $(d, 0)$.

♦ Corresponding to the 2-torsion point, there is a 2-isogeny $\phi : E_d^0 \longrightarrow E_d'$ which has the kernel $\{\mathcal{O}, (d, 0)\}$ with the image curve is

$$E_d' : y^2 = x^3 - 6dx^2 - 3d^2x,$$

and $\phi$ given by

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

♦ quadratic twist of the Mordell curve $E^0 : y^2 = x^3 - 1$:

$$E^0_d : y^2 = x^3 - d^3$$

♦ It is easy to check that $E^0_d$ has a 2- torsion point, namely $(d, 0)$.

♦ Corresponding to the 2-torsion point, there is a 2-isogeny $\phi : E^0_d \longrightarrow E'_d$ which has the kernel $\{\mathcal{O}, (d, 0)\}$ with the image curve is

$$E'_d : y^2 = x^3 - 6dx^2 - 3d^2x,$$

and $\phi$ given by

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

♦ Using standard techniques of Galois cohomology, we obtain an exact

sequence:

$$0 \to \frac{E'_d(\mathbb{Q})}{\phi(E^0_d(\mathbb{Q}))} \to Sel^{(\phi)}(E^0_d/\mathbb{Q}) \to Sha(E^0_d/\mathbb{Q})[\phi] \to 0,$$

♦ quadratic twist of the Mordell curve $E^0 : y^2 = x^3 - 1$:

$$E^0_d : y^2 = x^3 - d^3$$

♦ It is easy to check that $E^0_d$ has a 2- torsion point, namely $(d, 0)$.

♦ Corresponding to the 2-torsion point, there is a 2-isogeny $\phi : E^0_d \longrightarrow E'_d$ which has the kernel $\{\mathcal{O}, (d, 0)\}$ with the image curve is

$$E'_d : y^2 = x^3 - 6dx^2 - 3d^2x,$$

and $\phi$ given by

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

♦ Using standard techniques of Galois cohomology, we obtain an exact

sequence:

$$0 \to \frac{E'_d(\mathbb{Q})}{\phi(E^0_d(\mathbb{Q}))} \to Sel^{(\phi)}(E^0_d/\mathbb{Q}) \to Sha(E^0_d/\mathbb{Q})[\phi] \to 0,$$

♦ The above is also true for the dual isogeny $\widehat{\phi}$

♦ For a square-free positive integer $d$, define a finite set $S$ of prime divisors of the rational numbers $\mathbb{Q}$ by

$$S = \{\infty\} \cup \{\text{primes } p : p | 6d\}.$$

♦ For a square-free positive integer $d$, define a finite set $S$ of prime divisors of the rational numbers $\mathbb{Q}$ by

$$S = \{\infty\} \cup \{\text{primes } p : p|6d\}.$$

♦ Let $M$ be the multiplicative subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by $-1$ and the divisors of $6d$.

♦ For a square-free positive integer $d$, define a finite set $S$ of prime divisors of the rational numbers $\mathbb{Q}$ by

$$S = \{\infty\} \cup \{\text{primes } p : p|6d\}.$$

♦ Let $M$ be the multiplicative subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by $-1$ and the divisors of $6d$.

♦ For each $k \in M$ we have the homogeneous spaces $C_k$ and $C'_k$ defined by

$$C_k : kw^2 = k^2t^4 - 6kdt^2z^2 - 3d^2z^4,$$
$$C'_k : kw^2 = k^2t^4 + 3kdt^2z^2 - 3d^2z^4.$$

♦ For a square-free positive integer $d$, define a finite set $S$ of prime divisors of the rational numbers $\mathbb{Q}$ by

$$S = \{\infty\} \cup \{\text{primes } p : p | 6d\}.$$

♦ Let $M$ be the multiplicative subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by $-1$ and the divisors of $6d$.

♦ For each $k \in M$ we have the homogeneous spaces $C_k$ and $C'_k$ defined by

$$C_k : kw^2 = k^2t^4 - 6kdt^2z^2 - 3d^2z^4,$$
$$C'_k : kw^2 = k^2t^4 + 3kdt^2z^2 - 3d^2z^4.$$

♦ The Selmer group $Sel^{(\phi)}(E_d^0/\mathbb{Q})$ (respectively $Sel^{(\hat{\phi})}(E_d^{'}/\mathbb{Q})$) measures the possibility of $C_k$ (or $C'_k$) having non-trivial solutions in the local field $\mathbb{Q}_v$ for all $v \in S$.

♦ For a square-free positive integer $d$, define a finite set $S$ of prime divisors of the rational numbers $\mathbb{Q}$ by

$$S = \{\infty\} \cup \{\text{primes } p : p|6d\}.$$

♦ Let $M$ be the multiplicative subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by $-1$ and the divisors of $6d$.

♦ For each $k \in M$ we have the homogeneous spaces $C_k$ and $C_k'$ defined by

$$C_k : kw^2 = k^2t^4 - 6kdt^2z^2 - 3d^2z^4,$$
$$C_k' : kw^2 = k^2t^4 + 3kdt^2z^2 - 3d^2z^4.$$

♦ The Selmer group $Sel^{(\phi)}(E_d^0/\mathbb{Q})$ (respectively $Sel^{(\hat{\phi})}(E_d^{'}/\mathbb{Q})$) measures the possibility of $C_k$ (or $C_k'$) having non-trivial solutions in the local field $\mathbb{Q}_v$ for all $v \in S$.

♦

$$Sel^{(\phi)}(E_d^0/\mathbb{Q}) = \{k \in M : C_k(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in S\},$$
$$Sel^{(\hat{\phi})}(E_d'/\mathbb{Q}) = \{k \in M : C_k'(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in S\},$$

## Lemma

*Let $E/\mathbb{Q}$ be an elliptic curve with a rational point of order 2. Let $\phi : E \to E'$ be an isogeny of degree 2, with $\widehat{\phi} : E' \to E$ the dual of $\phi$. Then*

$$rank(E(\mathbb{Q})) \leq dim_{\mathbb{F}_2} Sel^{(\phi)}(E, \mathbb{Q}) + dim_{\mathbb{F}_2} Sel^{(\widehat{\phi})}(E', \mathbb{Q}) - 2.$$

**Lemma**

*Let $E/\mathbb{Q}$ be an elliptic curve with a rational point of order 2. Let $\phi : E \to E'$ be an isogeny of degree 2, with $\widehat{\phi} : E' \to E$ the dual of $\phi$. Then*

$$rank(E(\mathbb{Q})) \leq dim_{\mathbb{F}_2} Sel^{(\phi)}(E, \mathbb{Q}) + dim_{\mathbb{F}_2} Sel^{(\widehat{\phi})}(E', \mathbb{Q}) - 2.$$

By calculating $C_k(\mathbb{Q}_v)$ and $C'_k(\mathbb{Q}_v)$ precisely,

**Lemma**

*Let $E/\mathbb{Q}$ be an elliptic curve with a rational point of order 2. Let $\phi : E \to E'$ be an isogeny of degree 2, with $\widehat{\phi} : E' \to E$ the dual of $\phi$. Then*

$$rank(E(\mathbb{Q})) \leq dim_{\mathbb{F}_2} Sel^{(\phi)}(E, \mathbb{Q}) + dim_{\mathbb{F}_2} Sel^{(\widehat{\phi})}(E', \mathbb{Q}) - 2.$$

By calculating $C_k(\mathbb{Q}_v)$ and $C'_k(\mathbb{Q}_v)$ precisely,

$$\{1, -3\} = Sel^{(\phi)}(E^0_d/\mathbb{Q})$$

and

$$\{1, 3\} = Sel^{(\widehat{\phi})}(E'_d/\mathbb{Q})$$

□

# Positive rank evidence:

Both Goldfelds's Conjecture and Silverman's Conjecture are concerned with elliptic curves with positive rank.

Both Goldfelds's Conjecture and Silverman's Conjecture are concerned with elliptic curves with positive rank.

**Theorem: (2022)**

Let $E_d^0$ be the curve given by $y^2 = x^3 - d^3$. Then

Remark: There are infinitely many integers $n$ such that $E_n^0 : y^2 = x^3 - n^3$ has positive rank. There are infinitely many integers $m$ such that $E_m^0$ has rank zero.

# Positive rank evidence:

Both Goldfelds's Conjecture and Silverman's Conjecture are concerned with elliptic curves with positive rank.

**Theorem: (2022)**

Let $E_d^0$ be the curve given by $y^2 = x^3 - d^3$. Then

(a) There exist infinitely many integers $d$ such that $rank(E_d^0)$ is **positive**.

Remark: There are infinitely many integers $n$ such that $E_n^0 : y^2 = x^3 - n^3$ has positive rank. There are infinitely many integers $m$ such that $E_m^0$ has rank zero.

# Positive rank evidence:

Both Goldfelds's Conjecture and Silverman's Conjecture are concerned with elliptic curves with positive rank.

**Theorem: (2022)**

Let $E_d^0$ be the curve given by $y^2 = x^3 - d^3$. Then

(a) There exist infinitely many integers $d$ such that $rank(E_d^0)$ is **positive**.

(b) There is an infinite family of curves $E_d^0$, over the number field $\mathbb{Q}(m)$, with rank **at least** 2. Here $d$ and $m$ are related by the following equation:

$$d = \left(\frac{1 - 2m^2}{m^2 + 1}\right)^3 - 1.$$

Remark: There are infinitely many integers $n$ such that $E_n^0 : y^2 = x^3 - n^3$ has positive rank. There are infinitely many integers $m$ such that $E_m^0$ has rank zero.

[1] A. Dabrowski, On the proportion of rank 0 twists of elliptic curve; *C. R. Acad. Sci. Paris, Ser.* I, **346** (2008).

[2] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, in *Number Theory Carbondale 1979*, Lecture Notes in Mathematics, Vol. **751** (Springer, Berlin, 1979), pp. 108-118.

[3] J. Hofstein and W. Luo, Nonvanishing of L-series and the combinatorial sieve, *Math. Res. Lett.* **4** (1997), 435-444.

[4] K. James, L-series with non-zero central critical value, *J. Amer. Math. Soc.* **11** (1998), 635-641.

[5] A. Juyal, D. Moody and B. Roy ,*On ranks of quadratic twists of a Mordell curve,* The Ramanujan Journal **59** (2022), 31–50.

[6] W. Kohnen, On the proportion of quadratic twists of L-functions attached to cusp forms not vanishing at the central point,*J. reine angew. Math.* **508** (1999), 179-187.

[7] L. J. Mordell, On some Diophantine equations $y^2 = x^3 + k$ with no rational solutions (II), in: *Number Theory and Analysis*, Springer, Boston, MA, 1969, pp. 224-232.

[8] K. Ono, Twists Of Elliptic Curves, *Compositio Math.* **106** (1997), no. 3, 349-360.

[9] K. Ono and C. Skinner, Non-vanishing of quadratic twists of modular L-functions, *Invent. Math.* **34** (1998), 651-660.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York-Berlin- Heidelberg-tokyo, 1986.

[11] A. Smith, $2^{\infty}$-Selmer groups, $2^{\infty}$-class groups, and Goldfeld's conjecture. arxiv.org/abs/1702.02325.

[12] V. Vatsal, Rank-one twists of a certain elliptic curve, *Math. Ann.* 311 (1998), 791-794.

[13] **Talk of Tomasz Jedrzejak in Journées Arithmétiques 2023.**

Thank You for Your Attention!