On the Arithmetic of Twists of Superelliptic Curves

Sungkon Chang

University of Georgia
Plan

• Diophantine Equations

• Elliptic Curves and Twists

• Superelliptic Curves and Twists
Diophantine Equations

Notation: \( \mathbb{Z}, \mathbb{Q}, K, \mathbb{R}, \mathbb{C} \).

A Diophantine equation is

\[ P(x_1, \ldots, x_n) = 0 \]

where \( P \) is a polynomial of \( n \) variables with \underline{integer coefficients}.

Let

\[ X_P := \{v \in \mathbb{C}^n : P(v) = 0\}; \]

\[ X_P(K) := \{v \in K^n : P(v) = 0\}. \]

Question: \( X_P(\mathbb{Q}) = ? \)

Hilbert 10-th Problem is unsolvable.
Examples

• $P := ax + by - c$ where $b \neq 0$.
  \[
  X_P(\mathbb{Q}) = \{(t, (c - at)/b) \in \mathbb{Q}^2 : t \in \mathbb{Q}\}.
  \]

• $P := x^2 + y^2 - 1$.
  \[
  X_P(\mathbb{Q}) = \left\{\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) : t \in \mathbb{Q}\right\}.
  \]
Examples of Quadratic Equations

- Given $P = ax^2 + by^2 + cxy + dx + ey + f = 0$, can we determine whether

  $\# X_P(\mathbb{Q}) = 0$?

- Quadratic Form: $Q := ax^2 + bxy + cy^2$. Let $e \in \mathbb{Z}$ be nonzero, and $P := Q(x, y) - e$. Then $\# X_P(\mathbb{Q}) =$?

Local-Global Principle for $\mathbb{Z}$ (Hasse Principle)

- $Q(x, y) \equiv e \mod p$ for some prime $p$ has no mod-$p$ solutions

  $\implies Q(x, y) = e$ has no $\mathbb{Z}$-solutions.

  e.g., $x^2 - 333y^2 = 335$ has no $\mathbb{Z}$-solutions.

- Question: $Q(x, y) \equiv e \mod p$ for all primes $p$ has mod-$p$ solutions

  $\implies Q(x, y) = e$ has a $\mathbb{Z}$-solution?
Local-Global Principle fpr $\mathbb{Q}$ (Hasse Principle)

- $Q(x, y) \equiv e \mod p$ for all primes $p$ has mod-$p$ solutions
  $\implies Q(x, y) = e$ has a $\mathbb{Z}$-solution?

Considering $\mathbb{Z}$-solutions of $P(x, y) = 0$ under mod-$p$ defines the reduction-at-$p$ map

$$X_P(\mathbb{Z}) \longrightarrow X_P(\mathbb{F}_p).$$

- Analogue of the reduction-at-$p$ for $\mathbb{Q}$-solution: There is a field extension $\mathbb{Q}_p$ of $\mathbb{Q}$, called the $p$-adic field such that

$$X_P(\mathbb{Q}) \longrightarrow X_P(\mathbb{Q}_p).$$

**Thm.** Let $P := Q(x, y) - e$ and $Q$ be a regular quad. form. If $\# X_P(\mathbb{Q}_p) \neq 0$ for all primes $p$, and $\# X_P(\mathbb{R}) \neq 0$, then

$$\# X_P(\mathbb{Q}) \neq 0.$$

The local-to-global principle worked for quadratic forms.
Cubic Equations

\[ P := y^2 - (x^3 + ax + b) \text{ s.t. } x^3 + ax + b \text{ has no multiple roots.} \]

\[ \exists \ P \text{'s with} \]

\[ \# X_P(\mathbb{Q}) = 0, \ 0 < \# X_P(\mathbb{Q}) < \infty, \ \# X_P(\mathbb{Q}) = \infty. \]

“Any structure” on \( X_P(\mathbb{Q}) \)? e.g., \( \mathbb{Q} \rightarrow X_P(\mathbb{Q}) \)?

**Fact:** There is no (non-constant) alg. map \( \mathbb{Q} \rightarrow X_P(\mathbb{Q}) \) for all such \( P \).

**Fact:** Let \( \infty \) be an auxiliary point. For a field ext. \( F \) of \( \mathbb{Q} \), let

\[ E(F) := X_P(F) \cup \{\infty\}. \]

Then there is a group law on \( E(\mathbb{C}) \) with indentity \( \infty \) given by \( \mathbb{Q} \)-rational functions.

\( E(\mathbb{C}) \) forms an **abelian group**.

\( E := E(\mathbb{C}) \) is called an **elliptic curve**. Under this group law,

\[ E(\mathbb{Q}) \text{ forms a subgroup of } E(\mathbb{C}), \]

called the **Mordell-Weil group of** \( E \).
The group law on $E(\mathbb{R})$

$$y^2 = x^3 + ax + b$$
Elliptic Curves

Mordell-Weil Thm.
The Mordell-Weil group $E(\mathbb{Q})$ is a finitely generated abelian group, i.e.,

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times E(\mathbb{Q})_{\text{Tor}}$$

(where $r$ is invariant).

The integer $r$ is denoted by rank $E(\mathbb{Q})$.

Open Questions

- Find an algorithm that computes rank $E(\mathbb{Q})$.
- Find generators of $E(\mathbb{Q})$.
- Prove $\exists \infty$ many $E$ with arbitrarily large rank $E(\mathbb{Q})$.

Record: Martin-McMillen found $E$ and proved rank $E(\mathbb{Q}) \geq 24$. 
Local-Global Principle

"Reduction at $p$"

$$E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}_p).$$

For all elliptic curves $E$ and for any prime $p$,

$$\# E(\mathbb{Q}_p) = \infty.$$ 

But there are elliptic curves $E$ s.t. $E(\mathbb{Q}) = \{\infty\}$.

**Obstruction** to the local-global principle:

existence of a curve $C$ s.t.

1. $C(\mathbb{C}) \cong E(\mathbb{C})$;
2. $C(\mathbb{R}) \cong E(\mathbb{R})$;
3. $C(\mathbb{Q}_p) \cong E(\mathbb{Q}_p)$ for all primes $p$;
4. $C(\mathbb{Q}) \not\cong E(\mathbb{Q})$.

The collection $\{C\}$ has a cohomological interpretation, which gives rise to a group structure of

$$\mathrm{III}(E) := \{[C] : (1),(2),(3) \text{ hold}\}.$$ 

**Conj:** For all elliptic curves $E$,

$$\# \mathrm{III}(E) < \infty.$$ 

$E(\mathbb{Q})$ and $\mathrm{III}(E)$

are two fundamental groups attached to $E$. 
Birch and Swinnerton-Dyer Conj.

Award: $2^6 \cdot 5^6$

**BSD:** \( L(E, s) := \text{analytic function on a domain of } \mathbb{C} \)
made out of \( \# \tilde{E}(\mathbb{F}_p), \forall p \). Then,

1. \( L(E, s) \) analytically continued to \( \mathbb{C} \)
   (proved by Wiles et al);

2. \( L(E, s) = \gamma \cdot \# \text{III}(E) \cdot (s - 1)^{\text{rank} E(\mathbb{Q})} + \cdots \)
   where \( \gamma \) is a computable real number \( \neq 0 \).
   In particular, \( \# \text{III}(E) < \infty \).

BSD implies: \( L(E, 1) \neq 0 \implies \text{rank} E(\mathbb{Q}) = 0 \)
(proved by Kolyvagin + Gross-Zagier + Wiles).
Quadratic Twists of Elliptic Curves

Let $E$ be given by $y^2 = x^3 + ax + b$.

A quadratic twist of $E$ is an elliptic curve given by

$$Dy^2 = x^3 + ax + b$$

where $D \in \mathbb{Q}^*$. We denote it by $E_D$.

Let $K := \mathbb{Q}(\sqrt{D})$ be a quadratic extension. Then,

$$E(K) \cong E_D(K), \text{ not necc. } E(\mathbb{Q}) \cong E_D(\mathbb{Q}).$$

- $T(X) := \text{integers } D \text{ s.t. } |D| < X \text{ and } D \text{ is square-free.}$

Natural Question: How is rank $E_D(\mathbb{Q})$ distributed as a function of $D \in \mathbb{Z}$?

- Given a non-negative integer $n$,

$$\# \{D \in T(X) : \text{rank } E_D(\mathbb{Q}) \leq n\} =?$$

- $\limsup_D \text{rank } E_D(\mathbb{Q}) = \infty$?

In connection with BSD:

$$L(E, s) = \gamma \cdot \# \text{III}(E) \cdot (s - 1)^{\text{rank } E(\mathbb{Q})} + \cdots.$$ 

BSD + Func. eq. on $L(E_D, s)$

$\implies$ Uniform distr. of parities of rank $E_D(\mathbb{Q})$.

- Are the parities of rank $E_D(\mathbb{Q})$ uniformly distributed?
Quadratic Twists of Elliptic Curves

Uniform Distr.:

- Goldfeld, '79: Assuming BSD, (Modularity), and RH,

\[
\limsup_{X \to \infty} \frac{\sum_{D \in T(X)} \text{rank} E_D(\mathbb{Q})}{\# T(X)} \leq 3.25.
\]

(reduced to 3/2 by Heath-Brown, (Duke Journal,'04))

Goldfeld’s conjecture: This average must be 1/2. An (very weak) evidence of BSD.

- Heath-Brown (Invent. '94): Let \( E \) be \( y^2 = x^3 - x \).
  The lim sup of the average over odd sq.fr. \( D \) is \( \leq 1.26 \)

- C. (J. Number Thoery): Let \( E \) be \( y^2 = x^3 - A \) where \( A \equiv 1, 25 \mod 36 \), and sq. fr.
  The lim sup of the average over sq.fr. \( D \equiv 1 \mod 12A \) is \( \leq 1 \) if \( A > 0 \), and \( \leq 4/3 \) if \( A < 0 \).

Heath-Brown’s average:

Average of 2-Selmer groups of \( E_D \).

\[
\text{Sel}^{(2)}(E_D) \cong E_D(\mathbb{Q})/2E_D(\mathbb{Q}) \oplus \text{III}(E_D)[2]
\]
Quadratic Twists of Elliptic Curves

Natural Question:

Given a non-negative integer \( n \),

\[
R^n_E(X) := \# \{ D \in T(X) : \text{rank } E_D(\mathbb{Q}) \leq n \} = ?
\]

- Ono-Skinner (Invent. '98): \( R^0_E(X) \gg X/(\log X) \) for all \( E/\mathbb{Q} \).

- Ono (Crelle's J. '01): If \( x^3 + ax + b \) is irreducible/\( \mathbb{Q} \), then \( \exists 0 < \epsilon < 1 \text{ s.t. } R^0_E(X) \gg X/(\log X)^\epsilon \).

- Heath-Brown, Yu, James, Ono, and Wong: Examples of \( E/\mathbb{Q} \) s.t. \( R^0_E(X) \gg X \).

- C. (JNT): Let \( E \) be given by \( y^2 = x^3 - A \) where \( A \) pos.sq.fr., \( \equiv 1, 25 \mod 36 \). For \( k \geq 0 \),

\[
\frac{R^{2k}_E(X)^+}{\# T(X)^+} \geq \frac{1}{8} \cdot \frac{3^{k+1} - 2}{3^{k+1} - 1} \cdot \prod_{p | A} \frac{p}{(p - 1)(p + 1)}.
\]
Curves of higher degree

A superelliptic curve is given by $y^\ell = f(x)$ where $f(x)$ is a polynomial over $\mathbb{Z}$ with distinct roots. When $\ell = 2$, it is called a hyperelliptic curve.

Question: Let $P := y^2 - f(x)$, $\deg f > 3$. Then

$$X_P(\mathbb{Q}) =?$$
$$\mathbb{Q} \rightarrow X_P(\mathbb{Q})?$$

Is there a group law on $X_P$?

Faltings’ Theorem implies that

$$\deg f > 3 \implies \# X_P(\mathbb{Q}) < \infty.$$
Curves of higher degree

\[ P := y^2 - f(x), \ \text{deg} \ f > 3 \]
\[ X_P(\mathbb{Q}) =? \quad \text{Is there a group law on } X_P? \]

An abelian variety \( A \) is a higher dimensional analogue of an elliptic curve, i.e.,

\[ A \text{ is a compactification of the } \mathbb{C} \text{-solutions of a system of equations with dim } A \geq 1 \text{ as a compact complex manifold, and there is a group law on } A. \]

**Mordell-Weil Theorem:**

\[ A(\mathbb{Q}) \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times A(\mathbb{Q})_{\text{Tor}}. \]

\[ \text{rank } A(\mathbb{Q}) := r. \]

**Thm.** Given \( P \), there is an abelian variety \( J \) associated with \( X_P \) such that

\[ X_P \hookrightarrow J; \]
\[ X_P(\mathbb{Q}) \hookrightarrow J(\mathbb{Q}); \]

much more.

\( J \) is the Jacobian variety of \( X_P \).

**Mazur’s question:**

Can \( \# X_P(\mathbb{Q}) \) be bounded in terms of rank \( J(\mathbb{Q})? \)
Twists of Hyperelliptic Curves

Let $P := y^2 - f(x)$ where $\deg(f) > 3$ is odd.

$$P_D := D y^2 - f(x).$$

$X := X_P, \ X_D := X_{P_D}.$

i.e., $X_D$ is a quadratic twists of $X$.

Let $J$ and $J_D$ be the Jacobian varieties of $X$ and $X_D$, resp. $X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})$, and $X_D(\mathbb{Q}) \hookrightarrow J_D(\mathbb{Q})$.

Question: $T(X) := \{ \text{ sq.fr. } D \text{ s.t. } |D| < X \}.$

- Given $N$,

$$\{D \in T(X) : \# X_D(\mathbb{Q}) \leq N\} = ?$$

- Given $N$,

$$\{D \in T(X) : \text{rank } J_D(\mathbb{Q}) \leq N\} = ?$$

Silverman (LBM,'93) There is a constant $\gamma$ s.t.

$$\# X_D(\mathbb{Q}) < \gamma \cdot 7^{\text{rank } J_D(\mathbb{Q})}.$$
Twists of Hyperelliptic Curves

Assume deg$(f) = p$ is prime.

**Thm.** Suppose that $f(x)$ is irreducible over $\mathbb{Q}$. Let $D_0$ be a positive integer, and

$$N := \dim \mathbb{F}_2 J_{D_0}(\mathbb{Q})/2J_{D_0}(\mathbb{Q}) \oplus III(J_{D_0})[2].$$

Then there is a positive constant $\epsilon$ s.t.

$$\# \{D \in T(X)^+ : \text{rank} \ J_D(\mathbb{Q}) \leq N\} \gg \frac{X}{(\log X)^\epsilon}.$$ 

Hence,

$$\# \{D \in T(X)^+ : \# X_D(\mathbb{Q}) \leq \gamma 7^N\} \gg \frac{X}{(\log X)^\epsilon}.$$ 

**Thm.** Suppose that $f(x)$ is irreducible over $\mathbb{Q}$, and that $\exists \ D_0$, a positive integer s.t.

$$N := \dim \mathbb{F}_2 J_{D_0}(\mathbb{Q})/2J_{D_0}(\mathbb{Q}) \oplus III(J_{D})[2] < (p - 1)/2.$$ 

Then, there is a positive constant $\epsilon$ s.t.

$$\# \{D \in T(X)^+ : \# X_D(\mathbb{Q}) \leq 2N\} \gg \frac{X}{(\log X)^\epsilon}.$$