Elliptic Curves: The State of the Art
What Number Theorists Want to Know

Alice Silverberg
ECC 2001
October 31, 2001
Outline:

• The Conjecture of Birch and Swinnerton-Dyer
• Ranks
• Integral Points
• Generalizations to Abelian Varieties
• Conclusions, Summary, References
Mordell (1922): “Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational [points on elliptic curves].”

We still do not know an algorithm that is guaranteed to find the rational points on elliptic curves.
Elliptic Curves over the Rationals

\[ E(\mathbb{Q}) \cong \text{finite group} \times \mathbb{Z}^r \]
\[ \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r \]

\( r = \text{rank} \)

Poincaré introduced ranks in 1901, and said they’re clearly an interesting invariant to study.

Alice Silverberg, ECC 2001, October 31, 2001
Example: \( y^2 = x^3 - x \)

\[
E(\mathbb{Q}) = \{(0, 0), (1, 0), (-1, 0), O\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}
\]
Hasse-Weil \( L \)-function

Take a minimal Weierstrass equation for \( E \) (coefficients in \( \mathbb{Z} \), \( |\Delta(E)| \) minimal).

Let \( a_p = p + 1 - \#E(\mathbb{F}_p) \).

Let \( L(E, s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - \frac{a_p}{p^s}} + \prod_{p \mid \Delta(E)} \frac{1}{1 - \frac{a_p}{p^{2s}}} \).

The product converges absolutely for \( \text{Re}(s) > \frac{3}{2} \).
**Hasse-Weil $L$-function**

**Theorem** (Wiles, Taylor, Conrad, Diamond, Breuil). $L(E, s)$ has an analytic continuation to the complex plane, and a functional equation relating $L(E, s)$ and $L(E, 2 - s)$. 
Hasse-Weil $L$-function

$$L(E, s) = b_r (s - 1)^r + b_{r+1} (s - 1)^{r+1} + \ldots$$

$$b_i \in \mathbb{R}, \ b_r \neq 0, \ r \in \mathbb{Z}_{\geq 0}.$$

This $r$ is called the analytic rank of $E$ (over $\mathbb{Q}$).
Conjecture. \( \text{rank} = \text{analytic rank} \)
Conjecture BSD Part I \iff

**Parity Conjecture.** The rank and the analytic rank have the same parity.
Congruent Number Problem

Conjecture BSD Part I implies an algorithm for solving the classical:

**Congruent Number Problem.** Which positive integers are the areas of right triangles with rational sides?
What’s known about BSD Part I?

**Theorem** (Kolyvagin, Gross & Zagier, ...).

(1) *If the analytic rank is 0, then the rank is 0.*

(2) *If the analytic rank is 1, then the rank is 1.*
Conjecture.

\[ b_r = \frac{\Omega R \# \# \prod p | \Delta(E) c_p}{\#(E(\mathbb{Q})_{tors})^2} \]

Recall:

\[ E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r \]

\[ L(E, s) = b_r (s - 1)^r + b_{r+1} (s - 1)^{r+1} + \ldots \]
The Period

$$\Omega = \int_{E(\mathbb{R})} \frac{dx}{|2y + a_1x + a_3|} \in \mathbb{R}$$

where

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$\Omega R \# \text{III} \prod c_p$$

$$b_r = \frac{\# p | \Delta(E)}{\#(E(\mathbb{Q})_{tors})^2}$$
The Fudge Factors

$c_p$ are small positive integers that measure the bad reduction of $E$ at $p$.

$\Omega R^\#III \prod c_p$

$b_r = \frac{\prod_{p|\Delta(E)} p}{\#(E(\mathbb{Q})_{tors})^2}$
The Regulator

$R$ measures the complexity of a minimal set of generators for $E(\mathbb{Q})$. 

$$b_r = \frac{\Omega R \# \mathfrak{M} \prod_{p|\Delta(E)} c_p}{\#(E(\mathbb{Q})_{tors})^2}$$
The Tate-Shafarevich Group

measures the failure of the Hasse Principle.

**Hasse Principle** (Local-to-Global Principle).

\[ \exists \text{ points locally (over } \mathbb{R} \text{ and over all } \mathbb{Q}_p) \implies \exists \text{ points globally (over } \mathbb{Q}). \]

\[ b_r = \frac{\Omega R \# \prod_{p|\Delta(E)} c_p}{\#(E(\mathbb{Q})_{\text{tors}})^2} \]
The Tate-Shafarevich Group

**Conjecture.** III is finite.

**Theorem (Cassels).** If III is finite, then \#III is a square.
The Tate-Shafarevich Group

**Theorem** (Rubin). If the analytic rank is 0, and \( E \) has CM, then:

(a) \( \Sha \) is finite,

(b) BSD Part II is true up to powers of 2 and 3.

**Theorem** (Kolyvagin, . . . ). If the analytic rank is 0 or 1, then \( \Sha \) is finite.
BSD Part II: Example

\[ y^2 = x^3 - x \quad \Delta(E) = 2^6 \]

\[ b_0 = L(E, 1) \approx 0.655514 \ldots \neq 0 \]
so analytic rank is 0.

Fermat: \( E(\mathbb{Q}) = \{ (0, 0), (1, 0), (-1, 0), O \} \)
\[ y^2 = x^3 - x \quad \Delta(E) = 2^6 \]

\[ b_0 = L(E, 1) \approx 0.655514 \ldots \neq 0 \]

so analytic rank is 0.

Fermat: \( E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong E(\mathbb{Q})_{\text{tors}} \) so rank = 0 and \( \#E(\mathbb{Q})_{\text{tors}} = 4 \).

\( R = 1, \quad \Omega \approx 5.2441 \ldots, \quad c_2 = 2 \)

Rubin proved \( III = 0 \).

B\&SD proved \( b_0 = \frac{\Omega}{8} \).

BSD Parts I and II are true.
BSD Part II: Example

\[ y^2 = x^3 - 25x \quad \Delta(E) = 2^6 \cdot 5^6 \]

\[ b_0 = L(E, 1) = 0, \quad b_1 = L'(E, 1) \approx 2.227 \ldots \neq 0, \]
so analytic rank is 1.

A descent shows \( E(\mathbb{Q}) \) is generated by \( P = (-4, 6) \) and points of order 2 so rank is 1, \( \# E(\mathbb{Q})_{\text{tors}} = 4 \).

\( \Omega \approx 2.3452 \ldots, \quad R \approx 1.89948 \ldots, \quad c_2 = 2, \quad c_5 = 4 \)
Kolyvagin proved \( \Sha = 0 \).

Gross & Zagier proved \( b_1 = \frac{\Omega R}{2} \).

BSD Parts I and II are true.

Alice Silverberg, ECC 2001, October 31, 2001
Ranks

Recall:

\[ E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r \]

\[ r = \text{rank} \]

There is no known algorithm guaranteed to determine the rank.

It is not known which integers can occur as ranks.

It is not known if ranks are unbounded.
## Rank Records

<table>
<thead>
<tr>
<th>Rank ≥</th>
<th>Year</th>
<th>Discoverers</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1945</td>
<td>Billing</td>
</tr>
<tr>
<td>4</td>
<td>1945</td>
<td>Wiman</td>
</tr>
<tr>
<td>6</td>
<td>1974</td>
<td>Penney &amp; Pomerance</td>
</tr>
<tr>
<td>7</td>
<td>1975</td>
<td>Penney &amp; Pomerance</td>
</tr>
<tr>
<td>8</td>
<td>1977</td>
<td>Grunewald &amp; Zimmert</td>
</tr>
<tr>
<td>9</td>
<td>1977</td>
<td>Brumer &amp; Kramer</td>
</tr>
<tr>
<td>12</td>
<td>1982</td>
<td>Mestre</td>
</tr>
<tr>
<td>14</td>
<td>1986</td>
<td>Mestre</td>
</tr>
<tr>
<td>15</td>
<td>1992</td>
<td>Mestre</td>
</tr>
<tr>
<td>17</td>
<td>1992</td>
<td>Nagao</td>
</tr>
<tr>
<td>19</td>
<td>1992</td>
<td>Fermigier</td>
</tr>
<tr>
<td>20</td>
<td>1993</td>
<td>Nagao</td>
</tr>
<tr>
<td>21</td>
<td>1994</td>
<td>Nagao-Kouya</td>
</tr>
<tr>
<td>22</td>
<td>1997</td>
<td>Fermigier</td>
</tr>
<tr>
<td>23</td>
<td>1998</td>
<td>Martin-McMillen</td>
</tr>
<tr>
<td>24</td>
<td>2000</td>
<td>Martin-McMillen</td>
</tr>
</tbody>
</table>
Rank Records

Martin and McMillen’s curve with rank at least 24:

\[ y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x + 504224992484910670010801799168082726759443756222911415116. \]
Quadratic Twists

\[ E : y^2 = f(x) \]

\[ E_d : dy^2 = f(x) \]  quadratic twist by \( d \)

**Honda’s Conjecture.** Ranks are bounded in families of quadratic twists.
Ranks in the family $dy^2 = x^3 - x$

<table>
<thead>
<tr>
<th>rank</th>
<th>$d$</th>
<th>$d$ factored</th>
<th>person</th>
<th>year</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>Fermat</td>
<td>~1640</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>5</td>
<td>Billing</td>
<td>1937</td>
</tr>
<tr>
<td>2</td>
<td>34</td>
<td>2 · 17</td>
<td>Wiman</td>
<td>1945</td>
</tr>
<tr>
<td>3</td>
<td>1254</td>
<td>2 · 3 · 11 · 19</td>
<td>Wiman</td>
<td>1945</td>
</tr>
<tr>
<td>4</td>
<td>29274</td>
<td>2 · 3 · 7 · 17 · 41</td>
<td>Wiman</td>
<td>1945</td>
</tr>
<tr>
<td>5</td>
<td>205015206</td>
<td>2 · 3 · 11 · 17 · 19 · 59 · 163</td>
<td>Rogers</td>
<td>2000</td>
</tr>
<tr>
<td>6</td>
<td>61471349610</td>
<td>2 · 3 · 5 · 11 · 19 · 41 · 43 · 67 · 83</td>
<td>Rogers</td>
<td>2000</td>
</tr>
</tbody>
</table>

Wiman said that if $d$ with rank greater than 4 exist in this family, they would be almost insurmountably difficult to find.

Rogers used a clever computer search, using ideas of Silverberg and Rubin.
A Density Conjecture

Fix $E$.

Parity Conjecture $\Rightarrow$

A Density Conjecture.

(i) $\frac{1}{2}$ the $E_d$’s have even rank;

(ii) $\frac{1}{2}$ the $E_d$’s have odd rank;

(iii) average rank of the $E_d$’s is $\geq \frac{1}{2}$.
Goldfeld Conjecture

Conjecture (Goldfeld).

Average rank of the $E_d$'s is $\frac{1}{2}$.

Goldfeld + Parity Conjectures $\implies$

Density Conjecture.

(i) $\frac{1}{2}$ the $E_d$'s have rank 0;

(ii) $\frac{1}{2}$ the $E_d$'s have rank 1;

(iii) density 0 have rank $\geq 2$. 
Density

\[ N_{\ast}(X) := \#\{\text{squarefree } d \in \mathbb{Z} : |d| \leq X, \text{rank of } E_d \text{ is } \ast\} \]

\[ N_{\geq 0}(X) \sim \frac{2}{\zeta(2)}X = \frac{12}{\pi^2}X \]

Parity Conjecture \[\implies\]

\[ N_{\text{odd}}(X) \sim N_{\text{even}}(X) \sim \frac{1}{2}N_{\geq 0}(X) \]

Goldfeld + Parity Conjectures \[\implies\]

\[ N_0(X) \sim N_1(X) \sim \frac{1}{2}N_{\geq 0}(X), \quad N_{\geq 2}(X) = o(X) \]
Density

**Theorem** (Gouvêa & Mazur, Stewart & Top, Rubin & Silverberg).

(i) $N_{\geq 1}(X) \gg X^{1/2}$.

(ii) *For certain* $E$, $N_{\geq 2}(X) \gg X^{1/3}$.

(iii) *For a smaller class of* $E$, $N_{\geq 3}(X) \gg X^{1/6}$.
Density

**Theorem** (Gouvêa & Mazur, Stewart & Top, Rubin & Silverberg).

*Parity Conjecture* \(\implies\)

(iv) \(N_{\geq 2}(X) \gg X^{1/2}\).

(v) *For certain* \(E\), \(N_{\geq 3}(X) \gg X^{1/3}\).

(vi) *For a smaller class of* \(E\), \(N_{\geq 4}(X) \gg X^{1/6}\).
Some Connections with ECC

• Silverman’s Xedni Calculus attack on ECC is based on work of Mestre on finding ECs with high rank. (See Jacobson-Koblitz-Silverman-Stein-Teske for an analysis of the attack.)

• Huang et al. (ANTS IV) have shown a relationship between the (conjectured) unboundedness of ranks of ECs and attacks on ECC.
Integral Points

**Conjecture** (Lang). There is an absolute constant $C$ such that if $E$ is given by a minimal (affine) Weierstrass equation, then the number of integral points is at most $C^{1 + \text{rank of } E}$.

**Theorem** (Silverman). True if $E$ has everywhere potentially good reduction (i.e., $j(E) \in \mathbb{Z}$).
Abelian Varieties

Let $A$ be an abelian variety over a number field $F$.

$$A(F) \cong A(F)_{\text{tors}} \times \mathbb{Z}^r$$

There are Birch and Swinnerton-Dyer Conjectures for abelian varieties.

Not much is known about ranks of abelian varieties.
Torsion Conjecture for Abelian Varieties

**Torsion Conjecture.** \( \#A(F)_{\text{tors}} \) is bounded above by a constant depending only on the degree of \( F \) and the dimension \( d \) of \( A \).

Proved for \( d = 1 \) and \( F = \mathbb{Q} \) by Mazur.

Proved for \( d = 1 \) by Merel.

Open for abelian varieties of dimension \( > 1 \).
Abelian Varieties and Modularity

Modularity Conjecture. Every elliptic curve over $\mathbb{Q}$ is modular.

(was proved by Wiles, Taylor, Conrad, Diamond, and Breuil)

There’s a Modularity Conjecture for (certain) abelian varieties.
Open Questions: BSD

BSD I: rank = analytic rank

- Parity Conjecture: rank and analytic rank have same parity

- Congruent Number Problem

BSD II

- Finiteness of \( \mathbb{I} \)
Open Questions: Ranks

- Which integers can occur as ranks?
- Unboundedness of ranks

In families of quadratic twists:

- Unboundedness of ranks
- Goldfeld’s Conjecture: average rank $= \frac{1}{2}$
- Density Conjecture: $\frac{1}{2}$ the ranks are 0, $\frac{1}{2}$ are 1

- Find behavior of $N_r$'s (# of d with rank r)

Alice Silverberg, ECC 2001, October 31, 2001
Open Questions: Integral Points

- Lang’s Conjecture: bound the number of integral points in terms of the rank
Open Questions: Abelian Varieties

- BSD
- Ranks
- Torsion
- Modularity
Reference

A. Silverberg, *Open questions in arithmetic algebraic geometry*, in Arithmetic Algebraic Geometry (Park City, UT, 1999), IAS/Park City Mathematics Series 9, AMS, Providence, RI (2001).