Elliptic Curves: A Survey

SUMSRI Number Theory Seminar

Samuel Ivy
Morehouse College

Brett Jefferson
Morgan State University

Michele Josey
North Carolina Central University

July 17, 2008
Outline

1 Motivating Questions

2 Basic Properties
   - Elliptic Curves
   - Chord-Tangent Method
   - Group Law

3 Mordell-Weil Group
   - Poincaré’s Conjecture / Mordell’s Theorem
   - Torsion Subgroup
   - Mordell-Weil Rank

4 Conclusion
Rational Triangles

Can you find a right triangle with rational sides having area $A = 6$?
Rational Triangles

Consider rational numbers $a$, $b$, and $c$ satisfying

$$a^2 + b^2 = c^2 \quad \text{and} \quad \frac{1}{2} a b = 6.$$

Recall the $(a, b, c) = (3, 4, 5)$ triangle!
Cubic Equations

Are there more rational solutions \((a, b, c)\) to
\[
\begin{align*}
a^2 + b^2 &= c^2 \\
\frac{1}{2} a b &= 6
\end{align*}
\]

**Proposition**

Let \(X\) and \(Y\) be rational numbers, and denote the rational numbers
\[
\begin{align*}
a &= \frac{X^2 - 36}{Y}, \\
b &= \frac{12X}{Y}, \\
c &= \frac{X^2 + 36}{Y}.
\end{align*}
\]

Then
\[
\begin{align*}
a^2 + b^2 &= c^2 \\
\frac{1}{2} a b &= 6
\end{align*}
\]

if and only if
\[
Y^2 = X^3 - 36X.
\]

**Example:** \((X, Y) = (12, 36)\) corresponds to \((a, b, c) = (3, 4, 5)\).

Can we find infinitely many rational solutions \((a, b, c)\)?
What types of properties does this cubic equation have?
**What is an Elliptic Curve?**

**Definition**

Let $A$ and $B$ be rational numbers such that $4A^3 + 27B^2 \neq 0$. An elliptic curve $E$ is the set of all $(X, Y)$ satisfying the equation

$$Y^2 = X^3 + AX + B.$$  

We will also include the “point at infinity” $O$.

**Example:** $Y^2 = X^3 - 36X$ is an elliptic curve.

**Non-Example:** $Y^2 = X^3 - 3X + 2$ is not an elliptic curve.
Fix a rational number \( k \) different from \(-1, 0, 1\). Then the quartic curve

\[ E : \quad y^2 = (1 - x^2)(1 - k^2 x^2) \]

is an elliptic curve.

**Proof:** Make the substitutions

\[
\begin{align*}
  x &= \frac{X - 3(5 - k^2)}{X - 3(5k^2 - 1)} \\
  y &= \frac{6(k^2 - 1)Y}{(X - 3(5k^2 - 1))^2}
\end{align*}
\]

\[
\begin{align*}
  X &= \frac{3(5k^2 - 1)x - 3(5 - k^2)}{x - 1} \\
  Y &= \frac{54(k^2 - 1)y}{(x - 1)^2}
\end{align*}
\]

Then \( E \) is birationally equivalent to the curve

\[ Y^2 = X^3 + AX + B \quad \text{where} \quad \begin{cases} 
  A = -27(k^4 + 14k^2 + 1) \\
  B = -54(k^6 - 33k^4 - 33k^2 + 1)
\end{cases} \]
Fix an elliptic curve $E$. Given two rational points, we explain how to construct more.

1. Start with two rational points $P$ and $Q$.
2. Draw a line through $P$ and $Q$.
3. The intersection, denoted by $P \ast Q$, is another rational point on $E$. 

Chord-Tangent Method
Example: \( Y^2 = X^3 - 36X \)

Consider the two rational points

\[
P = (6, 0) \quad \text{and} \quad Q = (12, 36).
\]

\[
P \ast Q = (18, 72)
\]
Example: \( Y^2 = X^3 - 36X \)

Consider the two rational points

\[
P = (6, 0) \quad \text{and} \quad Q = (12, 36).
\]
Example: $Y^2 = X^3 - 36X$

Consider the two rational points

\[ P = (6, 0) \quad \text{and} \quad Q = (12, 36). \]

\[ Q \star Q = \left( \frac{25}{4}, \frac{35}{8} \right) \]
Definition

Let $E$ be an elliptic curve, and denote $E(\mathbb{Q})$ as the set of rational points on $E$. Define the operation $\oplus$ as

$$P \oplus Q = (P \ast Q) \ast \mathcal{O}.$$
**Example:** \( Y^2 = X^3 - 36X \)

Consider the two rational points

\[ P = (6, 0) \quad \text{and} \quad Q = (12, 36). \]

\[ P \oplus Q = (18, -72) \]
Example: $Y^2 = X^3 - 36X$

Consider the two rational points

$P = (6, 0)$ and $Q = (12, 36)$.

$P \oplus P = O$
Example: \( Y^2 = X^3 - 36X \)

Consider the two rational points

\[
P = (6, 0) \quad \text{and} \quad Q = (12, 36).
\]

\[
Q \oplus Q = \left(\frac{25}{4}, -\frac{35}{8}\right)
\]
Poincaré’s Theorem

Theorem (Henri Poincaré, 1901)

$E(\mathbb{Q})$ is an abelian group under $\oplus$.

Recall that to be an abelian group, the following axioms must be satisfied:

- Closure: If $P, Q \in E(\mathbb{Q})$ then $P \oplus Q \in E(\mathbb{Q})$.
- Associativity: $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.
- Commutativity: $P \oplus Q = Q \oplus P$.
- Identity: $P \oplus \mathcal{O} = P$ for all $P$.
- Inverses: $[-1]P = P * \mathcal{O}$ satisfies $P \oplus [-1]P = \mathcal{O}$.
What types of properties does this abelian group have?
Conjecture (Henri Poincaré, 1901)

Let $E$ be an elliptic curve. Then $E(\mathbb{Q})$ is finitely generated.

Recall that an abelian group $G$ is said to be finitely generated if there exists a finite generating set

$$\{a_1, a_2, \ldots, a_n\}$$

such that, for each given $g \in G$, there are integers $m_1, m_2, \ldots, m_n$ such that

$$g = [m_1]a_1 \circ [m_2]a_2 \circ \cdots \circ [m_n]a_n.$$

**Example:** $G = \mathbb{Z}$ is a finitely generated abelian group because all integers are generated by $a_1 = 1$. 
Mordell’s Theorem

Theorem (Louis Mordell, 1922)

Let $E$ be an elliptic curve. Then $E(\mathbb{Q})$ is finitely generated.

That is, there exists a finite group $E(\mathbb{Q})_{\text{tors}}$ and a nonnegative integer $r$ such that

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

- The set $E(\mathbb{Q})$ is called the Mordell-Weil group of $E$.
- The finite set $E(\mathbb{Q})_{\text{tors}}$ is called the torsion subgroup of $E$. It contains all of the points of finite order, i.e., those $P \in E(\mathbb{Q})$ such that

$$[m]P = \mathcal{O}$$

for some positive integer $m$.
- The nonnegative integer $r$ is called the Mordell-Weil rank of $E$. 

Consider the three rational points
\[ P_1 = (0, 0), \quad P_2 = (6, 0), \quad \text{and} \quad P_3 = (12, 36). \]

\[ [2]P_1 = [2]P_2 = \mathcal{O}, \] i.e., both \( P_1 \) and \( P_2 \) have order 2. They are torsion.

\[ E(\mathbb{Q})_{\text{tors}} = \langle P_1, P_2 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \]
Example: \( Y^2 = X^3 - 36X \)

Consider the three rational points

\[
P_1 = (0, 0), \quad P_2 = (6, 0), \quad \text{and} \quad P_3 = (12, 36).
\]

\[ [2]P_3 = \left(\frac{25}{4}, -\frac{35}{8}\right) \text{ and } [3]P_3 = \left(\frac{16428}{529}, -\frac{2065932}{12167}\right). \]

\[ E(\mathbb{Q}) = \langle P_1, P_2, P_3 \rangle \sim \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z} \]
Theorem (Barry Mazur, 1977)

Let $E$ is an elliptic curve, then

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}_n & \text{where } 1 \leq n \leq 10 \text{ or } n = 12; \\ \mathbb{Z}_2 \times \mathbb{Z}_{2m} & \text{where } 1 \leq m \leq 4. \end{cases}$$

Remark: $\mathbb{Z}_n$ denotes the cyclic group of order $n$.

Example: The elliptic curve $Y^2 = X^3 - 36X$ has torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ generated by $P_1 = (0, 0)$ and $P_2 = (6, 0)$.

Mordell’s Theorem states that

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r.$$ 

What can we say about the Mordell-Weil rank $r$?
Not much is known about the rank $r$...

- The highest rank ever found for all known examples of elliptic curves is $r = 28$.

Is there a constant $B$ such that $r \leq B$ for all elliptic curves $E$?

- Let $T$ be one of the fifteen groups in Mazur’s Theorem, and consider the collection of all elliptic curves $E$ with $E(\mathbb{Q})_{\text{tors}} \cong T$.

Is there a constant $B(T)$ such that $r \leq B(T)$ for all elliptic curves with $E(\mathbb{Q})_{\text{tors}} \cong T$?
## Records for Prescribed Torsion and Rank

<table>
<thead>
<tr>
<th>$E(\mathbb{Q})_{\text{tors}}$</th>
<th>Known $r \leq$</th>
<th>Author (Year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}_1$</td>
<td>28</td>
<td>Elkies (2006)</td>
</tr>
<tr>
<td>$\mathbb{Z}_2$</td>
<td>18</td>
<td>Elkies (2006)</td>
</tr>
<tr>
<td>$\mathbb{Z}_3$</td>
<td>13</td>
<td>Eroshkin (2007, 2008)</td>
</tr>
<tr>
<td>$\mathbb{Z}_4$</td>
<td>12</td>
<td>Elkies (2006)</td>
</tr>
<tr>
<td>$\mathbb{Z}_5$</td>
<td>6</td>
<td>Dujella – Lecacheux (2001)</td>
</tr>
<tr>
<td>$\mathbb{Z}_6$</td>
<td>8</td>
<td>Eroshkin (2008), Dujella – Eroshkin (2008)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elkies (2008), Dujella (2008)</td>
</tr>
<tr>
<td>$\mathbb{Z}_8$</td>
<td>6</td>
<td>Elkies (2006)</td>
</tr>
<tr>
<td>$\mathbb{Z}_9$</td>
<td>3</td>
<td>Dujella (2001), MacLeod (2004)</td>
</tr>
<tr>
<td>$\mathbb{Z}_{10}$</td>
<td>4</td>
<td>Dujella (2005), Elkies (2006)</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>14</td>
<td>Elkies (2005)</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_4$</td>
<td>8</td>
<td>Elkies (2005), Eroshkin (2008), Dujella - Eroshkin (2008)</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_6$</td>
<td>6</td>
<td>Elkies (2006)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flores - Jones - Rollick - Weigandt (2007)</td>
</tr>
</tbody>
</table>

http://web.math.hr/~duje/tors/tors.html
How does one compute $r$?

The current method uses ideas from Mordell’s proof of the Poincaré Conjecture:

- Mordell proved that the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is always finite. Note that

$$E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2\times \mathbb{Z}^r \implies \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong \mathbb{Z}_{2^{r+2}}.$$

It suffices to find a way to count the number of elements in this finite group.

- The only known method for counting the number of elements might take days – or even years – to finish.

Is there a better method of determining the rank $r$?

Determining rank is a hard problem!
How does this help answer the motivating questions?
Rational Triangles Revisited

Can we find infinitely many right triangles \((a, b, c)\) having rational sides and area \(A = 6\)?

**Proposition**

Let \(X\) and \(Y\) be rational numbers, and denote the rational numbers

\[
\begin{align*}
a &= \frac{X^2 - 36}{Y}, \\
b &= \frac{12X}{Y}, \\
c &= \frac{X^2 + 36}{Y}.
\end{align*}
\]

Then

\[
\begin{align*}
a^2 + b^2 &= c^2 \\
\frac{1}{2} ab &= 6
\end{align*}
\]

if and only if

\[
Y^2 = X^3 - 36X.
\]

**Example:** \((X, Y) = (12, 36)\) corresponds to \((a, b, c) = (3, 4, 5)\).
The elliptic curve \( E : Y^2 = X^3 - 36X \) has Mordell-Weil group
\[
E(\mathbb{Q}) = \langle P_1, P_2, P_3 \rangle \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}
\]
as generated by the rational points
\[
P_1 = (0, 0), \quad P_2 = (6, 0), \quad \text{and} \quad P_3 = (12, 36).
\]

\( P_3 \) is not a torsion element, so we find triangles for each \([m]P_3\):

\[
[1]P_3 = (12, 36) \quad \implies \quad (a, b, c) = (3, 4, 5)
\]
\[
[-2]P_3 = \left( \frac{25}{4}, \frac{35}{8} \right) \quad \implies \quad (a, b, c) = \left( \frac{49}{70}, \frac{1200}{70}, \frac{1201}{70} \right)
\]
\[
[-3]P_3 = \left( \frac{16428}{529}, \frac{2065932}{12167} \right) \quad \implies \quad (a, b, c) = \left( \frac{7216803}{1319901}, \frac{2896804}{1319901}, \frac{7776485}{1319901} \right)
\]

There are infinitely many rational right triangles with area \( A = 6 \)!
We would like to thank...

- National Security Agency (NSA)
- National Science Foundation (NSF)
- Miami University
- Edray Goins and Beth Fowler
- Dennis Davenport and Vasant Waikar
- Other SUMSRI Participants