Four-Covering Maps for Elliptic Curves

SUMSRI Number Theory Seminar

Cheryl Outing
Spelman College

Cliff Taylor
Grand Valley State University

Staci White
Shawnee State University

July 17, 2008
Outline

1 Mordell-Weil Group
   - Mordell’s Theorem
   - Mazur’s Theorem
   - Records of Mordell-Weil Ranks

2 Computing the Mordell-Weil Rank
   - “Weak” Mordell Theorem
   - Quotient Groups
   - Homogeneous Spaces

3 Covering Maps
   - 2-Covering Maps
   - 4-Covering Maps
   - Future Work
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

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

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

- 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 $E$. 

Example

Consider the elliptic curve

\[ E : \quad Y^2 = X^3 - 36X. \]
Example

Consider the elliptic curve

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

- The **Mordell-Weil group** is
  \[ E(\mathbb{Q}) = \langle P_1, P_2, P_3 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z} \]
  as generated by the rational points
  \[ P_1 = (0, 0), \quad P_2 = (6, 0), \quad \text{and} \quad P_3 = (12, 36). \]

- The **torsion subgroup** is
  \[ E(\mathbb{Q})_{\text{tors}} = \langle P_1, P_2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2. \]

- The **Mordell-Weil rank** is \( r = 1 \).
Now consider the elliptic curve

\[ E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X \\ + 234238430204114181370252185964622864112853337413958990400. \]
Now consider the elliptic curve

\[ E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X \\
+ 234238430204114181370252185964622864112853337413958990400. \]

- What is the **Mordell-Weil group** \( E(\mathbb{Q}) \)?
- What is the **torsion subgroup** \( E(\mathbb{Q})_{\text{tors}} \)?
- What is the **Mordell-Weil rank** \( r \)?
Torsion Subgroups

**Theorem (Barry Mazur, 1977)**

Let $E$ be an elliptic curve, then

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} 
Z_n & \text{where } 1 \leq n \leq 10 \text{ or } n = 12; \\
Z_2 \times Z_{2m} & \text{where } 1 \leq m \leq 4.
\end{cases}$$

**Remark:** $Z_n$ denotes the cyclic group of order $n$. 

---

**SUMSRI Number Theory Seminar**

**Four-Covering Maps for Elliptic Curves**
Torsion Subgroups

**Theorem (Barry Mazur, 1977)**

Let $E$ be an elliptic curve, then

$$E(\mathbb{Q})_{tors} \cong \begin{cases} Z_n & \text{where } 1 \leq n \leq 10 \text{ or } n = 12; \\ Z_2 \times Z_{2m} & \text{where } 1 \leq m \leq 4. \end{cases}$$

**Remark:** $Z_n$ denotes the cyclic group of order $n$.

Mordell’s Theorem states that

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

What can we say about the **Mordell-Weil rank** $r$?
Recall the elliptic curve

\[ E : \quad Y^2 + X \cdot Y = X^3 - 71813598680248384341084284771096244120 \cdot X \]
\[ + 234238430204114181370252185964622864112853337413958990400. \]
Recall the elliptic curve

\[ E : \quad Y^2 + X \cdot Y = X^3 - 71813598680248384341084284771096244120 \cdot X \\
+ 234238430204114181370252185964622864112853337413958990400. \]

We have the two rational points

\[ P_1 = (4892533141966211376, -2446266570983105688); \]
\[ P_2 = (6793371071343566640, 7739207808589340925333304680). \]

It is easy to verify that \([2]P_1 = [8]P_2 = O\). The torsion subgroup of \(E\) is

\[ E(\mathbb{Q})_{\text{tors}} = \langle P_1, P_2 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_8. \]
Recall the elliptic curve
\[ E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X 
+ 234238430204114181370252185964622864112853337413958990400. \]

We have the two rational points
\[ P_1 = (4892533141966211376, -2446266570983105688); \]
\[ P_2 = (6793371071343566640, 7739207808589340925333304680). \]

It is easy to verify that \([2]P_1 = [8]P_2 = O\). The torsion subgroup of \(E\) is
\[ E(\mathbb{Q})_{\text{tors}} = \langle P_1, P_2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_8. \]

How does one compute the Mordell-Weil rank \(r\)?
Given an elliptic curve $E$, where we know its torsion subgroup $E(\mathbb{Q})_{\text{tors}}$, what can we say about its rank $r$?
### 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>$\mathbb{Z}_8$</td>
<td>6</td>
<td>Elkies (2006)</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>
</tbody>
</table>

http://web.math.hr/~duje/tors/tors.html
In 2007, the SUMSRI Number Theory Seminar found the elliptic curve

\[ E : \quad Y^2 + X Y = X^3 - 250878395393474545316759183209311840250 X \\
+ 1479979592022167493224960512910755689574299477808903560932. \]
In 2007, the SUMSRI Number Theory Seminar found the elliptic curve

\[ E : \quad Y^2 + XY = X^3 - 250878395393474545316759183209311840250X + 1479979592022167493224960512910755689574299477808903560932. \]

The torsion subgroup is

\[ E(\mathbb{Q})_{\text{tors}} = \langle P_1, P_2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_8 \]

as generated by the rational points

\[ P_1 = (7766447618213273204, -3883223809106636602); \]
\[ P_2 = (-9594066305658249586, 54807180976759570709832434408). \]
Example

The Mordell-Weil group is

\[ E(\mathbb{Q}) = \langle P_1, P_2, P_3, P_4, P_5 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}^3 \]

as generated by the rational points

\[ P_1 = (7766447618213273204, -3883223809106636602); \]
\[ P_2 = (-9594066305658249586, 54807180976759570709832434408); \]
\[ P_3 = \left( \frac{621727883860331879066288}{80089}, -\frac{11195733275105659072676635210992274}{22665187} \right); \]
\[ P_4 = \left( -\frac{3121826350817955803774630199394084}{180524403067969}, \frac{61692108418757143009501414171937398097766847203574}{2425514506583838201953} \right); \]
\[ P_5 = \left( \frac{6278248665149487218097131208426297104}{8547022989099698401}, -\frac{144593985742523950403942776316687052257460712416405160202}{24987471290251272975616507601} \right). \]
The Mordell-Weil group is

\[ E(\mathbb{Q}) = \langle P_1, P_2, P_3, P_4, P_5 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}^3 \]

as generated by the rational points

\[
\begin{align*}
P_1 &= (7766447618213273204, -3883223809106636602); \\
P_2 &= (-9594066305658249586, 54807180976759570709832434408); \\
P_3 &= \left( \frac{621727883860331879066288}{80089}, -\frac{11195733275105659072676635210992274}{22665187} \right); \\
P_4 &= \left( -\frac{3121826350817955803774630199394084}{180524403067969}, \frac{6169210841875714300950141141171937398097766847203574}{2425514506583838201953} \right); \\
P_5 &= \left( \frac{62782486665149487218097131208426297104}{8547022989099698401}, -\frac{144593985742523950403942776316687052257460712416405160202}{24987471290251272975616507601} \right).
\]

Hence the Mordell-Weil rank is \( r = 3 \).
Given an elliptic curve $E$, how do we compute the Mordell-Weil rank $r$?
Mordell’s proof was in two parts:

1. Show the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

2. Use the generators of $E(\mathbb{Q})/2E(\mathbb{Q})$ to compute generators of $E(\mathbb{Q})$. 
Mordell’s proof was in two parts:

1. Show the quotient group \( E(\mathbb{Q})/2E(\mathbb{Q}) \) is finite.

2. Use the generators of \( E(\mathbb{Q})/2E(\mathbb{Q}) \) to compute generators of \( E(\mathbb{Q}) \).

Note that

\[
E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2m} \times \mathbb{Z}^r
\]

\[
\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong \mathbb{Z}_{2^{r+2}}.
\]
**Quotient Groups**

**Definition**

Let $G$ be an abelian group under $\circ$, and let $H$ be a subgroup.

For each $a \in G$, define a **coset** as the set

$$a \mod H = \left\{ g \in G \mid g = a \circ h \text{ for some } h \in H \right\}.$$

Define the **quotient group** $G/H$ as the collection of cosets:

$$G/H = \left\{ a \mod H \mid a \in G \right\}.$$

**Remark:** We will sometimes write $G/H$ as $\frac{G}{H}$. 
Example

Let $G = \mathbb{Q}^\times$ be the group of nonzero rational numbers under multiplication, and consider the subgroup

$$H = (\mathbb{Q}^\times)^2 = \left\{ h \in \mathbb{Q}^\times \mid h = q^2 \text{ for some } q \in \mathbb{Q}^\times \right\}.$$ 

Proposition

We may identify the quotient group

$$G/H = \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}$$

as the collection of square-free integers.
Example

Now let $G = E(\mathbb{Q})$ be the group under $\oplus$ of the set of rational points on $E$, and consider the subgroup

$$H = 2E(\mathbb{Q}) = \left\{ P \in E(\mathbb{Q}) \,\bigg|\, P = [2]Q \text{ for some } Q \in E(\mathbb{Q}) \right\}.$$

Proposition

We may identify the quotient group

$$G/H = \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \simeq \mathbb{Z}_2^{r+2}$$

whenever we have the Mordell-Weil group $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2^m \times \mathbb{Z}^r$.

Remark: $|G/H| = 2^{r+2}$.

How can we compute this quotient group?
In order to compute $|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+2}$, we will use smaller quotient groups.

**Theorem**

*There are group homomorphisms giving a diagram*

\[
\begin{array}{cccccc}
\{O\} & \longrightarrow & \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} & \overset{\hat{\phi}}{\longrightarrow} & \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} & \longrightarrow & \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} & \longrightarrow & \{O\} \\
\downarrow{\delta} & & \downarrow{\delta} & & \downarrow{\delta} & & \downarrow{\delta} & & \downarrow{\delta} \\
\{1\} & \longrightarrow & \frac{\mathbb{Q}^\times}{(\mathbb{Q} \times \mathbb{Q})^2} & \longrightarrow & \frac{\mathbb{Q}^\times}{(\mathbb{Q} \times \mathbb{Q})^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q} \times \mathbb{Q})^2} & \longrightarrow & \frac{\mathbb{Q}^\times}{(\mathbb{Q} \times \mathbb{Q})^2} & \longrightarrow & \{1\}
\end{array}
\]

*In particular,*

\[
\left| \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \right| = \left| \text{image of } \delta \right| \left| \text{image of } \hat{\delta} \right|.
\]

It suffices then to compute the orders of the images of the connecting homomorphisms $\delta$ and $\hat{\delta}$ by counting certain square-free integers.
Homogeneous Spaces

**Theorem (Edray Goins, 2008)**

Say that $E$ is an elliptic curve over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_8$.

- There exists a rational number $t$ such that
  \[
  E : \quad y^2 = (1 - x^2) (1 - k^2 x^2) \quad \text{where} \quad k = \frac{t^4 - 6 t^2 + 1}{(t^2 + 1)^2};
  \]
  \[
  E' : \quad y^2 = (1 + x^2) (1 + \kappa^2 x^2) \quad \text{where} \quad \kappa = \left(\frac{2 t}{t^2 - 1}\right).
  \]

- The images of $\delta$ and $\hat{\delta}$ are those square-free integers $d_1$ and $d_2$, respectively, such that (1) the only primes which divide them must also divide $k$ and $\kappa$, respectively, and (2) the homogeneous spaces
  \[
  C_{d_1} : \quad d_1 w^2 = (1 - d_1 z^2) (1 - d_1 k^2 z^2)
  \]
  \[
  \hat{C}_{d_2} : \quad d_2 w^2 = (1 + d_2 z^2) (1 + d_2 \kappa^2 z^2)
  \]
  have a rational point $(z, w)$, respectively.
Recall the elliptic curve

\[ E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X \]
\[ + 23423843020411418137025218596462864112853337413958990400. \]
Recall the elliptic curve

\[ E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X \]
\[ + 234238430204114181370252185964622864112853337413958990400. \]

The Mordell-Weil group is

\[ E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_r \]

for some nonnegative integer \( r \). This curve corresponds to

\[ t = \frac{9}{296} \implies k = \frac{7633988641}{7690763809} \text{ and } \kappa = \frac{28387584}{7662376225}. \]

There are group homomorphisms \( \phi : E \to E' \) and \( \hat{\phi} : E' \to E \) in terms of

\[ E' : \quad Y^2 + X Y = X^3 - 71828384105861957682230266860325044120 X \]
\[ + 234137152575130885252407456517423577517272419831108430400. \]
In order to compute the rank, we must calculate $|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+2}$. We wish to determine the images of the connecting homomorphisms

$$\delta : \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \rightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2},$$

$$(X, Y) \mapsto 4X + 39141876845580405121;$$

$$\hat{\delta} : \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \rightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2},$$

$$(X, Y) \mapsto X - 4892734605697550640.$$
Current Project

For square-free integers

\[ d_1 \in \langle -1, 82207, 87697, 92863 \rangle, \]
\[ d_2 \in \langle -1, 2, 3, 5, 7, 37, 41, 61 \rangle; \]

we consider the homogeneous spaces

\[ C_{d_1} : \quad d_1 w^2 = (1 - d_1 z^2) (1 - d_1 k^2 z^2) \quad \text{where} \quad k = \frac{7633988641}{7690763809}, \]
\[ \hat{C}_{d_2} : \quad d_2 w^2 = (1 + d_2 z^2) (1 + d_2 \kappa^2 z^2) \quad \text{where} \quad \kappa = \frac{28387584}{7662376225}. \]

The number of pairs \((d_1, d_2)\) such that \(C_{d_1}\) and \(\hat{C}_{d_2}\) both have rational points \((z, w)\) is

\[ 2^{r+2} = \left| \text{image of } \delta \right| \left| \text{image of } \hat{\delta} \right|. \]
Partial Results

**Theorem (SUMSRI, 2007)**

\[
E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X \\
+ 234238430204114181370252185964622864112853337413958990400
\]

has Mordell-Weil group \( E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}^r \) where \( r = 2 \) or \( 3 \).
Theorem (SUMSRI, 2007)

\[
E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X \\
+ 234238430204114181370252185964622864112853337413958990400
\]

has Mordell-Weil group \( E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}^r \) where \( r = 2 \) or \( 3 \).

**Proof.** The software package mwrank found that

\[
\text{image of } \delta = \{1\}, \quad \text{image of } \hat{\delta} \subseteq \langle -1, 6477590, 2, 7, 37 \rangle.
\]

Thus \( 2^{r+2} \leq 1 \cdot 2^5 \). Moreover, SUMSRI 2007 found the four points

\[
P_1 = (4892533141966211376, -2446266570983105688);
\]

\[
P_2 = (6793371071343566640, 773920780859340925333304680);
\]

\[
P_3 = \left( \frac{125691121567490117748583092936841344290}{16027875241^2}, \frac{7866983958078557295967422153373068932127604005333639780}{16027875241^3} \right);
\]

\[
P_4 = \left( \frac{419146355190134411415222739650581610769161840}{9255646526131^2}, \frac{105211386192778469849488967231903854157073005646773612879981880}{9255646526131^3} \right).
\]

Thus \( E(\mathbb{Q}) \supset \langle P_1, P_2, P_3, P_4 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}^2 \). Hence \( r = 2 \) or \( 3 \).
The image of $\hat{\delta}$ is contained in $\langle -1, 6477590, 2, 7, 37 \rangle$. The four points on $E$ from the previous slide have the following images via $\hat{\delta}$.

<table>
<thead>
<tr>
<th>$P$ on $E$</th>
<th>$d_2 = \hat{\delta}(P)$</th>
<th>Point $(z, w)$ on $\hat{C}_{d_2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>$-1$</td>
<td>$(1, 0)$</td>
</tr>
<tr>
<td>$P_2$</td>
<td>$6477590$</td>
<td>$(\frac{305}{7992}, \frac{8143806511}{200779379640})$</td>
</tr>
<tr>
<td>$P_3$</td>
<td>$2$</td>
<td>$(\frac{116263507795895}{683172154272384}, \frac{11901847559384869074927861139}{163644731958920474581067710080})$</td>
</tr>
<tr>
<td>$P_4$</td>
<td>$7$</td>
<td>$(\frac{9477908247062185}{147942254073677904}, \frac{2802930777448484302006837377371105071}{7311568666378397912349147334466220240})$</td>
</tr>
</tbody>
</table>

Can we find a point $P_5$ on $E$ corresponding to $d_2 = \hat{\delta}(P_5) = 37$?
Is there an efficient way to find rational points \((z, w)\) on the homogeneous spaces \(C_{d_1}\) and \(\hat{C}_{d_2}\)?
Recall that we have the following elliptic curves:

\[ E : \quad y^2 = (1 - x^2) \left(1 - k^2 x^2\right) \quad \text{in terms of} \quad k = \frac{t^4 - 6 t^2 + 1}{(t^2 + 1)^2}; \]
\[ E' : \quad y^2 = (1 + x^2) \left(1 + \kappa^2 x^2\right) \quad \text{in terms of} \quad \kappa = \left(\frac{2 t}{t^2 - 1}\right)^2. \]
Recall that we have the following elliptic curves:

\[ E : \quad y^2 = (1 - x^2) (1 - k^2 x^2) \quad \text{in terms of} \quad k = \frac{t^4 - 6 t^2 + 1}{(t^2 + 1)^2}; \]

\[ E' : \quad y^2 = (1 + x^2) (1 + \kappa^2 x^2) \quad \text{in terms of} \quad \kappa = \left(\frac{2 t}{t^2 - 1}\right)^2. \]

Recall their corresponding homogeneous spaces

\[ C_{d_1} : \quad d_1 \, w^2 = (1 - d_1 \, z^2) (1 - d_1 \, k^2 \, z^2); \]

\[ \hat{C}_{d_2} : \quad d_2 \, w^2 = (1 + d_2 \, z^2) (1 + d_2 \, \kappa^2 \, z^2). \]
Recall that we have the following elliptic curves:

\[ E : \quad y^2 = (1 - x^2) (1 - k^2 x^2) \quad \text{in terms of} \quad k = \frac{t^4 - 6 t^2 + 1}{(t^2 + 1)^2}; \]

\[ E' : \quad y^2 = (1 + x^2) (1 + \kappa^2 x^2) \quad \text{in terms of} \quad \kappa = \left( \frac{2 t}{t^2 - 1} \right)^2. \]

Recall their corresponding homogeneous spaces

\[ C_{d_1} : \quad d_1 w^2 = (1 - d_1 z^2) (1 - d_1 k^2 z^2); \]

\[ \hat{C}_{d_2} : \quad d_2 w^2 = (1 + d_2 z^2) (1 + d_2 \kappa^2 z^2). \]

These curves fit together using the following diagrams:
Proposition

Let \( t = 9/296 \). There is a 2-covering map \( \hat{\psi} : \hat{C}_{d_2} \rightarrow E \) which sends a \( \mathbb{Q} \)-rational point \((z, w)\) to a \( \mathbb{Q} \)-rational point \((X, Y)\) in terms of

\[
X = 4892734605697550640 + 201463731339264 d_2 z^2; \\
Y = -2446367302848775320 \\
- 100731865669632 d_2 z^2 + 771845452606881941299200 d_2 w z.
\]
Proposition

Let \( t = 9/296 \). There is a 2-covering map \( \hat{\psi} : \hat{C}_{d_2} \to E \) which sends a \( \mathbb{Q} \)-rational point \((z, w)\) to a \( \mathbb{Q} \)-rational point \((X, Y)\) in terms of

\[
X = 4892734605697550640 + 201463731339264 d_2 z^2;
\]
\[
Y = -2446367302848775320
- 100731865669632 d_2 z^2 + 771845452606881941299200 d_2 w z.
\]

It is half as difficult to find points on \( \hat{C}_{d_2} \) as it is to find points on \( E \).
Points on Homogeneous Spaces

<table>
<thead>
<tr>
<th>$P$ on $E$</th>
<th>$d_2 = \delta(P)$</th>
<th>Point $(z, w)$ on $\hat{C}_{d_2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>$-1$</td>
<td>$(1, 0)$</td>
</tr>
<tr>
<td>$P_2$</td>
<td>6477590</td>
<td>$(\frac{305}{7992}, \frac{8143806511}{200779379640})$</td>
</tr>
<tr>
<td>$P_3$</td>
<td>2</td>
<td>$(\frac{116263507795895}{683172154272384}, \frac{11901847559384869074927861139}{163644731958920474581067710080})$</td>
</tr>
<tr>
<td>$P_4$</td>
<td>7</td>
<td>$(\frac{9477908247062185}{147942254073677904}, \frac{280293077744848430200683737371105071}{7311568666378397912349147334466220240})$</td>
</tr>
</tbody>
</table>

Recall the four points

\[ P_1 = (4892533141966211376, -2446266570983105688) \];
\[ P_2 = (6793371071343566640, 7739207808589340925333304680) \];
\[ P_3 = \left( \frac{1256911215674901177485830929368441344290}{16027875241^2}, \frac{786698395807855729596742215337306893212760400533639780}{16027875241^3} \right) \];
\[ P_4 = \left( \frac{419146355190134411415222739650581610769161840}{9255646526131^2}, \frac{105211386192778469849488967231903854157073005646773612879981880}{9255646526131^3} \right) \].
4-Covering Maps

Now introduce the elliptic curve

\[ E'' : \quad y^2 = (1 + x^2)(1 + k'^2 x^2) \quad \text{in terms of} \quad k' = \frac{4(t^3 - t)}{(t^2 + 1)^2}. \]

Its corresponding homogeneous space is

\[ \hat{C}'_{d_2} : \quad d_2 w^2 = (1 + d_2 z^2)(1 + d_2 k'^2 z^2). \]
Now introduce the elliptic curve

\[ E'' : \quad y^2 = (1 + x^2)(1 + k'^2 x^2) \quad \text{in terms of} \quad k' = \frac{4(t^3 - t)}{(t^2 + 1)^2}. \]

Its corresponding homogeneous space is

\[ \hat{C}'_{d_2} : \quad d_2 w^2 = (1 + d_2 z^2)(1 + d_2 k'^2 z^2). \]

These curves fit together using the following diagram:
Now introduce the elliptic curve

\[ E'' : \quad y^2 = (1 + x^2)(1 + k'^2 x^2) \quad \text{in terms of} \quad k' = \frac{4(t^3 - t)}{(t^2 + 1)^2}. \]

Its corresponding homogeneous space is

\[ \hat{\mathcal{C}}'_{d^2} : \quad d^2 w^2 = (1 + d^2 z^2)(1 + d^2 k'^2 z^2). \]

These curves fit together using the following diagram:

\[ \begin{array}{ccc}
E'' & \longrightarrow & E' \\
\downarrow & & \downarrow \\
\hat{\mathcal{C}}'_{d^2} & \longrightarrow & \hat{\mathcal{C}}_{d^2}
\end{array} \]

\[ \phi \quad \psi \]

Is it easier to find points on \( \hat{\mathcal{C}}'_{d^2} \) than it is for \( \hat{\mathcal{C}}_{d^2} \)?
**Proposition**

Let $t = 9/296$. There is a 2-covering map $\hat{\psi}' : \hat{C}_{d_2} \to E'$ which sends a $\mathbb{Q}$-rational point $(z, w)$ to a $\mathbb{Q}$-rational point $(X, Y)$ in terms of

\[
X = 5001492780060945840 + 217516348726790400 d_2 z^2;
\]
\[
Y = -2500746390030472920 - 108758174363395200 d_2 z^2 + 836433431326911418524316800 d_2 w z.
\]
4-Covering Maps

Proposition

Let $t = 9/296$. There is a 2-covering map $\hat{\psi}': \hat{C}'_{d_2} \to E'$ which sends a $\mathbb{Q}$-rational point $(z, w)$ to a $\mathbb{Q}$-rational point $(X, Y)$ in terms of

$$X = 5001492780060945840 + 217516348726790400 \cdot d_2 \cdot z^2;$$

$$Y = -2500746390030472920$$

$$- 108758174363395200 \cdot d_2 \cdot z^2 + 836433431326911418524316800 \cdot d_2 \cdot w \cdot z.$$

We define $\varphi : \hat{C}'_{d_2} \to \hat{C}_{d_2}$ via the composition $\hat{\psi}' = \phi \circ \hat{\psi} \circ \varphi.$
## Points on Homogeneous Spaces

<table>
<thead>
<tr>
<th>( P' ) on ( E' )</th>
<th>( d_2 = \hat{\delta}(P) )</th>
<th>( P' ) point on ( \mathcal{C}_{d_2}' )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \phi(P_1) )</td>
<td>(-1)</td>
<td>(7690763809, 0)</td>
</tr>
<tr>
<td>( \phi(P_2) )</td>
<td>(6477590)</td>
<td>( \left( \frac{87697}{7731080}, \frac{8623536769}{6816782522760} \right) )</td>
</tr>
<tr>
<td>( \phi(P_3) )</td>
<td>(2)</td>
<td>( \left( \frac{402721445539793209371967}{16689898742884224439568}, \frac{54679029697172970037144799838907324414667329763}{5319738216468998004248404711869988353017875184} \right) )</td>
</tr>
<tr>
<td>( \phi(P_4) )</td>
<td>(7)</td>
<td>( \left( \frac{1434298275377041049916550061461}{78309867527655769246487587761}, \frac{45852135158706046452821064687371285272034083270789515130064924}{41982527953301741489751898779797875973801679251659817777} \right) )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( P ) on ( E )</th>
<th>( d_2 = \hat{\delta}(P) )</th>
<th>( P ) point on ( \mathcal{C}_{d_2} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P_1 )</td>
<td>(-1)</td>
<td>(1, 0)</td>
</tr>
<tr>
<td>( P_2 )</td>
<td>(6477590)</td>
<td>( \left( \frac{305}{7992}, \frac{8143806511}{200779379640} \right) )</td>
</tr>
<tr>
<td>( P_3 )</td>
<td>(2)</td>
<td>( \left( \frac{116263507795895}{683172154272384}, \frac{1190184755938486907469278661139}{163644731958920474581067710080} \right) )</td>
</tr>
<tr>
<td>( P_4 )</td>
<td>(7)</td>
<td>( \left( \frac{9477908247062185}{147942254073677904}, \frac{2802930777448484302006837377371105071}{7311568666378397912349147334466220240} \right) )</td>
</tr>
</tbody>
</table>
When $t = 9/296$, we have the elliptic curve

$$E : Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X$$
$$+ 234238430204114181370252185964622864112853337413958990400.$$

We have determined that the Mordell-Weil rank is either $r = 2$ or $3$. 
When $t = 9/296$, we have the elliptic curve

$$E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X$$
$$+ 234238430204114181370252185964622864112853337413958990400.$$

We have determined that the Mordell-Weil rank is either $r = 2$ or 3.

We seek a point $P_5$ on $E$ such that $d_2 = \delta(P_5) = 37$. It suffices to find a point on the homogeneous space

$$\hat{C}_{37} : \quad 37 w^2 = (1 + 37 z^2)(1 + 37 \kappa^2 z^2) \quad \text{where} \quad \kappa = \frac{28387584}{7662376225}.$$
When $t = 9/296$, we have the elliptic curve

$$E : \quad Y^2 + X Y = X^3 - 71813598680248384341084284771096244120 X + 234238430204114181370252185964622864112853337413958990400.$$ 

We have determined that the Mordell-Weil rank is either $r = 2$ or $3$.

We seek a point $P_5$ on $E$ such that $d_2 = \hat{\delta}(P_5) = 37$. It suffices to find a point on the homogeneous space

$$\hat{C}_{37} : \quad 37 \ w^2 = (1 + 37 \ z^2) \ (1 + 37 \ \kappa^2 \ z^2) \quad \text{where} \quad \kappa = \frac{28387584}{7662376225}.$$ 

Similarly, it suffices to find a point on the homogeneous space

$$\hat{C}'_{37} : \quad 37 \ w^2 = (1 + 37 \ z^2) \ (1 + 37 \ k'^2 \ z^2) \quad \text{where} \quad k' = \frac{932772960}{7690763809}.$$
Michael Stoll at Jacob’s University at Bremen has written a program called `ratpoints` which should find the points \((z, w)\) on these curves.
Future Work

- Michael Stoll at Jacob’s University at Bremen has written a program called `ratpoints` which should find the points \((z, w)\) on these curves.

- We have been searching for points for nearly two weeks on the high powered computing cluster RedHawk at Miami University.
Future Work

- Michael Stoll at Jacob’s University at Bremen has written a program called \texttt{ratpoints} which should find the points \((z, w)\) on these curves.

- We have been searching for points for nearly two weeks on the high powered computing cluster \texttt{RedHawk} at Miami University.

- The methods outlined here should work for any value of \(t\).
Acknowledgments

We would like to thank...

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