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

Mordell-Weil Group

Theorem (Louis Mordell, 1922)

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

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

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

Mordell-Weil Group

Theorem (Louis Mordell, 1922)

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

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

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

- 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

$$[m]P = \mathcal{O} \qquad \text{for some positive integer } m.$$

- The nonnegative integer r is called the Mordell-Weil rank of E.

Example

Consider the elliptic curve

$$E : \qquad Y^2 = X^3 - 36\,X.$$

Example

Consider the elliptic curve

$$E : \qquad Y^2 = X^3 - 36\,X.$$

- The Mordell-Weil group is

$$E(\mathbb{Q}) = \langle P_1,\ P_2,\ P_3 \rangle \simeq Z_2 \times Z_2 \times \mathbb{Z}$$

  as generated by the rational points

$$P_1 = (0,\,0)\,, \qquad P_2 = (6,\,0)\,, \qquad \text{and} \qquad P_3 = (12,\,36)\,.$$

- The torsion subgroup is

$$E(\mathbb{Q})_{\text{tors}} = \langle P_1,\ P_2 \rangle \simeq Z_2 \times Z_2.$$

- The Mordell-Weil rank is $r = 1$.

Current Project

Now consider the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 71813598680248384341084284771096244120\,X \\ &+ 234238430204114181370252185964622864112853337413958990400. \end{aligned}$$

Current Project

Now consider the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 718135986802483843410842847710962441 20\,X \\ &+ 2342384302041141813702521859646228641128533374139589904 00. \end{aligned}$$

- What is the Mordell-Weil group $E(\mathbb{Q})$?
- What is the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$?
- What is the Mordell-Weil rank r?

Torsion Subgroups

Theorem (Barry Mazur, 1977)

Let E is an elliptic curve, then

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

Remark: Z_n denotes the cyclic group of order n.

Torsion Subgroups

Theorem (Barry Mazur, 1977)

Let E is an elliptic curve, then

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

Remark: Z_n denotes the cyclic group of order n.

Mordell's Theorem states that

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

What can we say about the Mordell-Weil rank r?

Current Project

Recall the elliptic curve

$$E: \begin{aligned} Y^2 + XY = X^3 &- 718135986802483843410842847710962441 20\,X \\ &+ 2342384302041141813702521859646228641128533374139589904 00. \end{aligned}$$

Current Project

Recall the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 7181359868024838434108428477109624412\,0\,X \\ &+ 234238430204114181370252185964622864112853337413958990400. \end{aligned}$$

We have the two rational points

$$P_1 = (4892533141966211376, \, -2446266570983105688);$$

$$P_2 = (6793371071343566640, \, 7739207808589340925333304680).$$

It is easy to verify that $[2]P_1 = [8]P_2 = \mathcal{O}$. The torsion subgroup of E is

$$E(\mathbb{Q})_{\text{tors}} = \langle P_1, \, P_2 \rangle \simeq Z_2 \times Z_8.$$

Current Project

Recall the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 71813598680248384341084284771096244120\,X \\ &+ 234238430204114181370252185964622864112853337413958990400. \end{aligned}$$

We have the two rational points

$$P_1 = (4892533141966211376, \ -2446266570983105688);$$

$$P_2 = (6793371071343566640, \ 7739207808589340925333304680).$$

It is easy to verify that $[2]P_1 = [8]P_2 = \mathcal{O}$. The torsion subgroup of E is

$$E(\mathbb{Q})_{\text{tors}} = \langle P_1, \, P_2 \rangle \simeq Z_2 \times Z_8.$$

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

$E(\mathbb{Q})_{\text{tors}}$	**Known** $r \leq$	**Author (Year)**
Z_1	28	Elkies (2006)
Z_2	18	Elkies (2006)
Z_3	13	Eroshkin (2007, 2008)
Z_4	12	Elkies (2006)
Z_5	6	Dujella – Lecacheux (2001)
Z_6	8	Eroshkin (2008), Dujella – Eroshkin (2008) Elkies (2008), Dujella (2008)
Z_7	5	Dujella – Kulesz (2001), Elkies (2006)
Z_8	6	Elkies (2006)
Z_9	3	Dujella (2001), MacLeod (2004) Eroshkin (2006), Eroshkin - Dujella (2007)
Z_{10}	4	Dujella (2005), Elkies (2006)
Z_{12}	3	Dujella (2001, 2005, 2006), Rathbun (2003, 2006)
$Z_2 \times Z_2$	14	Elkies (2005)
$Z_2 \times Z_4$	8	Elkies (2005), Eroshkin (2008), Dujella - Eroshkin (2008)
$Z_2 \times Z_6$	6	Elkies (2006)
$Z_2 \times Z_8$	3	Connell (2000), Dujella (2000, 2001, 2006) Campbell - Goins (2003), Rathbun (2003, 2006) Flores - Jones - Rollick - Weigandt (2007)

`http://web.math.hr/~duje/tors/tors.html`

Example

In 2007, the SUMSRI Number Theory Seminar found the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 250878395393474545316759183209311840250\,X \\ &+ 14799795920221674932249605129107556895742994778089035609 32. \end{aligned}$$

Example

In 2007, the SUMSRI Number Theory Seminar found the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 250878395393474545316759183209311840250\,X \\ &+ 1479979592022167493224960512910755689574299477808903560932. \end{aligned}$$

The torsion subgroup is

$$E(\mathbb{Q})_{\text{tors}} = \langle P_1,\ P_2 \rangle \simeq Z_2 \times Z_8$$

as generated by the rational points

$$P_1 = (7766447618213273204,\ -3883223809106636602);$$

$$P_2 = (-9594066305658249586,\ 5480718097675957070983243408).$$

Example

The Mordell-Weil group is

$$E(\mathbb{Q}) = \langle P_1,\ P_2,\ P_3,\ P_4,\ P_5 \rangle \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$$

as generated by the rational points

$$P_1 = (7766447618213273204,\ -3883223809106636602);$$

$$P_2 = (-9594066305658249586,\ 5480718097675957070983243440 8);$$

$$P_3 = \left(\frac{6217278838603318790662 88}{80089},\ -\frac{1119573327510565907267663521099227 4}{22665187}\right);$$

$$P_4 = \left(-\frac{3121826350817955803774630199394084}{180524403067969},\ \frac{6169210841875714300950141417193739809776684720357 4}{24255145065838382019 53}\right);$$

$$P_5 = \left(\frac{6278248666514948721809713120842629710 4}{8547022989099698401},\ -\frac{1445939857425239504039427763166870522574607124164051602 02}{24987471290251272975616507601}\right).$$

Example

The Mordell-Weil group is

$$E(\mathbb{Q}) = \langle P_1,\ P_2,\ P_3,\ P_4,\ P_5 \rangle \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$$

as generated by the rational points

$$\begin{aligned}
P_1 &= (7766447618213273204,\ \ -3883223809106636602);\\
P_2 &= (-9594066305658249586,\ \ 5480718097675957070983243408);\\
P_3 &= \left(\frac{62172788386033187906628 8}{80089},\ -\frac{1119573327510565907267663521099227 4}{22665187}\right);\\
P_4 &= \left(-\frac{312182635081795580377463019939408 4}{180524403067969},\ \ \frac{61692108418757143009501414171937398097766847203574}{24255145065838382019 53}\right);\\
P_5 &= \left(\frac{62782486665149487218097131208426297104}{8547022989099698401},\ -\frac{14459398574252395040394277631668705225746071241640516020 2}{2498747129025127297561650760 1}\right).
\end{aligned}$$

Hence the Mordell-Weil rank is $r = 3$.

Given an elliptic curve E,
how do we compute
the Mordell-Weil rank r?

Proof of Poincaré's Conjecture

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 $E(\mathbb{Q})$.

Proof of Poincaré's Conjecture

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

$$E(\mathbb{Q}) \simeq Z_2 \times Z_{2m} \times \mathbb{Z}^r \qquad \Longrightarrow \qquad \frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \simeq {Z_2}^{r+2}.$$

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

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

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

$$G/H = \left\{ a \mod H \;\middle|\; a \in G \right\}.$$

Remark: We will sometimes write G/H as $\dfrac{G}{H}$.

Example

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

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

Proposition

We may identify the quotient group

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

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

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

Proposition

We may identify the quotient group

$$G/H = \frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \simeq {Z_2}^{r+2}$$

whenever we have the Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_{2m} \times \mathbb{Z}^r$.

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

How can we compute this quotient group?

Connecting Homomorphisms

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

$$\begin{tikzcd}
\{\mathcal{O}\} \arrow[r] & \dfrac{E'(\mathbb{Q})}{\phi\,(E(\mathbb{Q}))} \arrow[r, "\widehat{\phi}"] \arrow[d, "\delta"] & \dfrac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \arrow[r] \arrow[d] & \dfrac{E(\mathbb{Q})}{\widehat{\phi}\,(E'(\mathbb{Q}))} \arrow[r] \arrow[d, "\widehat{\delta}"] & \{\mathcal{O}\} \\
\{1\} \arrow[r] & \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \arrow[r] & \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \arrow[r] & \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \arrow[r] & \{1\}
\end{tikzcd}$$

In particular,

$$\left|\frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})}\right| = \left|\textit{image of } \delta\right| \left|\textit{image of } \widehat{\delta}\right|.$$

It suffices then to compute the orders of the images of the connecting homomorphisms δ and $\widehat{\delta}$ 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 $Z_2 \times Z_8$.

- *There exists a rational number t such that*

$$E: \quad y^2 = \left(1 - x^2\right)\left(1 - k^2\,x^2\right) \qquad \text{where} \quad k = \frac{t^4 - 6\,t^2 + 1}{(t^2+1)^2};$$

$$E': \quad y^2 = \left(1 + x^2\right)\left(1 + \kappa^2\,x^2\right) \qquad \text{where} \quad \kappa = \left(\frac{2\,t}{t^2 - 1}\right)^2.$$

- *The images of δ and $\widehat{\delta}$ 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 κ, respectively, and (2) the homogeneous spaces*

$$C_{d_1}: \quad d_1\,w^2 = \left(1 - d_1\,z^2\right)\left(1 - d_1\,k^2\,z^2\right)$$
$$\widehat{C}_{d_2}: \quad d_2\,w^2 = \left(1 + d_2\,z^2\right)\left(1 + d_2\,\kappa^2\,z^2\right)$$

have a rational point (z, w), respectively.

Current Project

Recall the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 718135986802483843410842847710962441 20\,X \\ &+ 234238430204114181370252185964622864112853337413958990400. \end{aligned}$$

Current Project

Recall the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 71813598680248384341084284771096244120\,X \\ &+ 2342384302041141813702521859646228641128533374139589904 00. \end{aligned}$$

The Mordell-Weil group is

$$E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^r$$

for some nonnegative integer r. This curve corresponds to

$$t = \frac{9}{296} \quad \Longrightarrow \quad k = \frac{7633988641}{7690763809} \quad \text{and} \quad \kappa = \frac{28387584}{7662376225}.$$

There are group homomorphisms $\phi : E \to E'$ and $\widehat{\phi} : E' \to E$ in terms of

$$E': \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 71828384105861957682230266860325044120\,X \\ &+ 234137152575130885252407456517423577517272419831108430400. \end{aligned}$$

Current Project

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

$$\delta: \begin{array}{ccc} \dfrac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} & \longrightarrow & \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}, \\ (X, Y) & \longmapsto & 4\,X + 391418768455804051 21; \end{array}$$

$$\widehat{\delta}: \begin{array}{ccc} \dfrac{E(\mathbb{Q})}{\widehat{\phi}(E'(\mathbb{Q}))} & \longrightarrow & \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}, \\ (X, Y) & \longmapsto & X - 4892734605697550640. \end{array}$$

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

$$C_{d_1}: \quad d_1\, w^2 = \left(1 - d_1\, z^2\right)\left(1 - d_1\, k^2\, z^2\right) \qquad \text{where} \quad k = \frac{7633988641}{7690763809},$$

$$\widehat{C}_{d_2}: \quad d_2\, w^2 = \left(1 + d_2\, z^2\right)\left(1 + d_2\, \kappa^2\, z^2\right) \qquad \text{where} \quad \kappa = \frac{28387584}{7662376225}.$$

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

$$2^{r+2} = \left|\text{image of } \delta\right| \left|\text{image of } \widehat{\delta}\right|.$$

Partial Results

Theorem (SUMSRI, 2007)

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 71813598680248384341084284771096244120\,X \\ &+ 234238430204114181370252185964622864112853337413958990400 \end{aligned}$$

has Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^r$ *where* $r = 2$ *or 3.*

Partial Results

Theorem (SUMSRI, 2007)

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 7181359868024838434108428477109624412\,0\,X \\ &+ 2342384302041141813702521859646228641128533374139589904 00 \end{aligned}$$

has Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^r$ *where* $r = 2$ *or* 3.

Proof. The software package `mwrank` found that

$$\text{image of } \delta = \{1\}, \qquad \text{image of } \widehat{\delta} \subseteq \langle -1,\, 6477590,\, 2,\, 7,\, 37 \rangle.$$

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

$$\begin{aligned}
P_1 &= (4892533141966211376,\ -2446266570983105688); \\
P_2 &= (6793371071343566640,\ 7739207808589340925333304680); \\
P_3 &= \left(\frac{1256911215674901177485830929368441344290}{16027875241^2},\ \frac{786698395807855729596742215337306893212760400533639780}{16027875241^3} \right); \\
P_4 &= \left(\frac{4191463551901344114152227396505816107691618 40}{9255646526131^2},\ \frac{10521138619277846984948896723190385415707300564677361287 9981880}{9255646526131^3} \right).
\end{aligned}$$

Thus $E(\mathbb{Q}) \supset \langle P_1,\, P_2,\, P_3,\, P_4 \rangle \simeq Z_2 \times Z_8 \times \mathbb{Z}^2$. Hence $r = 2$ or 3. $\square$

Points on Homogeneous Spaces

The image of $\widehat{\delta}$ is contained in $\langle -1, 6477590, 2, 7, 37 \rangle$. The four points on E from the previous slide have the following images via $\widehat{\delta}$.

P on E	$d_2 = \widehat{\delta}(P)$	Point (z, w) on $\widehat{C}_{d_2}$
P_1	-1	$(1, 0)$
P_2	6477590	$\left(\frac{305}{7992}, \frac{8143806511}{200779379640}\right)$
P_3	2	$\left(\frac{116263507795895}{683172154272384}, \frac{119018475593848690746927861139}{163644731958920474581067710080}\right)$
P_4	7	$\left(\frac{9477908247062185}{14794225407367790 4}, \frac{28029307774484843020068373773711 05071}{73115686663783979123491473344662 20240}\right)$

Can we find a point P_5 on E corresponding to $d_2 = \widehat{\delta}(P_5) = 37$?

Is there an efficient way
to find rational points (z, w)
on the homogeneous spaces C_{d_1} and $\widehat{C}_{d_2}$?

2-Covering Maps

Recall that we have the following elliptic curves:

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

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

2-Covering Maps

Recall that we have the following elliptic curves:

$$E: \quad y^2 = \left(1 - x^2\right)\left(1 - k^2\, x^2\right) \qquad \text{in terms of} \quad k = \frac{t^4 - 6\,t^2 + 1}{(t^2+1)^2};$$

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

Recall their corresponding homogeneous spaces

$$C_{d_1}: \quad d_1\, w^2 = \left(1 - d_1\, z^2\right)\left(1 - d_1\, k^2\, z^2\right);$$

$$\widehat{C}_{d_2}: \quad d_2\, w^2 = \left(1 + d_2\, z^2\right)\left(1 + d_2\, \kappa^2\, z^2\right).$$

2-Covering Maps

Recall that we have the following elliptic curves:

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

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

Recall their corresponding homogeneous spaces

$$C_{d_1} : \quad d_1\,w^2 = \left(1 - d_1\,z^2\right)\left(1 - d_1\,k^2\,z^2\right);$$

$$\widehat{C}_{d_2} : \quad d_2\,w^2 = \left(1 + d_2\,z^2\right)\left(1 + d_2\,\kappa^2\,z^2\right).$$

These curves fit together using the following diagrams:

$$\begin{tikzcd} E' & E \arrow[l, "\phi"'] \arrow[d, dotted, no head] \\ & C_{d_1} \arrow[ul] \end{tikzcd} \qquad \begin{tikzcd} E' \arrow[r, "\hat{\phi}"] \arrow[d, dotted, no head] & E \\ \widehat{C}_{d_2} \arrow[ur] & \end{tikzcd}$$

2-Covering Maps

$$\begin{tikzcd} E' & E \arrow[l, "\phi"'] \arrow[d, dotted, no head] \\ & C_{d_1} \arrow[ul] \end{tikzcd} \qquad \begin{tikzcd} E' \arrow[r, "\widehat{\phi}"] \arrow[d, dotted, no head] & E \\ \widehat{C}_{d_2} \arrow[ur, "\widehat{\psi}"'] & \end{tikzcd}$$

Proposition

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

$$\begin{aligned} X &= 4892734605697550640 + 201463731339264\, d_2\, z^2; \\ Y &= -2446367302848775320 \\ &\qquad - 100731865669632\, d_2\, z^2 + 771845452606881941299200\, d_2\, w\, z. \end{aligned}$$

2-Covering Maps

$$\begin{tikzcd} E' & E \arrow[l, "\phi"'] \arrow[d, dotted, dash] \\ & C_{d_1} \arrow[ul] \end{tikzcd} \qquad \begin{tikzcd} E' \arrow[r, "\widehat{\phi}"] \arrow[d, dotted, dash] & E \\ \widehat{C}_{d_2} \arrow[ur, "\widehat{\psi}"'] & \end{tikzcd}$$

Proposition

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

$$\begin{aligned} X &= 4892734605697550640 + 201463731339264\, d_2\, z^2; \\ Y &= -2446367302848775320 \\ &\qquad - 100731865669632\, d_2\, z^2 + 771845452606881941299200\, d_2\, w\, z. \end{aligned}$$

It is half as difficult to find points on $\widehat{C}_{d_2}$ as it is to find points on E.

Points on Homogeneous Spaces

P on E	$d_2 = \widehat{\delta}(P)$	Point (z, w) on $\widehat{C}_{d_2}$
P_1	-1	$(1, 0)$
P_2	6477590	$\left(\frac{305}{7992}, \frac{8143806511}{200779379640}\right)$
P_3	2	$\left(\frac{116263507795895}{683172154272384}, \frac{119018475593848690746927861139}{163644731958920474581067710080}\right)$
P_4	7	$\left(\frac{9477908247062185}{147942254073677904}, \frac{2802930777448484302006837377371105071}{7311568666378397912349147334466220240}\right)$

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

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

Its corresponding homogeneous space is

$$\widehat{C}'_{d_2} : \quad d_2\, w^2 = \left(1 + d_2\, z^2\right)\left(1 + d_2\, {k'}^2\, z^2\right).$$

4-Covering Maps

Now introduce the elliptic curve

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

Its corresponding homogeneous space is

$$\widehat{C}'_{d_2} : \quad d_2\, w^2 = \left(1 + d_2\, z^2\right)\left(1 + d_2\, k'^2\, z^2\right).$$

These curves fit together using the following diagram:

$$\begin{tikzcd}
E'' \arrow[r] \arrow[d, dash, dotted] & E' \arrow[r, "\widehat{\phi}"] \arrow[d, dash, dotted] & E \\
\widehat{C}'_{d_2} \arrow[r] \arrow[ur] & \widehat{C}_{d_2} \arrow[ur, "\widehat{\psi}"'] &
\end{tikzcd}$$

4-Covering Maps

Now introduce the elliptic curve

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

Its corresponding homogeneous space is

$$\widehat{C}'_{d_2} : \quad d_2\, w^2 = \left(1 + d_2\, z^2\right)\left(1 + d_2\, {k'}^2\, z^2\right).$$

These curves fit together using the following diagram:

$$\begin{tikzcd} E'' \arrow[r] \arrow[d, dash, dotted] & E' \arrow[r, "\widehat{\phi}"] \arrow[d, dash, dotted] & E \\ \widehat{C}'_{d_2} \arrow[r] \arrow[ur] & \widehat{C}_{d_2} \arrow[ur, "\widehat{\psi}"'] & \end{tikzcd}$$

Is it easier to find points on $\widehat{C}'_{d_2}$ than it is for $\widehat{C}_{d_2}$?

4-Covering Maps

$$
\begin{tikzcd}
E'' \arrow[r] \arrow[d, dotted, no head] & E' \arrow[r, "\widehat{\phi}"] \arrow[d, dotted, no head] & E \\
\widehat{C}'_{d_2} \arrow[r, "\varphi"'] \arrow[ur, "\widehat{\psi}'"'] & \widehat{C}_{d_2} \arrow[ur, "\widehat{\psi}"'] &
\end{tikzcd}
$$

Proposition

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

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

$$\begin{aligned} Y = {} & -2500746390030472920 \\ & - 108758174363395200\, d_2\, z^2 + 836433431326911418524316800\, d_2\, w\, z. \end{aligned}$$

4-Covering Maps

$$\begin{tikzcd}
E'' \arrow[r] \arrow[d, dotted, dash] & E' \arrow[r, "\widehat{\phi}"] \arrow[d, dotted, dash] & E \\
\widehat{C}'_{d_2} \arrow[r, "\varphi"'] \arrow[ur, "\widehat{\psi}'"'] & \widehat{C}_{d_2} \arrow[ur, "\widehat{\psi}"'] &
\end{tikzcd}$$

Proposition

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

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

$$\begin{aligned} Y &= -2500746390030472920 \\ &\quad - 108758174363395200\, d_2\, z^2 + 836433431326911418524316800\, d_2\, w\, z. \end{aligned}$$

We define $\varphi : \widehat{C}'_{d_2} \to \widehat{C}_{d_2}$ via the composition $\widehat{\psi}' = \phi \circ \widehat{\psi} \circ \varphi$.

Points on Homogeneous Spaces

P' on E'	$d_2 = \widehat{\delta}(P)$	Point (z, w) on $\widehat{C}'_{d_2}$
$\phi(P_1)$	-1	$\left(\frac{7690763809}{932772960},\ 0\right)$
$\phi(P_2)$	6477590	$\left(\frac{87697}{77731080},\ \frac{8623536769}{6816782522760}\right)$
$\phi(P_3)$	2	$\left(\frac{4027214455397932093719 67}{166898987428842244395 68},\ -\frac{546790296971729700371447998389073244144667329763}{531973821646899800424840471186998835301787518 4}\right)$
$\phi(P_4)$	7	$\left(\frac{14342982753770410499165500 61461}{78309867527655769246487587761},\ -\frac{458521351587060464528210646873712852720340832707895151300649 24}{419825279533017414897518986779479787597378016792616598177777}\right)$

P on E	$d_2 = \widehat{\delta}(P)$	Point (z, w) on $\widehat{C}_{d_2}$
P_1	-1	$(1, 0)$
P_2	6477590	$\left(\frac{305}{7992},\ \frac{8143806511}{200779379640}\right)$
P_3	2	$\left(\frac{116263507795895}{683172154272384},\ \frac{119018475593848690746927861139}{163644731958920474581067710080}\right)$
P_4	7	$\left(\frac{9477908247062185}{14794225407367790 4},\ \frac{280293077744848430200683737737110 5071}{731156866637839791234914733446622024 0}\right)$

Current Project

When $t = 9/296$, we have the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 71813598680248384341084284771096244120\,X \\ &+ 234238430204114181370252185964622864112853337413958990400. \end{aligned}$$

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

Current Project

When $t = 9/296$, we have the elliptic curve

$$E : \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 718135986802483843410842847710962441 20\,X \\ &+ 2342384302041141813702521859646228641128533374139589904 00. \end{aligned}$$

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

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

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

Current Project

When $t = 9/296$, we have the elliptic curve

$$E: \quad \begin{aligned} Y^2 + X\,Y = X^3 &- 7181359868024838434108428477109624412\,0\,X \\ &+ 234238430204114181370252185964622864112853337413958990400. \end{aligned}$$

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

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

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

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

$$\widehat{C}'_{37}: \quad 37\,w^2 = \left(1 + 37\,z^2\right)\left(1 + 37\,k'^2\,z^2\right) \quad \text{where} \quad k' = \frac{932772960}{7690763809}.$$

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.

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 `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.
- 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