

SUMSRI NUMBER THEORY SEMINAR: WEEK #4

Research Project. This week, we wish to determine the Mordell-Weil group of the elliptic curve

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

History. Mordell's Theorem states that $E(\mathbb{Q})$ is finitely generated, so $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$ for some finite group $E(\mathbb{Q})_{\text{tors}}$ and nonnegative integer r . Using the substitution

$$\begin{aligned} X &= \frac{4838355518515853040 x - 4947113692879248240}{x - 1} \\ Y &= \frac{209108357831727854631079200 y - 2520 (x - 1) (959991174308701 x - 981570177158581)}{(x - 1)^2} \end{aligned}$$

we see that this cubic curve corresponds to the quartic curve

$$y^2 = (1 - x^2) (1 - k^2 x^2) \quad \text{where} \quad k = \frac{t^4 - 6t^2 + 1}{(t^2 + 1)^2} \quad \text{for} \quad t = \frac{9}{296}.$$

We showed during Week #3 that the torsion subgroup of such curves is $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$. In fact, generators of this torsion subgroup are

$$\begin{aligned} P_1 &= (4892533141966211376 : -2446266570983105688 : 1) \\ P_2 &= (6793371071343566640 : 7739207808589340925333304680 : 1) \end{aligned}$$

It suffices then to compute the Mordell-Weil r .

In July 2007, the SUMSRI Number Theory Seminar discovered this curve in an attempt to find elliptic curves with Mordell-Weil group $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}^3$. They verified that the following sixteen values of t have associated elliptic curve with this Mordell-Weil group:

$$t = \frac{5}{29}, \frac{18}{47}, \frac{15}{76}, \frac{74}{207}, \frac{47}{219}, \frac{19}{220}, \frac{101}{299}, \frac{86}{333}, \frac{65}{337}, \frac{87}{407}, \frac{143}{419}, \frac{17}{439}, \frac{145}{444}, \frac{159}{569}, \frac{230}{923}, \frac{223}{1012}.$$

They conjectured that $t = 9/296$ should also correspond to this Mordell-Weil group. In November 2007, Randall Rathbun found two independent rational points of infinite order on E :

$$\begin{aligned} P_3 &= \left(\frac{33298562853213963241125980}{2609^2} : \frac{49642491581394149413941877921274860}{2609^3} : 1 \right) \\ P_4 &= \left(\frac{1256911215674901177485830929368441344290}{16027875241^2} : \frac{786698395807855729596742215337306893212760400533639780}{16027875241^3} : 1 \right) \end{aligned}$$

Randall Rathbun and James Weigandt have conjectured that this elliptic curve has rank $r = 3$.

Conjecture: There exists a third independent rational point P_5 of infinite order.

We will break into two research groups in order to attempt to find this third point P_5 .

Descent via 2-Isogeny. Last week, we saw that in order to compute the rank r , we must compute the size of the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$. It is easy to show that there exists a 2-isogeny $\hat{\phi} : E' \rightarrow E$ in terms of the elliptic curve

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

Using various connecting homomorphisms, we see that there is a diagram

$$\begin{array}{ccccccc} \{\mathcal{O}\} & \longrightarrow & \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} & \xrightarrow{\hat{\phi}} & \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} & \longrightarrow & \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \longrightarrow \{\mathcal{O}\} \\ & & \downarrow \delta & & \downarrow \delta_E & & \downarrow \delta' \\ \{1\} & \longrightarrow & \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} & \longrightarrow & \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} & \longrightarrow & \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \longrightarrow \{1\} \end{array}$$

Rather explicitly, we have the map

$$\delta' : \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \rightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}, \quad (X : Y : 1) \mapsto X - 4892734605697550640 \pmod{(\mathbb{Q}^\times)^2}.$$

As the two rows above are exact sequences, we have the formula

$$2^{r+2} = \left| \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \right| = \left| \delta \left(\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \right) \right| \cdot \left| \delta' \left(\frac{E(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \right) \right|.$$

Hence to compute r it suffices to compute the number of elements in the images of the connecting homomorphisms.

Homogeneous Spaces. We compute the images of the connecting homomorphisms by reducing to the problem of computing rational points on certain quartic curves. It is easy to check that the primes ℓ which divide the discriminant $\Delta(E)$ comprise the set

$$S(k) = \{2, 3, 5, 7, 37, 41, 61, 82207, 87697, 92863\}.$$

By considering the primes which divide k and $\kappa = (1-k)/(1+k)$, respectively, we form the groups

$$\Gamma_k = \left\{ d_1 \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \mid d_1 \equiv \pm \prod_{\ell \in \Sigma(k)} \ell^{e(\ell)} \right\} \quad \Sigma(k) = \{82207, 87697, 92863\};$$

in terms of

$$\Gamma_\kappa = \left\{ d_2 \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \mid d_2 \equiv \pm \prod_{\ell \in \Sigma(\kappa)} \ell^{e(\ell)} \right\} \quad \Sigma(\kappa) = \{2, 3, 5, 7, 37, 41, 61\}.$$

Recall that the connecting homomorphisms have images

$$\begin{aligned} \delta \left(\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \right) &= \left\{ d_1 \in \Gamma_k \mid \begin{array}{l} C_{d_1} : d_1 y^2 = (1 - d_1 x^2)(1 - d_1 k^2 x^2) \\ \text{has a } \mathbb{Q}\text{-rational point } (x, y) \end{array} \right\} \\ \delta' \left(\frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \right) &= \left\{ d_2 \in \Gamma_\kappa \mid \begin{array}{l} C'_{d_2} : d_2 y^2 = (1 + d_2 x^2)(1 + d_2 \kappa^2 x^2) \\ \text{has a } \mathbb{Q}\text{-rational point } (x, y) \end{array} \right\} \end{aligned}$$

Hence to compute r it suffices to find rational points (x, y) on both C_{d_1} and C'_{d_2} . Our goal is to prove the following:

Conjecture: $\delta(E'(\mathbb{Q})) = \{1\}$ and $\delta'(E(\mathbb{Q})) = \langle -1, 6477590, 2, 7, 37 \rangle$.

We do so in two different ways by performing the following steps.

Method #1: Rational Points on Quartic Curves. The goal is to prove the following:

#1. Determine the image $\delta'(E(\mathbb{Q})_{\text{tors}})$ of the torsion subgroup of E . Similarly, determine the image of the subgroup generated by the points P_3 and P_4 .

#2. Following the conjecture above, determine which $d_2 \in \Gamma_\kappa$ should correspond to the point P_5 .

#3. Write code in Maple which searches rational points (x, y) on these homogeneous spaces:

```
p:=Numerator(k); q = Denominator(k);
For integers a and b define
c = sqrt(d*(b^2-d*a^2)*(b^2*q^2-d*q^2*p^2));
If type(c,integer) and gcd(a,b)=1 then
x = a/b; y = c/(d*b^2*q);
Return([x,y]);
fi;
```

#4. Log into `redhawk.hpc.muohio.edu` using username `goinse` and password `sumsri2007`. Type in the following commands to gain information about the quartic curves defining the images above:

```
module load mwrnk
mwrnk -v 5 -p 250 -b 5
[1,0,0,-71813598680248384341084284771096244120,
 234238430204114181370252185964622864112853337413958990400]
```

Search the curve listed after seeing `After minimalizing`, `gg = .` We need to use Michael Stoll's `RatPoints` to find more rational points.

Method #2: Rational Points on Quadric Intersections. We may have to use a different approach to determine the rational points on the quartic curves.

#1. Using d_1 and d_2 as above, we wish to find rational points on the quartic curves

$$d_1 y^2 = (1 - d_1 x^2) (1 - d_1 k^2 x^2) \quad \text{and} \quad d_2 y^2 = (1 + d_2 x^2) (1 + d_2 \kappa^2 x^2).$$

Show that we can express these in terms of the pairs of 4×4 matrices

$$A_1 = \begin{bmatrix} 2d_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \quad \text{and} \quad B_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2d_1 & 0 & 0 \\ 0 & 0 & -2k^2 & k^2 + 1 \\ 0 & 0 & k^2 + 1 & -2 \end{bmatrix}.$$

$$A_2 = \begin{bmatrix} 2d_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \quad \text{and} \quad B_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2d_2 & 0 & 0 \\ 0 & 0 & -2\kappa^2 & -\kappa^2 - 1 \\ 0 & 0 & -\kappa^2 - 1 & -2 \end{bmatrix}.$$

#2. Use MAGMA and the `PointsQI()` command to find rational points on these quadric intersections:

```
k := (t^4-6*t^2+1)/(t^2+1)^2;
kappa := (1-k)/(1+k);
A1 := Matrix( RationalField(), 4, 4,
  [2*d1,0,0,0,0,0,0,0,0,0,-1,0,0,-1,0] );
B1 := Matrix( RationalField(), 4, 4,
  [0,0,0,0,0,2*d1,0,0,0,0,-2*k^2,k^2+1,0,0,k^2+1,-2] );
C := QuadricIntersection( [A1, B1] );
PointsQI(C, 10^5);
```