Distributions of 2-Selmer Ranks for Elliptic Curves: Part 1 of 3

Edray Herber Goins

Department of Mathematics
Purdue University

January 17, 2008

PURDUE
UNIVERSITY

Abstract

Consider the family of all elliptic curves E defined over $\mathbb{Q}$ such that the kernel of the multiplication-by-2-map $[2] : E \to E$ is rational. Galois cohomology asserts that the finite quotient $E(\mathbb{Q})/2\,E(\mathbb{Q})$ may be embedded in the infinite group $H^1(G_{\mathbb{Q}},\ E[2])$ in a canonical way. The latter contains is a "nice" finite subgroup, the 2-Selmer group $\mathrm{Sel}^{(2)}(E/\mathbb{Q})$, which in turn contains the former. Fortunately, there are efficient algorithms to compute the size of this group – even though none really exist to compute the size of the aforementioned quotient.

In this the first of three talks, we review the basics of Galois cohomology by introducing the 2-Selmer group from first principles. We explain how to compute the rank of an elliptic curve by focusing on a certain subfamily of elliptic curves with prescribed torsion. We assume only knowledge of basic Algebraic Number Theory.

Outline of Talk

Elliptic Curves

An elliptic curve E over $\mathbb{Q}$ is a nonsingular projective curve of genus 1 possessing a $\mathbb{Q}$-rational point $\mathcal{O}$.

Such a curve is birationally equivalent over $\mathbb{Q}$ to a cubic equation in Weierstrass form:

$$E: \qquad Y^2 = X^3 + AX + B;$$

with integer coefficients A and B, and nonzero discriminant $\Delta(E) = -16\left(4A^3 + 27B^2\right)$. For any embedding $\mathbb{Q} \hookrightarrow K$, define

$$E(K) = \left\{ (X_1 : X_2 : X_0) \in \mathbb{P}^2(K) \;\middle|\; X_2^2 X_0 = X_1^3 + A X_1 X_0^2 + B X_0^3 \right\};$$

where $\mathcal{O} = (0 : 1 : 0)$ is on the projective line at infinity $X_0 = 0$.

Remark: In practice we will choose either $K = \mathbb{Q}$ or $\mathbb{Q}_\ell$.

Example

Fix a rational number $k \neq -1, 0, 1$ and consider the quartic curve

$$E: \qquad y^2 = \left(1 - x^2\right)\left(1 - k^2\, x^2\right).$$

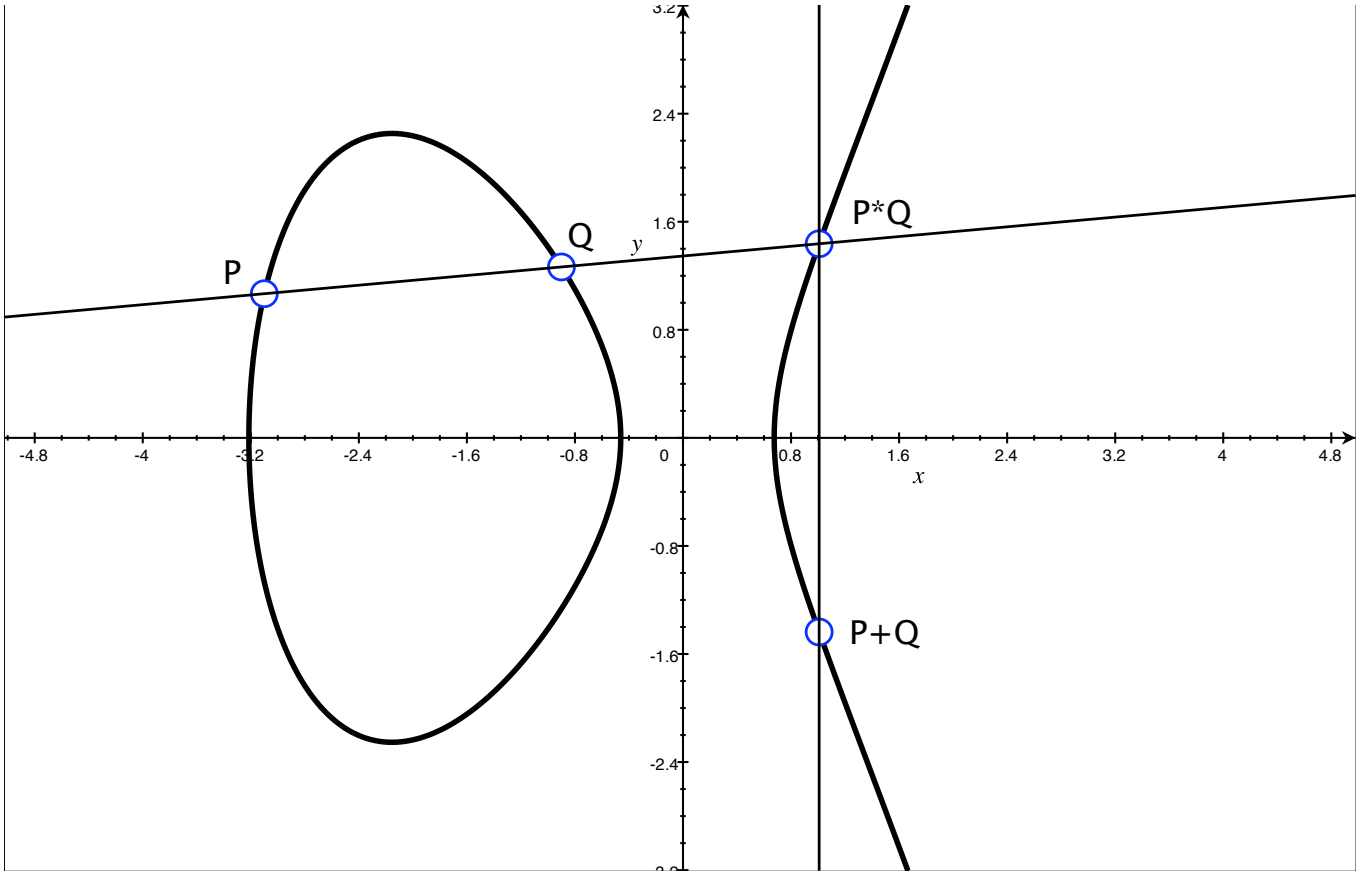
This is an elliptic curve! Write $k = \dfrac{p}{q}$, and consider the transformation

$$\left.\begin{aligned} x &= \frac{X - 3\left(5\,q^2 - p^2\right)}{X - 3\left(5\,p^2 - q^2\right)} \\ y &= \frac{6\left(p^2 - q^2\right) Y}{q\left(X - 3\left(5\,p^2 - q^2\right)\right)^2} \end{aligned}\right\} \quad \leftrightarrow \quad \left\{\begin{aligned} X &= \frac{3\left(5\,p^2 - q^2\right) x - 3\left(5\,q^2 - p^2\right)}{x - 1} \\ Y &= \frac{54\,q\left(p^2 - q^2\right) y}{(x-1)^2} \end{aligned}\right.$$

Then E is birationally equivalent to the Weierstrass equation

$$Y^2 = X^3 + A\,X + B \qquad \text{where} \qquad \begin{aligned} A &= -27\left(p^4 + 14\,p^2\,q^2 + q^4\right), \\ B &= -54\left(p^6 - 33\,p^4\,q^2 - 33\,p^2\,q^4 + q^6\right). \end{aligned}$$

Group Law



Let $P, Q \in E(K)$. Denote $P * Q$ as the point of intersection of E and the line through P and Q, and $P \oplus Q = (P * Q) * \mathcal{O}$. Then $(E(K), \oplus)$ is abelian group with identity $\mathcal{O} = (0 : 1 : 0)$ and inverses $[-1]P = P * \mathcal{O}$.

Mordell-Weil Group

Conjecture (Henri Poincaré, 1901)

Let E be an elliptic curve over $\mathbb{Q}$. Then $(E(\mathbb{Q}), \oplus)$ is a finitely generated abelian group.

Theorem (Louis Mordell, 1922)

Let E be an elliptic curve over $\mathbb{Q}$. There exists a finite group $E(\mathbb{Q})_{\text{tors}}$ and a nonnegative integer r such that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$.

Outline of Proof:

- First show that the quotient $E(\mathbb{Q})/2\,E(\mathbb{Q})$ is finite.
- Then show, using a "Height Machine," that one can lift the generators of the quotient above to bonafide generators of $E(\mathbb{Q})$.

Remark: When the torsion subgroup is $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2n}$, we may write

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

Assumptions

For the remainder of this talk, we place the following assumptions on our elliptic curve

$$E: \qquad Y^2 = X^3 + A\,X + B.$$

- A and B are integers such that $\Delta(E) = -16\left(4\,A^3 + 27\,B^2\right) \neq 0$.
- The roots of the cubic in X are rational. That is,

$$X^3 + A\,X + B = (X - e_1)\,(X - e_2)\,(X - e_3), \qquad e_1,\, e_2,\, e_3 \in \mathbb{Z}.$$

In particular, we assume that the 2-torsion is rational:

$$\begin{aligned} E[2] &= \left\{ T \in E(\overline{\mathbb{Q}}) \;\middle|\; [2]\,T = \mathcal{O} \right\} \\ &= \left\{ (e_1 : 0 : 1),\, (e_2 : 0 : 1),\, (e_3 : 0 : 1),\, (0 : 1 : 0) \right\} \subseteq E(\mathbb{Q}). \end{aligned}$$

Definition

Proposition

With assumptions as above, the following map is a group homomorphism:

$$\delta_E : \quad E(\mathbb{Q}) \to \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}, \qquad (P,\ T) \mapsto (X - e_1,\ X - e_2)\,.$$

Proof: Choose rational points$P = (X_1,\ Y_1)$ and $Q = (X_2\ Y_2)$ on E, and denote $P \oplus Q = (X_3,\ Y_3)$ as their sum. Draw a line through P and Q, say $Y = m\,X + b$, so that we have the polynomial

$$X^3 + A\,X + B - (m\,X + b)^2 = (X - X_1)\,(X - X_2)\,(X - X_3)\,.$$

Upon substituting $X = e_i$ for $i = 1$ or 2, we find the expression

$$(X_3 - e_i) = (X_1 - e_i)\,(X_2 - e_i) \cdot \left(\frac{X_3 - e_i}{m\,e_i + b}\right)^2, \qquad i = 1,\ 2.$$

Hence $\delta_E(P \oplus Q) = \delta_E(P) \cdot \delta_E(Q)$ as desired. □

Kernel

Proposition

The kernel of the connecting homomorphism is $\ker \delta_E = 2\,E(\mathbb{Q})$.

Proof: Say $P \in 2\,E(\mathbb{Q})$. Then $P = [2]\,Q$ for some $Q \in E(\mathbb{Q})$. We have $\delta_E(P) = \delta_E(Q)^2 = 1$ so that $P \in \ker \delta_E$. Hence $2\,E(\mathbb{Q}) \subseteq \ker \delta_E$.

Conversely, say $P \in \ker \delta_E$. It suffices to exhibit $Q \in E(\mathbb{Q})$ such that $P = [2]\,Q$. By assumption, $f_i = \sqrt{X - e_i} \in \mathbb{Q}$ for $i = 1, 2, 3$; we choose the signs so that $Y = f_1\,f_2\,f_3$. It is easy to check that

$$Q = \left(\frac{(e_1 - e_3)\,(e_2 - e_3)}{(f_1 - f_3)\,(f_2 - f_3)} + e_3,\ \frac{(e_1 - e_2)\,(e_1 - e_3)\,(e_2 - e_3)}{(f_1 - f_2)\,(f_1 - f_3)\,(f_2 - f_3)} \right) \in E(\mathbb{Q})$$

satisfies $P = [2]\,Q$, so that $P \in 2\,E(\mathbb{Q})$. Hence $\ker \delta_E \subseteq 2\,E(\mathbb{Q})$. □

In particular, we have an injective group homomorphism

$$\delta_E : \quad \frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \hookrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}.$$

Image

Proposition

The image $\operatorname{im}\delta_E$ is finite.

Sketch of Proof: Say $\delta_E(P) \equiv (d_1, d_2)$ for $d_1,\ d_2 \in \mathbb{Z}$. It suffices to show that d_1 and d_2 each divide the discriminant

$$\Delta(E) = -16\left(4\,A^3 + 27\,B^2\right) = 16\,(e_1 - e_2)^2\,(e_1 - e_3)^2\,(e_2 - e_3)^2\,.$$

There exist relatively prime $u,\ v,\ w,\ t \in \mathbb{Z}$ such that

$$X - e_1 = d_1\left(\frac{u}{t}\right)^2, \qquad X - e_2 = d_2\left(\frac{v}{t}\right)^2, \qquad X - e_3 = d_1\,d_2\left(\frac{w}{t}\right)^2$$

where $d_1\,d_2\,u\,v\,w = t^3\,Y$. Upon eliminating X, we find that

$$d_1\,u^2 - d_2\,v^2 = (e_2 - e_1)\,t^2$$
$$d_1\,u^2 - d_1\,d_2\,w^2 = (e_3 - e_1)\,t^2$$
$$d_2\,v^2 - d_1\,d_2\,w^2 = (e_3 - e_2)\,t^2$$

It is clear that d_1 divides $(e_3 - e_1)$ and d_2 divides $(e_3 - e_2)$. □

Image

Corollary

Continue notation as above, and define the homogeneous spaces

$$C_{(d_1,d_2)}: \begin{array}{c} d_1\,u^2 - d_2\,v^2 = (e_2 - e_1)\,t^2 \\ d_1\,u^2 - d_1\,d_2\,w^2 = (e_3 - e_1)\,t^2, \end{array} \qquad (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}.$$

The image of the connecting homomorphism is

$$\operatorname{im}\delta_E = \left\{ (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \,\middle|\, C_{(d_1,d_2)}(\mathbb{Q}) \neq \emptyset \right\}.$$

Proof: Say $(d_1, d_2) \equiv \delta_E(P)$ is in the image. We saw above that $(u : v : w : t) \in C_{(d_1,d_2)}(\mathbb{Q})$, so that $C_{(d_1,d_2)}(\mathbb{Q}) \neq \emptyset$. Conversely, say that there is a rational point $(u : v : w : t)$ on $C_{(d_1,d_2)}$, and define

$$P = \left(d_1\,u^2\,t + e_1\,t^3 \;:\; d_1\,d_2\,u\,v\,w \;:\; t^3\right).$$

It is easy to see that $P \in E(\mathbb{Q})$, and $\delta_E(P) \equiv (d_1, d_2)$. □

Complete 2-Descent

Recall that if

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

We have just shown

$$\frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \simeq \left\{ (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \,\middle|\, C_{(d_1,d_2)}(\mathbb{Q}) \neq \emptyset \right\}.$$

Hence in order to determine the rank r, we must:

1. Consider pairs (d_1, d_2) of square-free integers which divide
$$\Delta(E) = -16\left(4\,A^3 + 27\,B^2\right) = 16\,(e_1 - e_2)^2\,(e_1 - e_3)^2\,(e_2 - e_3)^2.$$
2. Determine which homogeneous spaces
$$C_{(d_1,d_2)}: \qquad \begin{aligned} d_1\,u^2 - d_2\,v^2 &= (e_2 - e_1)\,t^2 \\ d_1\,u^2 - d_1\,d_2\,w^2 &= (e_3 - e_1)\,t^2 \end{aligned}$$
have a (global) rational point $(u : v : w : t)$.

Selmer and Shafarevich-Tate Groups

With notation as above, we have a finite group which has order 2^{r+2}:

$$\frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \simeq \left\{ (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \,\middle|\, C_{(d_1,d_2)}(\mathbb{Q}) \neq \emptyset \right\}$$

Using the embeddings $\mathbb{Q} \hookrightarrow \mathbb{Q}_\ell$, we have a short exact sequence

$$1 \longrightarrow \frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \xrightarrow{\delta_E} \text{Sel}^{(2)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[2] \longrightarrow 1$$

- The 2-Selmer group which has order 2^{s+2}:

$$\text{Sel}^{(2)}(E/\mathbb{Q}) = \left\{ (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \,\middle|\, \begin{array}{c} C_{(d_1,d_2)}(\mathbb{Q}_\ell) \neq \emptyset \\ \text{for all primes } \ell \end{array} \right\}$$

- The Shafarevich-Tate group which has order 2^{s-r}:

$$Ш(E/\mathbb{Q})[2] = \left\{ (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \,\middle|\, \begin{array}{c} C_{(d_1,d_2)}(\mathbb{Q}_\ell) \neq \emptyset \\ \text{for all primes } \ell \\ \text{yet } C_{(d_1,d_2)}(\mathbb{Q}) = \emptyset \end{array} \right\}$$

Kummer Theory

We can also think of this using Galois cohomology. Consider the "multiplication-by-2" map acting on the points defined over an algebraic closure of $\mathbb{Q}$:

$$0 \longrightarrow E[2] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{[2]} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

Using Galois cohomology, we have the following exact sequence:

$$\begin{array}{ccccc} 0 & \longrightarrow & \dfrac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} & \xrightarrow{\delta_E} & H^1\left(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),\ E[2]\right) \\ & & & & \Big\downarrow \simeq \\ & & & & \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \end{array}$$

This last isomorphism comes about using Kummer Theory. We have chosen to make this map δ_E explicit.

Weil-Châtalet Groups

Using the following exact diagram, the 2-Selmer and Shafarevich-Tate groups may also be defined as kernels of the following vertical maps:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \dfrac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} & \longrightarrow & \mathrm{Sel}^{(2)}(E/\mathbb{Q}) & \longrightarrow & Ш(E/\mathbb{Q})[2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \dfrac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} & \xrightarrow{\delta_E} & H^1\left(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),\ E[2]\right) & \longrightarrow & H^1\left(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),\ E(\overline{\mathbb{Q}})\right)[2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & \longrightarrow & \prod_{\ell} H^1\left(\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell),\ E(\overline{\mathbb{Q}}_\ell)\right) & \longrightarrow & \prod_{\ell} H^1\left(\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell),\ E(\overline{\mathbb{Q}}_\ell)\right) & \longrightarrow & 0
\end{array}$$

Remark: Unfortunately, for either $K = \mathbb{Q}$ or $\mathbb{Q}_\ell$, the Weil-Châtalet groups $WC(E/K) = H^1\left(\mathrm{Gal}(\overline{K}/K),\ E(\overline{K})\right)$ are extremely difficult to compute!

Questions?