CTNT 2024

Connecticut Summer School in Number Theory

Introduction to Elliptic Curves

Álvaro Lozano-Robledo
(University of Connecticut)

Lecture 4

The Rank

Back to Rank:

Ex. $E: y^2+y = x^3-7x+6 \,/\mathbb{Q}$

$E(\mathbb{Q}) = \langle P, Q, R \rangle \cong \mathbb{Z}^3$

$P=(1,0)$, $Q=(2,0)$, $R=(0,2)$

This curve has lots of integral points:

Integral points

$(-3,0), (-3,-1), (-2,3), (-2,-4), (-1,3), (-1,-4), (0,2), (0,-3), (1,0), (1,-1), (2,0), (2,-1), (3,3), (3,-4), (4,6), (4,-7), (8,21), (8,-22), (11,35), (11,-36), (14,51), (14,-52), (21,95), (21,-96), (37,224), (37,-225), (52,374), (52,-375), (93,896), (93,-897), (342,6324), (342,-6325), (406,8180), (406,-8181), (816,23309), (816,-23310)$

Q: $(-3,0) = aP + bQ + cR$, find a, b, c.

Heights

Definition

- $h\left(\frac{m}{n}\right) = \log\left(\max\left(|m|, |n|\right)\right)$ if $\frac{m}{n} \in \mathbb{Q}$ lowest terms
- $E/\mathbb{Q}$, $P \in E(\mathbb{Q})$, $P = (x(P), y(P))$

$$H(P) = h(x(P))$$

- Néron-Tate Canonical Height

$$\hat{h}(P) = \frac{1}{2} \lim_{N \to \infty} \frac{H(2^N \cdot P)}{4^N}$$

PROPERTIES: $E/\mathbb{Q}$, $P \in E(\mathbb{Q})$, $m \geq 1$

- $\hat{h}(mP) = m^2 \hat{h}(P)$
- $\hat{h}(P) \geq 0$
- $\hat{h}(P) = 0 \iff P$ is a torsion pt
- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$

  if $P, Q \in E(\mathbb{Q})$.
- $\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$

  is a non-deg symmetric bilinear form.

$$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

Height Pairing Matrix:

$$\mathcal{H}(\{P_i\}_{i=1}^n) = \begin{pmatrix} \langle P_1, P_1 \rangle & \langle P_1, P_2 \rangle & \cdots \\ \langle P_2, P_1 \rangle & & \ddots \\ \vdots & & \\ & & \langle P_n, P_n \rangle \end{pmatrix}$$

THEOREM

$\det(\mathcal{H}(\{P_i\})) \neq 0$ iff the points $\{P_i\}_{i=1}^n$ are $\mathbb{Z}$-linearly independent.*

(in $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$!)

Ex $E: y^2+y = x^3-7x+6 \ / \mathbb{Q}$

$$E(\mathbb{Q}) = \langle P, Q, R \rangle \cong \mathbb{Z}^3$$

$$P = (1, 0), \ Q = (2, 0), \ R = (0, 2)$$

$$\mathcal{H}(\{P,Q,R\}) = \begin{pmatrix} \langle P,P\rangle & \langle P,Q\rangle & \langle P,R\rangle \\ \langle Q,P\rangle & \langle Q,Q\rangle & \langle Q,R\rangle \\ \langle R,P\rangle & \langle R,Q\rangle & \langle R,R\rangle \end{pmatrix}$$

$\mathcal{H}(\{P,Q,R\}) =$

$$\begin{bmatrix} 0.6682051657 & 0.03333800782 & -0.2365919007 \\ 0.03333800782 & 0.7670433553 & -0.2764342921 \\ -0.2365919007 & -0.2764342921 & 0.9909063331 \end{bmatrix}$$

$\det(\mathcal{H}) = 0.4171435587\ldots \neq 0$

$\Rightarrow \{P,Q,R\}$ are $\mathbb{Z}$-linearly indep.

up to torsion, but here $E(\mathbb{Q})_{tors} = \{O\}$.

So $\mathbb{Z}$-lin. indep.

What about

$\{P, Q, R, T = (-3,0)\}$?

$P = (1,0)$, $Q = (2,0)$, $R = (0,2)$

$\mathcal{H}(\{P,Q,R,T\}) =$

[0.6682051657 0.03333800782 -0.2365919007 -0.7015431735]
[0.03333800782 0.7670433553 -0.2764342921 -0.8003813631]
[-0.2365919007 -0.2764342921 0.9909063331 0.5130261929]
[-0.7015431735 -0.8003813631 0.5130261929 1.501924537]

$\det(\mathcal{H}) = 1.423416106E\text{-}10$ $(\stackrel{??}{=} 0)$

Find $\ker(H) = \langle w \rangle$ with

$w =$

(-0.5773502692 -0.5773502692 -3.201421350E-10 -0.5773502691)

$\frac{w}{(-0.577\ldots)} =$

[1.000000000, 0.9999999998, 2.016372522E-10, 1.000000000]

$\approx (1, 1, 0, 1)$

$\Rightarrow P + Q + T = \text{TORSION POINT} = O \Rightarrow \boxed{T = -(P+Q)}$ ✓

Bounds for the rank ($R_{E/\mathbb{Q}}$)

THEOREM

Let $E/\mathbb{Q}$ be an elliptic curve given by

$$y^2 = x^3 + Cx^2 + Dx \quad , C, D \in \mathbb{Z}.$$

Then

$$R_{E/\mathbb{Q}} \leq \nu(C^2 - 4D) + \nu(D) - 1,$$

where $\nu(N) = \#$ of distinct prime divisors of N.

Ex $y^2 = x(x+1)(x+2) = x^3 + 3x^2 + 2x$

$\Rightarrow R_{E/\mathbb{Q}} \leq \nu(1) + \nu(2) - 1 = 0 \Rightarrow \boxed{R_{E/\mathbb{Q}} = 0}$

Analytic Methods ... BSD.

The Hasse-Weil L-function of $E/\mathbb{Q}$:

$$L(E,s) = \prod_p L_p(E,p^{-s})^{-1} \approx \prod \frac{\#E(\mathbb{F}_p)}{p}$$

where

$$L_p(E,T) = \begin{cases} 1 - a_p \cdot T + p \cdot T^2 & p \text{ of good red'n} \\ 1 - (\pm 1) \cdot T & p \text{ of bad mult. red'n} \begin{pmatrix} \text{split } +1 \\ \text{non } -1 \end{pmatrix} \\ 1 & p \text{ of bad add. red'n} \end{cases}$$

and $a_p = p + 1 - \#E(\mathbb{F}_p)$.

BSD Conjecture

(Birch and Swinnerton-Dyer Conjecture)

Taylor at $s=1$

(1) $$L(E,s) = \lambda_R \cdot (s-1)^R + \lambda_{R+1}(s-1)^{R+1} + \cdots$$

where $R = R_{E/\mathbb{Q}}$.

(2) λ_R = formula that depends on fine invariants of $E/\mathbb{Q}$.

Ex $E: y^2 + y = x^3 - 7x + 6$

```
L:=LSeries(E);
L;
Evaluate(LSeries(E),1);
Evaluate(L, 1 : Derivative:=1);
Evaluate(L, 1 : Derivative:=2);
Evaluate(L, 1 : Derivative:=3);
```

Magma input

Output:

```
L-series of Elliptic Curve defined by y^2 + y = x^3 - 7*x + 6 over Rational
Field
0.00000000000000000000000000000000
4.09505256260772367597929348060E-42
-1.51610735948089545842469279952E-41
10.391099400715804138751850510 4
```

Algebraic methods ... Descent !

(complete 2-descent)

$$E/\mathbb{Q} : y^2 = (x-e_1)(x-e_2)(x-e_3), \quad e_i \in \mathbb{Z}, \; e_i \neq e_j$$

Suppose $P = (x_0, y_0) \in E(\mathbb{Q})$:

$$y_0^2 = (x_0 - e_1)(x_0 - e_2)(x_0 - e_3)$$

then
$$\begin{cases} x_0 - e_1 = a \cdot u^2 \\ x_0 - e_2 = b \cdot v^2 \\ x_0 - e_3 = c \cdot w^2 \end{cases}$$

and $abc = \square = \dfrac{y_0^2}{(uvw)^2}$

Ex $E: y^2 = x^3 - 556x + 3120$

$= (x-6)(x-20)(x+26)$

$e_1 = 6$

$e_2 = 20$

$e_3 = -26$

$P = (-8, 84)$, $Q = (24, 60)$, $S = P + Q = \left(-\frac{247}{16}, -\frac{5733}{64}\right)$

$x(P) - e_1 = -14 \cdot 1^2$

$x(P) - e_2 = -7 \cdot 4^2$

$x(P) - e_3 = 2 \cdot 3^2$

$(-14) \cdot (-7) \cdot 2 = 14^2$

$x(Q) - e_1 = 2 \cdot 3^2$

$x(Q) - e_2 = 2^2$

$x(Q) - e_3 = 2 \cdot 5^2$

$2 \cdot 1 \cdot 2 = 4 = 2^2$

$$\chi(P) - e_1 = -14 \cdot 1^2$$

$$\chi(P) - e_2 = -7 \cdot 4^2$$

$$\chi(P) - e_3 = 2 \cdot 3^2$$

$$(-14) \cdot (-7) \cdot 2 = 14^2$$

$$\chi(Q) - e_1 = 2 \cdot 3^2$$

$$\chi(Q) - e_2 = 2^2$$

$$\chi(Q) - e_3 = 2 \cdot 1^2$$

$$2 \cdot 1 \cdot 2 = 4 = 2^2$$

$S = P + Q$

$$\chi(S) - e_1 = -7 \cdot (7/4)^2$$

$$\chi(S) - e_2 = -7 \cdot (9/4)^2$$

$$\chi(S) - e_3 = \left(\frac{13}{4}\right)^2$$

	P	Q	S
a	-14	2	-7
b	-7	1	-7
c	2	2	1

THEOREM Let $E/\mathbb{Q}$ be an ell. curve

$$y^2 = x^3 + Ax + B = (x-e_1)(x-e_2)(x-e_3) \qquad e_i \neq e_j$$

$$e_1 + e_2 + e_3 = 0$$

There is a gp. hom:

$$\delta : E(\mathbb{Q}) \longrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}$$

s.t. $\delta(P) = \delta((x_0, y_0)) =$

$$\begin{cases} (1,1,1) & \text{if } P = \mathcal{O} \\ (x-e_1,\ x-e_2,\ x-e_3) & \text{if } y_0 \neq 0 \\ ((e_1-e_2)(e_1-e_3),\ e_1-e_2,\ e_1-e_3) & \text{if } P = (e_1, 0) \\ (e_2-e_1,\ (e_2-e_1)(e_2-e_3),\ e_2-e_3) & \text{if } P = (e_2, 0) \\ (e_3-e_1,\ e_3-e_2,\ (e_3-e_1)(e_3-e_2)) & \text{if } P = (e_3, 0) \end{cases}$$

$$\begin{cases} (1,1,1) & \text{if } P = \mathcal{O} \\ (x-e_1,\ x-e_2,\ x-e_3) & \text{if } y_0 \neq 0 \\ ((e_1-e_2)(e_1-e_3),\ e_1-e_2,\ e_1-e_3) & \text{if } P=(e_1,0) \\ (e_2-e_1,\ (e_2-e_1)(e_2-e_3),\ e_2-e_3) & \text{if } P=(e_2,0) \\ (e_3-e_1,\ e_3-e_2,\ (e_3-e_1)(e_3-e_2)) & \text{if } P=(e_3,0) \end{cases}$$

Moreover:

- $\delta(P) = (\delta_1, \delta_2, \delta_3)$ with $\delta_1 \cdot \delta_2 \cdot \delta_3 = 1$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$

- $\ker(\delta) = 2 \cdot E(\mathbb{Q}) = \{2P : P \in E(\mathbb{Q})\}$

Ex $E : y^2 = x^3 - 556x + 3120$

$$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^2$$

$$\langle T_1 = (6,0),\ T_2 = (20,0),\ P = (-8,84),\ Q = (24,60) \rangle$$

$$\delta(T_1) = (-7, -14, 2)$$

$$\delta(T_2) = (14, 161, 46)$$

$$\delta(P) = (-14, -7, 2)$$

$$\delta(Q) = (2, 1, 2)$$

$$\Rightarrow \#\delta\left(\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}\right) = 16$$

PROPOSITION

$\delta_i \in \mathbb{Z}$

If $\delta(P) = (\delta_1, \delta_2, \delta_3)$, $\delta_i \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$

and $p \mid \delta_i$

then $p \mid (e_1-e_2)(e_1-e_3)(e_2-e_3) = \Delta$

Thus

$$\delta : \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \hookrightarrow \Gamma \subseteq \left(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2\right)^3$$

s.t. $\Gamma = \langle (\delta_1, \delta_2, \delta_3) : \delta_i \in \mathbb{Z}$: if $p \mid \delta_i$ then $p \mid \Delta \rangle$

FINITE!!

MOREOVER !!!

$(\delta_1, \delta_2, \delta_3) \in \Gamma$ is in $\mathrm{Image}(\delta)$

:!

$$\begin{cases} y^2 = (x-e_1)(x-e_2)(x-e_3) \\ x-e_1 = \delta_1 u^2 \\ x-e_2 = \delta_2 v^2 \\ x-e_3 = \delta_3 w^2 \end{cases}$$

$\rightsquigarrow$ $\underbrace{C = C(\delta_1, \delta_2)}_{\text{homogeneous space}}$: $\begin{cases} e_1 - e_2 = \delta_2 y^2 - \delta_1 x^2 \\ e_3 - e_2 = \delta_3 y^2 - \delta_1 \delta_2 z^2 \end{cases}$

$$0 \to \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \xrightarrow{\delta} Sel_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0$$

δ : $\subset$ Γ

Spaces $C(S_1, S_2)$ w/ $\mathbb{R}$-points and $\mathbb{Q}_p$-points for all prime p

Spaces $C(S_1, S_2)$ in Sel_2 s.t there are NO $\mathbb{Q}$-points.

Ex $E : y^2 + xy + y = x^3 - 234x + 1352$ (910.a4)

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \hookrightarrow Sel_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0$$

$$1 \quad\quad\quad\quad 1 \quad\quad\quad\quad 1$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad\quad\quad\quad \{0\}$$

$$\Rightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{TWO-TORSION POINT}} \oplus \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{GENERATOR OF INFINITE ORDER}} \to \boxed{\text{RANK}_{/\mathbb{Q}} = 1}$$

Thank

You !