The Birch and Swinnerton-Dyer Conjecture

Joel Fredin

Stockholm University

17 December 2018.

Road map

- Introduce Arithmetic on elliptic curves

Road map

- Introduce Arithmetic on elliptic curves
- Define geometric rank of an elliptic curve

Road map

- Introduce Arithmetic on elliptic curves
- Define geometric rank of an elliptic curve
- Define analytic rank for elliptic curves

Road map

- Introduce Arithmetic on elliptic curves
- Define geometric rank of an elliptic curve
- Define analytic rank for elliptic curves
- **Goal:** Relate the geometric and analytic rank of elliptic curve.

Elliptic Curve

- $E: y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6.$

Elliptic Curve

- $E : y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6$.

Elliptic Curve

- $E : y^2 = x^3 + Ax + B$

Elliptic Curve

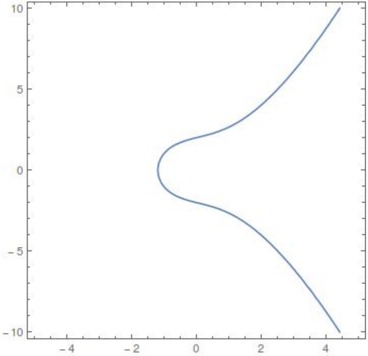
- $E : y^2 = x^3 + Ax + B$
  A and B constants
  x and y variables
  $E/\mathbb{Q} \rightsquigarrow A, B, x, y \in \mathbb{Q}$

Elliptic Curve

- $E : y^2 = x^3 + Ax + B$
  A and B constants
  x and y variables
  $E/\mathbb{Q} \rightsquigarrow A, B, x, y \in \mathbb{Q}$
- $\Delta_E = -16(4A^3 + 27B^2) \neq 0$

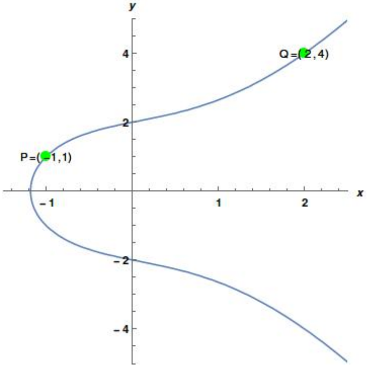
Elliptic Curve

- $E : y^2 = x^3 + Ax + B$
  A and B constants
  x and y variables
  $E/\mathbb{Q} \rightsquigarrow A, B, x, y \in \mathbb{Q}$
- $\Delta_E = -16(4A^3 + 27B^2) \neq 0$
- Geometry
  - Set of rational points on E has a group strcture, $E(\mathbb{Q})$.



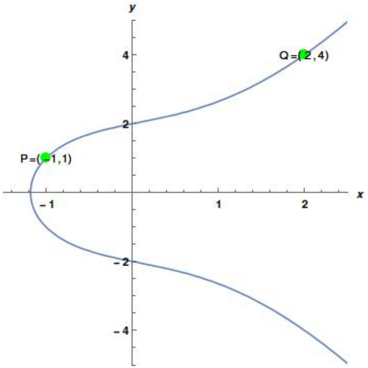
Group Law on Elliptic Curves

$E : y^2 = x^3 + 2x + 4$



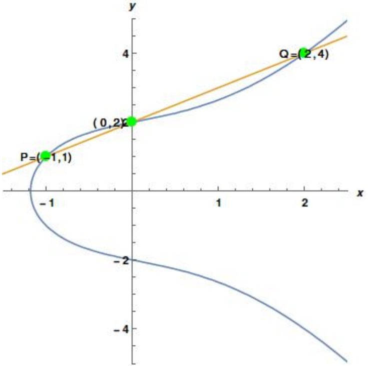
Group Law on Elliptic Curves

$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P + Q = ?$



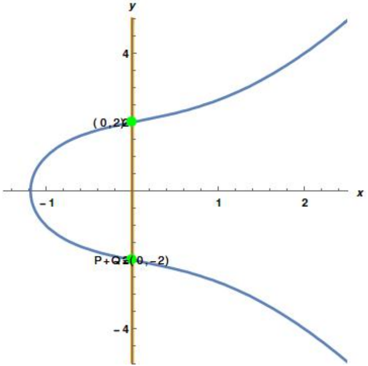
Group Law on Elliptic Curves

$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P + Q = ?$



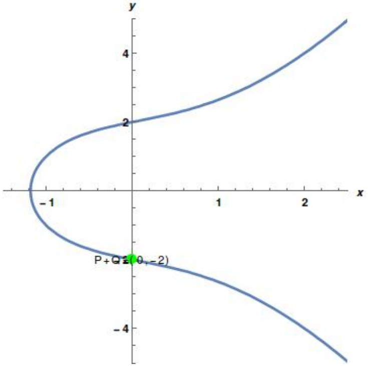
Group Law on Elliptic Curves

$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P + Q = ?$



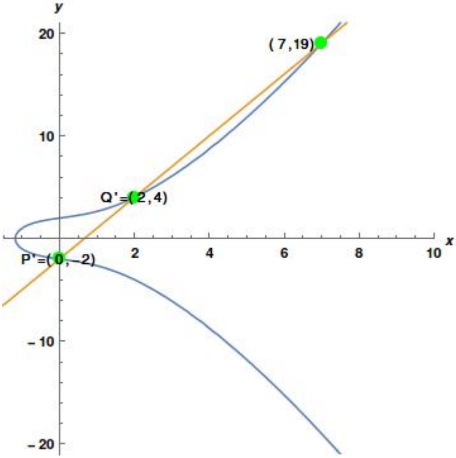
Group Law on Elliptic Curves

$E : y^2 = x^3 + 2x + 4$ $\quad\quad$ $P + Q = (0, -2)!$



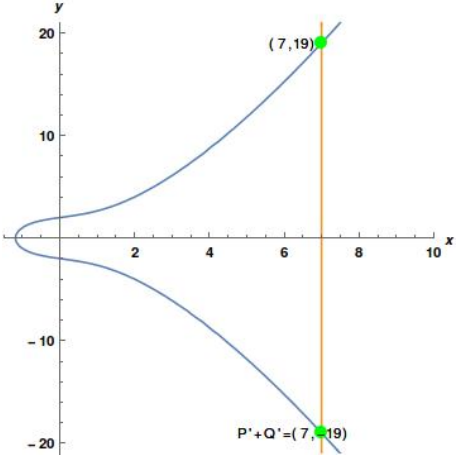
Group Law on Elliptic Curves

$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P' + Q' = ?$

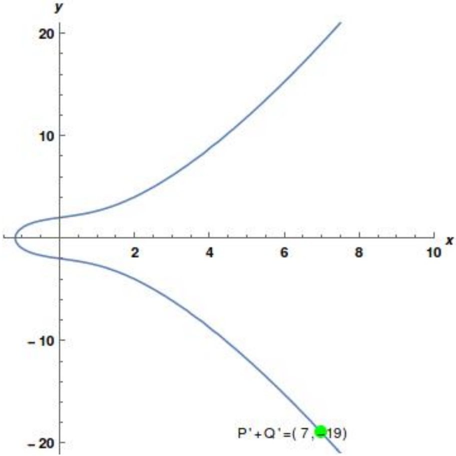


Group Law on Elliptic Curves

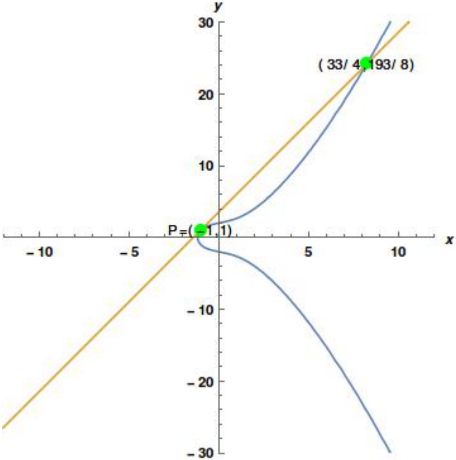
$E : y^2 = x^3 + 2x + 4 \qquad\qquad P' + Q' = ?$



$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P' + Q' = (7, -19)$

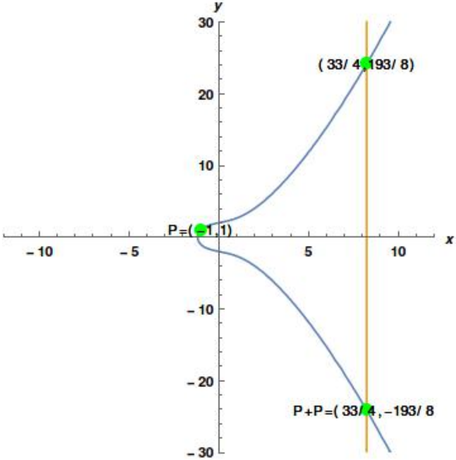


$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P + P = ?$

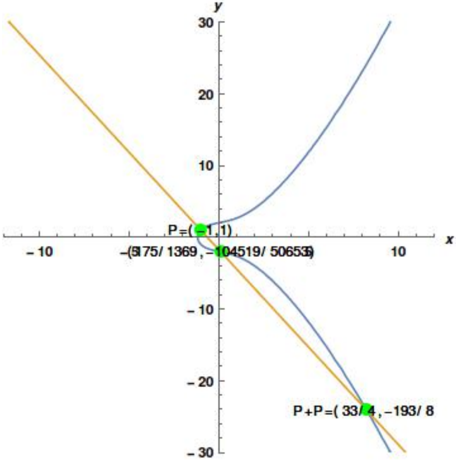


Group Law on Elliptic Curves

$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P + P = \left(\frac{33}{4}, -\frac{193}{8}\right)$

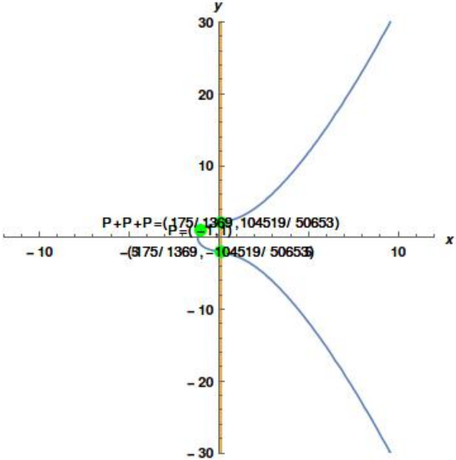


$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P + (P + P) = ?$



Group Law on Elliptic Curves

$E : y^2 = x^3 + 2x + 4$ $\qquad$ $P + (P + P) = \left(\frac{175}{1369}, \frac{104519}{50653}\right)$



Important Definition

Definition

An abelian group G is called finitely generated if there exists elements $x_1, .., x_n \in G$ such that every $x \in G$ can be written as a linear combination of these generators

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

with integers $\alpha_1, ..., \alpha_n$.

$x_1, ..., x_n$ are called generators of G.

Important Definition

Definition

An abelian group G is called finitely generated if there exists elements $x_1, .., x_n \in G$ such that every $x \in G$ can be written as a linear combination of these generators

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

with integers $\alpha_1, ..., \alpha_n$.

$x_1, ..., x_n$ are called generators of G.

$$P = C_1 P_1 + \cdots C_n P_n?$$

Rank of Elliptic Curve

Theorem (Mordell-Weil Theorem)

The group $E(\mathbb{Q})$ is finitely generated.

Rank of Elliptic Curve

Theorem (Mordell-Weil Theorem)

The group $E(\mathbb{Q})$ is finitely generated.

Consequence: $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^{R_g}$!

Theorem (Mordell-Weil Theorem)

The group $E(\mathbb{Q})$ is finitely generated.

Consequence: $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^{R_g}$!

The geometric rank of an elliptic curve E is defined to be the integer R_g.

$R_g(E) = 2$, with $(-1, 1)$ and $(0, 2)$ as linearly independent elements.

$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$.

Analytic rank

- Step 1: Local L-function

Analytic rank

- Step 1: Local L-function
- Step 2: Global L-function

Analytic rank

- Step 1: Local L-function
- Step 2: Global L-function
- Step 3: Analytic Continuation $\rightsquigarrow$ Define analytic rank.

Local L-function

Assume: $p \not| \Delta_E$ ($p \not| -2^8 \cdot 29$ in our example).

Define: $a_p = p + 1 - |E(\mathbb{F}_p)|$.

$$L_p(s, E) = 1 - a_p p + p^{2s-1}$$

$$L_p^*(s, E) = \frac{1}{L_p(s,E)}$$

Local L-function

$E : y^2 = x^3 + 2x + 4 \qquad a_p = p + 1 - |E(\mathbb{F}_p)|$

Example ($p = 3$)

$y^2 \equiv x^3 + 2x + 1 \bmod 3.$

Local L-function

$E : y^2 = x^3 + 2x + 4$ $\qquad a_p = p + 1 - |E(\mathbb{F}_p)|$

Example ($p = 3$)

$y^2 \equiv x^3 + 2x + 1 \bmod 3.$

Solutions: $(0, 1)$, $(0, 2)$, $(1, 1)$, $(1, 2)$, $(2, 1)$ and $(2, 2)$ $\rightsquigarrow |E(\mathbb{F}_3)| = 6.$

Local L-function

$E : y^2 = x^3 + 2x + 4 \qquad a_p = p + 1 - |E(\mathbb{F}_p)|$

Example ($p = 3$)

$y^2 \equiv x^3 + 2x + 1 \bmod 3.$

Solutions: $(0,1)$, $(0,2)$, $(1,1)$, $(1,2)$, $(2,1)$ and $(2,2)$ $\rightsquigarrow$ $|E(\mathbb{F}_3)| = 6.$

$a_3 = 3 + 1 - |E'(\mathbb{F}_3)| = -2.$

Local L-function

$E : y^2 = x^3 + 2x + 4 \qquad a_p = p + 1 - |E(\mathbb{F}_p)|$

Example ($p = 3$)

$y^2 \equiv x^3 + 2x + 1 \bmod 3.$

Solutions: $(0,1)$, $(0,2)$, $(1,1)$, $(1,2)$, $(2,1)$ and $(2,2)$ $\rightsquigarrow |E(\mathbb{F}_3)| = 6.$

$a_3 = 3 + 1 - |E'(\mathbb{F}_3)| = -2.$

$L_3(s, E) = 1 + a_p p + p^{2s-1} = 1 + 6 + 3^{2s-1} = 7 + 3^{2s-1}.$

Local L-function

$E : y^2 = x^3 + 2x + 4 \qquad a_p = p + 1 - |E(\mathbb{F}_p)|$

$$L_3^*(s, E) = \frac{1}{7 + 3^{2s-1}}.$$

Example ($p = 5$)

$y^2 \equiv x^3 + 2x + 4 \bmod 5.$

Local L-function

$$E : y^2 = x^3 + 2x + 4 \qquad a_p = p + 1 - |E(\mathbb{F}_p)|$$

$$L_3^*(s, E) = \frac{1}{7 + 3^{2s-1}}.$$

Example ($p = 5$)

$y^2 \equiv x^3 + 2x + 4 \bmod 5.$

Solutions: $(0, 2)$, $(0, 3)$, $(2, 1)$, $(2, 4)$, $(4, 1)$ and $(4, 4)$ $\rightsquigarrow |E(\mathbb{F}_5)| = 6.$

Local L-function

$$E : y^2 = x^3 + 2x + 4 \qquad a_p = p + 1 - |E(\mathbb{F}_p)|$$

$$L_3^*(s, E) = \frac{1}{7 + 3^{2s-1}}.$$

Example ($p = 5$)

$y^2 \equiv x^3 + 2x + 4 \bmod 5.$

Solutions: $(0, 2)$, $(0, 3)$, $(2, 1)$, $(2, 4)$, $(4, 1)$ and $(4, 4)$ $\rightsquigarrow |E(\mathbb{F}_5)| = 6.$

$a_5 = 5 + 1 - |E(\mathbb{F}_5)| = 0.$

Local L-function

$E : y^2 = x^3 + 2x + 4 \qquad a_p = p + 1 - |E(\mathbb{F}_p)|$

$$L_3^*(s, E) = \frac{1}{7 + 3^{2s-1}}.$$

Example ($p = 5$)

$y^2 \equiv x^3 + 2x + 4 \mod 5.$

Solutions: $(0,2)$, $(0,3)$, $(2,1)$, $(2,4)$, $(4,1)$ and $(4,4)$ $\rightsquigarrow |E(\mathbb{F}_5)| = 6.$

$a_5 = 5 + 1 - |E(\mathbb{F}_5)| = 0.$

$L_3(s, E) = 1 + 0 + 5^{2s-1} = 1 + 5^{2s-1}.$

Global L-function

$$L(s,E) = f(s,E) \prod_{p \nmid \Delta_E} L_p^*(s,E).$$

Global L-function

$$L(s,E) = f(s,E) \cdot \frac{1}{7+3^{2s-1}} \prod_{\substack{p \nmid \Delta_E \\ p \neq 3}} L_p^*(s,E).$$

Global L-function

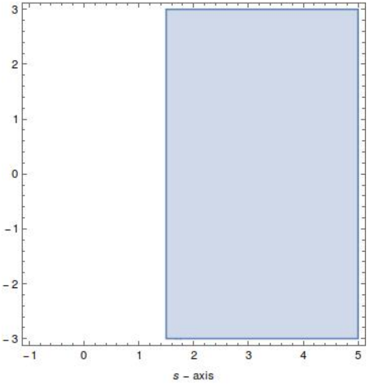
$$L(s, E) = f(s, E) \cdot \frac{1}{7 + 3^{2s-1}} \cdot \frac{1}{1 + 5^{2s-1}} \prod_{\substack{p \nmid \Delta_E \\ p \neq 3,5}} L_p^*(s, E).$$

Local L-function

$$L(s,E) = f(s,E) \cdot \frac{1}{7+3^{2s-1}} \cdot \frac{1}{1+5^{2s-1}} \cdot \frac{1}{8+7^{2s-1}} \prod_{\substack{p \nmid \Delta_E \\ p \neq 3,5,7}} L_p^*(s,E).$$

Woops, problem!

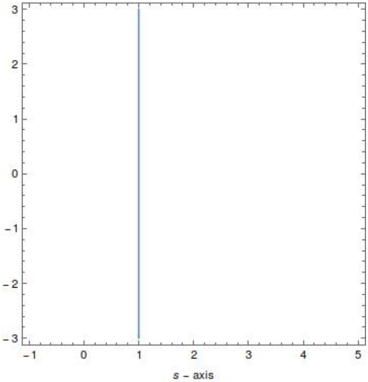
$L(s, E)$ only defined on blue area.



Woops, problem!

What happens at the strip $s = 1$?

Want to evaluate $L(s, E)$ at $s = 1$!



Analytic Continuation

Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$. Then the function $L(s, E)$ has an analytic continuation to the entire complex plane.

Analytic Continuation

Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$. Then the function $L(s, E)$ has an analytic continuation to the entire complex plane.

$$=$$

Theorem (A. Wiles, C. Breuil, B. Conrad, F. Diamond, R. Taylor)

If $E/\mathbb{Q}$ is an elliptic curve. Then E is modular.

$$+$$

Theorem (Hecke)

The L-function of a modular form has an analytic continuation to the entire complex plane.

Conjecture

Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve then,

$L(s, E)$ has a zero at $s = 1$ of order equal to the geometric rank of $E(\mathbb{Q})$.

References

[1] Àlvaro Lozano-Robledo, "*Elliptic Curves, Modular Forms and their L-functions*", American Mathematical Society Institute for Advanced Study, (2011).

[2] Joseph H. Silverman. "*The Arithmetic of Elliptic Curves*" (Second edition). Springer-Verlag, 1986.

[3] Avner Ash, Robert Gross, `"Elliptic Tales: Curves, Counting, and Number Theory"`, Princeton University Press, 2012.

[4] `http://www.lmfdb.org`