The Arithmetic of Elliptic Curves

Luca NOTARNICOLA

PhD Away Days 2017

September, 2017

UNIVERSITÉ DU LUXEMBOURG

Elliptic curve

Definition

An elliptic curve E over a field K of $\mathrm{char}(K) \neq 2, 3$ is a non-singular algebraic plane curve given by an equation of the form

$$Y^2 = X^3 - AX - B \quad ; \; A, B \in K \; .$$

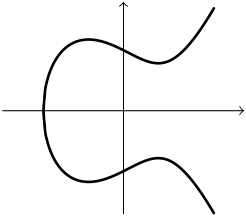
Elliptic curve

Definition

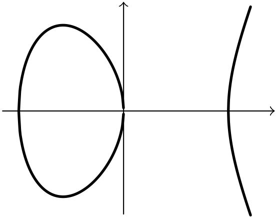
An elliptic curve E over a field K of $\mathrm{char}(K) \neq 2, 3$ is a non-singular algebraic plane curve given by an equation of the form

$$Y^2 = X^3 - AX - B \quad ; \; A, B \in K \; .$$

$E : Y^2 = X^3 - X + 1$



$E : Y^2 = X^3 - 3X$



Elliptic curve

- *Discriminant Δ of E*: discriminant of the cubic polynomial
- E elliptic curve $\iff \Delta \neq 0$
- Homogeneous equation of *projective curve* E in $\mathbf{P}^2(K)$:

$$y^2 z = x^3 - Axz^2 - Bz^3$$

- For $z \neq 0$, $[x : y : z] \in \mathbf{P}^2(K) \longleftrightarrow (X, Y) = (x/z, y/z)$
- Unique point with $z = 0$: *point at infinity* $\mathcal{O} = [0 : 1 : 0]$

Other definition encountered

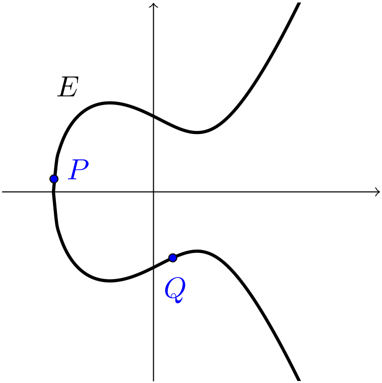
An elliptic curve over a field K is a smooth projective curve of genus 1 together with a distinguished point $\mathcal{O}$.

Group structure

- Elliptic curves define group varieties: The set of points on E is an abelian group for $+$ with neutral element $\mathcal{O}$

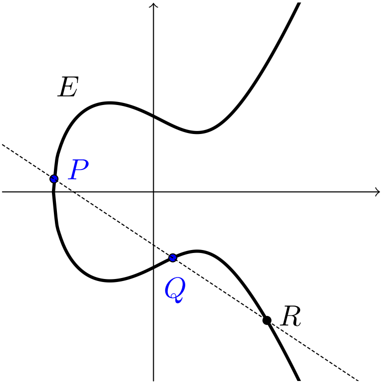
Group structure

- Elliptic curves define group varieties: The set of points on E is an abelian group for $+$ with neutral element $\mathcal{O}$



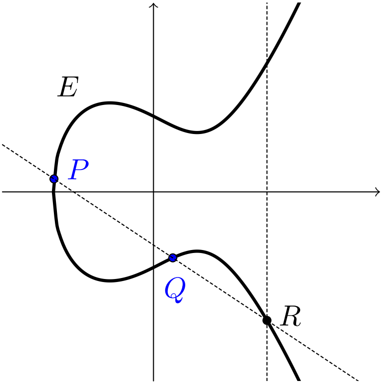
Group structure

- Elliptic curves define group varieties: The set of points on E is an abelian group for $+$ with neutral element $\mathcal{O}$



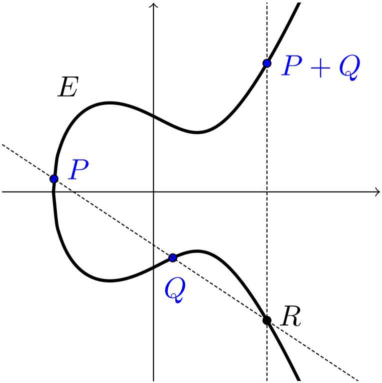
Group structure

- Elliptic curves define group varieties: The set of points on E is an abelian group for $+$ with neutral element $\mathcal{O}$



Group structure

- Elliptic curves define group varieties: The set of points on E is an abelian group for $+$ with neutral element $\mathcal{O}$



Torsion points on elliptic curves

Consider:

- E elliptic curve over $K = \mathbb{Q}$
- $E(\mathbb{Q})$ group of points of E with coordinates in $\mathbb{Q}$

Torsion points on elliptic curves

Consider:

- E elliptic curve over $K = \mathbb{Q}$
- $E(\mathbb{Q})$ group of points of E with coordinates in $\mathbb{Q}$

Definition

For $n \in \mathbb{N}_{\geq 2}$, the n-th torsion group of E is defined by

$$E[n] = \{P \in E(\mathbb{Q}) \ : \ [n]P := \underbrace{P + \ldots + P}_{n \text{ times}} = \mathcal{O}\}$$

Torsion points on elliptic curves

Consider:

- E elliptic curve over $K = \mathbb{Q}$
- $E(\mathbb{Q})$ group of points of E with coordinates in $\mathbb{Q}$

Definition

For $n \in \mathbb{N}_{\geq 2}$, the n-th torsion group of E is defined by

$$E[n] = \{P \in E(\mathbb{Q}) \ : \ [n]P := \underbrace{P + \ldots + P}_{n \text{ times}} = \mathcal{O}\}$$

- Important fact: $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as abelian groups

Elliptic curves and Galois representations

Consider E elliptic curve over $K = \mathbb{Q}$

Elliptic curves and Galois representations

Consider E elliptic curve over $K = \mathbb{Q}$

- $\overline{\mathbb{Q}}$ field of algebraic numbers

Elliptic curves and Galois representations

Consider E elliptic curve over $K = \mathbb{Q}$

- $\overline{\mathbb{Q}}$ field of algebraic numbers
- Galois group of the field extension $\overline{\mathbb{Q}}/\mathbb{Q}$

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}) \ : \ \sigma(x) = x \ , \ \forall x \in \mathbb{Q}\}$$

Elliptic curves and Galois representations

Consider E elliptic curve over $K = \mathbb{Q}$

- $\overline{\mathbb{Q}}$ field of algebraic numbers
- Galois group of the field extension $\overline{\mathbb{Q}}/\mathbb{Q}$

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}) \ : \ \sigma(x) = x \ , \ \forall x \in \mathbb{Q}\}$$

- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Elliptic curves and Galois representations

Consider E elliptic curve over $K = \mathbb{Q}$

- $\overline{\mathbb{Q}}$ field of algebraic numbers
- Galois group of the field extension $\overline{\mathbb{Q}}/\mathbb{Q}$

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}) \ : \ \sigma(x) = x \ , \ \forall x \in \mathbb{Q}\}$$

- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
- Obtain a Galois representation

$$\rho_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

The Tate module

- Consider a prime number ℓ and the projective system

$$\ldots \to E[\ell^n] \to \ldots \to E[\ell^2] \to E[\ell] \tag{1}$$

with transition maps given by $P \mapsto [l]P$

The Tate module

- Consider a prime number ℓ and the projective system

$$\ldots \to E[\ell^n] \to \ldots \to E[\ell^2] \to E[\ell] \tag{1}$$

with transition maps given by $P \mapsto [l]P$

Definition

The Tate module is defined as the projective limit of (1)

$$T_\ell E = \lim_{\leftarrow} E[\ell^n]$$

The Tate module

- Recall the ring of ℓ-adic integers $\mathbb{Z}_\ell$

$$\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$$

- From $E[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ it follows

$$T_\ell E \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $T_\ell E$
- Obtain a Galois representation

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

Elliptic curves over finite fields

Consider an elliptic curve E over $\mathbb{Q}$ given by $Y^2 = X^3 - AX - B$

- Without loss of generality coefficients A, B lie in $\mathbb{Z}$
- Reduction of E modulo prime number q

Elliptic curves over finite fields

Consider an elliptic curve E over $\mathbb{Q}$ given by $Y^2 = X^3 - AX - B$

- Without loss of generality coefficients A, B lie in $\mathbb{Z}$
- Reduction of E modulo prime number q
- Obtain a cubic curve $\hat{E}$ over finite field $\mathbb{F}_q$

Elliptic curves over finite fields

Consider an elliptic curve E over $\mathbb{Q}$ given by $Y^2 = X^3 - AX - B$

- Without loss of generality coefficients A, B lie in $\mathbb{Z}$
- Reduction of E modulo prime number q
- Obtain a cubic curve $\hat{E}$ over finite field $\mathbb{F}_q$ – not necessarily elliptic curve, may have singular points !

Elliptic curves over finite fields

Consider an elliptic curve E over $\mathbb{Q}$ given by $Y^2 = X^3 - AX - B$

- Without loss of generality coefficients A, B lie in $\mathbb{Z}$
- Reduction of E modulo prime number q
- Obtain a cubic curve $\hat{E}$ over finite field $\mathbb{F}_q$ – not necessarily elliptic curve, may have singular points !

Definition

- q is called a good prime if $\hat{E}$ is non-singular
- q is called a bad prime otherwise

Elliptic curves over finite fields

- For good primes $q \neq \ell$, $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ acts on $T_\ell \hat{E}$, ℓ-adic Tate module of E modulo q
- Galois representation $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$
- We define integers $a_q \in \mathbb{Z}$ by the relation

$$|E(\mathbb{F}_q)| = q + 1 - a_q \tag{2}$$

- Theorem (Hasse): $|a_q| \leq 2\sqrt{q}$

The L-series of an elliptic curve

Definition

For $s \in \mathbb{C}$, the L-series of an elliptic curve E is defined by

$$L(E,s) = \prod_{q \text{ good}} \frac{1}{1 - a_q q^{-s} + q^{1-2s}} \prod_{q \text{ bad}} \frac{1}{1 - a_q q^{-s}} = \sum_{n \geq 1} \frac{a_n}{n^s}$$

The L-series of an elliptic curve

Definition

For $s \in \mathbb{C}$, the L-series of an elliptic curve E is defined by

$$L(E,s) = \prod_{q \text{ good}} \frac{1}{1 - a_q q^{-s} + q^{1-2s}} \prod_{q \text{ bad}} \frac{1}{1 - a_q q^{-s}} = \sum_{n \geq 1} \frac{a_n}{n^s}$$

- Compute a_q as follows
  - If q good prime, use (2)
  - If q bad prime, look at the unique singular point P of E modulo q

$$a_q = \begin{cases} \pm 1 & \text{if } P \text{ is an ordinary double point (node)} \\ 0 & \text{if } P \text{ is not an ordinary double point (cusp)} \end{cases}$$

A worked example

Consider $E : y^2 = x^3 + 3$ over $\mathbb{Q}$

- Look for reduction modulo prime q

A worked example

Consider $E : y^2 = x^3 + 3$ over $\mathbb{Q}$

- Look for reduction modulo prime q
- discriminant $\Delta = -3^5 \cdot 2^4 \implies \begin{cases} q \geq 5 & \text{good primes} \\ q = 2, 3 & \text{bad primes} \end{cases}$

A worked example

Consider $E : y^2 = x^3 + 3$ over $\mathbb{Q}$

- Look for reduction modulo prime q
- discriminant $\Delta = -3^5 \cdot 2^4 \implies \begin{cases} q \geq 5 & \text{good primes} \\ q = 2, 3 & \text{bad primes} \end{cases}$
- E modulo 7 defines an elliptic curve $\hat{E}$ over $\mathbb{F}_7$
  - $|\hat{E}(\mathbb{F}_7)| = 13$
  - Compute a_7 using (2): $a_7 = 7 + 1 - 13 = -5$

A worked example

Consider $E : y^2 = x^3 + 3$ over $\mathbb{Q}$

- Look for reduction modulo prime q
- discriminant $\Delta = -3^5 \cdot 2^4 \implies \begin{cases} q \geq 5 & \text{good primes} \\ q = 2, 3 & \text{bad primes} \end{cases}$
- E modulo 7 defines an elliptic curve $\hat{E}$ over $\mathbb{F}_7$
  - $|\hat{E}(\mathbb{F}_7)| = 13$
  - Compute a_7 using (2): $a_7 = 7 + 1 - 13 = -5$
- E modulo 3 given by $y^2 = x^3$ is not an elliptic curve
  - $(0, 0)$ is a cusp $\implies a_3 = 0$

Thank you for your attention.