On Never Primitive points for Elliptic curves

The 8th International Conference on Science and Mathematical Education in Developing Countries

University of Yangon

Myanmar
4th-6th December 2015,

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre
& *Roman Number Theory Association*

Notations

Fields of characteristics 0

1. $\mathbb{Z}$ is the ring of integers
2. $\mathbb{Q}$ is the field of rational numbers
3. $\mathbb{R}$ is the field of real numbers
4. $\mathbb{C}$ is the fields of complex numbers
5. For every prime p, $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ is the prime field;

$$\mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

$\mathbb{Z} \twoheadrightarrow \mathbb{F}_p, n \longmapsto n(\bmod p)$ surjective map

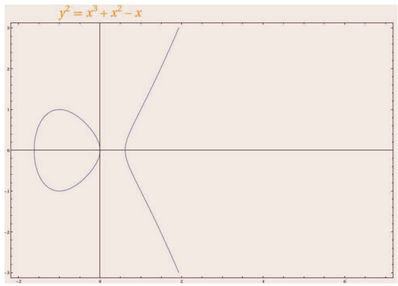
Dip. Matem. & Fisica
Università Roma Tre

The Weierstraß Equation

A Weierstraß equation E over a K (field) is an equation

$$E : y^2 = x^3 + Ax^2 + Bx + C$$

where $A, B, C \in K$



A Weierstraß equation is called **elliptic curve** if it is *non singular*!
(i.e. $4A^3C - A^2B^2 - 18ABC + 4B^3 + 27C^2 \neq 0$)

We consider (most of times) simplified Weierstraß equation $y^2 = x^3 + ax + b$ that are elliptic curves when $4a^3 + 27b^2 \neq 0$

Dip. Matem. & Fisica
Università Roma Tre

The definition of $E(K)$

Let E/K elliptic curve and consider ∞ to be an extra point. Set

$$E(K) = \{(x, y) \in K^2 : y^2 + = x^3 + ax + b\} \cup \{\infty\} \subseteq K^2 \cup \{\infty\}$$

∞ might be though as the "vertical direction"

Definition (line through points $P, Q \in E(K)$)

$$r_{P,Q} : \begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q \end{cases}$$

projective or affine

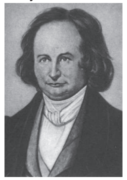
- if $\#(r_{P,Q} \cap E(K)) \geq 2 \Rightarrow \#(r_{P,Q} \cap E(K)) = 3$

  if tangent line, contact point is counted with multiplicity
- $r_{P,Q} : aX + b = 0$ (vertical) $\Rightarrow \infty \in r_{P,Q}$
- $r_{\infty,\infty} \cap E(K) = \{\infty, \infty, \infty\}$

Dip. Matem. & Fisica
Università Roma Tre

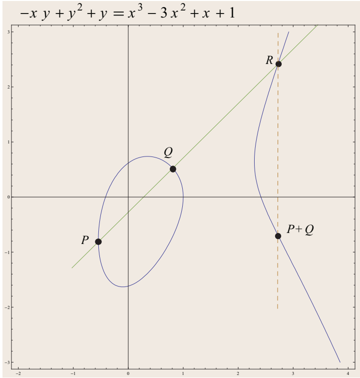
History (from Wikipedia)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$



$r_{P,Q} \cap E(K) = \{P, Q, R\}$
$r_{R,\infty} \cap E(K) = \{\infty, R, R'\}$

$$P +_E Q := R'$$

$r_{P,\infty} \cap E(K) = \{P, \infty, P'\}$

$$-P := P'$$

Properties of the operation "$+_E$"

Theorem

The addition law on $E(K)$ has the following properties:

(a) $P +_E Q \in E(K)$ $\quad \forall P, Q \in E(K)$
(b) $P +_E \infty = \infty +_E P = P$ $\quad \forall P \in E(K)$
(c) $P +_E (-P) = \infty$ $\quad \forall P \in E(K)$
(d) $P +_E (Q +_E R) = (P +_E Q) +_E R$ $\quad \forall P, Q, R \in E(K)$
(e) $P +_E Q = Q +_E P$ $\quad \forall P, Q \in E(K)$

- $(E(K), +_E)$ commutative group
- All group properties are easy except associative law (d)
- Geometric proof of associativity uses *Pappo's Theorem*

Formulas for Addition on E

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

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K) \setminus \{\infty\}$,

Addition Law

- If $P_1 \neq P_2$
  - $x_1 \neq x_2$
    $$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$
  - $x_1 = x_2 \Rightarrow P_1 +_E P_2 = \infty$
- If $P_1 = P_2$
  - $y_1 \neq 0$
    $$\lambda = \frac{3x_1^2 + A}{2y_1}, \nu = -\frac{x_1^3 - Ax_1 - 2B}{2y_1}$$
  - $y_1 = 0 \Rightarrow P_1 +_E P_2 = 2P_1 = \infty$

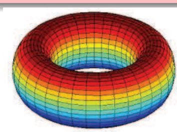
Then

$$P_1 +_E P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu)$$

Elliptic curves over $\mathbb{C}$ and over $\mathbb{R}$

$$E(\mathbb{C}) \cong \mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$$

It is a compact Rieman surface of genus 1



$$E(\mathbb{R}) \cong \begin{cases} \mathbb{R}/\mathbb{Z} \\ \mathbb{R}/\mathbb{Z} \oplus \{\pm 1\} \end{cases}$$

It is a circle or two circles

Elliptic curves over $\mathbb{Q}$

Theorem (Mordell Theorem)

If $E/\mathbb{Q}$ is an elliptic curve, then $\exists r \in \mathbb{N}$ and G and finite abelian group G such that

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus G.$$

In other words, $E(\mathbb{Q})$ is finitely generated.

Theorem (Mazur Torsion Theorem)

If $\mathbb{Z}/n\mathbb{Z}$ denotes the cyclic group of order n, then the possible torsion subgroups

$$G = \mathrm{Tor}(E(\mathbb{Q})) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{with } 1 \leq n \leq 10 \\ \mathbb{Z}/12\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} & \text{with } 1 \leq n \leq 4. \end{cases}$$

It is not known if r (the rank of E) is bounded.

Elliptic curves over $\mathbb{F}_p$

Theorem

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nk\mathbb{Z} \qquad \exists n, k \in \mathbb{N}^{>0}$$

(i.e. $E(\mathbb{F}_p)$ is either cyclic ($n = 1$) or the product of 2 cyclic groups)

Theorem (Weil)

$$n \mid p - 1$$

Theorem (Hasse)

Let E be an elliptic curve over the finite field $\mathbb{F}_p$. Then the order of $E(\mathbb{F}_p)$ satisfies

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

From Elliptic curves over $\mathbb{Q}$ to Elliptic curves over $\mathbb{F}_p$

If $E/\mathbb{Q}$ then $\exists a, b \in \mathbb{Z}$ s.t.:

$$E : y^2 = x^3 + ax + b$$

For all primes $p \nmid 4a^3 + 27b^2$, we can consider *the reduces curve* $\bar{E}/\mathbb{F}_p$:

$$\bar{E} : y^2 = x^3 + \bar{a}x + \bar{b}.$$

where $\bar{a} = a \bmod p$ and $\bar{b} = b \bmod p$.
Given a certain property $\mathbb{P}$ "defined on finite groups", we consider

$$\pi_E(x, \mathbb{P}) = \#\{p \leq x : \bar{E}(\mathbb{F}_p) \text{ satisfies } \mathbb{P}\}.$$

We are interested in studying the behaviour of $\pi_E(x, \mathbb{P})$ and $x \to \infty$ for various properties $\mathbb{P}$.

Lang Trotter Conjecture for *primitive points*

Theorem (Serre's Cyclicity Conjecture under the Riemann Hypothesis (1976))

Let $E/\mathbb{Q}$ be an elliptic curve and assume GRH Then $\exists \gamma_{E,P} \in \mathbb{R}^{\geq 0}$ s.t.

$$\#\{p \leq x : \bar{E}(\mathbb{F}_p) \text{ is cyclic}\} \sim \gamma_{E,P} \frac{x}{\log x} \qquad \text{as } x \to \infty$$

Conjecture (Lang–Trotter primitive points Conjecture (1977))

Let $E/\mathbb{Q}$, $P \in E(\mathbb{Q})$ with infinite order. $\exists \alpha_{E,P} \in \mathbb{R}^{\geq 0}$ s.t.

$$\#\{p \leq x : \bar{E}(\mathbb{F}_p) = \langle P \bmod p \rangle\} \sim \alpha_{E,P} \frac{x}{\log x} \qquad \text{as } x \to \infty$$

For most of the E's:

- If $C = \prod_\ell \left(1 - \frac{1}{\ell(\ell-1)^2(\ell+1)}\right) = 0.81375190610681571\cdots$, then $\gamma_{E,P} = q \cdot C$ with $q \in \mathbb{Q}^{\geq 0}$
- If $B = \prod_\ell \left(1 - \frac{\ell^3-\ell-1}{\ell^2(\ell-1)^2(\ell+1)}\right) = 0.440147366792057866\cdots$, then $\alpha_{E,P} = q' \cdot B$ with $q' \in \mathbb{Q}^{\geq 0}$
- It is possible that $\alpha_{E,P} = 0$ or that $\gamma_{E,P} = 0$
- $\gamma_{E,P} = 0 \iff \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{Q})$
- if $P = kQ$, $Q \in E(\mathbb{Q})$ and $d = \gcd(k, \#\,\mathrm{Tor}(E(\mathbb{Q})) > 1$, then $\alpha_{E,P} = 0$

Comparison between empirical data in Serre's Conjecture and Lang–Trotter Conjecture

Tests on Curves of rank 1, no torsion, Galois surjective $\forall \ell$

$$\pi_P(x) = \#\{p \le x : \langle P \bmod p\rangle = \bar{E}(\mathbb{F}_p^*)\} \qquad \pi_{\mathrm{cycl}}(x) = \#\{p \le x : \bar{E}(\mathbb{F}_p^*) \text{ is cyclic}\}$$

label	$\frac{\pi_P(2^{25})}{\pi(2^{25})}$	$B - \frac{\pi_P(2^{25})}{\pi(2^{25})}$
37.a1	$0.44017485\cdots$	$-0.000027\cdots$
43.a1	$0.44034784\cdots$	$-0.000200\cdots$
53.a1	$0.44020198\cdots$	$-0.000054\cdots$
57.a1	$0.44016176\cdots$	$-0.000014\cdots$
58.a1	$0.44012203\cdots$	$0.000025\cdots$
61.a1	$0.44034299\cdots$	$-0.000195\cdots$
77.a1	$0.43964812\cdots$	$0.000499\cdots$
79.a1	$0.44043021\cdots$	$-0.000282\cdots$

label	$\frac{\pi_{cycl}(2^{25})}{\pi(2^{25})}$	$C - \frac{\pi_{cycl}(2^{25})}{\pi(2^{25})}$
37.a1	$0.81383047\cdots$	$-0.000078\cdots$
43.a1	$0.81363907\cdots$	$0.000112\cdots$
53.a1	$0.81389250\cdots$	$-0.000140\cdots$
57.a1	$0.81387263\cdots$	$-0.000120\cdots$
58.a1	$0.81374131\cdots$	$0.000010\cdots$
61.a1	$0.81397584\cdots$	$-0.000223\cdots$
77.a1	$0.81380285\cdots$	$-0.000050\cdots$
79.a1	$0.81392157\cdots$	$-0.000169\cdots$

The notion of never primitive point

Definition

Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \not\subseteq E(\mathbb{Q})$. A point $P \in E(\mathbb{Q})$ is called a **never primitive** if

- P has infinite order
- for all $\ell \mid \#\,\mathrm{Tor}(E(\mathbb{Q}))$, P is not the ℓ–th power of a rational point $Q \in E(\mathbb{Q})$
- $\langle P \bmod p\rangle \neq \bar{E}(\mathbb{F}_p)$ for all p large enough

- Hence, given p, a *primitive point* P modulo p satisfies $\langle P \bmod p\rangle = \bar{E}(\mathbb{F}_p)$.
- A **never primitive** point never satisfies the above
- if $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{Q})$, no point is ever primitive since $\bar{E}(\mathbb{F}_p)$ is never cyclic
  we avoid such obvious cases
- we are interested in examples of curves with **never primitive points**

Twists with a Never Primitive point

Definition

Given an elliptic curve $E/\mathbb{Q}$ with Weierstraß equation

$$E : y^2 = x^3 + Ax^2 + Bx + C$$

and $D \in \mathbb{Q}^*$, the **twisted curve** E_D of E by D is

$$E_D : y^2 = x^3 + ADx^2 + BD^2x + CD^3.$$

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q})$ contains a point of order 2.
There $\exists\infty D \in \mathbb{Z}$ s.t. the twisted curve E_D is such that $E_D(\mathbb{Q})$ contains a never primitive point.

Every elliptic curve with a point of order 2 can be written in the form:

$$E : y^2 = x^3 + ax^2 + bx \quad \text{with } a^2 - 4b \neq 0$$

Set $D = s(as+2)\left(1 - bs^2\right)$. Then, $\forall s \in \mathbb{Q}$ except possibly when D is a perfect square,

$$P_D\left(\left(1 - bs^2\right)^2, \left(as + 1 + bs^2\right)\left(b - s^2\right)^2\right) \in E_D(\mathbb{Q}) \quad \textbf{is never primitive}.$$

Other parametric families of curves with a never primitive point

Theorem (1 - Jones, Pappalardi)

Let $s \in \mathbb{Q} \setminus \{\pm 1\}$ and let

$$E_s : y^2 = x^3 - 27(s^2 - 1)^2.$$

Then

- $P_s(s^2 + 3, s(s^2 - 9)) \in E(\mathbb{Q}) \setminus \mathrm{Tor}(E(\mathbb{Q}))$
- $\mathrm{Tors}(E_s(\mathbb{Q}))$ is trivial
- P_s is a *never–primitive* point

Theorem (2 - Jones, Pappalardi)

Let $s \in \mathbb{Q} \setminus \{0, \pm 3, \pm\frac{1}{3}\}$, and let

$$E_s : y^2 = x^3 - 3s^2(s^2 - 8)x - 2s^2(s^4 - 12s^2 + 24).$$

Then

- $P_s(2s^2 + 1, 9s^2 - 1) \in E(\mathbb{Q}) \setminus \mathrm{Tor}(E(\mathbb{Q}))$
- $\mathrm{Tors}(E_s(\mathbb{Q}))$ is trivial
- P_s is a *never–primitive* point

Galois Action on the root sets

The construction and its proof is based on the study of the Galois Action on the root-sets of P:

Definition

Given E/Q, $P \in E(\mathbb{Q})$ and $n \in \mathbb{N}$.

$$E[n] := \{Q \in \mathbb{C} : nQ = \infty\}$$

and

$$\frac{1}{n}P := \{Q \in \mathbb{C} : nQ = P\}$$

Remark

Note that

- $E[n]$ is an abelian group
- $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$
- if $R \in E[n]$ and $S \in \frac{1}{n}P$, then $R + S \in \frac{1}{n}P$
- $\frac{1}{n}P$ is a $\mathbb{Z}/n\mathbb{Z}$–affine space.
- $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subset \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$
- $\mathrm{Gal}(\mathbb{Q}(\frac{1}{n}P)/\mathbb{Q}) \subset \mathrm{Aff}(\frac{1}{n}P) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ltimes \mathbb{Z}/n\mathbb{Z}$
- To verify the Theorems one needs to compute the above Galois Groups for each elements of the family under consideration

Dip. Matem. & Fisica
Università Roma Tre

Idea of the proof of Theorem 2

Lemma (1)

Let $E/\mathbb{Q}$ be an elliptic curve, $P \in E(\mathbb{Q}) \setminus \mathrm{Tor}(E(\mathbb{Q}))$ and $\ell \geq 3$ be a prime such that

- P is not an ℓ-th power of a point in $E(\mathbb{Q})$
- $\mathbb{Q}(E[\ell]) = \mathbb{Q}(\zeta_\ell, \alpha^{1/\ell}), \qquad \exists \alpha \in \mathbb{Q}^*$
- $\mathbb{Q}(\frac{1}{\ell}P) \cap \mathbb{R} = \{Q_1, \ldots, Q_\ell\}$
- $\mathbb{Q}(Q_i) = \mathbb{Q}((\alpha^i\beta)^{1/\ell}), i = 1, \ldots, \ell, \qquad \exists \beta \in \mathbb{Q}^*.$

Then $\mathbb{Q}(\frac{1}{\ell}P) = \mathbb{Q}(\zeta_\ell, \alpha^{1/\ell}, \beta^{1/\ell})$ and P is **never primitive**.

The proofs of both Theorems use the previous Lemma with $\ell = 3$

Lemma (2)

Let $s \in \mathbb{Z} \setminus \{0, \pm1, \pm3, \pm13\}$ and consider E_s, the elliptic curve in Theorem 2. Let $\alpha = \sqrt[3]{s(s^2-9)}$ and set $T\left(\frac{1}{3}(s^2 + 4s\alpha + \alpha^2), \frac{4}{3}(\alpha^3 + s\alpha^2 + s^2\alpha)\right) \in E_s(\mathbb{C})$.Then

$$E_s[3] := \left\{\infty, (-s^2, \pm4\sqrt{-3}s)\right\} \cup \{\pm T, \pm T^\sigma, \pm T^\sigma\}$$

where $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ is such that $\sigma(\sqrt[3]{d}) = e^{2\pi i/3}\sqrt[3]{d}\ \forall d \in \mathbb{Q}$. Hence

$$\mathbb{Q}(E_s[3]) = \mathbb{Q}(e^{2\pi i/3}, \sqrt[3]{s(s^2-9)}).$$

Dip. Matem. & Fisica
Università Roma Tre

Idea of the proof of Theorem 2

Lemma (3)

Let $s \in \mathbb{Z} \setminus \{0, \pm1, \pm3, \pm13\}$ and consider E_s, the elliptic curve in Theorem 2. Set

$$\beta = \sqrt[3]{s^2(s+3)}, \qquad \gamma = \sqrt[3]{s^2(s-3)} = \frac{\alpha\beta^2}{s(s+3)}, \qquad \delta = \sqrt[3]{(s-3)^2(s+3)} = \frac{\alpha^2\beta^2}{s^2(s+3)}$$

and $P_\gamma(x_\gamma, y_\gamma)$, $P_\beta(x_\beta, y_\beta)$, $P_\delta(x_\delta, y_\delta)$ dove

$$\begin{aligned} x_\beta &= s(3s-8) + 4(s-1)\beta + 4\beta^2, & y_\beta &= 4(s(3-s)(1-3s) - s(7-3s)\beta - (4-3s)\beta^2) \\ x_\gamma &= s(3s+8) + 4(s+1)\gamma + 4\gamma^2, & y_\gamma &= 4(s(3+s)(1+3s) + s(7+3s)\gamma + (4+3s)\gamma^2) \\ x_\delta &= 3 + (s+1)\delta + \frac{s-1}{s-3}\delta^2, & y_\delta &= s^2 - 9 + (s-3)\delta + \frac{s+3}{s-3}\delta^2. \end{aligned}$$

Then $\mathbb{Q}(P_\gamma) = \mathbb{Q}(\gamma)$, $\mathbb{Q}(P_\beta) = \mathbb{Q}(\beta)$, $\mathbb{Q}(P_\delta) = \mathbb{Q}(\beta)$ and

$$\tfrac{1}{3}P = \left\{P_\beta, P_\beta^\sigma, P_\beta^{\sigma^2}, P_\gamma, P_\gamma^\sigma, P_\gamma^{\sigma^2}, P_\delta, P_\delta^\sigma, P_\delta^{\sigma^2}\right\}.$$

Hence

$$\mathbb{Q}(E_s[3], \frac{1}{3}P) = \mathbb{Q}(e^{2\pi i/3}, \sqrt[3]{s(s^2-9)}, \sqrt[3]{s^2(s-3)}).$$

The result follows from the previous lemmas

Dip. Matem. & Fisica
Università Roma Tre