Critical Points of Toroidal Belyĭ Maps

PRiME 2021: Pomona Research in Mathematics Experience
Project #2: Critical Points of Toroidal Belyĭ Maps

Research Advisor: Dr. Edray Goins
Tesfa Asmara (Pomona College)
Erik Imathiu-Jones (California Institute of Technology)
Maria Maalouf (California State University at Long Beach)
Isaac Robinson (Harvard University)
Sharon Sneha Spaulding (University of Connecticut)

Motivation

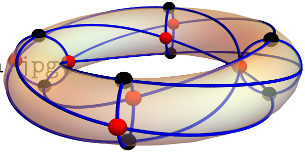
We studied the question of whether or not a set of points on an elliptic curve forms a group for a specific subset of points on an elliptic curve over the complex numbers.

Our Objects of Study:

Elliptic curves over $\mathbb{C}$

graphics/EllipticDessinPlanar8a.jpg

Critical points of Toroidal Belyĭ maps



Question: When do these critical points form a group?

Background

Definition

A group is a pair $(G, \oplus)$ which consists of a non-empty set G and a binary operation $\oplus : G \times G \to G$ such that G contains an identity element O, every element $P \in G$ has an inverse element $[-1]P \in G$, and $\oplus$ is associative. A group is said to be abelian if $\oplus$ is also commutative.

Example: Consider the pair $(Z_n, +)$ where $Z_n = \{0, 1, \ldots, n-1\}$ and $+$ denotes addition modulo n. $(Z_n, +)$ is an abelian group.

Definition

A subset $H \subseteq G$ is said to be a subgroup of G if H forms a group under $\oplus$. More generally, we may consider the subgroup *generated* by the elements of H: this is the smallest subgroup of G containing H.

Proposition 1

Let G be finite group and let $P \in G$. Then the order of P divides the order of G.

Number Fields

Let $\nu \in \mathbb{C}$ be a root of an irreducible polynomial $f(t) = c_n\,T^n + \cdots + c_1\,T + c_0$ with coefficients $c_k \in \mathbb{Q}$.

Denote $K = \mathbb{Q}(\nu)$ as the collection of complex numbers in the form $a_0 + a_1\,\nu + \cdots + a_{n-1}\,\nu^{n-1}$ where $a_k \in \mathbb{Q}$.

- The set K is called a number field.

Say that $s \in \mathbb{C}$ is the root of a irreducible polynomial $g(T) = d_m\,T^m + \cdots + d_1\,T + d_0$ with coefficients $d_k \in K$.

Denote $L = K(s)$ as the collection of complex numbers in the form $b_0 + b_1\,s + \cdots + b_{m-1}\,s^{m-1}$ where $b_k \in K$.

- The set L is called an extension of K; note that L is also a number field.

We define an embedding L into $\mathbb{C}$ fixing K to be that map where we evaluate $s \mapsto s_i$ for some root $s_i \in \mathbb{C}$ of $g(T)$.

- Denote $\mathrm{Emb}(L/K)$ as the collection of embeddings $L \hookrightarrow \mathbb{C}$ fixing K.

Elliptic Curves

Definition

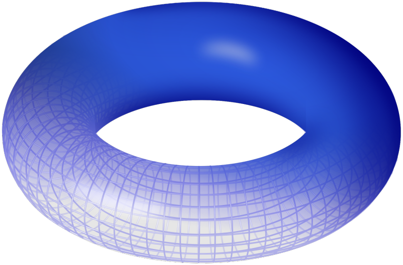
An elliptic curve, E, is a non-singular curve of genus one. In other words, it is a curve generated by an equation $f(x, y) = 0$ where

$$f(x, y) = y^2 + a_1\, x\, y + a_3\, y - (x^3 + a_2\, x^2 + a_4\, x + a_6)$$

and where a_1, a_2, a_3, a_4, a_6 are complex numbers with O_E being the "point at infinity."

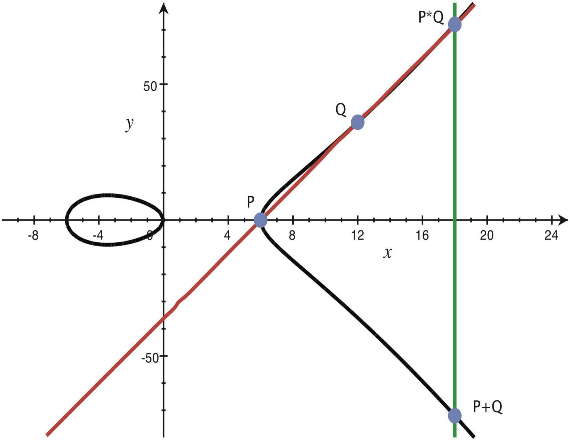
Theorem

The set of complex points on an elliptic curve, $E(\mathbb{C})$, is a torus.



Proposition 2

1. There exists a binary operation $\oplus$ such that $(E(\mathbb{C}), \oplus)$ is an abelian group with identity O_E.
2. Points P, Q, R on $E(\mathbb{C})$ lie on a line if and only if $P \oplus Q \oplus R = O_E$.



Definition

An isogeny $\psi : E(\mathbb{C}) \to X(\mathbb{C})$ is a group homomorphism between two elliptic curves, that is, $\psi(P \oplus Q) = \psi(P) \oplus \psi(Q)$ for $P, Q \in E(\mathbb{C})$.

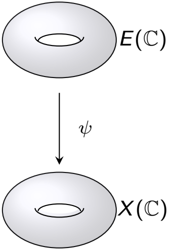


Figure: An isogeny

Proposition 3

Let $\psi : E(\mathbb{C}) \to X(\mathbb{C})$ be a non-constant isogeny. Then ψ is surjective, and $\ker(\psi)$ is a finite subgroup of $E(\mathbb{C})$.

Definition

The order of $P \in E(\mathbb{C})$ is the smallest positive integer n such that $[n]P = O$, where $[n]P$ denotes $P \oplus P \oplus \cdots \oplus P$ for exactly n summands P. A torsion point is a point of finite order. The set of torsion elements for an elliptic curve E over the complex numbers is denoted $E(\mathbb{C})_{\text{tors}}$.

Proposition 4

1. $E(\mathbb{C})_{\text{tors}} \simeq (\mathbb{Q}/\mathbb{Z}) \times (\mathbb{Q}/\mathbb{Z})$.
2. Assume $G \subseteq E(\mathbb{C})_{\text{tors}}$ is a finite subgroup. Then $G \simeq Z_m \times Z_n$ for some positive integers m and n.

Belyĭ Maps

In the following we focus on the sphere and torus $S = \mathbb{P}^1(\mathbb{C})$ and $S = E(\mathbb{C})$, but many of the definitions hold for any compact, connected Riemann surface S.

Definition

- A meromorphic function is a map $\beta : S \to \mathbb{P}^1(\mathbb{C})$ that is a ratio of two polynomials. Denote $\mathcal{K}(S)$ as the collection of all such functions.
- For each point $P = (x_0, y_0)$ in S, denote $\mathcal{O}_P \subseteq \mathcal{K}(S)$ as the collection of meromorphic functions such that $\beta(P) \neq \infty$.
- For any positive integer e, denote

$$M_P{}^e = \left\{ \phi \in \mathcal{O}_P \;\middle|\; \phi(x,y) = g(x,y)f(x,y) + \sum_{i+j=e} p_{ij}(x,y)(x-x_0)^i(y-y_0)^j \right\}$$

  for g, $p_{ij} \in \mathcal{O}_P$. For example, M_P is just the collection of those meromorphic satisfying $\beta(P) = 0$ when $e = 1$.
- Denote the order of β at P as the integer

$$\mathrm{ord}_P(\beta) = \begin{cases} e \geq 0 & \text{if } \beta(P) \neq \infty \text{ and } \beta \in M_P{}^e \text{ but } \beta \notin M_P{}^{e+1}\text{, and} \\ e < 0 & \text{if } \beta(P) = \infty \text{ and } 1/\beta \in M_P{}^{-e} \text{ but } 1/\beta \notin M_P{}^{1-e}. \end{cases}$$

- The ramification index of β at $P \in E(\mathbb{C})$ denoted $e_\beta(P)$ is defined as $e_\beta(P) = \mathrm{ord}_P\,[\beta(x,y) - \beta(P)]$. Order and ramification can also be defined via places and valuations.

Proposition 5

Let S be a compact, connected Riemann surface defined by a polynomial $f(x,y)$. Given meromorphic function $\beta : S \to \mathbb{P}^1(\mathbb{C})$, the ramification index $e_\beta(P) \geq 2$ at a point $P \in S$ if and only if

$$\frac{\partial f}{\partial x}(P)\ \frac{\partial \beta}{\partial y}(P) - \frac{\partial f}{\partial y}(P)\ \frac{\partial \beta}{\partial x}(P) = 0.$$

To see why, note that, for any function $g \in \mathcal{O}_P$, we have a series expansion around $P = (x_0, y_0)$ in the form

$$\left[\beta(x,y) - \beta(P)\right] + \left[g(P)\ \frac{\partial f}{\partial x}(P) - \frac{\partial \beta}{\partial x}(P)\right](x - x_0) + \left[g(P)\ \frac{\partial f}{\partial y}(P) - \frac{\partial \beta}{\partial y}(P)\right](y - y_0)$$

$$= g(x,y) \cdot f(x,y) + \sum_{i+j=2} p_{ij}(x,y) \cdot (x - x_0)^i (y - y_0)^j \in {M_P}^2$$

for some $p_{ij} \in \mathcal{O}_P$. This means $\beta(x,y) - \beta(P) \in {M_P}^2$ if and only if we can find $q = g(P) \in \mathbb{C}$ such that

$$\frac{\partial \beta}{\partial x}(P) = q \cdot \frac{\partial f}{\partial x}(P) \quad \text{and} \quad \frac{\partial \beta}{\partial y}(P) = q \cdot \frac{\partial f}{\partial y}(P) \iff \qquad \frac{\partial \beta}{\partial x}(P)\ \frac{\partial f}{\partial y}(P) - \frac{\partial \beta}{\partial y}(P)\ \frac{\partial f}{\partial x}(P).$$

Definition

- A point $P \in S$ for which the conditions in Proposition 5 hold is called a critical point.
- A critical value $q \in \mathbb{P}^1(\mathbb{C})$ is a number $q = \beta(P)$ for some critical point P.
- A point $Q \in S$ is a quasi-critical point if $\beta(Q) = \beta(P)$ for some critical point P.
- The degree of a meromorphic function $\beta : S \to \mathbb{P}^1(\mathbb{C})$ is the size of the inverse image $\beta^{-1}(\{q\})$ for any $q \in \mathbb{P}^1(\mathbb{C})$ that is not a critical value.

Definition

A Belyĭ pair (S, β) is a Riemann surface S along with a meromorphic function $\beta : S \to \mathbb{P}^1(\mathbb{C})$ with at most three critical values. We can – and do – choose these values to be contained in $\{0, 1, \infty\} \subseteq \mathbb{P}^1(\mathbb{C})$.

Proposition 6

Let S be a compact, connected Riemann surface of genus $g(S)$. Let (S, β) be a Belyĭ pair with critical values contained in $\{0,\ 1,\ \infty\} \subseteq \mathbb{P}^1(\mathbb{C})$ with ramification indices $e_P = e_\beta(P)$ as well as preimages $B = \beta^{-1}(\{0\})$, $W = \beta^{-1}(\{1\})$, and $F = \beta^{-1}(\{\infty\})$. Then the quasi-critical points are contained in the disjoint union $B \cup W \cup F$, and we have the identity

$$\deg(\beta) = \sum_{P \in B} e_P = \sum_{P \in W} e_P = \sum_{P \in F} e_P = |B| + |W| + |F| + \big(2\, g(S) - 2\big).$$

Definition

- A Belyĭ map $\gamma : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is dynamical if $\gamma\big(\{0,1,\infty\}\big) \subseteq \{0,1,\infty\}$.
- A Toroidal Belyĭ pair (E,β) consists of an elliptic curve E and a Belyĭ map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$.
- A Toroidal Belyĭ pair is defined to be imprimitive if it can be written as a non-trivial composition $\beta = \gamma \circ \phi \circ \psi$ for some isogeny $\psi : E(\mathbb{C}) \to X(\mathbb{C})$, meromorphic function $\phi \in \mathcal{K}\big(X(\mathbb{C})\big)$, and dynamical Belyĭ map $\gamma \in \mathcal{K}\big(\mathbb{P}^1(\mathbb{C})\big)$.

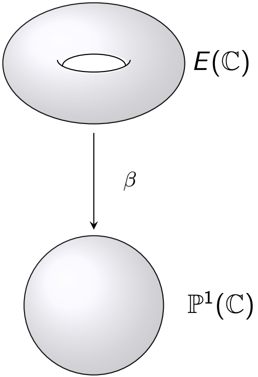


Figure: A Toroidal Belyĭ Map

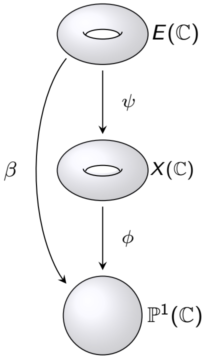


Figure: An imprimitive Toroidal Belyĭ Map

Divisors

Denote either $S = \mathbb{P}^1(\mathbb{C})$ or $S = E(\mathbb{C})$. A divisor is a formal sum

$$D = \sum_{P \in S} n_P(P), \qquad \text{with} \quad n_P \in \mathbb{Z} \quad \text{and all but finitely many } n_P \text{ being zero}$$

The degree of a divisor is the integer $\deg D = \sum_{P \in S} n_P$.

Let $\beta : S \to \mathbb{P}^1(\mathbb{C})$ be a meromorphic function. We can associate to β a divisor of the form

$$\text{div}(\beta) = \sum_{P \in S} n_P\,(P) \qquad \text{where} \qquad n_P = \text{ord}_P(\beta)$$

.

A divisor D is principal if $D = \text{div}(\beta)$ for some meromorphic function β. The degree of a principal divisor is zero.

Proposition 7

Let E be an elliptic curve over $\mathbb{C}$. A divisor $D = \sum_{P \in S} n_P\,(P)$ on $S = E(\mathbb{C})$ is principal if and only if

$$\sum_{P \in S} n_P = 0 \quad \text{in } \mathbb{Z} \qquad \text{and} \qquad \bigoplus_{P \in S} [n_P]P = O_E \quad \text{in } S.$$

Say $\phi : S \to \mathbb{P}^1(\mathbb{C})$ is a meromorphic function. There is a group homomorphism $\phi^* : \mathrm{Div}^0(\mathbb{P}^1(\mathbb{C})) \to \mathrm{Div}^0(S)$, called the pullback of ϕ, which is defined as follows: If $D = \sum_{q \in \mathbb{P}^1(\mathbb{C})} n_q\,(q)$ is a divisor of degree 0 on $\mathbb{P}^1(\mathbb{C})$, then $\phi^* D = \sum_{P \in S} m_P\,(P)$ is a divisor of degree 0 on S, where $m_P = e_\phi(P) \cdot n_{\phi(P)}$.

Proposition 8

For any meromorphic function $\phi : S \to \mathbb{P}^1(\mathbb{C})$ which is not identically zero, we have the pullback

$$\phi^*\left((0) - (\infty)\right) = \sum_{P \in \phi^{-1}(\{0\})} n_P\,(P) \quad - \sum_{P \in \phi^{-1}(\{\infty\})} n_P\,(P) \quad \text{in terms of } n_P = ord_P(\phi).$$

The following proposition shows that divisors behave similarly to logarithms.

Proposition 9

Let $f, g : S \to \mathbb{P}^1(\mathbb{C})$ be meromorphic functions which are not identically zero.

- $\mathrm{div}(f^a \cdot g^b) = a \cdot \mathrm{div}(f) + b \cdot \mathrm{div}(g)$ for any integers a and b.
- $\mathrm{div}(f) = \mathrm{div}(g)$ if and only if $f = k \cdot g$ for some nonzero $k \in \mathbb{C}$.

Remark: The first property is similar to $\log(a \cdot b) = \log(a) + \log(b)$.

Initial Investigations

Main Research Questions

Recall:
For an elliptic curve E we fix a Belyĭ map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$. β is a rational function with at most 3 critical values $\{0, 1, \infty\}$. Denote G to be the set of quasi-critical points (inverse images of the critical values): $G = \beta^{-1}(\{0, 1, \infty\})$.

Motivating Question #1

When does a set of quasi-critical points G form a group?

Remark:
If the set of quasi-critical points G form a group, then the quasi-critical points are torsion.

Motivating Question #2

When are the quasi-critical points torsion?

Example #1: 4T1-4_4_2.2-a

Consider the following Toroidal Belyĭ pair (E, β):

$\beta(x, y) = x^2$ for the elliptic curve E defined by $f(x, y) = y^2 - (x^3 - x)$

- Critical Points: These are the points $P = (x, y)$ which make the following function vanish:

$$\frac{\partial f}{\partial x}(P)\,\frac{\partial \beta}{\partial y}(P) - \frac{\partial f}{\partial y}(P)\,\frac{\partial \beta}{\partial x}(P) = -4xy$$

$$x = 0 \quad \text{or} \quad y = 0$$

  Use the condition $f(x, y) = 0$ to solve for these points:

$$\{(0,0),\ (-1,0),\ (+1,0),\ O_E\}$$

  .

- Quasi-critical points: These are the points which map to critical values.

$$\beta(x,y) = 0 \qquad \{(0,0)\}$$

$$\beta(x,y) = 1 \qquad \{(-1,0),\ (+1,0)\}$$

$$\beta(x,y) = \infty \qquad \{O_E\}$$

  These points are $\beta^{-1}(\{0, 1, \infty\}) = \{(0,0),\ (-1,0),\ (+1,0),\ O_E\}$.

The critical points form a group:

$$\beta^{-1}(\{0, 1, \infty\}) = \{(0,0),\ (-1,0),\ (+1,0),\ O_E\} \simeq Z_2 \times Z_2$$

Recall from the previous slide the Toroidal Belyĭ pair (E, β):

$$\beta(x, y) = x^2 \qquad \text{for the elliptic curve } E \text{ defined by} \qquad f(x, y) = y^2 - (x^3 - x)$$

	O_E	(0,0)	(-1,0)	(+1, 0)
O_E	O_E	(0,0)	(-1,0)	(+1,0)
(0, 0)	(0, 0)	O_E	(+1,0)	(-1,0)
(-1, 0)	(-1, 0)	(+1,0)	O_E	(0,0)
(+1, 0)	(+1, 0)	(-1,0)	(0,0)	O_E

graphics/example1.png

The critical points form a group: $\{O_E, (0,0), (-1,0), (+1,0)\} \simeq Z_2 \times Z_2$

- This is a very pretty example. All the critical points are rational torsion points. However, this is not the case in general.

Consider the following Toroidal Belyĭ pair (E, β):

$$\beta(x,y) = ((x+13)y + 3x^2 + 4x + 220)/432 \qquad E : y^2 + xy = x^3 - 28x + 272$$

Apply the same process outlined in "Example #1" to find:

- Critical Points:

Point	$(-4, 20)$	$(2, -16)$
Order	5	10

- Quasi-critical points:

Point	$(-4, 20)$	$(-13 \pm 3\sqrt{-15},\ 2(37 \pm 3\sqrt{-15}))$	$(2, -16)$	O_E
Order	5	10	10	1

Note:

- The quasi-critical points do not form a group.
- All the quasi-critical points are torsion.
- The quasi-critical points are defined over $\mathbb{Q}(\sqrt{-15}) = \{a + b\sqrt{-15} \mid a,\ b \in \mathbb{Q}\}$.

Example #3: 5T5-5_4.1_4.1-a

Consider the following Toroidal Belyĭ pair (E, β):

$$\beta(x, y) = ((x-5)y+16)/32 \qquad E : y^2 = x^3 + 5x + 10$$

Apply the same process outlined in "Example #1" to find:

- Critical Points:

Point	$(1, -4)$	$(1, 4)$
Order	∞	∞

- Quasi-critical points:

Point	$(1, -4)$	$(1, 4)$	$(6, -16)$	$(6, 16)$	O_E
Order	∞	∞	∞	∞	1

Note:

- The quasi-critical points do not form a group.
- None of the quasi-critical points are torsion.

LMFDB Label	Elliptic Curve X	Belyĭ Map ϕ	Generated Group
3T1-3_3_3-a	$y^2 = x^3 + 1$	$\frac{1-y}{2}$	Z_3
4T1-4_4_2.2-a	$y^2 = x^3 - x$	$1 - x^2$	$Z_2 \times Z_2$
4T5-4_4_3.1-a	$y^2 = x^3 + x^2 + 16x + 180$	$\frac{4y + x^2 + 56}{108}$	Z_8
5T4-5_5_3.1.1-a	$y^2 + xy = x^3 - 28x + 272$	$\frac{(x+13)y + 3x^2 + 4x + 220}{432}$	$Z_2 \times Z_{10}$
6T1-6_2.2.2_3.3-a	$y^2 = x^3 + 1$	$-x^3$	$Z_2 \times Z_6$
6T4-3.3_3.3_3.3-a	$y^2 = x^3 - 15x + 22$	$\frac{8(x-2)^2 - (x^2 - 4x + 7)y}{16(x-2)^2}$	Z_6
6T5-6_6_3.1.1.1-a	$y^2 = x^3 + 1$	$\frac{(1-y)(3+y)}{4}$	$Z_2 \times Z_6$
6T6-6_6_2.2.1.1-a	$y^2 = x^3 + 6x - 7$	$\frac{(x-1)^3}{27}$	$Z_2 \times Z_4$
6T7-4.2_4.2_3.3-a	$y^2 = x^3 - 10731x + 408170$	$\frac{11907(x-49)}{(x-7)^3}$	$Z_2 \times Z_4$
6T12-5.1_5.1_3.3-b	$y^2 + xy + y = x^3 + x^2 - 10x - 10$	$27\,\frac{(x+4)(2x^2 - 2x - 13) - (x+1)^2 y}{(x^2 - x - 11)^3}$	$Z_2 \times Z_8$
6T12-5.1_5.1_5.1-a	$y^2 = x^3 + x^2 + 4x + 4$	$-16\,\frac{(x^2 - 2x - 4)y + 8(x+1)}{(x-4)x^5}$	Z_6
8T2-4.4_4.4_2.2.2.2-a	$y^2 = x^3 + x$	$\frac{(x+1)^4}{8x(x^2+1)}$	$Z_2 \times Z_4$
8T7-8_8_2.2.1.1.1.1-a	$y^2 = x^3 - x$	x^4	$Z_2 \times Z_4$

Main Results

Main Research Questions

- When does a set of quasi-critical points G form a group?
- When are the quasi-critical points torsion?

Theorem (PRiME 2021

Say (E, β) is a Toroidal Belyĭ pair, with $N = \deg(\beta)$, and denote

$$Q_0 = \bigoplus_{P \in \beta^{-1}(\{0\})} [e_P]P = \bigoplus_{P \in \beta^{-1}(\{1\})} [e_P]P = \bigoplus_{P \in \beta^{-1}(\{\infty\})} [e_P]P.$$

Then β can be normalized, that is, there exists $P_0 \in E(\mathbb{C})$ satisfying $[N]P_0 = Q_0$ such that $\beta\big((x, y) \oplus P_0\big) = f(x, y)/g(x, y)$ for two polynomials f, $g \in \mathcal{K}\big(E(\mathbb{C})\big)$ with divisors

$$\begin{aligned} \operatorname{div}(f) &= \sum_{P \in B} e_P\,(P) - N\,(O_E) \\ \operatorname{div}(f - g) &= \sum_{P \in W} e_P\,(P) - N\,(O_E) \\ \operatorname{div}(g) &= \sum_{P \in F} e_P\,(P) - N\,(O_E) \end{aligned} \qquad \text{where} \qquad \begin{aligned} B &= \beta^{-1}(\{0\}) \ominus P_0, \\ W &= \beta^{-1}(\{1\}) \ominus P_0, \\ F &= \beta^{-1}(\{\infty\}) \ominus P_0. \end{aligned}$$

Denote $\phi(x,y) = \beta\big((x,y) \oplus P_0\big)$. Then, observe that $\phi^{-1}(\{q\}) = \beta^{-1}(\{q\}) \ominus P_0$, for any $q \in \mathbb{P}^1(\mathbb{C})$. Recall that $e_P = e_\beta(P) = e_\phi(P \ominus P_0)$. Then, by Proposition 8, we have the principal divisors

$$\operatorname{div}(\phi) = \sum_{P \in B} e_P(P) - \sum_{P \in F} e_P(P)$$

$$\operatorname{div}(\phi - 1) = \sum_{P \in W} e_P(P) - \sum_{P \in F} e_P(P)$$

where

$$B = \beta^{-1}(\{0\}) \ominus P_0 = \phi^{-1}(\{0\}),$$

$$W = \beta^{-1}(\{1\}) \ominus P_0 = \phi^{-1}(\{1\}),$$

$$F = \beta^{-1}(\{\infty\}) \ominus P_0 = \phi^{-1}(\{\infty\}).$$

Then, it follows from Proposition 7 that

$$\left(\bigoplus_{P \in B} [e_P]P\right) \ominus \left(\bigoplus_{P \in F} [e_P]P\right) = \left(\bigoplus_{P \in W} [e_P]P\right) \ominus \left(\bigoplus_{P \in F} [e_P]P\right) = O_E.$$

The statement for Q_0 follows. To show that P_0 exists as claimed, consider the map $\psi : E(\mathbb{C}) \to E(\mathbb{C})$ defined by $\psi(P) = [N]P$. Proposition 3 asserts that ψ is surjective, hence the statement for P_0 follows.

We will show that f, g exist as claimed by showing that $D_1,\ D_2$ are principal divisors, where

$$D_1 = \sum_{P \in B} e_P\,(P) - N\,(O_E) \qquad \text{and} \qquad D_2 = \sum_{P \in F} e_P\,(P) - N\,(O_E)$$

First, consider D_1. Then, by Proposition 6,

$$\deg(D_1) = \sum_{P \in B} e_P \ - N \ = N - N \ = 0$$

And, by the definition of $Q_0 = [N]P_0$,

$$\left(\bigoplus_{P \in B} [e_P]P\right) \oplus [-N]O_E \ = \bigoplus_{P \in \beta^{-1}(\{0\})} [e_P](P \ominus P_0) \ = [N]P_0 \ominus [N]P_0 \ = O_E.$$

It follows from Proposition 7 that there exists $f \in \mathcal{K}\big(E(\mathbb{C})\big)$ such that $\operatorname{div}(f) = D_1$. By a similar argument, there exists $g \in \mathcal{K}\big(E(\mathbb{C})\big)$ such that $\operatorname{div}(g) = D_2$. Now observe that

$$\operatorname{div}(f/g) = \operatorname{div}(f) - \operatorname{div}(g) = \left(\sum_{P \in B} e_P\,(P) - N\,(O_E)\right) - \left(\sum_{P \in F} e_P\,(P) - N\,(O_E)\right) = \operatorname{div}(\phi).$$

Therefore, Proposition 9 asserts that $\phi = k \cdot f/g$, for some constant k. Substituting $k \cdot f$ as f, if necessary, we see that $\phi = f/g$. Consider $\mathrm{div}(f-g)$. Using that $\phi = f/g$, substitute in $f = \phi \cdot g$ to see that

$$\begin{aligned}
\mathrm{div}(f-g) &= \mathrm{div}\big(g \cdot (\phi - 1)\big) \\
&= \mathrm{div}(g) + \mathrm{div}(\phi - 1) \\
&= \left(\sum_{P \in F} e_P\,(P) - N\,(O_E) \right) + \left(\sum_{P \in W} e_P(P) - \sum_{P \in F} e_P(P) \right) \\
&= \sum_{P \in W} e_P\,(P) - N\,(O_E).
\end{aligned}$$

□

Theorem (PRiME 2021)

Say X is an elliptic curve and ϕ a toroidal Belyĭ map, and denote $G = \phi^{-1}(\{0, 1, \infty\})$ as the set of quasi-critical points.

- $\beta = \phi \circ \psi$ yields a Toroidal Belyĭ map on E for any non-constant isogeny ψ.
- $\Gamma = \beta^{-1}(\{0, 1, \infty\})$ is contained in the set of all torsion points in $E(\mathbb{C})$ whenever G is a subset of the set of all torsion points in $X(\mathbb{C})$.
- Γ is a group whenever G is group.

Corollary (PRiME 2021)

There are infinitely many imprimitive Belyĭ pairs where the set of quasi-critical points form a group.

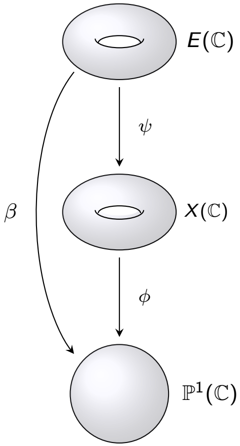


Figure: An imprimitive Toroidal Belyĭ Map

Observe that $\Gamma = \{P \in E(\mathbb{C}) \mid \psi(P) \in G\} = \psi^{-1}(G)$; this will be useful in the proofs.

Lemma 1

(E, β) is a Toroidal Belyĭ pair.

Assume by way of contradiction that $\beta = \phi \circ \psi$ is not a Belyĭ map. By assumption, there exists a point $P \in E(\mathbb{C})$ such that $\beta(P) = q \notin \{0, 1, \infty\}$ is a critical value. Since q is a critical value, $e_\beta(P) \geq 2$. However $e_\beta(P) = e_\phi(\psi(P))$, it follows that $e_\phi(Q) \geq 2$ for some $Q = \psi(P) \in X(\mathbb{C})$. Then Q is a critical point for ϕ with value $q = \beta(P) = \phi(Q)$. Then, ϕ has a critical value $q \notin \{0, 1, \infty\}$, which is a contradiction. Therefore, β is a Belyĭ map.

Lemma 2

If $G \subseteq X(\mathbb{C})_{\text{tors}}$ then $\Gamma \subseteq E(\mathbb{C})_{\text{tors}}$.

Take $Q = \psi(P) \in G$ with $P \in \Gamma$. Since $G \subseteq X(\mathbb{C})_{\text{tors}}$, then there exists a positive integer n such that $[n]Q = O_X$. Since ψ is a group homomorphism, then $[n]Q = [n]\psi(P) = \psi([n]P)$. It follows that $\psi([n]P) = O_X$. Thus, $[n]P \in \ker(\psi)$, which is shown to be finite in Proposition 3. By Proposition 1, there exists a positive integer m such that $[m]R = O_E$ for any $R \in \ker(\psi)$. Denoting $N = mn$, we have $[N]P = [m]\big([n]P\big) = O_E$, showing $P \in E(\mathbb{C})_{\text{tors}}$. Thus, $\Gamma \subseteq E(\mathbb{C})_{\text{tors}}$.

Lemma 3

Suppose $(G, \oplus)$ is a group. Then Γ is a subgroup of $(E(\mathbb{C}), \oplus)$.

To show that Γ is a subgroup of $(E(\mathbb{C}), \oplus)$, we show that (i) Γ is a non-empty set and (ii) that Γ is closed under differences. For (i), $\psi(O_E) = O_X \in G$ because $(G, \oplus)$ is a group and ψ is a group homomorphism, so $O_E \in \psi^{-1}(G) = \Gamma$. For (ii), consider $\psi(P), \psi(Q) \in G$ where $P, Q \in \Gamma$. Since $(G, \oplus)$ is a group, we have $\psi(P \ominus Q) = \psi(P) \ominus \psi(Q) \in G$, which means that $P \ominus Q \in \Gamma$. Thus, Γ is a subgroup of $(E(\mathbb{C}), \oplus)$.

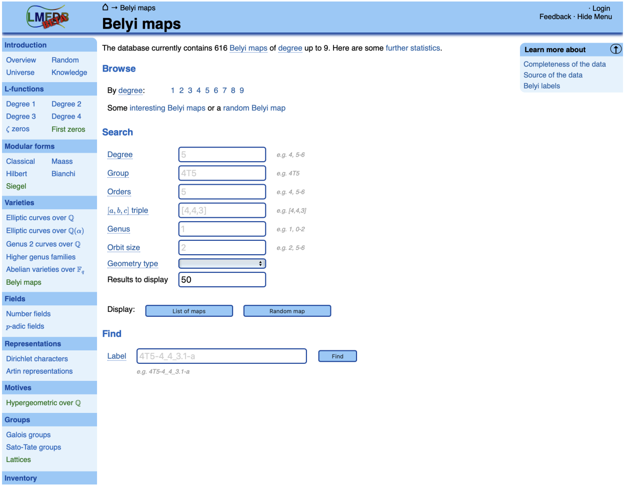
Corollary

There are infinitely many imprimitive Toroidal Belyĭ pairs where the set of quasi-critical points forms a group.

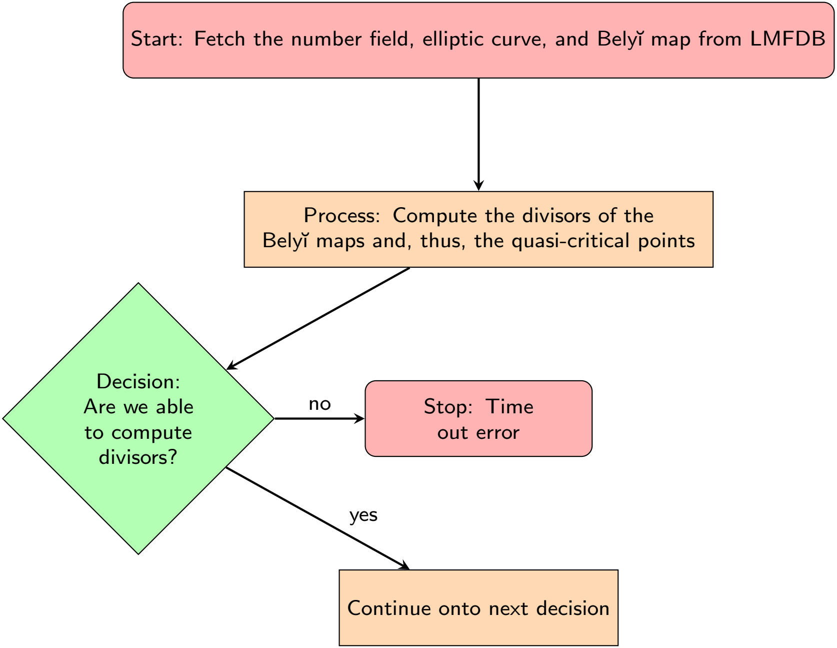
Consider $X : y^2 = x^3 + 1$ and the Belyĭ map $\phi(x, y) = (1 - y)/2$. We have seen that the quasi-critical points, namely $G = \phi^{-1}(\{0,\ 1,\ \infty\}) = \{(0, -1),\ (0, 1),\ O_E\} \simeq Z_3$, forms a group. Our theorem asserts that (E, β) forms a Toroidal Belyĭ pair for any non-constant isogeny $\psi : E(\mathbb{C}) \to X(\mathbb{C})$ where $\Gamma = \beta^{-1}(\{0,\ 1,\ \infty\})$ forms a group. Since there are infinitely such isogenies, the result follows.

Methods

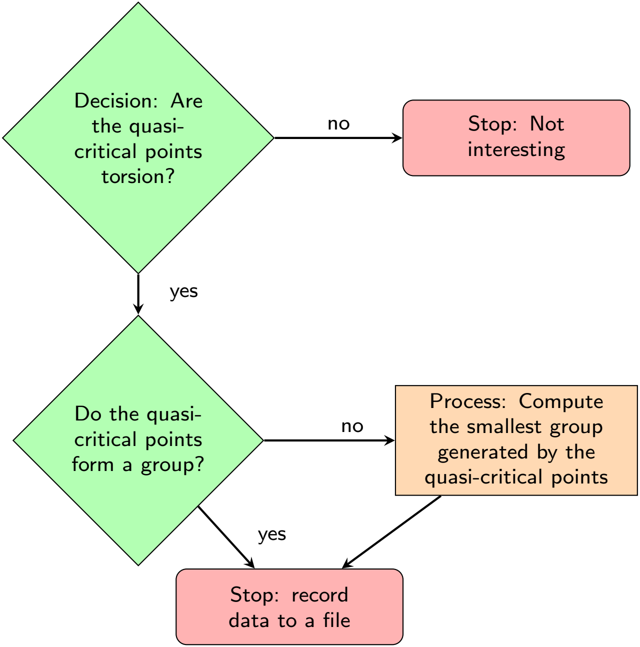
The L-functions and modular forms database (LMFDB)



https://beta.lmfdb.org/Belyi/



Start: Fetch the number field, elliptic curve, and Belyĭ map from LMFDB
Process: Compute the divisors of the Belyĭ maps and, thus, the quasi-critical points
Decision: Are we able to compute divisors?
no
Stop: Time out error
yes
Continue onto next decision


Decision: Are the quasi-critical points torsion?
no
Stop: Not interesting
yes
Do the quasi-critical points form a group?
no
Process: Compute the smallest group generated by the quasi-critical points
yes
Stop: record data to a file

- We input Belyĭ pairs to our program and process if all the quasi-critical points are torsion.
- We hope to process all 251 available Belyĭ pairs.
- Our current program has a bottleneck caused by difficulty in computing field extensions.
- The table below records how many of the available Belyĭ pairs we have successfully processed.

Degree of Belyĭ Pair	Number Of Belyĭ Pairs We Successfully Processed	Number Of Belyĭ Pairs With All The Quasi-Critical Points As Torsion Points
3	1/1	1
4	2/2	2
5	7/7	1
6	29/35	7
7	15/73	0
8	30/94	2
9	23/39	0
All	107/251	13

Future Work

Future Work

- Modify the Sage code so that we can process more examples.
- We have 13 examples where the quasi-critical points are torsion, and we have 1 example that can we explained by our main theorem. We'd like to know if there are more examples, where the quasi-critical points are torsion, that cannot be explained by our main theorem.
- Create a web page where we can host the data found over the summer so that others may see our results.

Thank you for listening!

Special Thanks to:

- Pomona College and everyone who contributed to making PRiME possible this year.
- The NSA for funding our project (NSA H98230-21-1-0015).
- Alex Barrios, Rachel Davis, and the other PRiME students for a productive and inclusive environment. Special thanks to Aurora Hiveley for her invaluable help with our diagrams.
- John Voight for the Toroidal Belyĭ pair data in LMFDB, as well as all the mathematicians who have contributed to LMFDB over the years.
- Our research advisor Edray Goins for leading and guiding us through the preparation and completion of this project.