CRITICAL POINTS OF TOROIDAL BELYĬ MAPS

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)

ABSTRACT. A Belyĭ map $\beta : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is a rational function with at most three critical values; we may assume these values are $\{0,\, 1,\, \infty\}$. Replacing $\mathbb{P}^1$ with an elliptic curve $E:\ y^2 = x^3 + A\,x + B$, there is a similar definition of a Belyĭ map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$. Since $E(\mathbb{C}) \simeq \mathbb{T}^2(\mathbb{R})$ is a torus, we call (E, β) a Toroidal Belyĭ pair. There are many examples of Belyĭ maps $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ associated to elliptic curves; several can be found online at LMFDB. Given such a Toroidal Belyĭ map of degree N, the inverse image $G = \beta^{-1}\big(\{0,\, 1,\, \infty\}\big)$ is a set of N elements which contains the critical points of the Belyĭ map. In this project, we investigate when G is contained in $E(\mathbb{C})_{\text{tors}}$. This is work done as part of the Pomona Research in Mathematics Experience (NSA H98230-21-1-0015).

1. INTRODUCTION

Let S be a compact, connected Riemann Surface. For example, $S = \mathbb{P}^1(\mathbb{C}) \simeq S^2(\mathbb{R})$ may be the Riemann Sphere, or $S = E(\mathbb{C}) \simeq (\mathbb{R}/\mathbb{Z})\times(\mathbb{R}/\mathbb{Z})$ may be a torus associated to an elliptic curve E. It is well-known that S is a curve, that is, can be defined by a single equation $f(x, y) = 0$ for some polynomial $f(x, y) = \sum_{ij} a_{ij}\, x^i\, y^j$ having complex coefficients a_{ij}. André Weil proved in 1956 that one can choose these coefficients to lie in a number field if there exists a meromorphic function $\beta : S \to \mathbb{P}^1(\mathbb{C})$ with at most three critical values; Gennadiĭ Vladimirovich Belyĭ proved the converse to this in 1979. For this reason, we call β a Belyĭ map. One can always choose the critical values of a Belyĭ map $\beta : S \to \mathbb{P}^1(\mathbb{C})$ to lie in $\{0,\, 1,\, \infty\} \subseteq \mathbb{P}^1(\mathbb{C})$. We denote $\Gamma = \beta^{-1}\big(\{0,\, 1,\, \infty\}\big) \subseteq S$ as the quasi-critical points of β.

There are many examples of Belyĭ maps $\beta : S \to \mathbb{P}^1(\mathbb{C})$ associated to a Riemann surface S. Several can be found online at the L-Series and Modular Forms Database (LMFDB). In this work, we are primarily interested in Belyĭ maps associated to elliptic curves: we call (E, β) a Toroidal Belyĭ pair. We consider how the quasi-critical points $\Gamma \subseteq E(\mathbb{C})$ of a Toroidal Belyĭ pair (E, β) interact with the Group Law $\oplus$ on an elliptic curve. As a motivating example, consider the elliptic curve $E : y^2 = x^3 + 1$ and the Belyĭ map $\beta(x, y) = (1 - y)/2$. The set of quasi-critical points is $\Gamma = \{(0, 1),\, (0, -1),\, O_E\} \simeq Z_3$, a subgroup of $S = E(\mathbb{C})$.

We are motivated by two primary research questions. Given a Toroidal Belyĭ pair (E, β), when does its set of quasi-critical points Γ form a subgroup of $(E(\mathbb{C}), \oplus)$? If Γ is a group, then its elements must have finite order. When are the quasi-critical points torsion elements in $E(\mathbb{C})$ – regardless of Γ being a group? Our main results are as follows.

Theorem. *Say (X, ϕ) is a Toroidal Belyĭ pair, and denote $G = \phi^{-1}\big(\{0,\, 1,\, \infty\}\big)$ as the set of quasi-critical points. Take $\beta = \phi \circ \psi$, where $\psi : E \to X$ is any non-constant isogeny, and denote $\Gamma = \beta^{-1}\big(\{0,\, 1,\, \infty\}\big)$.*

(1) (E, β) is a Toroidal Belyĭ pair.
(2) Γ is contained in the torsion in $E(\mathbb{C})$ whenever G is contained in the torsion in $X(\mathbb{C})$.
(3) Γ is a group whenever G is group.

As a direct consequence, we find the following.

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

Date: December 19, 2022.

We would like to thank our research advisor Edray Goins for leading and guiding us throughout the preparation and completion of this project. We would also like to acknowledge Alex Barrios, Rachel Davis, and the other PRiME students for a productive and inclusive environment, John Voight for the Toroidal Belyĭ pair data in LMFDB, and all the mathematicians who have contributed to LMFDB over the years. We would also like to thank the NSA for funding our project (H98230-21-1-0015).

2. Background and Notation

We begin by introducing definitions and known results relevant for our main research questions.

2.1. **Groups.** 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. As an example of an abelian group, consider the pair $(Z_n, +)$ where $Z_n = \{0, 1, \ldots, n-1\}$ and $+$ denotes addition modulo n.

The order of a group is the number of elements in G. A group is said to be finite if the set G is finite. The order of $P \in G$ 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. If no such n exists, then an element is said to have infinite order. Otherwise, an element has finite order and is called a torsion element.

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.

We may also define maps between groups. Given two groups $(G, \oplus)$ and $(\Gamma, \star)$, a group homomorphism is a map $\psi : G \to \Gamma$ such that $\psi(P \oplus Q) = \psi(P) \star \psi(Q)$ for $P, Q \in G$. The kernel, denoted $\ker(\psi)$, is the set $P \in G$ such that $\psi(P) = O_\Gamma$ where O_Γ is the identity element in Γ; this is a subgroup of G. If $\psi : G \to \Gamma$ is a group homomorphism for which $\ker(\psi) = \{O_\Gamma\}$ and ψ is surjective, ψ is said to be an isomorphism between G and Γ. In this case, we denote $G \simeq \Gamma$.

The following proposition provides a group theoretic result relevant to this paper.

Proposition 1. *Let G be finite group and let $P \in G$. Then the order of P divides the order of G.*

2.2. **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 $c_k \in \mathbb{Q}$. We 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 $d_k \in K$. We 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 $g(T)$. We denote $\mathrm{Emb}(L/K)$ as the collection of embeddings $L \hookrightarrow \mathbb{C}$ fixing K. (For those who know about Galois groups, we can write $\mathrm{Emb}(L/K) = \mathrm{Gal}\big(\overline{\mathbb{Q}}/L\big)/\mathrm{Gal}\big(\overline{\mathbb{Q}}/K\big)$ as a collection of cosets.)

2.3. **Riemann Sphere.** We define the extended complex line, denoted by $\mathbb{P}^1(\mathbb{C})$, as the set of complex numbers together with infinity; recall that there is a one-to-one correspondence between the points on the extended complex line and the points on the unit sphere $S^2(\mathbb{R})$. For this reason, we often call $\mathbb{P}^1(\mathbb{C}) \simeq S^2(\mathbb{R})$ the Riemann Sphere. It will be useful for us to view $\mathbb{P}^1(\mathbb{C})$ as a non-singular curve of genus 0, that is, the collection of complex points $P = (x, y)$ satisfying $f(x, y) = 0$, where $f(x, y) = y$.

2.4. **Elliptic Curves.** We will now outline some of the general theory of elliptic curves relevant for this paper. An elliptic curve, denoted by 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, and a_6 are complex numbers. We denote $E(\mathbb{C})$ to be the collection of complex points $P = (x, y)$ on E augmented by a "point at infinity" O_E. For more details, see [ST92, Chapter I.4, page 28].

Proposition 2. *Let E be an elliptic curve over $\mathbb{C}$.*

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 $P \oplus Q \oplus R = O_E$.*

For details on the Chord-Tangent method, see [ST92, Chapter I.4]. For details on the collinearity property, see [Sil09, Chapter III.2, Proposition 2.2, pages 51-52].

Similar to homomorphisms between two groups, 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 $P, Q \in E(\mathbb{C})$.

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 $E(\mathbb{C})$.*

For details, see [Sil09, Chapter IV, Corollary 4.9] and [Sil09, Chapter 2, Theorem 2.3].

Since we consider the points of an elliptic curve as forming a group, we define the order of a point $P \in E(\mathbb{C})$ in the same way as we previously defined the order of a group element $P \in G$. In the same way, we define a torsion point as 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. *Let E be an elliptic curve over $\mathbb{C}$.*

(1) $E(\mathbb{C}) \simeq (\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z})$. In particular, this set of complex points forms a torus.
(2) $E(\mathbb{C})_{tors} \simeq (\mathbb{Q}/\mathbb{Z}) \times (\mathbb{Q}/\mathbb{Z})$.
(3) Assume $G \subseteq E(\mathbb{C})_{tors}$ is a finite subgroup. Then $G \simeq Z_m \times Z_n$ for some positive integers m and n.

For details, see [Sil09, Chapter VI.5, Corollary 5.1.1, page 173].

2.5. **Belyĭ Maps.** Denote either $S = E(\mathbb{C})$ or $S = \mathbb{P}^1(\mathbb{C})$. Note that in either case, S is a curve generated by an equation $f(x, y) = 0$ for some polynomial $f(x, y)$. (In the projects discussed in this exposition, we will focus on the sphere and the torus, but many of the definitions hold for any compact, connected Riemann surface S. It is well-known that such surfaces may be identified as a curve, that is, generated by an equation $f(x, y) = 0$ for some polynomial $f(x, y)$.)

A meromorphic function is a map $\beta : S \to \mathbb{P}^1(\mathbb{C})$ that is a ratio of two polynomials; denote the function field $\mathcal{K}(S)$ 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

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

For example, M_P is just the collection of those meromorphic satisfying $\beta(P) = 0$. Denote the order of β at P as the integer

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

The ramification index of β at $P \in E(\mathbb{C})$ denoted $e_\beta(P)$ is defined as $e_\beta(P) = \text{ord}_P\left[\beta(x, y) - \beta(P)\right]$. (Order and ramification can also be defined via places and valuations; for further details see [GG12, Chapter 3.4].)

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

$$\frac{\partial \beta}{\partial x}(P) = q \cdot \frac{\partial f}{\partial x}(P) \quad \text{and} \quad \frac{\partial \beta}{\partial y}(P) = q \cdot \frac{\partial f}{\partial y}(P) \qquad \Longleftrightarrow \qquad \frac{\partial \beta}{\partial x}(P)\ \frac{\partial f}{\partial y}(P) - \frac{\partial \beta}{\partial y}(P)\ \frac{\partial f}{\partial x}(P) = 0.$$

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.

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 $\{0, 1, \infty\} \subseteq \mathbb{P}^1(\mathbb{C})$. There are two types of Belyĭ pairs which we are specifically interested in for this exposition. 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 $\gamma \in \mathcal{K}\big(\mathbb{P}^1(\mathbb{C})\big)$.

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*

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

For details see [Sil09, Proposition 2.6, Chapter II.2, page 24].

2.6. **Divisors.** Continue to denote either $S = \mathbb{P}^1(\mathbb{C})$ or $S = E(\mathbb{C})$, although many of the definitions which follow hold for any compact, connected Riemann surface S.

A divisor is a formal sum $D = \sum_{P \in S} n_P(P)$, with $n_P \in \mathbb{Z}$ and all but finitely many being zero. The degree of a divisor is the integer $\deg D = \sum_{P \in S} n_P$. Denote the collection of degree 0 divisors as $\mathrm{Div}^0(S)$. Observe that $(\mathrm{Div}^0(S), +)$ is an abelian group under addition. Indeed, given two divisors $D_1 = \sum_{P \in S} c_P\,(P)$ and $D_2 = \sum_{P \in S} d_P\,(P)$ as well as integers a and b, define $a\,D_1 + b\,D_2 = \sum_{P \in S} n_P\,(P)$ in terms of the integers $n_P = a\,c_P + b\,d_P$. For details, see [Sil09, Chapter II.3, page 27].

Let $\beta : S \to \mathbb{P}^1(\mathbb{C})$ be a meromorphic function which is not identically zero. We can associate to β a divisor of the form $\mathrm{div}(\beta) = \sum_{P \in S} n_P\,(P)$ where $n_P = \mathrm{ord}_P(\beta)$. A divisor D is principal if $D = \mathrm{div}(\beta)$ for some meromorphic function β. The degree of a principal divisor is zero, and the collection of principal divisors forms a subgroup of $\mathrm{Div}^0(S)$.

Divisors on elliptic curves are intimately related to the group law.

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

For details, see [Sil09, Chapter III.3, Corollary 3.5, page 63]

Say $\phi : S \to \mathbb{P}^1(\mathbb{C})$ is a meromorphic function which is not identically zero. There is a group homomorphism $\phi^* : \mathrm{Div}^0\big(\mathbb{P}^1(\mathbb{C})\big) \to \mathrm{Div}^0(S)$, 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. *Denote either $S = \mathbb{P}^1(\mathbb{C})$ or $S = E(\mathbb{C})$.*

(1) Assume that $D = div(\gamma)$ is a principal divisor on $\mathbb{P}^1(\mathbb{C})$. Then $\phi^* D = div(\beta)$ is a principal divisor on S where $\beta = \gamma \circ \phi$.

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

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

For more details, see [Sil09, Chapter II.3, Proposition 3.6, page 29] and [Sil09, Chapter II.3, Example 3.5, page 29]. The following proposition shows that divisors behave similarly to logarithms.

Proposition 9. *Let $\beta_1,\, \beta_2 : S \to \mathbb{P}^1(\mathbb{C})$ be meromorphic functions which are not identically zero.*

(1) $div(\beta_1^a \cdot \beta_2^b) = a \cdot div(\beta_1) + b \cdot div(\beta_2)$ for any integers a and b.

(2) $div(\beta_1) = div(\beta_2)$ if and only if $\beta_1 = k \cdot \beta_2$ for some nonzero $k \in \mathbb{C}$.

For more details, see [Sil09, Chapter II.3, Proposition 3.1, page 28].

3. Initial Investigations

3.1. **Motivating Examples and Questions.** Given a Belyĭ map on an elliptic curve, we can look at its quasi-critical points. We can look at how the quasi-critical points interact with the elliptic curve group law. To get a better idea of this, let us look at a couple of examples.

Consider the Toroidal Belyĭ pair (E, β) with E the curve defined by $f(x, y) = y^2 - (x^3 + 1)$ and $\beta(x, y) = (1-y)/2$. We can compute the critical points $P = (x, y)$ of β by finding when the following function vanishes: $(\partial f/\partial x)\,(\partial \beta/\partial y) - (\partial f/\partial y)\,(\partial \beta/\partial x) = (3/2)\,x^2$. We find that the critical points are $\{(0, 1),\ (0, -1),\ O_E\}$, which is isomorphic to Z_3.

As a second example, consider the Toroidal Belyĭ pair (E, β) with E the curve defined by $f(x, y) = y^2 - (x^3 - x)$ and $\beta(x, y) = x^2$. Again, we can compute the critical points $P = (x, y)$ of β by finding when the following function vanishes: $(\partial f/\partial x)\,(\partial \beta/\partial y) - (\partial f/\partial y)\,(\partial \beta/\partial x) = -4\,x\,y$. We find that the critical points are $\{(-1, 0),\ (0, 0),\ (+1, 0),\ O_E\}$, which is isomorphic to $Z_2 \times Z_2$.

Following our observations from these examples, there are two main questions that arise.

Research Question. *Say (E, β) is a Toroidal Belyĭ pair, and denote $\Gamma = \beta^{-1}\big(\{0,\ 1,\ \infty\}\big)$ as the collection of quasi-critical points. When does Γ form a subgroup of $\big(E(\mathbb{C}), \oplus\big)$? By Proposition 1, the elements in Γ must be points with finite order whenever Γ is a group. When are the points in Γ torsion elements in $E(\mathbb{C})$, regardless of Γ being a group?*

3.2. **Searching for Examples.** We began our exploratory analysis by calculating a number of examples. We started by pulling examples of Toroidal Belyĭ pairs (X, ϕ) from the L-Series and Modular Forms Database (LMFDB) [LMFDB], computing quasi-critical points $P \in \phi^{-1}\big(\{0,\ 1,\ \infty\}\big)$ and their ramification indices $e_P = e_\phi(P)$; some data can be found in Table 2. We soon realized that we would need to write a computer program to systematically compute the quasi-critical points and their orders. Simply put, even though the Toroidal Belyĭ pair (X, ϕ) was defined over a number field $K = \mathbb{Q}(\nu)$, the quasi-critical points in general would be defined over an extension $L = K(s)$. Figure 1 contains a diagram of the various function fields where we need to carry out our computations.

The outline of our methodology is as follows:

Algorithm Compute Examples

1: Choose Toroidal Belyĭ pair (X, ϕ) defined over a number field $K = \mathbb{Q}(\nu)$ from LMFDB.
2: Viewing $\phi \in \mathcal{K}\big(X(\mathbb{C})\big)$, compute $\operatorname{div}(\phi)$, $\operatorname{div}(\phi - 1)$, and $\operatorname{div}(1/\phi)$ to find the quasi-critical points over $\mathbb{C}$.
3: Compute the smallest number field $L = K(s)$ containing all the quasi-critical points.
4: Extend the function field $K(X) = \mathcal{K}\big(X(K)\big)$ of the elliptic curve to L, that is, $L(X) = \mathcal{K}\big(X(L)\big)$.
5: Working over L, compute the divisors, quasi-critical points, and their orders.
6: Identify the smallest subgroup that contains all of the quasi-critical points.
7: Write divisors, quasi-critical points, and the group generated by them to an external file.

The above was all implemented using a combination of `python` and `sage` on the cloud computing provider `CoCalc`. Computational power limited our ability to calculating the number field L in many cases. As a result, we implemented a "time-out," a specified time interval for computing the number field after which the example would be skipped. Still, we were able to compute 13 examples of Toroidal Belyĭ pairs (X, ϕ) for which the quasi-critical points are all torsion, that is, $\phi^{-1}\big(\{0,\ 1,\ \infty\}\big) \subseteq X(\mathbb{C})_{\text{tors}}$. A summary of the results can be found in Table 1, and the complete list of examples can be found in Table 3. The full code can be found in our `GitHub` repository [Asm+21].

4. Main Results

In this section, we list the main results from our research.

We observed that, given a Toroidal Belyĭ pair (E, β), we could construct another Toroidal Belyĭ pair (X, ϕ) where $X = E$ is the same elliptic curve but $\phi(x, y) = \beta\big((x, y) \oplus P_0\big)$ could be the translate by point $P_0 \in E(\mathbb{C})$. If there is any hope of the collection of quasi-critical points being torsion, then we would need

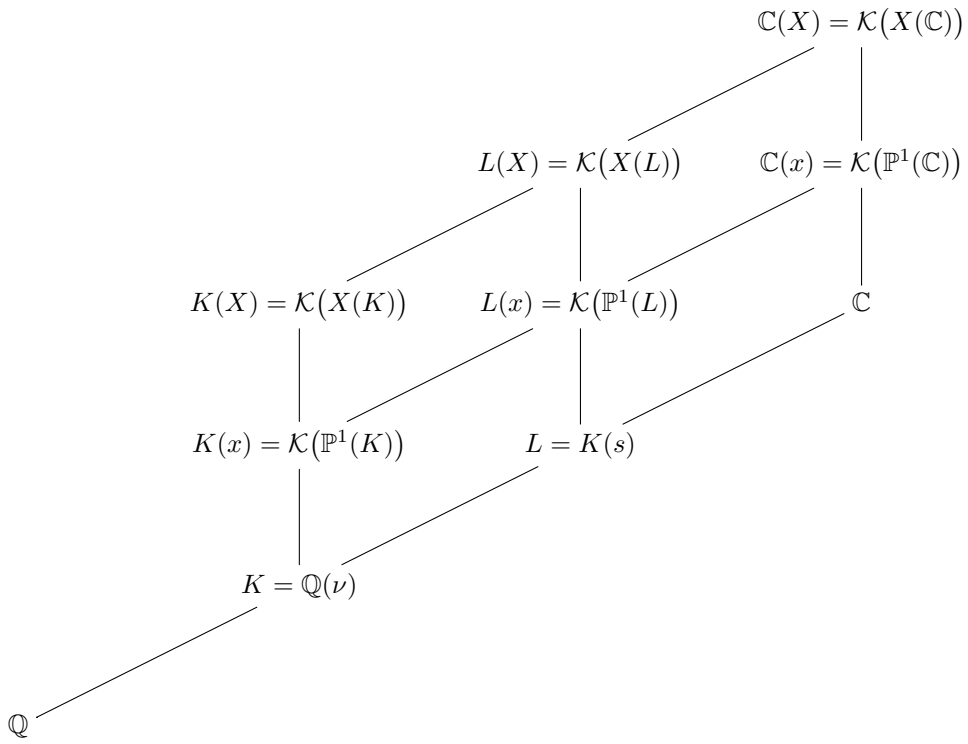

FIGURE 1. Function Fields related to a Toroidal Belyĭ Pair (X, ϕ) defined over K

$\deg(\phi)$	Total from LMDFB	Total Number of Successfully Processed	Number with Quasi-Critical Points All Torsion
3	1	1 (100%)	1 (100%)
4	2	2 (100%)	2 (100%)
5	7	7 (100%)	1 (14%)
6	35	29 (83%)	7 (24%)
7	73	15 (21%)	0 (0%)
8	94	30 (32%)	2 (7%)
9	39	23 (59%)	0 (0%)
Totals	251	107 (43%)	13 (12%)

TABLE 1. Processing of Toroidal Belyĭ pairs (X, ϕ) from LMFDB. We wish to find a number field L such that $\phi^{-1}\big(\{0,\, 1,\, \infty\}\big) \subseteq X(L)$ – which we may not be able to do in `sage`.

to limit the possibilities of quasi-critical points by choosing certain translates of Belyĭ maps. The following proposition explains one way we can do this.

Theorem 10. *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

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

Observe that if $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is a normalized Toroidal Belyĭ map, then we may choose $P_0 = Q_0 = O_E$. Hence the quasi-critical points, i.e. the points in B, W, and F, have relations involving their ramification indices. For instance, if we have a normalized Belyĭ map with $\beta^{-1}(\{q\}) = \{P\}$ for some $q \in \mathbb{P}^1(\mathbb{C})$, then $q \in \{0,\, 1,\, \infty\}$ must be a critical value, and so $[N]P = O_E$ since $e_\beta(P) = N$ is the degree of the Belyĭ map.

Proof. 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

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

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 $D_1 = \sum_{P\in B} e_P\,(P) - N\,(O_E)$ and $D_2 = \sum_{P\in F} e_P\,(P) - N\,(O_E)$ are principal divisors. First, consider D_1. Then, $\deg(D_1) = \sum_{P\in B} e_P - N = N - N = 0$ by Proposition 6; 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 $\operatorname{div}(f-g)$. Using that $\phi = f/g$, substitute in $f = \phi \cdot g$ to see that

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

□

Recall from Table 3 that we have 13 examples of Toroidal Belyĭ pairs (E, β) where the collection of quasi-critical points are torsion. The phenomenon that we have seen so far where the quasi-critical points forms a group occurs infinitely often.

Theorem 11. *Say (X, ϕ) a Toroidal Belyĭ pair, and denote $G = \phi^{-1}\big(\{0,\, 1,\, \infty\}\big)$ as the set of quasi-critical points. Take $\beta = \phi \circ \psi$, where $\psi : E \to X$ is any non-constant isogeny, and denote $\Gamma = \beta^{-1}\big(\{0,\, 1,\, \infty\}\big)$.*

(1) (E, β) is a Toroidal Belyĭ pair.
(2) Γ is contained in the torsion in $E(\mathbb{C})$ whenever G is contained in the torsion in $X(\mathbb{C})$.
(3) Γ is a group whenever G is group.

In order to prove this theorem, we will proceed with the proofs of numerous lemmata. Observe that $\Gamma = \{P \in E(\mathbb{C}) \mid \psi(P) \in G\} = \psi^{-1}(G)$; this will be useful in the proofs.

Lemma 12. *(E, β) is a Toroidal Belyĭ pair.*

Proof. 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 13. *If $G \subseteq X(\mathbb{C})_{tors}$ then $\Gamma \subseteq E(\mathbb{C})_{tors}$.*

Proof. 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 $N = m\,n$, 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 14. *Suppose $(G, \oplus)$ is a group. Then Γ is a subgroup of $(E(\mathbb{C}), \oplus)$.*

Proof. 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 15. *There are infinitely many imprimitive Toroidal Belyĭ pairs where the set of quasi-critical points forms a group.*

Proof. 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 $G = \phi^{-1}\big(\{0,\, 1,\, \infty\}\big) = \big\{(0, -1),\, (0, 1),\, O_E\big\} \simeq Z_3$, forms a group. Theorem 11 asserts that (E, β) forms a Toroidal Belyĭ pair for any non-constant isogeny $\psi : E(\mathbb{C}) \to X(\mathbb{C})$ where $\Gamma = \beta^{-1}\big(\{0,\, 1,\, \infty\}\big)$ forms a group. Since there are infinitely many such isogenies, the result follows. □

It appears that Corollary 15 can generate infinitely many examples of Toroidal Belyĭ pairs (E, β) where the quasi-critical points forms a group, but we can only show this for imprimitive such pairs. Table 4 shows how many of the examples from Table 3 are actually associated to imprimitive Toroidal Belyĭ pairs.

5. Future Work

Upon completion of this project, we have three main goals for future related work. Firstly, we would like to modify the Sage code so that we can process more examples. Next, we would like to know if there are more examples with quasi-critical points and which cannot be explained by our main theorem. We have 13 examples where the quasi-critical points are torsion, and we have one example that can be explained by our main theorem. Finally, we would like to create a web page where we can host the data found over the summer so that others may easily access and view our results.

References

[Asm+21] Tesfa Asmara et al. *PRiME 2021 GitHub Repository*. 2021. URL: https://github.com/PRiME-2021/Algorithms.

[Dev20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.1)*. 2020. URL: http://www.sagemath.org.

[GG12] Ernesto Girondo and Gabino González-Diez. *Introduction to compact Riemann surfaces and dessins d'enfants*. Vol. 79. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 2012, pp. xii+298. ISBN: 978-0-521-74022-7.

[LMFDB] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. 2013. URL: http://www.lmfdb.org.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9.

[ST92] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. 1992.

Elliptic Curve X	Belyĭ Map $\phi(x,y)$	Quasi-Critical $P \in \phi^{-1}\big(\{0,\,1,\,\infty\}\big)$	Ramification $e_\phi(P)$
$y^2 = x^3 + 1$	$\dfrac{y+1}{2}$	$(0,\pm1)$, O_E	3, 3, 3
$y^2 = x^3 - x$	x^2	$(\pm1,0)$, $(0,0)$, O_E	2, 2, 4, 4
$y^2 = x^3 + x^2 + 16\,x + 180$	$\dfrac{4\,y + x^2 + 56}{108}$	$(22,-108)$, $(-2,12)$, $(4,-18)$, O_E	1, 3, 4, 4
$y^2 + x\,y + y$ $= x^3 + x^2 + 22\,x - 9$	$\dfrac{x\,y + 3\,x^2 + 3\,x + 63}{64}$	$(9,-37)$, $(-1 \pm 2\sqrt{-5}, 3)$, $(1,-5)$, O_E	1, 2, 2, 5, 5
$y^2 + x\,y = x^3 - 28\,x + 272$	$\dfrac{(x+13)\,y + 3\,x^2 + 4\,x + 220}{432}$	$\big(-13 \pm 3\sqrt{-15},\ 2\,(37 \pm 3\sqrt{-15})\big)$, $(2,-16)$, $(-4,20)$, O_E	1, 1, 3, 5, 5
$y^2 + y = x^3 + x^2 + 2\,x + 4$	$\dfrac{(x+7)\,y - 5\,x^2 - 2\,x + 15}{27}$	$\big((13 \pm 3\sqrt{-15})/2,\ 13 \pm 6\sqrt{-15}\big)$, $(-1,-2)$, $(2,4)$, O_E	1, 1, 3, 5, 5
$y^2 = x^3 - 120\,x + 740$	$\dfrac{(x+5)\,y + 162}{324}$	$(-11,\pm27)$, $(4,\pm18)$, O_E	2, 2, 3, 3, 5
$y^2 = x^3 + 5\,x + 10$	$\dfrac{(x-5)\,y + 16}{32}$	$(6,\pm16)$, $(1,\pm4)$, O_E	1, 1, 4, 4, 5

TABLE 2. Examples of Toroidal Belyĭ Pairs (X,ϕ) with Quasi-Critical Points and Ramification Indices

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

TABLE 3. Examples of Toroidal Belyĭ Pairs (X, ϕ) with Quasi-Critical Points $G = \phi^{-1}\big(\{0,\,1,\,\infty\}\big) \subseteq X(\mathbb{C})_{\mathrm{tors}}$

LMFDB Label	Elliptic Curve E	Toroidal Belyĭ $\beta(x,y)$	Belyĭ $\gamma(z)$	Meromorphic $\phi(x,y)$
4T1-4_4_2.2-a	$y^2 = x^3 - x$	$1 - x^2$	$4\,z\,(1-z)$	$\dfrac{x+1}{2}$
6T1-6_2.2.2_3.3-a	$y^2 = x^3 + 1$	$-x^3$	$4\,z\,(1-z)$	$\dfrac{1-y}{2}$
6T5-6_6_3.1.1.1-a	$y^2 = x^3 + 1$	$\dfrac{(1-y)\,(3+y)}{4}$	$4\,z\,(1-z)$	$\dfrac{3+y}{4}$
6T6-6_6_2.2.1.1-a	$y^2 = x^3 + 6\,x - 7$	$\dfrac{(x-1)^3}{27}$	z^3	$\dfrac{x-1}{3}$
6T7-4.2_4.2_3.3-a	$y^2 = x^3 - 10731\,x + 408170$	$\dfrac{11907\,(x-49)}{(x-7)^3}$	$z^2\,(3-2\,z)$	$\dfrac{63}{x-7}$
8T2-4.4_4.4_2.2.2.2-a	$y^2 = x^3 + x$	$\dfrac{(x+1)^4}{8\,x\,(x^2+1)}$	$\dfrac{(z^2+1)^2}{4\,z^2}$	$\dfrac{\sqrt{2}\,x}{y}$
8T7-8_8_2.2.1.1.1.1-a	$y^2 = x^3 - x$	x^4	z^4	x

LMFDB Label	Elliptic Curve E	Toroidal Belyĭ $\beta(x,y)$	Belyĭ $\phi(x,y)$	Isogeny $\psi(x,y)$
6T4-3.3_3.3_3.3-a	$y^2 = x^3 - 15\,x + 22$	$\dfrac{8\,(x-2)^2 - (x^2-4\,x+7)\,y}{16\,(x-2)^2}$	$\dfrac{1-y}{2}$	$\left(\dfrac{x^2-2\,x-3}{4\,(x-2)},\ \dfrac{(x^2-4\,x+7)\,y}{8\,(x-2)^2}\right)$

TABLE 4. Toroidal Belyĭ Pairs (E,β) from Table 3 which are Imprimitive: $\beta = \gamma \circ \phi \circ \psi$