Dessins d'Enfant on the Torus

PRiME 2015
Department of Mathematics
Purdue University

Summer Project Presentation
Purdue University

August 06, 2015

PRiME 2015

Purdue Research in Mathematics Experience (PRiME):

Staff:
Dr. Edray Herber Goins
Hongshan Li
Avi Steiner

Undergraduate Participants:
Leonardo Azopardo
Sofia Lyrintzis
Bronz McDaniels
Maxim Millan
Yesid Sánchez
Danny Sweeney
Sarah Thomaz

Outline of Talk

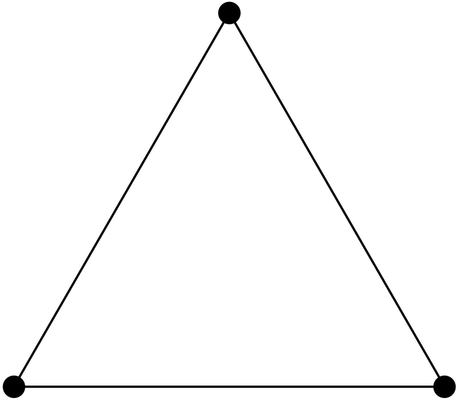
1. Riemann Surfaces
   - Riemann-Hurwitz Formula
2. Belyĭ Maps
   - Dessins d'Enfant
   - Graph Theory
   - Degree Sequences
3. Examples
   - Verifying a rational function is a Belyĭ Map
   - Degree Sequences
   - Finding more examples
4. Algorithm

Motivation

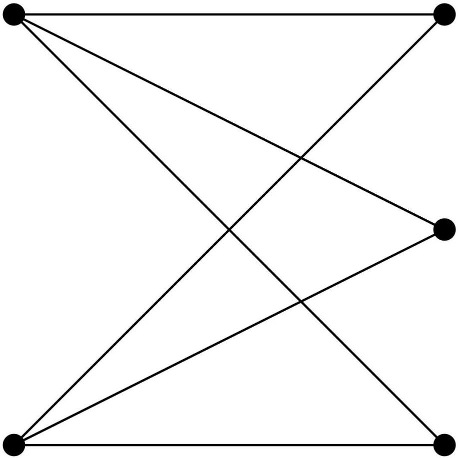
Project 1: Find and verify Belyĭ maps for elliptic curves.

Project 2: Write code that will plot Dessins d'Enfants on the Torus

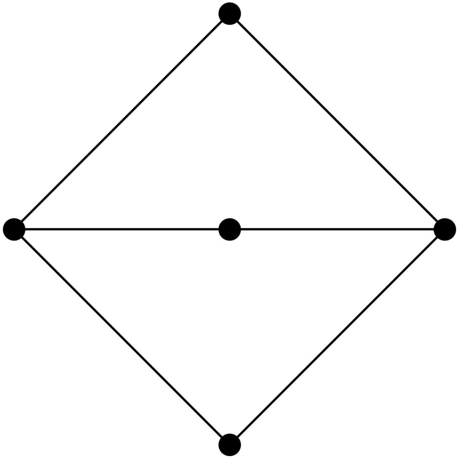
K_3



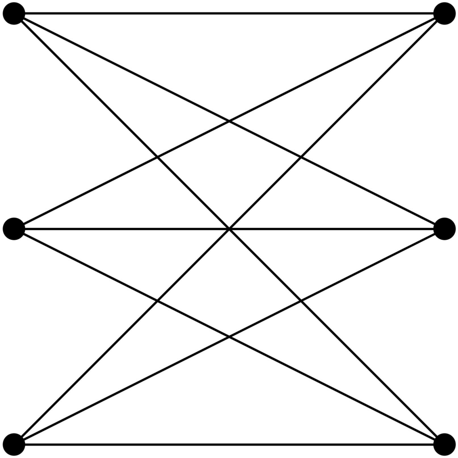
$K_{2,3}$



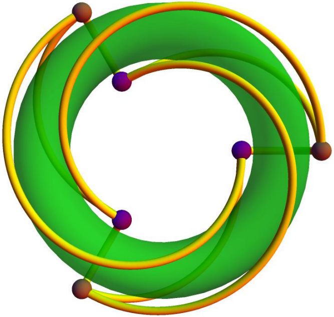
$K_{2,3}$



$K_{3,3}$



$K_{3,3}$



Riemann Surfaces

Riemann Surfaces

A **Riemann Surface** is a triple $(X, \{U_\alpha\}, \{\mu_\alpha\})$ satisfying:

- **Coordinate Charts and Maps:** For a countable indexing set I,

$$X = \bigcup_{\alpha \in I} U_\alpha \qquad \text{and} \qquad \mu_\alpha : U_\alpha \hookrightarrow \mathbb{C}$$

- **Locally Euclidean:** Each $\mu_\alpha(U_\alpha)$ is a connected, open subset of $\mathbb{C}$; and the composition $\mu_\beta \circ \mu_\alpha^{-1}$ is a smooth function.
- **Hausdorff:** For distinct $z \in U_\alpha$ and $w \in U_\beta$ there exist open subsets:

$$\begin{array}{l} \mu_\alpha(z) \in \mathcal{U}_\alpha \subseteq \mu_\alpha(U_\alpha) \\ \mu_\beta(w) \in \mathcal{U}_\beta \subseteq \mu_\beta(U_\beta) \end{array} \quad \text{such that} \quad \mu_\alpha^{-1}(\mathcal{U}_\alpha) \cap \mu_\beta^{-1}(\mathcal{U}_\beta) = \emptyset$$

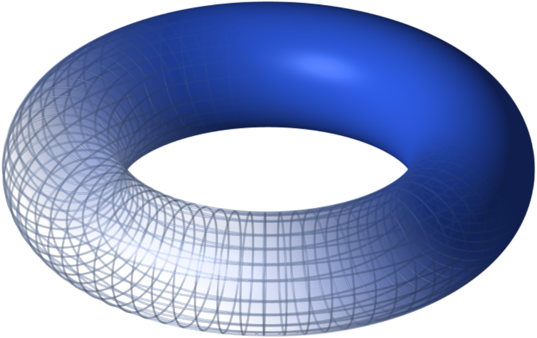
We always embed $X \hookrightarrow \mathbb{R}^3$.

Examples of Riemann surfaces

Surface of genus 0:

Examples of Riemann surfaces

Surface of genus 1:



Elliptic Curves

An elliptic curve E is a set

$$E(\mathbb{C}) = \left\{ (x : y : z) \in \mathbb{P}^2(\mathbb{C}) \,\middle|\, y^2 z + a_1 x\, y\, z + a_3 y\, z^2 = x^3 + a_2 x^2 z + a_4 x z^2 + a_6 z^3 \right\}$$

for complex numbers $a_1,\ a_3,\ a_2,\ a_4,\ a_6$.
Let E be an elliptic curve. Then we can place E in the form $E' : y^2 z = (x - e_1 z)(x - e_2 z)(x - e_3 z)$ for different complex numbers $e_1,\ e_2,\ e_3$.

Theorem

Every elliptic curve $E : y^2 z = (x - e_1 z)(x - e_2 z)(x - e_3 z)$ is isomorphic to a **torus**
$T^2(\mathbb{R}) = \{(u, v, w) \in \mathbb{R}^3 \mid (\sqrt{u^2 + v^2} - R)^2 + w^2 = r^2\}$

Upon defining the **lattice** $\Lambda = \left\{ m\,\omega_1 + n\,\omega_2 \,\middle|\, m,\ n \in \mathbb{Z} \right\}$ in terms of the **periods**

$$\omega_1 = 2 \int_{e_1}^{e_3} \frac{dt}{\sqrt{(t-e_1)\,(t-e_2)\,(t-e_3)}}$$

and

$$\omega_2 = 2 \int_{e_2}^{e_3} \frac{dt}{\sqrt{(t-e_1)\,(t-e_2)\,(t-e_3)}}$$

We have then the following isomorphism

$$\begin{array}{ccccc}
E(\mathbb{C}) & \xrightarrow{\simeq} & \mathbb{C}/\Lambda & \xrightarrow{\simeq} & T^2(\mathbb{R}) \\
 & & & & u = \left(R + r\ \cos 2\pi m\right)\ \cos 2\pi n \\
(x,\, y) & & \operatorname{sgn}(y) \displaystyle\int_x^\infty \frac{dt}{\sqrt{(t-e_1)\,(t-e_2)\,(t-e_3)}} & & v = \left(R + r\ \cos 2\pi m\right)\ \sin 2\pi n \\
 & & = m\,\omega_1 + n\,\omega_2 & & w = r\ \sin 2\pi n
\end{array}$$

Riemann-Hurwitz Formula

Riemann-Hurwitz Genus Formula

Let $\beta : X \to Y$ be a rational map between Riemann surfaces. The Euler characteristics $\chi(X) = 2 - 2\,g_X$ and $\chi(Y) = 2 - 2\,g_Y$ are related by

$$\chi(X) = \deg(\beta) \cdot \chi(Y) - \sum_{p \in X} (e_p - 1)$$

for some positive integers e_p called the ramification indices.

As a special case:

$$\begin{array}{lll} X = E(\mathbb{C}) \simeq \mathbb{T}^2(\mathbb{R}) : & g_X = 1 & \chi(X) = 0 \\ Y = \mathbb{P}^1(\mathbb{C}) \simeq S^2(\mathbb{R}) : & g_Y = 0 & \chi(Y) = 2 \end{array}$$

Belyĭ Maps

In the 2003 paper "What is. . . a Dessin d'Enfant?" by Leonardo Zapponi, the author recounts how Gennadiĭ Belyĭ proved in 1979 that a Riemann surface X is completely determined by the existence of a rational map $\beta : X \to \mathbb{P}^1(\mathbb{C})$ which has three critical values.

Theorem

Let X be a compact, connected Riemann surface.

- X can be defined by a polynomial equation $\sum_{i,j} a_{ij} z^i w^j = 0$.
- If the coefficients a_{ij} are not transcendental then there exists a rational function $\beta : X \to \mathbb{P}^1(\mathbb{C})$ which has at most three critical values.
- Conversely, if there exists a rational function $\beta : X \to \mathbb{P}^1(\mathbb{C})$ which has at most three critical values, then X can be defined by a polynomial equation $\sum_{i,j} a_{ij} z^i w^j = 0$ where the coefficients a_{ij} are not transcendental.

Belyĭ Maps

Let E be an elliptic curve.
A **rational function** $\beta : E(\mathbb{C}) \hookrightarrow \mathbb{P}^1(\mathbb{C})$ is a map which is a ratio $\beta(x,y,z) = p(x,y,z)/q(x,y,z)$ in terms of relatively prime homogeneous polynomials $p(x,y,z), q(x,y,z) \in \mathbb{C}[x,y,z]$.
Define its **degree** as the natural number

$$\deg(\beta) = \max_{\omega \in \mathbb{P}^1(\mathbb{C})} \left| \left\{ P \in E(\mathbb{C}) \,\middle|\, \beta(P) = \omega \right\} \right|$$

- $\omega \in \mathbb{P}^1(\mathbb{C})$ is said to be a **critical value** if $|\beta^{-1}(\omega)| \neq \deg(\beta)$.
- A **Belyĭ map** is a rational function β such that its collection of critical values ω is contained within the set $\{(0:1),\ (1:1),\ (1,0)\} \subseteq \mathbb{P}^1(\mathbb{C})$

Dessins d'Enfant

Fix a Belyĭ map $\beta(x, y, z) = p(x, y, z)/q(x, y, z)$ for $E(\mathbb{C})$. Denote the preimages

$$\begin{aligned} B &= \beta^{-1}((0:1)) &= \{P \in E(\mathbb{C}) | p(P) = 0\} \\ W &= \beta^{-1}((1:1)) &= \{P \in E(\mathbb{C}) | p(P) - q(P) = 0\} \\ E &= \beta^{-1}([0, 1]) &= \{P \in E(\mathbb{C}) | \beta(P) \in \mathbb{R} \text{ and } 0 \leq \beta(P) \leq 1\} \end{aligned}$$

The bipartite graph (V, E) with vertices $V = B \cup W$ and edges E is called **Dessins d'Enfant**. We embed the graph on $E(\mathbb{C})$ in $\mathbb{R}^3$.

$$\begin{array}{ccccc} B & W & E & E(\mathbb{C}) & \xrightarrow{\beta} \mathbb{P}^1(\mathbb{C}) \\ \downarrow & \downarrow & \downarrow & \downarrow & \\ \left\{ \begin{array}{c} \text{black} \\ \text{vertices} \end{array} \right\} & \left\{ \begin{array}{c} \text{white} \\ \text{vertices} \end{array} \right\} & \left\{ \text{edges} \right\} & \mathbb{R}^3 & \end{array}$$

Riemann Existence Theorem

Every graph on the torus can be realized as the Dessin d'Enfant of some Belyi map.

Corollary

Given $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, let
$B = \beta^{-1}(0) \quad W = \beta^{-1}(1) \quad F = \beta^{-1}(\infty)$. Then,

- $|E| = \deg(\beta)$
- $\sum_{P \in \beta^{-1}(\omega)} e_P = \deg(\beta)$ for any $\omega \in \mathbb{P}^1(\mathbb{C})$

meaning that $\sum_{P \in B} e_P = \sum_{P \in W} e_P = \sum_{P \in F} e_P = \deg(\beta)$

Graphs

- A **(finite) graph** is an ordered pair (V, E) consisting of **vertices** V and **edges** E.
- A **connected graph** is a graph in which there exists a route of edges and vertices between any two vertices.
  Every graph in this research is a connected graph.
- A **bipartite graph** is a graph whose vertices can be divided into two disjoint sets B and W such that every edge connects a vertex in B to a vertex in W.
- A **complete bipartite graph** $(K_{m,n})$ is a bipartite graph such that every vertex in B is connected to every vertex in W.

Graphs

Given a bipartite graph (V, E) where $V = B \cup W$ and faces F, denote

$$\{e_P \mid P \in B\} \qquad \{e_P \mid P \in W\} \qquad \{e_P \mid P \in F\}$$

where e_p = number of edges adjacent to a vertex P for $P \in V$.

Degree Sum Formula

$$\sum_{P \in V} e_P = 2|E|$$

Proposition for Bipartite Graphs

$$\sum_{P \in W} e_P = \sum_{P \in B} e_P = |E|$$

Important Theorems of Graph Theory

Euler Formula

If graph G is a connected graph then $|V| - |E| + |F| = 2 - 2g$

Where g is a a genus of a surface on which the graph G can be drawn without any edges crossing.

The genus of a graph is the minimum number of handles that must be added to the plane to draw the graph without any edges crossing.

Ringel's Theorem, 1963

$$g(K_{m,n}) = \left\lfloor \frac{(m-2)(n-2)+3}{4} \right\rfloor$$

So all complete bipartite graphs that can be drawn on the torus are $K_{3,3}, K_{3,4}, K_{3,5}, K_{3,6}, K_{4,4}$

Degree Sequences

Proposition

Let $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ be a Belyĭ map. Then the sets

$$\left\{ e_P \,\middle|\, P \in B \right\} \qquad\qquad B = \beta^{-1}\big((0:1)\big)$$

$$\left\{ e_P \,\middle|\, P \in W \right\} \qquad \text{in terms of} \qquad W = \beta^{-1}\big((1:1)\big)$$

$$\left\{ e_P \,\middle|\, P \in F \right\} \qquad\qquad F = \beta^{-1}\big((1:0)\big)$$

are each integer partitions of $\deg(\beta)$ such that

$$2 \deg(\beta) = \sum_{P \in B} \big(e_P - 1\big) + \sum_{P \in W} \big(e_P - 1\big) + \sum_{P \in F} \big(e_P - 1\big).$$

These integer partitions are called the degree sequences of the Belyĭ map.

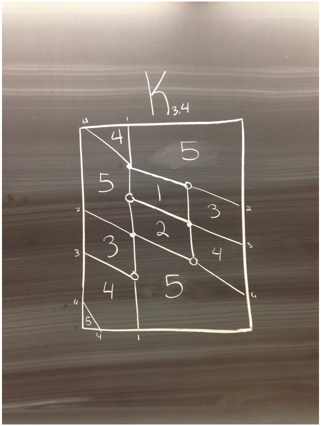
Unique degree sequences of the Complete Bipartite Graphs

By Ringel, we know that the only $K_{m,n}$ that can be drawn on the torus without edges crossing are $K_{3,3}$, $K_{3,4}$, $K_{3,5}$, $K_{3,6}$, $K_{4,4}$. Recall

$$|B| = m, \quad |W| = n, \quad |E| = m\,n, \quad \text{and} \quad |F| = mn - (m+n).$$

$K_{m,n}$	$\lvert B\rvert$	$\lvert W\rvert$	$\lvert F\rvert$	Degree Sequence
$K_{3,3}$	3	3	3	$\{\{3,3,3\}\{3,3,3\},\{3,3,3\}\}$
$K_{3,4}$	3	4	5	$\{\{4,4,4\}\{3,3,3,3\},\{4,2,2,2,2\}\}$
$K_{3,5}$	4	5	7	$\{\{5,5,5\}\{3,3,3,3,3\},\{3,2,2,2,2,2,2\}\}$
$K_{3,6}$	5	6	9	$\{\{6,6,6\}\{3,3,3,3,3,3\},\{2,2,2,2,2,2,2,2,2\}\}$
$K_{4,4}$	4	4	8	$\{\{4,5,5\}\{3,3,3,3,3\},\{2,2,2,2,2,2,2,2\}\}$

$K_{3,4} : \{\{4, 4, 4\}\{3, 3, 3, 3\}, \{4, 2, 2, 2, 2\}\}$



Examples of

Belyĭ Maps

Examples of Belyĭ Maps on Noam Elkies Webpage

Noam Elkies of Harvard University maintains a webpage which lists several examples of Belyĭ maps:
http://www.math.harvard.edu/~elkies/nature.html.
The following examples appear on the paper:

$$E: \; y^2 = x^3 + 1 \qquad \beta(x,y) = \frac{y+1}{2}$$

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

$$E: \; y^2 = x^3 - 120\,x + 740 \qquad \beta(x,y) = \frac{(x+5)\,y + 162}{324}$$

$$E: \; y^2 + 15\,x\,y + 128\,y = x^3 \qquad \beta(x,y) = \frac{\left(y - x^2 - 17\,x\right)^3}{2^{14}\,y}$$

Examples of Belyĭ Maps on Noam Elkies' Webpage

$$E : y^2 + x\,y + y = x^3 + x^2 + 35\,x - 28$$

$$\beta(x, y) = \frac{4\left(9\,x\,y - x^3 - 15\,x^2 - 36\,x + 32\right)}{3125}$$

And

$$E : y^2 = x^3 - 15\,x - 10$$

$$\beta(x, y) = \frac{\left(3\,x^2 + 12\,x + 5\right)y + \left(-10\,x^3 - 30\,x^2 - 6\,x + 6\right)}{-16\left(9\,x + 26\right)}$$

Examples of Belyĭ Maps on different papers

In Leonardo Zapponi's "On the Belyĭ degree(s) of a curve defined over a number field" (although the term "6 Y" should be "12 Y") there is the following example of a Belyĭ map:

$$E: \; y^2 = x^3 + x^2 + 16\,x + 180 \quad \beta(x,y) = \frac{x^2 + 4\,y + 56}{108}$$

In Lily Khadjavi and Victor Scharaschkin's "Belyĭ Maps, Elliptic Curves and the *ABC* Conjecture" one can find this other example of a Belyĭ map:

$$E: \; y^2 = x^3 - x \qquad \beta(x,y) = x^2$$

Verifying a rational function is a Belyĭ Map

Given an elliptic curve:

$$E(\mathbb{C}) = \left\{ (x, y) \in \mathbb{C}^2 \,\middle|\, y^2 + a_1\, x\, y + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6 \right\}$$

We verify that $\beta(x, y)$ is a Belyĭ map for $E(\mathbb{C})$ following the next steps

- Compute the maps degree.
- Compute a potential list of critical values.
- Determine which of the potential critical values are critical values.

Degree Sequences of Belyĭ maps

By means of the previous propositions we have that:

- There do not exist any Belyĭ maps of $\deg(\beta) = 2$.
- Every Belyĭ map of $\deg(\beta) = 3$ or 4 has one of the following degree sequences, as illustrated by the accompanying examples:

$$\big\{\{3\},\{3\},\{3\}\big\} \qquad E:\ y^2 = x^3 + 1 \qquad \beta(x,y) = \frac{y+1}{2}$$

$$\big\{\{1,3\},\{4\},\{4\}\big\} \qquad E:\ y^2 = x^3 + x^2 + 16\,x + 180 \qquad \beta(x,y) = \frac{x^2 + 4\,y + 56}{108}$$

$$\big\{\{2,2\},\{4\},\{4\}\big\} \qquad E:\ y^2 = x^3 - x \qquad \beta(x,y) = x^2$$

Belyĭ Maps cant have Degree 2

Riemann Hurwitz Genus Formula for Belyĭ Maps on the torus

$$2\deg(\beta) = \sum_{P\in\beta^{-1}(0)} (e_P - 1) + \sum_{P\in\beta^{-1}(1)} (e_P - 1) + \sum_{P\in\beta^{-1}(\infty)} (e_P - 1)$$

- Critical Point when $e_P = 2$.
- $4 = (2-1) + (2-1) + (2-1) + (2-1)$
- 4 critical points $\Rightarrow$ 4 critical values
- Not a Belyĭ map.

Degree 3 Belyĭ Map

Set $E : y^2 = x^3 + Ax + B$ and $\beta(x, y) = \dfrac{ay + bx + c}{dy + ex + f} = \omega$

- Solve for y in terms of x and substitute into E.
- Factor $p(x) = (x - x_1)^{e_1} \cdots (x - x_n)^{e_n}$.
- Define y_k for $\beta(x_k, y_k) = \omega$ and $e_p = e_k$ for $P = (x_k, y_k)$.
- Have repeated roots when $\omega = 0, 1, \infty$.

$$2\deg(\beta) = \sum_{P\in\beta^{-1}(0)} (e_P - 1) + \sum_{P\in\beta^{-1}(1)} (e_P - 1) + \sum_{P\in\beta^{-1}(\infty)} (e_P - 1)$$

- $\omega = 0, 1, \infty$:

$$p(x) = (x - x_1)^3 \Rightarrow e_1 = 3$$

- $\{\{3\}, \{3\}, \{3\}\}$

Degree Sequences of Dessin d'Enfants of Belyi Maps

Riemann Hurwitz Genus Formula for Belyĭ Maps on the torus

$$2\deg(\beta) = \sum_{P\in\beta^{-1}(0)} (e_P - 1) + \sum_{P\in\beta^{-1}(1)} (e_P - 1) + \sum_{P\in\beta^{-1}(\infty)} (e_P - 1)$$

For example, consider Belyĭ maps with $\deg(\beta) = 5$.

$$2\cdot 5 = \sum_{P\in B}(e_P - 1) + \sum_{P\in W}(e_P - 1) + \sum_{P\in F}(e_P - 1) = \begin{cases} 4+4+2 \\ 4+3+3 \end{cases}$$

All representation of sums of elements in partitions are:

- $4 = (5-1)$
- $3 = (4-1) + (1-1)$ or $3 = (3-1) + (2-1)$
- $2 = (3-1) + (1-1) + (1-1)$ or
  $2 = (2-1) + (2-1) + (1-1)$

Degree Sequences of Belyĭ maps

- Every Belyĭ map of $\deg(\beta) = 5$ has one of the following degree sequences, as illustrated by the accompanying examples:

$\{\{1,4\},\{1,4\},\{5\}\}$	$E : y^2 = x^3 + 5x + 10$	$\beta(x,y) = \dfrac{(x-5)\,y + 16}{32}$
$\{\{2,3\},\{2,3\},\{5\}\}$	$E : y^2 = x^3 - 120x + 740$	$\beta(x,y) = \dfrac{(x+5)\,y + 162}{324}$
$\{\{1,4\},\{2,3\},\{5\}\}$	?	?
$\{\{1,2,2\},\{5\},\{5\}\}$	?	?
$\{\{1,1,3\},\{5\},\{5\}\}$	?	?

New examples

Generating new examples

Proposition

Every elliptic curve has degree $2, 3$ rational maps f with 4 critical values say $\{(0:1), (1:1), (1:0), (\omega_0:1)\}$

Corollary

Say $\omega_0 = \dfrac{p}{q}$ is a rational number. Then the composition

$$\beta : E(\mathbb{C}) \xrightarrow{f} \mathbb{P}^1(\mathbb{C}) \xrightarrow{h} \mathbb{P}^1(\mathbb{C})$$

in terms of $h(\omega) = \omega^{p-q}(\omega-1)^{-p}\left(\omega - \dfrac{p}{q}\right)^q$ is a Belyĭ map of $\deg(\beta) = \deg(f) \cdot \max\{|p|, |q|\}$

Degree 2 rational map

Given an elliptic curve E in general form, we can transform it into $E' : y^2z = (x - e_1z)(x - e_2z)(x - e_3z)$ for some complex numbers e_1, e_2, and e_3.

Proposition

Given an elliptic curve $E' : y^2z = (x - e_1z)(x - e_2z)(x - e_3z)$, we have that a corresponding rational map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ of $\deg(\beta) = 2$ with critical values $\{(0 : 1), (1 : 1), (1 : 0), (\omega_0 : 1)\}$ is given by

$$\beta(x, y, z) = \frac{e_2 - e_3}{e_2 - e_1} \cdot \frac{x - e_1z}{x - e_3z}$$

Degree 3 rational map

Every elliptic curve can be written in the form $y^2z + A_1xyz + A_3yz^2 = x^3$ for complex numbers A_1 and A_3 by some substitution.

Theorem

Given an elliptic curve $E : y^2z + A_1xyz + A_3yz^2 = x^3$, we have that a corresponding rational map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ of $\deg(\beta) = 3$ with critical values $\{(0:1), (1:1), (1:0), (\omega_0:1)\}$ is given by

$$\beta(x,y,z) = \frac{\left(2\,A_1^3 - 27\,A_3 - 2\,A_1\sqrt{A_1\left(A_1^3 - 27\,A_3\right)}\right)y - 27\,A_3^2 z}{\left(2\,A_1^3 - 27\,A_3 + 2\,A_1\sqrt{A_1\left(A_1^3 - 27\,A_3\right)}\right)y - 27\,A_3^2 z} \quad \text{if } A_1 \neq 0.$$

Database

Database

Theorem (Zapponi)

There are only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves of a given bounded Belyĭ degree.

Corollary

For a given positive integer N, there exists only finitely many $j_0 \in \mathbb{C}$ such that there exists an elliptic curve E and a Belyĭ map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $j(E) = j_0$ and $\deg(\beta) = N$.

Database

Given an integer N, we want to compute

- Elliptic curves E.
- Belyĭ maps $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $\deg(\beta) = N$.
- Dessin d'Enfant of β

Algorithm

Visualizing Dessins d'Enfants on the Torus

Overview of the algorithm

Input:

- An elliptic curve in the form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- A Belyĭ Map: $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$

Output: Points and coloring corresponding to a Dessin d'Enfant embedded on the torus, $\mathbb{T}^2(\mathbb{R})$.

Step 1: Setup

We find a set of points (x, y) that approximate β^{-1} on the curve from 0 to 1: $\beta^{-1}([0,1]) \subseteq E(\mathbb{C})$.

Recall:

- $\beta^{-1}(0) =$ Red Vertices
- $\beta^{-1}(1) =$ Black Vertices
- $\beta^{-1}([0,1]) =$ Edges

Step 1: Setup

Given our curve :

$$y^2 + a_1\, x\, y + a_3, y = x^3 + a_2\, x^2 + a_4\, x + a_6$$

We simplify it to the following

$$4(x^3 + a_2 x^2 + a_4 x + a6) + (a_1 x + a_3)^3 = 4(x - e_1)(x - e_2)(x - e_3)$$

Where e_1, e_2, and e_3 are roots of the elliptic curve

Step 2: The elliptic logarithm

Recall the lattice $\Lambda = \left\{ m\,\omega_1 + n\,\omega_2 \,\middle|\, m,\ n \in \mathbb{Z} \right\}$ in terms of the periods

$$\omega_1 = \int_{e_1}^{e_3} \frac{dt}{\sqrt{(t-e_1)\,(t-e_2)\,(t-e_3)}} \quad \text{and} \quad \omega_2 = \int_{e_2}^{e_3} \frac{dt}{\sqrt{(t-e_1)\,(t-e_2)\,(t-e_3)}}$$

For every point (x, y) calculated in step 1 we compute an elliptic logarithm, z by $\log_E : E(\mathbb{C}) \to \mathbb{C}/\Lambda$.:

$$\begin{aligned} z &= sgn(y) \int_{x}^{\infty} \frac{dt}{\sqrt{(t-e_1)\,(t-e_2)\,(t-e_3)}} \\ &= m\,\omega_1 + n\,\omega_2 \end{aligned}$$

Step 3: Projecting to the torii

We exploit the following isomorphisms

$$E(\mathbb{C}) \xrightarrow{\simeq} \mathbb{C}/\Lambda \xrightarrow{\simeq} T^2(\mathbb{R})$$

$$(x, y) \qquad \operatorname{sgn}(y) \int_x^{\infty} \frac{dt}{\sqrt{(t-e_1)(t-e_2)(t-e_3)}} = m\,\omega_1 + n\,\omega_2$$

$$u = \big(R + r \cos 2\pi m\big) \cos 2\pi n$$

$$v = \big(R + r \cos 2\pi m\big) \sin 2\pi n$$

$$w = r \sin 2\pi n$$

John Cremona and Thotasaphon Thongjunthug's Method

- One of the major issues was calculating the elliptic logarithm in Sage.
- We used the Arithmetic Geometric Mean(AGM) to approximate the elliptic integral.
- Without using an integral within a few steps you can acquire the elliptic integral quickly.

Overview of the Algorithm

- The algorithm is broken up into two steps
  1. Finding the periods ω_1 and ω_2
  2. Finding the elliptic logarithm
- To find the periods you set up one "for" loop that converges to ω_1 and ω_2 as you increase the iterations
- To find the elliptic logarithm you set up a nested "for" loop that calculates a complex number for every point on the elliptic curve.

Step 1 - Calculating the Periods

- To begin calculate four values in terms of the roots of the elliptic curve.

$$A_0 = \sqrt{e_1 - e_3} \quad B_0 = \sqrt{e_1 - e_2} \quad C_0 = \sqrt{e_2 - e_3} \quad D_0 = \sqrt{e_2 - e_1}$$

- Next we run through the "for" loop from $p = 0, 1, 2, 3 \ldots N - 1$

$$A_{p+1} = \frac{A_p + B_p}{2} \quad B_{p+1} = \sqrt{A_p B_p} \quad C_{p+1} = \frac{C_p + D_p}{2} \quad D_{p+1} = \sqrt{C_p D_p}$$

- As p iterates to N-1 the following ratio converges to the period

$$\omega_1 = \frac{\pi}{A_N} = \frac{\pi}{B_N} \qquad \omega_2 = \frac{\pi}{C_N} = \frac{\pi}{D_N}$$

Remark: There is a consistent way to choose the signs to guarantee convergence

Step 2 - Calculating the Elliptic Logarithm

Given a point (x, y) on the elliptic curve, compute the following

- To calculate the elliptic logarithm find the following values

$$I_1 = \sqrt{\frac{x - e_1}{x - e_2}} \qquad J_1 = \frac{-(2y + a_1 x + a_3)}{2I_1(x - e_2)}$$

- Then as $p = 0, 1, 2, 3, 4 \ldots N - 1$ calculate the following values

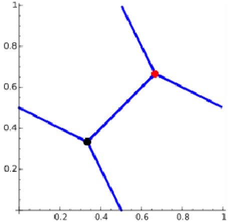
$$I_{p+1} = \sqrt{\frac{A_p(I_p + 1)}{B_{p-1} I_p + A_{p-1}}} \qquad J_{p+1} = I_{p+1} J_p$$

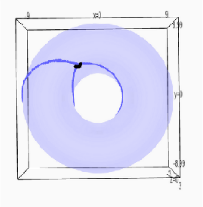
- This returns the elliptic logarithm

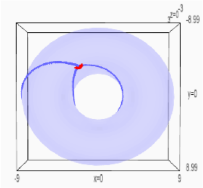
$$z = \frac{arctan \frac{A_N}{J_N}}{A_N}$$

Dessin of Degree 3

$$E : y^2 = x^3 + 1 \qquad \beta(x, y) = \frac{(y+1)}{2}$$



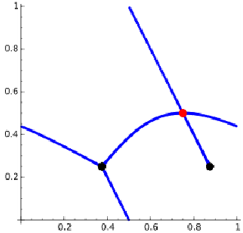


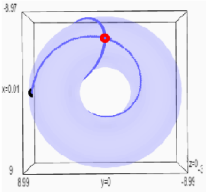


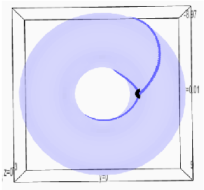
Dessin of Degree 4

$$E : y^2 = x^3 + x^2 + 16x + 180$$

$$\beta(x, y) = \frac{(x^2+4y+56)}{(108)}$$

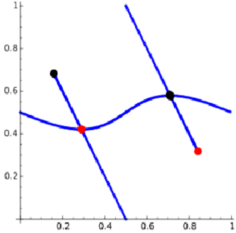


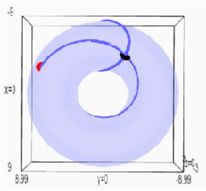


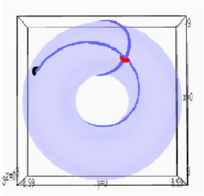


Dessin of Degree 5

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

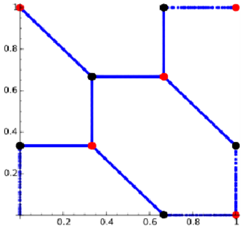


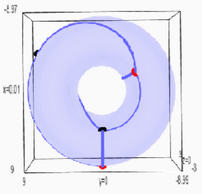


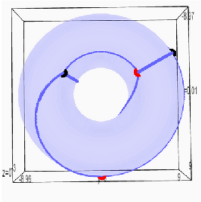


Dessin of Degree 9

$$E : y^2 = x^3 - 432 \qquad \beta(x,y) = \frac{(216x^3)}{(y+36)^3}$$







Future Projects

- Find remaining degree 5 Belyi maps
- Work with tori of g>1

Acknowledgments

- Dr. Edray Herber Goins
- Hongshan Li
- Avi Steiner

- Dr. Steve Bell
- Dr. David Goldberg
- Dr. Lazslo Lempert
- Dr. Joel and Mrs. Ruth Spira
- Dr. Uli Walther
- Dr. Mark Ward
- Dr. Lowell W. Beineke

- Dr. Gregery Buzzard / Department of Mathematics
- College of Science
- UREP-C / Universidad Nacional de Colombia
- National Science Foundation

Thank You!

Questions?