Computing Schneider p-adic heights on hyperelliptic Mumford curves

Enis Kaya (KU Leuven)
joint work in progress with Marc Masdeu,
J. Steffen Müller and Marius van der Put

Winter Workshop Chabauty–Kim 2024
Heidelberg University
February 16, 2024

Introduction

F	-	a number field
A	-	an abelian variety over F
$\tilde{A}$	-	the dual of A

Introduction

F	-	a number field
A	-	an abelian variety over F
$\tilde{A}$	-	the dual of A

The Néron–Tate height pairing

$$A(F) \times \tilde{A}(F) \to \mathbb{R}$$

is well known. It's determinant is one of the invariants that appear in the Birch and Swinnerton-Dyer conjecture.

Introduction

F - a number field
A - an abelian variety over F
$\tilde{A}$ - the dual of A

The Néron–Tate height pairing

$$A(F) \times \tilde{A}(F) \to \mathbb{R}$$

is well known. It's determinant is one of the invariants that appear in the Birch and Swinnerton-Dyer conjecture.

For a prime number p, a p-adic height pairing is a function

$$A(F) \times \tilde{A}(F) \to \mathbb{Q}_p$$

which can be regarded as a p-adic analogue of the Néron–Tate height pairing.

Introduction

In the literature, there are several p-adic height pairings. Some of them were constructed by Coleman–Gross, Schneider, Mazur–Tate and Nekovář.

Introduction

In the literature, there are several p-adic height pairings. Some of them were constructed by Coleman–Gross, Schneider, Mazur–Tate and Nekovář.

Algorithms for computing p-adic heights

- play a crucial role in carrying out the quadratic Chabauty method to determine rational points on curves of genus at least two.

Introduction

In the literature, there are several p-adic height pairings. Some of them were constructed by Coleman–Gross, Schneider, Mazur–Tate and Nekovář.

Algorithms for computing p-adic heights

- play a crucial role in carrying out the quadratic Chabauty method to determine rational points on curves of genus at least two.

The p-adic height pairing constructed by Schneider is particularly important because

- the corresponding p-adic regulator fits into p-adic versions of Birch and Swinnerton-Dyer conjecture.

Introduction

In the literature, there are several p-adic height pairings. Some of them were constructed by Coleman–Gross, Schneider, Mazur–Tate and Nekovář.

Algorithms for computing p-adic heights

- play a crucial role in carrying out the quadratic Chabauty method to determine rational points on curves of genus at least two.

The p-adic height pairing constructed by Schneider is particularly important because

- the corresponding p-adic regulator fits into p-adic versions of Birch and Swinnerton-Dyer conjecture.

Main goal

Present an algorithm to compute the Schneider p-adic height pairing on (Jacobians of) hyperelliptic Mumford curves.

But EXTENDED Coleman–Gross height first...

But EXTENDED Coleman–Gross height first...

Let C be a nice curve over $\mathbb{Q}$ (with not necessarily good reduction at p).

But EXTENDED Coleman–Gross height first...

Let C be a nice curve over $\mathbb{Q}$ (with not necessarily good reduction at p). The pairing

$$\langle \cdot, \cdot \rangle_{\mathrm{CG}} \colon \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p$$

is defined as

$$\langle \cdot, \cdot \rangle_{\mathrm{CG}} = \sum_{q \in \{\text{prime numbers}\}} \langle \cdot, \cdot \rangle_q = \langle \cdot, \cdot \rangle_p + \sum_{q \neq p} \langle \cdot, \cdot \rangle_q.$$

But EXTENDED Coleman–Gross height first...

Let C be a nice curve over $\mathbb{Q}$ (with not necessarily good reduction at p). The pairing

$$\langle \cdot, \cdot \rangle_{\mathrm{CG}} \colon \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p$$

is defined as

$$\langle \cdot, \cdot \rangle_{\mathrm{CG}} = \sum_{q \in \{\text{prime numbers}\}} \langle \cdot, \cdot \rangle_q = \langle \cdot, \cdot \rangle_p + \sum_{q \neq p} \langle \cdot, \cdot \rangle_q.$$

The local components away from p are described using "arithmetic intersection theory",

But EXTENDED Coleman–Gross height first...

Let C be a nice curve over $\mathbb{Q}$ (with not necessarily good reduction at p). The pairing

$$\langle \cdot, \cdot \rangle_{\mathrm{CG}} \colon \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p$$

is defined as

$$\langle \cdot, \cdot \rangle_{\mathrm{CG}} = \sum_{q \in \{\text{prime numbers}\}} \langle \cdot, \cdot \rangle_q = \langle \cdot, \cdot \rangle_p + \sum_{q \neq p} \langle \cdot, \cdot \rangle_q.$$

The local components away from p are described using "arithmetic intersection theory", and

$$\langle D, E \rangle_p := {}^{\mathrm{Vol}}\!\!\int_E \omega_D$$

where

- ω_D is a "canonical" differential form attached to D, and
- ${}^{\mathrm{Vol}}\!\!\int$ is the Vologodsky integration.

p-adic integration theories

Fix a smooth curve X over $\mathbb{Q}_p$.

p-adic integration theories

Fix a smooth curve X over $\mathbb{Q}_p$. Let ω be a differential form on X,

p-adic integration theories

Fix a smooth curve X over $\mathbb{Q}_p$. Let ω be a differential form on X, let $P, Q \in X(\mathbb{Q}_p)$.

p-adic integration theories

Fix a smooth curve X over $\mathbb{Q}_p$. Let ω be a differential form on X, let $P, Q \in X(\mathbb{Q}_p)$. To this data, Vologodsky associated an integral

$$^{\mathrm{Vol}}\int_P^Q \omega \in \mathbb{Q}_p$$

which satisfy the expected properties.

p-adic integration theories

Fix a smooth curve X over $\mathbb{Q}_p$. Let ω be a differential form on X, let $P, Q \in X(\mathbb{Q}_p)$. To this data, Vologodsky associated an integral

$$^{\mathrm{Vol}}\int_P^Q \omega \in \mathbb{Q}_p$$

which satisfy the expected properties. We call this integral the **Vologodsky integral**.

p-adic integration theories

Fix a smooth curve X over $\mathbb{Q}_p$. Let ω be a differential form on X, let $P, Q \in X(\mathbb{Q}_p)$. To this data, Vologodsky associated an integral

$$^{\mathrm{Vol}}\!\!\int_P^Q \omega \in \mathbb{Q}_p$$

which satisfy the expected properties. We call this integral the **Vologodsky integral**.

To X, one can associate a Berkovich space X^{an}.

p-adic integration theories

Fix a smooth curve X over $\mathbb{Q}_p$. Let ω be a differential form on X, let $P, Q \in X(\mathbb{Q}_p)$. To this data, Vologodsky associated an integral

$$^{\mathrm{Vol}}\int_P^Q \omega \in \mathbb{Q}_p$$

which satisfy the expected properties. We call this integral the **Vologodsky integral**.

To X, one can associate a Berkovich space X^{an}. Pick a path γ in X^{an} from P to Q.

p-adic integration theories

Fix a smooth curve X over $\mathbb{Q}_p$. Let ω be a differential form on X, let $P, Q \in X(\mathbb{Q}_p)$. To this data, Vologodsky associated an integral

$$^{\mathrm{Vol}}\!\!\int_P^Q \omega \in \mathbb{Q}_p$$

which satisfy the expected properties. We call this integral the **Vologodsky integral**.

To X, one can associate a Berkovich space X^{an}. Pick a path γ in X^{an} from P to Q. To this data, Berkovich associated an integral

$$^{\mathrm{BC}}\!\!\int_\gamma \omega \in \mathbb{C}_p$$

which satisfy the expected properties.

Fix a smooth curve X over $\mathbb{Q}_p$. Let ω be a differential form on X, let $P, Q \in X(\mathbb{Q}_p)$. To this data, Vologodsky associated an integral

$$ {}^{\mathrm{Vol}}\!\!\int_P^Q \omega \in \mathbb{Q}_p $$

which satisfy the expected properties. We call this integral the **Vologodsky integral**.

To X, one can associate a Berkovich space X^{an}. Pick a path γ in X^{an} from P to Q. To this data, Berkovich associated an integral

$$ {}^{\mathrm{BC}}\!\!\int_\gamma \omega \in \mathbb{C}_p $$

which satisfy the expected properties. We call this integral the **Berkovich–Coleman integral**.

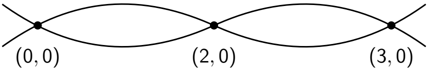
Example: Consider the hyperelliptic curve $X/\mathbb{Q}_5$ given by

$$y^2 = (x^2 - x - 1)(x^4 + x^3 - 6x^2 + 5x - 5).$$

Example: Consider the hyperelliptic curve $X/\mathbb{Q}_5$ given by

$$y^2 = (x^2 - x - 1)(x^4 + x^3 - 6x^2 + 5x - 5).$$

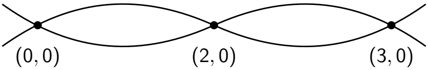
$p = 5$ is a prime of bad reduction for X, and X mod $\mathbb{F}_5$ is as follows:

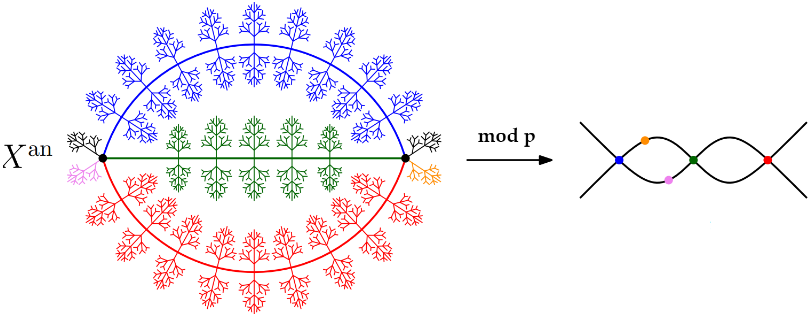


Example: Consider the hyperelliptic curve $X/\mathbb{Q}_5$ given by

$$y^2 = (x^2 - x - 1)(x^4 + x^3 - 6x^2 + 5x - 5).$$

$p = 5$ is a prime of bad reduction for X, and X mod $\mathbb{F}_5$ is as follows:





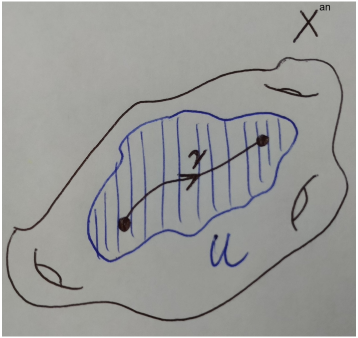
Remarks

- If X has good reduction, then ${}^{\mathrm{Vol}}\!\int_x^y \omega = {}^{\mathrm{BC}}\!\int_\gamma \omega$.

p-adic integration theories

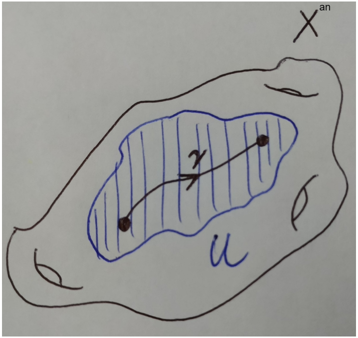
Remarks

- If X has good reduction, then ${}^{\mathrm{Vol}}\int_x^y \omega = {}^{\mathrm{BC}}\int_\gamma \omega$.
- The Berkovich–Coleman integral is local, i.e., if $U \subset X^{\mathrm{an}}$ is a subdomain containing γ, then the integral ${}^{\mathrm{BC}}\int_\gamma \omega$ can be computed from U, $\omega|_U$ and γ.



Remarks

- If X has good reduction, then ${}^{\mathrm{Vol}}\!\int_x^y \omega = {}^{\mathrm{BC}}\!\int_\gamma \omega$.
- The Berkovich–Coleman integral is local, i.e., if $U \subset X^{\mathrm{an}}$ is a subdomain containing γ, then the integral ${}^{\mathrm{BC}}\!\int_\gamma \omega$ can be computed from U, $\omega|_U$ and γ.



$${}^{\mathrm{BC}}\!\int_\gamma \omega : \text{BC-integral on } X^{\mathrm{an}}$$

$$=$$

$${}^{\mathrm{BC}}\!\int_\gamma \omega|_U : \text{BC-integral on } U$$

p-adic integration theories

${}^{\mathrm{BC}}\!\int$ is generally path-dependent and hence disagrees with ${}^{\mathrm{Vol}}\!\int$.

p-adic integration theories

${}^{\mathrm{BC}}\!\!\int$ is generally path-dependent and hence disagrees with ${}^{\mathrm{Vol}}\!\!\int$. What is the difference?

p-adic integration theories

${}^{\mathrm{BC}}\!\int$ is generally path-dependent and hence disagrees with ${}^{\mathrm{Vol}}\!\int$. What is the difference?

Theorem (Katz–K, K.)

We have

$$ {}^{\mathrm{Vol}}\!\int_P^Q \omega = {}^{\mathrm{BC}}\!\int_\gamma \omega - \sum_i \left(c_i \cdot {}^{\mathrm{BC}}\!\int_{\gamma_i} \omega \right) $$

p-adic integration theories

${}^{\mathrm{BC}}\!\!\int$ is generally path-dependent and hence disagrees with ${}^{\mathrm{Vol}}\!\!\int$. What is the difference?

Theorem (Katz–K, K.)

We have

$$ {}^{\mathrm{Vol}}\!\!\int_P^Q \omega = {}^{\mathrm{BC}}\!\!\int_\gamma \omega - \sum_i \left(c_i \cdot {}^{\mathrm{BC}}\!\!\int_{\gamma_i} \omega \right) $$

where

- γ_i*'s are the "loops" in* X^{an}*, and*

p-adic integration theories

${}^{\mathrm{BC}}\!\int$ is generally path-dependent and hence disagrees with ${}^{\mathrm{Vol}}\!\int$. What is the difference?

Theorem (Katz–K, K.)

We have

$$ {}^{\mathrm{Vol}}\!\int_P^Q \omega = {}^{\mathrm{BC}}\!\int_\gamma \omega - \sum_i \left(c_i \cdot {}^{\mathrm{BC}}\!\int_{\gamma_i} \omega \right) $$

where

- γ_i*'s are the "loops" in* X^{an}*, and*
- c_i*'s are certain "tropical" integrals.*

p-adic integration theories

${}^{\mathrm{BC}}\!\!\int$ is generally path-dependent and hence disagrees with ${}^{\mathrm{Vol}}\!\!\int$. What is the difference?

Theorem (Katz–K, K.)

We have

$$ {}^{\mathrm{Vol}}\!\!\int_P^Q \omega = {}^{\mathrm{BC}}\!\!\int_\gamma \omega - \sum_i \left(c_i \cdot {}^{\mathrm{BC}}\!\!\int_{\gamma_i} \omega \right) $$

where

- γ_i*'s are the "loops" in* X^{an}*, and*
- c_i*'s are certain "tropical" integrals.*

Algorithm (Katz–K, K.)

Compute Vologodsky integrals on hyperelliptic curves using this formula and the fact that the Berkovich–Coleman integral is local.

Come back to the main goal... Overview

§1. Schneider p-adic heights

F - a number field

C - a projective, geometrically connected and smooth curve over F of genus $g \geq 1$

§1. Schneider p-adic heights

F	-	a number field
C	-	a projective, geometrically connected and smooth curve over F of genus $g \geq 1$

Schneider's p-adic height pairing on C is denoted by

$$(\cdot, \cdot)_{\mathsf{Sch}} : \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p.$$

§1. Schneider p-adic heights

F - a number field

C - a projective, geometrically connected and smooth curve over F of genus $g \geq 1$

Schneider's p-adic height pairing on C is denoted by

$$(\cdot,\cdot)_{\mathrm{Sch}} : \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p.$$

It decomposes into local factors.

§1. Schneider p-adic heights

F - a number field
C - a projective, geometrically connected and smooth curve over F of genus $g \geq 1$

Schneider's p-adic height pairing on C is denoted by

$$(\cdot,\cdot)_{\mathrm{Sch}} : \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p.$$

It decomposes into local factors.

For a finite prime $\mathfrak{p}$ of F that lies over p, a formula for

$$(\cdot,\cdot)_{\mathfrak{p}}$$

was given by Werner in the case where C is a *Mumford* curve at $\mathfrak{p}$.

§2.1. Mumford curves

K	-	a finite extension of $\mathbb{Q}_p$
$\vert \cdot \vert$	-	absolute value on K

§2.1. Mumford curves

K	-	a finite extension of $\mathbb{Q}_p$
$\lvert \cdot \rvert$	-	absolute value on K

Definition: A **(p-adic) Schottky group** is a discrete, finitely generated, torsion-free subgroup of $\mathrm{PGL}_2(K)$.

§2.1. Mumford curves

K	-	a finite extension of $\mathbb{Q}_p$
$\lvert \cdot \rvert$	-	absolute value on K

Definition: A **(p-adic) Schottky group** is a discrete, finitely generated, torsion-free subgroup of $\mathrm{PGL}_2(K)$.

Fact: A Schottky group is a free group of finite rank.

§2.1. Mumford curves

K	-	a finite extension of $\mathbb{Q}_p$
$\lvert \cdot \rvert$	-	absolute value on K

Definition: A **(p-adic) Schottky group** is a discrete, finitely generated, torsion-free subgroup of $\mathrm{PGL}_2(K)$.

Fact: A Schottky group is a free group of finite rank.

Any subgroup Γ of $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$.

§2.1. Mumford curves

K - a finite extension of $\mathbb{Q}_p$
$|\cdot|$ - absolute value on K

Definition: A **(p-adic) Schottky group** is a discrete, finitely generated, torsion-free subgroup of $\mathrm{PGL}_2(K)$.

Fact: A Schottky group is a free group of finite rank.

Any subgroup Γ of $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$. Set

$$\mathcal{L}_\Gamma := \text{the set of } \textbf{limit} \text{ points of } \Gamma,$$
$$\Omega_\Gamma := \mathbb{P}^1(\mathbb{C}_p) \setminus \mathcal{L}_\Gamma : \text{the set of } \textbf{ordinary} \text{ points of } \Gamma.$$

§2.1. Mumford curves

K	-	a finite extension of $\mathbb{Q}_p$
$\vert\cdot\vert$	-	absolute value on K

Definition: A **(p-adic) Schottky group** is a discrete, finitely generated, torsion-free subgroup of $\mathrm{PGL}_2(K)$.

Fact: A Schottky group is a free group of finite rank.

Any subgroup Γ of $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$. Set

$$\mathcal{L}_\Gamma := \text{the set of } \textbf{limit} \text{ points of } \Gamma,$$
$$\Omega_\Gamma := \mathbb{P}^1(\mathbb{C}_p) \setminus \mathcal{L}_\Gamma : \text{the set of } \textbf{ordinary} \text{ points of } \Gamma.$$

Then Ω_Γ is the largest subset of $\mathbb{P}^1(\mathbb{C}_p)$ on which Γ acts discontinuously.

§2.1. Mumford curves

K - a finite extension of $\mathbb{Q}_p$
$|\cdot|$ - absolute value on K

Definition: A **(p-adic) Schottky group** is a discrete, finitely generated, torsion-free subgroup of $\mathrm{PGL}_2(K)$.

Fact: A Schottky group is a free group of finite rank.

Any subgroup Γ of $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$. Set

$$\mathcal{L}_\Gamma := \text{the set of } \textbf{limit} \text{ points of } \Gamma,$$
$$\Omega_\Gamma := \mathbb{P}^1(\mathbb{C}_p) \setminus \mathcal{L}_\Gamma : \text{the set of } \textbf{ordinary} \text{ points of } \Gamma.$$

Then Ω_Γ is the largest subset of $\mathbb{P}^1(\mathbb{C}_p)$ on which Γ acts discontinuously.

Question: What is Ω_Γ/Γ?

§2.1. Mumford curves

Theorem (Mumford): Let Γ be a Schottky group of rank g. Then there exists a smooth projective curve X_Γ over K of genus g such that

$$X_\Gamma \simeq \Omega_\Gamma/\Gamma.$$

§2.1. Mumford curves

Theorem (Mumford): Let Γ be a Schottky group of rank g. Then there exists a smooth projective curve X_Γ over K of genus g such that

$$X_\Gamma \simeq \Omega_\Gamma / \Gamma.$$

Example: Take $q \in K^\times$ with $|q| < 1$, and let Γ be the cyclic subgroup of $\mathrm{PGL}_2(K)$ generated by $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$. In this case, $X_\Gamma \simeq E_q$ (Tate elliptic curve).

§2.1. Mumford curves

Theorem (Mumford): Let Γ be a Schottky group of rank g. Then there exists a smooth projective curve X_Γ over K of genus g such that

$$X_\Gamma \simeq \Omega_\Gamma / \Gamma.$$

Example: Take $q \in K^\times$ with $|q| < 1$, and let Γ be the cyclic subgroup of $\mathrm{PGL}_2(K)$ generated by $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$. In this case, $X_\Gamma \simeq E_q$ (Tate elliptic curve).

Remark: For any Schottky group Γ, X_Γ has *split degenerate* reduction:

§2.1. Mumford curves

Theorem (Mumford): Let Γ be a Schottky group of rank g. Then there exists a smooth projective curve X_Γ over K of genus g such that

$$X_\Gamma \simeq \Omega_\Gamma / \Gamma.$$

Example: Take $q \in K^\times$ with $|q| < 1$, and let Γ be the cyclic subgroup of $\mathrm{PGL}_2(K)$ generated by $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$. In this case, $X_\Gamma \simeq E_q$ (Tate elliptic curve).

Remark: For any Schottky group Γ, X_Γ has *split degenerate* reduction: it has a semistable $\mathcal{O}_K$-model $\mathfrak{X}$ such that

- all irreducible components of $\mathfrak{X}_k$ are isomorphic to $\mathbb{P}^1_k$, and
- all double points are k-rational with two k-rational branches,

where k is the residue field.

§2.1. Mumford curves

Example 1: If X_Γ has genus 1, then

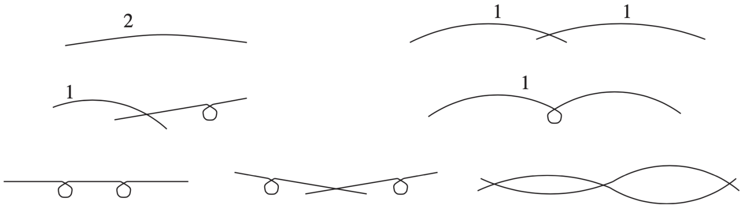
$$\text{split degenerate reduction} = \text{split multiplicative reduction}.$$

§2.1. Mumford curves

Example 1: If X_Γ has genus 1, then

$$\text{split degenerate reduction} = \text{split multiplicative reduction}.$$

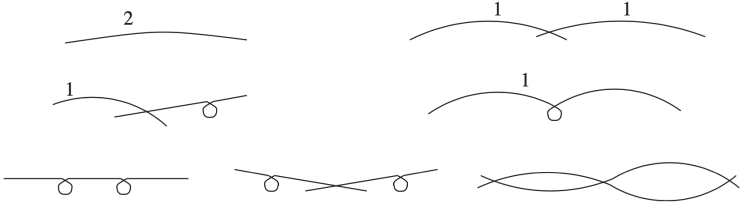
Example 2: There are precisely 7 stable curves of genus 2 (over an algebraically closed field):



Example 1: If X_Γ has genus 1, then

$$\text{split degenerate reduction} = \text{split multiplicative reduction}.$$

Example 2: There are precisely 7 stable curves of genus 2 (over an algebraically closed field):



A genus 2 curve has split degenerate reduction precisely when the special fiber of its stable model is one of the three pictures at the bottom (picture taken from Liu's **Algebraic Geometry and Arithmetic Curves** book).

§2.1. Mumford curves

Theorem (Mumford): The map $\Gamma \mapsto X_\Gamma$ induces a bijection

$$\left\{\begin{matrix}\text{conjugacy classes of Schottky} \\ \text{groups in } \mathrm{PGL}_2(K)\end{matrix}\right\} \to \left\{\begin{matrix}\text{isomorphism classes of curves over} \\ K \text{ with split degenerate reduction}\end{matrix}\right\}.$$

§2.1. Mumford curves

Theorem (Mumford): The map $\Gamma \mapsto X_\Gamma$ induces a bijection

$$\left\{\begin{array}{l}\text{conjugacy classes of Schottky} \\ \text{groups in } \mathrm{PGL}_2(K)\end{array}\right\} \to \left\{\begin{array}{l}\text{isomorphism classes of curves over} \\ K \text{ with split degenerate reduction}\end{array}\right\}.$$

Definition: A curve X over K is called a **Mumford curve** if

$$X \simeq X_\Gamma$$

for some Schottky group Γ in $\mathrm{PGL}_2(K)$.

§2.1. Mumford curves

Theorem (Mumford): The map $\Gamma \mapsto X_\Gamma$ induces a bijection

$$\left\{\begin{matrix}\text{conjugacy classes of Schottky} \\ \text{groups in } \mathrm{PGL}_2(K)\end{matrix}\right\} \to \left\{\begin{matrix}\text{isomorphism classes of curves over} \\ K \text{ with split degenerate reduction}\end{matrix}\right\}.$$

Definition: A curve X over K is called a **Mumford curve** if

$$X \simeq X_\Gamma$$

for some Schottky group Γ in $\mathrm{PGL}_2(K)$.

Remark: Mumford curves = curves with split degenerate reduction.

§2.2. Hyperelliptic Mumford curves

A matrix $\gamma \in \mathrm{PGL}_2(K)$ is called **elliptic** if its eigenvalues are different but have the same absolute value.

§2.2. Hyperelliptic Mumford curves

A matrix $\gamma \in \mathrm{PGL}_2(K)$ is called **elliptic** if its eigenvalues are different but have the same absolute value. Consider elliptic matrices $s_0, \ldots, s_g$ in $\mathrm{PGL}_2(K)$ of order 2 such that the group $\Gamma^{'} := \langle s_0, \ldots, s_g \rangle$ is

- discrete, and
- the free product $\langle s_0 \rangle * \cdots * \langle s_g \rangle$.

§2.2. Hyperelliptic Mumford curves

A matrix $\gamma \in \mathrm{PGL}_2(K)$ is called **elliptic** if its eigenvalues are different but have the same absolute value. Consider elliptic matrices $s_0, \dots, s_g$ in $\mathrm{PGL}_2(K)$ of order 2 such that the group $\Gamma^{'} := \langle s_0, \dots, s_g \rangle$ is

- discrete, and
- the free product $\langle s_0 \rangle * \cdots * \langle s_g \rangle$.

Note that $\Gamma^{'}$ is not a Schottky group.

§2.2. Hyperelliptic Mumford curves

A matrix $\gamma \in \mathrm{PGL}_2(K)$ is called **elliptic** if its eigenvalues are different but have the same absolute value. Consider elliptic matrices $s_0, \ldots, s_g$ in $\mathrm{PGL}_2(K)$ of order 2 such that the group $\Gamma' := \langle s_0, \ldots, s_g \rangle$ is

- discrete, and
- the free product $\langle s_0 \rangle * \cdots * \langle s_g \rangle$.

Note that Γ' is not a Schottky group.

Consider the homomorphism

$$\Phi : \Gamma' \to \{\pm 1\}, \quad s_i \mapsto -1 \text{ for all } i,$$

and set

$$\Gamma := \ker(\Phi).$$

§2.2. Hyperelliptic Mumford curves

A matrix $\gamma \in \mathrm{PGL}_2(K)$ is called **elliptic** if its eigenvalues are different but have the same absolute value. Consider elliptic matrices $s_0, \ldots, s_g$ in $\mathrm{PGL}_2(K)$ of order 2 such that the group $\Gamma' := \langle s_0, \ldots, s_g \rangle$ is

- discrete, and
- the free product $\langle s_0 \rangle * \cdots * \langle s_g \rangle$.

Note that Γ' is not a Schottky group.

Consider the homomorphism

$$\Phi : \Gamma' \to \{\pm 1\}, \quad s_i \mapsto -1 \text{ for all } i,$$

and set

$$\Gamma := \ker(\Phi).$$

Then

§2.2. Hyperelliptic Mumford curves

- Γ is an index 2 subgroup of Γ'.

§2.2. Hyperelliptic Mumford curves

- Γ is an index 2 subgroup of Γ'.
- Γ is a Schottky group, freely generated by $\gamma_i := s_i s_0$, $i = 1, \ldots, g$.

§2.2. Hyperelliptic Mumford curves

- Γ is an index 2 subgroup of Γ'.
- Γ is a Schottky group, freely generated by $\gamma_i := s_i s_0$, $i = 1, \ldots, g$.
- Γ and Γ' have the same set of ordinary points, call it Ω.

§2.2. Hyperelliptic Mumford curves

- Γ is an index 2 subgroup of $\Gamma^{'}$.
- Γ is a Schottky group, freely generated by $\gamma_i := s_i s_0$, $i = 1, \ldots, g$.
- Γ and $\Gamma^{'}$ have the same set of ordinary points, call it Ω.
- The following map has degree 2:

$$\Omega/\Gamma \to \Omega/\Gamma^{'}, \quad a\Gamma \mapsto a\Gamma^{'};$$

so the Mumford curve $X_\Gamma = \Omega/\Gamma$ is a double cover of $\Omega/\Gamma^{'}$.

§2.2. Hyperelliptic Mumford curves

- Γ is an index 2 subgroup of Γ'.
- Γ is a Schottky group, freely generated by $\gamma_i := s_i s_0$, $i = 1, \ldots, g$.
- Γ and Γ' have the same set of ordinary points, call it Ω.
- The following map has degree 2:

$$\Omega/\Gamma \to \Omega/\Gamma', \quad a\Gamma \mapsto a\Gamma';$$

so the Mumford curve $X_\Gamma = \Omega/\Gamma$ is a double cover of Ω/Γ'.

Question: What is Ω/Γ'?

§2.2. Hyperelliptic Mumford curves

- Γ is an index 2 subgroup of Γ'.
- Γ is a Schottky group, freely generated by $\gamma_i := s_i s_0$, $i = 1, \ldots, g$.
- Γ and Γ' have the same set of ordinary points, call it Ω.
- The following map has degree 2:

$$\Omega/\Gamma \to \Omega/\Gamma', \quad a\Gamma \mapsto a\Gamma';$$

so the Mumford curve $X_\Gamma = \Omega/\Gamma$ is a double cover of Ω/Γ'.

Question: What is Ω/Γ'?

For suitably chosen $a, b \in \Omega$, the (theta) function

$$F(z) := F_{a,b}(z) := \prod_{\gamma \in \Gamma'} \frac{z - \gamma(a)}{z - \gamma(b)}, \quad z \in \Omega$$

is Γ'-invariant and induces an isomorphism $\Omega/\Gamma' \simeq \mathbb{P}^1$.

§2.2. Hyperelliptic Mumford curves

Result: The Mumford curve $X_\Gamma = \Omega/\Gamma$ is actually a hyperelliptic Mumford curve.

§2.2. Hyperelliptic Mumford curves

Result: The Mumford curve $X_\Gamma = \Omega/\Gamma$ is actually a hyperelliptic Mumford curve.

Question: Can we be more precise?

§2.2. Hyperelliptic Mumford curves

Result: The Mumford curve $X_\Gamma = \Omega/\Gamma$ is actually a hyperelliptic Mumford curve.

Question: Can we be more precise?

Theorem (van der Put): Write the fixed points of s_i as $\{a_i, b_i\}$. Then $a_i, b_i \in \Omega$, and an equation of X_Γ is given by

$$y^2 = \prod_{i=0}^{g} (x - F(a_i))(x - F(b_i)).$$

§2.2. Hyperelliptic Mumford curves

Result: The Mumford curve $X_\Gamma = \Omega/\Gamma$ is actually a hyperelliptic Mumford curve.

Question: Can we be more precise?

Theorem (van der Put): Write the fixed points of s_i as $\{a_i, b_i\}$. Then $a_i, b_i \in \Omega$, and an equation of X_Γ is given by

$$y^2 = \prod_{i=0}^{g}(x - F(a_i))(x - F(b_i)).$$

Remarks:

- The group Γ is called a **(p-adic) Whittaker** group.

§2.2. Hyperelliptic Mumford curves

Result: The Mumford curve $X_\Gamma = \Omega/\Gamma$ is actually a hyperelliptic Mumford curve.

Question: Can we be more precise?

Theorem (van der Put): Write the fixed points of s_i as $\{a_i, b_i\}$. Then $a_i, b_i \in \Omega$, and an equation of X_Γ is given by

$$y^2 = \prod_{i=0}^{g}(x - F(a_i))(x - F(b_i)).$$

Remarks:

- The group Γ is called a **(p-adic) Whittaker** group.
- Every hyperelliptic Mumford curve can be parametrized by a Whittaker group in this way.

§2.3. Jacobians of Mumford curves

Now let A be an abelian variety over K of dimension g.

§2.3. Jacobians of Mumford curves

Now let A be an abelian variety over K of dimension g. We say A is **uniformizable** if

$$A(K) \simeq (K^\times)^g / \Lambda$$

for some lattice Λ.

Now let A be an abelian variety over K of dimension g. We say A is **uniformizable** if

$$A(K) \simeq (K^\times)^g/\Lambda$$

for some lattice Λ. Not every abelian variety is uniformizable.

§2.3. Jacobians of Mumford curves

Now let A be an abelian variety over K of dimension g. We say A is **uniformizable** if

$$A(K) \simeq (K^{\times})^g / \Lambda$$

for some lattice Λ. Not every abelian variety is uniformizable.

Question: Which abelian varieties are uniformizable?

§2.3. Jacobians of Mumford curves

Now let A be an abelian variety over K of dimension g. We say A is **uniformizable** if

$$A(K) \simeq (K^\times)^g/\Lambda$$

for some lattice Λ. Not every abelian variety is uniformizable.

Question: Which abelian varieties are uniformizable?

Theorem (Mumford): If A is the Jacobian variety of a Mumford curve over K, then it is uniformizable.

§2.3. Jacobians of Mumford curves

Now let A be an abelian variety over K of dimension g. We say A is **uniformizable** if

$$A(K) \simeq (K^\times)^g / \Lambda$$

for some lattice Λ. Not every abelian variety is uniformizable.

Question: Which abelian varieties are uniformizable?

Theorem (Mumford): If A is the Jacobian variety of a Mumford curve over K, then it is uniformizable.

Result: Not only Mumford curves, but also their Jacobians have nice reduction types.

§3.1. Theta functions

K - $F_{\mathfrak{p}}$; a finite extension of $\mathbb{Q}_p$
X - $C \otimes K$; a curve over K of genus g

§3.1. Theta functions

K - $F_{\mathfrak{p}}$; a finite extension of $\mathbb{Q}_p$
X - $C \otimes K$; a curve over K of genus g

Assume X is a Mumford curve. Let Γ be a Schottky group s.t. $X \simeq \Omega/\Gamma$.

§3.1. Theta functions

K - $F_{\mathfrak{p}}$; a finite extension of $\mathbb{Q}_p$
X - $C \otimes K$; a curve over K of genus g

Assume X is a Mumford curve. Let Γ be a Schottky group s.t. $X \simeq \Omega/\Gamma$.

Fix two parameters $a, b \in \Omega$, and define the **theta function** on Ω:

$$\Theta(a, b; z) := \prod_{\gamma \in \Gamma} \frac{z - \gamma(a)}{z - \gamma(b)}, \quad z \in \Omega.$$

§3.1. Theta functions

K - $F_{\mathfrak{p}}$; a finite extension of $\mathbb{Q}_p$
X - $C \otimes K$; a curve over K of genus g

Assume X is a Mumford curve. Let Γ be a Schottky group s.t. $X \simeq \Omega/\Gamma$.

Fix two parameters $a, b \in \Omega$, and define the **theta function** on Ω:

$$\Theta(a, b; z) := \prod_{\gamma \in \Gamma} \frac{z - \gamma(a)}{z - \gamma(b)}, \quad z \in \Omega.$$

It's an automorphic form with constant factors of automorphy: for all $\gamma \in \Gamma$ and all $z \in \Omega$,

$$\Theta(a, b; z) = c(a, b, \gamma) \cdot \Theta(a, b; \gamma(z))$$

for some $c(a, b, \gamma) \in K^\times$.

§3.2. Werner's formula for $(\cdot,\cdot)_{\mathfrak{p}}$

Now let $\rho\colon K^\times \to \mathbb{Q}_p$ be a non-trivial continuous homomorphism. In practice, it will be $\log_p \circ N_{K/\mathbb{Q}_p}$ where $\log_p$ is the branch of the p-adic logarithm that sends p to 0.

§3.2. Werner's formula for $(\cdot,\cdot)_{\mathfrak{p}}$

Now let $\rho\colon K^\times \to \mathbb{Q}_p$ be a non-trivial continuous homomorphism. In practice, it will be $\log_p \circ N_{K/\mathbb{Q}_p}$ where $\log_p$ is the branch of the p-adic logarithm that sends p to 0.

Take $D, E \in \mathrm{Div}^0(X)$. Since the pairing $(\cdot,\cdot)_{\mathfrak{p}}$ is additive in both arguments, we can assume that

$$D = (x) - (y) \quad \text{and} \quad E = (z) - (w)$$

for some $x, y, z, w \in X = \Omega/\Gamma$.

§3.2. Werner's formula for $(\cdot,\cdot)_{\mathfrak{p}}$

Now let $\rho\colon K^\times \to \mathbb{Q}_p$ be a non-trivial continuous homomorphism. In practice, it will be $\log_p \circ N_{K/\mathbb{Q}_p}$ where $\log_p$ is the branch of the p-adic logarithm that sends p to 0.

Take $D, E \in \mathrm{Div}^0(X)$. Since the pairing $(\cdot,\cdot)_{\mathfrak{p}}$ is additive in both arguments, we can assume that

$$D = (x) - (y) \quad \text{and} \quad E = (z) - (w)$$

for some $x, y, z, w \in X = \Omega/\Gamma$.

Theorem (Werner): Choose preimages x', y', z', w' in Ω.

§3.2. Werner's formula for $(\cdot,\cdot)_{\mathfrak{p}}$

Now let $\rho\colon K^\times \to \mathbb{Q}_p$ be a non-trivial continuous homomorphism. In practice, it will be $\log_p \circ N_{K/\mathbb{Q}_p}$ where $\log_p$ is the branch of the p-adic logarithm that sends p to 0.

Take $D, E \in \mathrm{Div}^0(X)$. Since the pairing $(\cdot,\cdot)_{\mathfrak{p}}$ is additive in both arguments, we can assume that

$$D = (x) - (y) \quad \text{and} \quad E = (z) - (w)$$

for some $x, y, z, w \in X = \Omega/\Gamma$.

Theorem (Werner): Choose preimages x', y', z', w' in Ω. We then have

$$(D, E)_{\mathfrak{p}} = \rho\left(\frac{\Theta(x', y'; z')}{\Theta(x', y'; w')}\right) - \begin{array}{c}\text{another function}\\ \text{in terms of } \Theta.\end{array}$$

§4.1. Setting

F - a number field

C - a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

§4.1. Setting

F	-	a number field
C	-	a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p.

§4.1. Setting

F - a number field

C - a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p. We'll use Werner's formula to compute $(D, E)_{\mathfrak{p}}$.

§4.1. Setting

F - a number field

C - a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p. We'll use Werner's formula to compute $(D, E)_\mathfrak{p}$. There are three main steps:

- Θ: computing theta functions Θ,

§4.1. Setting

F - a number field

C - a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p. We'll use Werner's formula to compute $(D, E)_{\mathfrak{p}}$. There are three main steps:

- Θ: computing theta functions Θ,
- Γ: determining the Schottky group Γ,

§4.1. Setting

F	-	a number field
C	-	a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p. We'll use Werner's formula to compute $(D, E)_{\mathfrak{p}}$. There are three main steps:

- Θ: computing theta functions Θ,
- Γ: determining the Schottky group Γ,
- Ω: lifting points from the curve to Ω.

§4.1. Setting

F	-	a number field
C	-	a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p. We'll use Werner's formula to compute $(D, E)_{\mathfrak{p}}$. There are three main steps:

- Θ: computing theta functions Θ,
- Γ: determining the Schottky group Γ,
- Ω: lifting points from the curve to Ω.

Set $K = F_{\mathfrak{p}}$ and $X = C \otimes K$.

§4.1. Setting

F - a number field
C - a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p. We'll use Werner's formula to compute $(D, E)_{\mathfrak{p}}$. There are three main steps:

- Θ: computing theta functions Θ,
- Γ: determining the Schottky group Γ,
- Ω: lifting points from the curve to Ω.

Set $K = F_{\mathfrak{p}}$ and $X = C \otimes K$. Since X is a hyperelliptic Mumford curve of genus g, we have

- Γ: Whittaker group such that $X \simeq \Omega/\Gamma$ with gens $\gamma_1, \ldots, \gamma_g$,

§4.1. Setting

F - a number field

C - a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p. We'll use Werner's formula to compute $(D, E)_{\mathfrak{p}}$. There are three main steps:

- Θ: computing theta functions Θ,
- Γ: determining the Schottky group Γ,
- Ω: lifting points from the curve to Ω.

Set $K = F_{\mathfrak{p}}$ and $X = C \otimes K$. Since X is a hyperelliptic Mumford curve of genus g, we have

- Γ: Whittaker group such that $X \simeq \Omega/\Gamma$ with gens $\gamma_1, \ldots, \gamma_g$,
- Γ': discrete and free group containing Γ with gens $s_0, \ldots, s_g$,

§4.1. Setting

F	-	a number field
C	-	a hyperell. curve over F of genus $g \geq 1$ s.t. for every finite prime $\mathfrak{p}$ of F above p, C is a Mumford curve at $\mathfrak{p}$.

Take $D, E \in \mathrm{Div}^0(C)$, and fix a finite prime $\mathfrak{p}$ of F above p. We'll use Werner's formula to compute $(D, E)_{\mathfrak{p}}$. There are three main steps:

- Θ: computing theta functions Θ,
- Γ: determining the Schottky group Γ,
- Ω: lifting points from the curve to Ω.

Set $K = F_{\mathfrak{p}}$ and $X = C \otimes K$. Since X is a hyperelliptic Mumford curve of genus g, we have

- Γ: Whittaker group such that $X \simeq \Omega/\Gamma$ with gens $\gamma_1, \ldots, \gamma_g$,
- Γ': discrete and free group containing Γ with gens $s_0, \ldots, s_g$,
- a_i, b_i: fixed points of s_i.

§4.2. Θ: computing theta functions

Recall that Γ is free.

Recall that Γ is free. Then every element γ in Γ can be written as a unique shortest product

$$\gamma = h_1 \dots h_\ell, \quad h_i \in \{\gamma_1^{\pm}, \dots, \gamma_g^{\pm}\}.$$

The **length** of γ is ℓ.

§4.2. Θ: computing theta functions

Recall that Γ is free. Then every element γ in Γ can be written as a unique shortest product

$$\gamma = h_1 \dots h_\ell, \quad h_i \in \{\gamma_1^{\pm}, \dots, \gamma_g^{\pm}\}.$$

The **length** of γ is ℓ. For $m \in \mathbb{Z}_{\geq 0}$, set

$$\Gamma_m := \text{the set of elements of } \Gamma \text{ with length } m,$$

$$\Theta_m(a, b; z) := \prod_{\gamma \in \Gamma_m} \frac{z - \gamma(a)}{z - \gamma(b)}.$$

§4.2. Θ: computing theta functions

Recall that Γ is free. Then every element γ in Γ can be written as a unique shortest product

$$\gamma = h_1 \dots h_\ell, \quad h_i \in \{\gamma_1^\pm, \dots, \gamma_g^\pm\}.$$

The **length** of γ is ℓ. For $m \in \mathbb{Z}_{\geq 0}$, set

$$\Gamma_m := \text{the set of elements of } \Gamma \text{ with length } m,$$

$$\Theta_m(a, b; z) := \prod_{\gamma \in \Gamma_m} \frac{z - \gamma(a)}{z - \gamma(b)}.$$

Then $\Theta_m(a, b; z)$ is a finite product and

$$\Theta(a, b; z) = \prod_{m=0}^{\infty} \Theta_m(a, b; z).$$

§4.2. Θ: computing theta functions

Recall that Γ is free. Then every element γ in Γ can be written as a unique shortest product

$$\gamma = h_1 \dots h_\ell, \quad h_i \in \{\gamma_1^{\pm}, \dots, \gamma_g^{\pm}\}.$$

The **length** of γ is ℓ. For $m \in \mathbb{Z}_{\geq 0}$, set

$$\Gamma_m := \text{the set of elements of } \Gamma \text{ with length } m,$$

$$\Theta_m(a, b; z) := \prod_{\gamma \in \Gamma_m} \frac{z - \gamma(a)}{z - \gamma(b)}.$$

Then $\Theta_m(a, b; z)$ is a finite product and

$$\Theta(a, b; z) = \prod_{m=0}^{\infty} \Theta_m(a, b; z).$$

Remark: Another method due to Masdeu–Xarles allows us to compute this function in a comparatively faster way.

§4.2. Γ: determining the Schottky group Γ

To find Γ, it suffices to compute

$$S := \{a_0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, a_g, b_g\}.$$

§4.2. Γ: determining the Schottky group Γ

To find Γ, it suffices to compute

$$S := \{a_0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, a_g, b_g\}.$$

Set

$$R := \{\text{roots of the defining polynomial of } X\}.$$

§4.2. Γ: determining the Schottky group Γ

To find Γ, it suffices to compute

$$S := \{a_0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, a_g, b_g\}.$$

Set

$$R := \{\text{roots of the defining polynomial of } X\}.$$

Recall that

$$S = F^{-1}(R), \quad F(z) = F_{a,b}(z) = \prod_{\gamma \in \Gamma'} \frac{z - \gamma(a)}{z - \gamma(b)} \text{ for suitable } a, b \in \Omega.$$

§4.2. Γ: determining the Schottky group Γ

To find Γ, it suffices to compute

$$S := \{a_0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, a_g, b_g\}.$$

Set

$$R := \{\text{roots of the defining polynomial of } X\}.$$

Recall that

$$S = F^{-1}(R), \quad F(z) = F_{a,b}(z) = \prod_{\gamma \in \Gamma'} \frac{z - \gamma(a)}{z - \gamma(b)} \text{ for suitable } a, b \in \Omega.$$

So it suffices to compute the inverse image of R under F. But F is defined in terms of Γ', which we don't know yet.

§4.2. Γ: determining the Schottky group Γ

To find Γ, it suffices to compute

$$S := \{a_0, b_0, a_1, b_1, \dots, a_{g-1}, b_{g-1}, a_g, b_g\}.$$

Set

$$R := \{\text{roots of the defining polynomial of } X\}.$$

Recall that

$$S = F^{-1}(R), \quad F(z) = F_{a,b}(z) = \prod_{\gamma \in \Gamma'} \frac{z - \gamma(a)}{z - \gamma(b)} \text{ for suitable } a, b \in \Omega.$$

So it suffices to compute the inverse image of R under F. But F is defined in terms of Γ', which we don't know yet.

Question: Can we invert a function we don't know?

§4.2. Γ: determining the Schottky group Γ

To find Γ, it suffices to compute

$$S := \{a_0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, a_g, b_g\}.$$

Set

$$R := \{\text{roots of the defining polynomial of } X\}.$$

Recall that

$$S = F^{-1}(R), \quad F(z) = F_{a,b}(z) = \prod_{\gamma \in \Gamma'} \frac{z - \gamma(a)}{z - \gamma(b)} \text{ for suitable } a, b \in \Omega.$$

So it suffices to compute the inverse image of R under F. But F is defined in terms of Γ', which we don't know yet.

Question: Can we invert a function we don't know?

Answer: Of course not. But, thanks to Kadziela's approximation theorem, we can simultaneously approximate both S and F such that

$$F(S) = R.$$

§4.2. Γ: determining the Schottky group Γ

We may assume that $S = \{0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, 1, \infty\}$. Then the parameters $a = 0$ and $b = 1$ are suitable.

§4.2. Γ: determining the Schottky group Γ

We may assume that $S = \{0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, 1, \infty\}$. Then the parameters $a = 0$ and $b = 1$ are suitable.

The following is a generalization of Kadziela's main approximation theorem:

§4.2. Γ: determining the Schottky group Γ

We may assume that $S = \{0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, 1, \infty\}$. Then the parameters $a = 0$ and $b = 1$ are suitable.

The following is a generalization of Kadziela's main approximation theorem:

Theorem (K.–Masdeu–Müller–van der Put)

- *$F(0) = 0$, $F(1) = \infty$, and $F(\infty) = 1$.*

§4.2. Γ: determining the Schottky group Γ

We may assume that $S = \{0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, 1, \infty\}$. Then the parameters $a = 0$ and $b = 1$ are suitable.

The following is a generalization of Kadziela's main approximation theorem:

Theorem (K.–Masdeu–Müller–van der Put)

- $F(0) = 0$, $F(1) = \infty$, *and* $F(\infty) = 1$.

For $z \in S \setminus \{0, 1, \infty\}$, *we have*

§4.2. Γ: determining the Schottky group Γ

We may assume that $S = \{0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, 1, \infty\}$. Then the parameters $a = 0$ and $b = 1$ are suitable.

The following is a generalization of Kadziela's main approximation theorem:

Theorem (K.–Masdeu–Müller–van der Put)

- *$F(0) = 0$, $F(1) = \infty$, and $F(\infty) = 1$.*

For $z \in S \setminus \{0, 1, \infty\}$, we have

- *$F(z) \equiv 0$ mod π,*

§4.2. Γ: determining the Schottky group Γ

We may assume that $S = \{0, b_0, a_1, b_1, \dots, a_{g-1}, b_{g-1}, 1, \infty\}$. Then the parameters $a = 0$ and $b = 1$ are suitable.

The following is a generalization of Kadziela's main approximation theorem:

Theorem (K.–Masdeu–Müller–van der Put)

- *$F(0) = 0$, $F(1) = \infty$, and $F(\infty) = 1$.*

For $z \in S \setminus \{0, 1, \infty\}$, we have

- *$F(z) \equiv 0 \mod \pi$,*
- $$F(z) \equiv \begin{cases} -4b_0 \prod_{i=1}^{g-1} \left(1 - \left(\frac{a_i - b_i}{a_i + b_i}\right)^2\right) \mod \pi^2 & \text{if } z = b_0, \\ -2z \prod_{i=1}^{g-1} \left(1 + \frac{(a_i - b_i)^2}{(a_i + b_i)(2z - a_i - b_i)}\right) \mod \pi^2 & \text{otherwise,} \end{cases}$$

§4.2. Γ: determining the Schottky group Γ

We may assume that $S = \{0, b_0, a_1, b_1, \ldots, a_{g-1}, b_{g-1}, 1, \infty\}$. Then the parameters $a = 0$ and $b = 1$ are suitable.

The following is a generalization of Kadziela's main approximation theorem:

Theorem (K.–Masdeu–Müller–van der Put)

- *$F(0) = 0$, $F(1) = \infty$, and $F(\infty) = 1$.*

For $z \in S \setminus \{0, 1, \infty\}$, we have

- *$F(z) \equiv 0 \mod \pi$,*
- $$F(z) \equiv \begin{cases} -4b_0 \prod_{i=1}^{g-1} \left(1 - \left(\frac{a_i - b_i}{a_i + b_i}\right)^2\right) \mod \pi^2 & \text{if } z = b_0, \\ -2z \prod_{i=1}^{g-1} \left(1 + \frac{(a_i - b_i)^2}{(a_i + b_i)(2z - a_i - b_i)}\right) \mod \pi^2 & \text{otherwise,} \end{cases}$$
- *$F(z) \mod \pi^t = \prod_{m=0}^{t-2} F_m(z \mod \pi^t)$ for $t \geq 3$,*

where π is a uniformizer in K.

§4.2. Γ: determining the Schottky group Γ

Recall that R consists the roots of the defining polynomial of X. We may assume that

$$R = \{0, r_0, r_1, \ldots, r_{2g-2}, 1, \infty\}.$$

§4.2. Γ: determining the Schottky group Γ

Recall that R consists the roots of the defining polynomial of X. We may assume that

$$R = \{0, r_0, r_1, \ldots, r_{2g-2}, 1, \infty\}.$$

If we know correctly the elements z in $S \setminus \{0, 1, \infty\}$ mod π^t, and use them to approximate

- the elliptic matrices s_i,
- the group Γ',
- the theta function $F(z)$,

§4.2. Γ: determining the Schottky group Γ

Recall that R consists the roots of the defining polynomial of X. We may assume that

$$R = \{0, r_0, r_1, \ldots, r_{2g-2}, 1, \infty\}.$$

If we know correctly the elements z in $S \setminus \{0, 1, \infty\}$ mod π^t, and use them to approximate

- the elliptic matrices s_i,
- the group Γ',
- the theta function $F(z)$,

then the images $F(z)$ will also correctly approximate the roots points in R mod π^t.

§4.2. Γ: determining the Schottky group Γ

Recall that R consists the roots of the defining polynomial of X. We may assume that

$$R = \{0, r_0, r_1, \ldots, r_{2g-2}, 1, \infty\}.$$

If we know correctly the elements z in $S \setminus \{0, 1, \infty\}$ mod π^t, and use them to approximate

- the elliptic matrices s_i,
- the group Γ',
- the theta function $F(z)$,

then the images $F(z)$ will also correctly approximate the roots points in R mod π^t.

In other words, we guess the elements in S digit by digit using the approximation theorem.

§4.2. Γ: determining the Schottky group Γ

Recall that R consists the roots of the defining polynomial of X. We may assume that

$$R = \{0, r_0, r_1, \ldots, r_{2g-2}, 1, \infty\}.$$

If we know correctly the elements z in $S \setminus \{0, 1, \infty\}$ mod π^t, and use them to approximate

- the elliptic matrices s_i,
- the group Γ',
- the theta function $F(z)$,

then the images $F(z)$ will also correctly approximate the roots points in R mod π^t.

In other words, we guess the elements in S digit by digit using the approximation theorem. This algorithm is a brute force algorithm but works quite well when g and p are small.

§4.2. Ω: lifting points from the curve to Ω

Take $P = (x, y)$ in $X = \Omega/\Gamma$. Our goal is to compute a lift z of P in Ω.

§4.2. Ω: lifting points from the curve to Ω

Take $P = (x, y)$ in $X = \Omega/\Gamma$. Our goal is to compute a lift z of P in Ω.

Consider the commutative diagram

$$\begin{array}{ccc} \Omega & & \\ \downarrow & \searrow & \\ \Omega/\Gamma & \rightarrow & \Omega/\Gamma' \\ \downarrow & & \downarrow \\ X & \rightarrow & \mathbb{P}^1 \end{array}$$

where the isomorphism $\Omega/\Gamma' \simeq \mathbb{P}^1$ is induced by $F = F_{a,b} : \Omega \rightarrow \mathbb{P}^1$ for parameters $a, b \in \Omega$.

§4.2. Ω: lifting points from the curve to Ω

Take $P = (x, y)$ in $X = \Omega/\Gamma$. Our goal is to compute a lift z of P in Ω.

Consider the commutative diagram

$$\begin{array}{ccc} \Omega & & \\ \downarrow & \searrow & \\ \Omega/\Gamma & \rightarrow & \Omega/\Gamma' \\ \downarrow & & \downarrow \\ X & \rightarrow & \mathbb{P}^1 \end{array}$$

where the isomorphism $\Omega/\Gamma' \simeq \mathbb{P}^1$ is induced by $F = F_{a,b} : \Omega \to \mathbb{P}^1$ for parameters $a, b \in \Omega$.

Using Newton iteration, we can find a $z \in \Omega$ such that $F(z) = x$.

§4.2. Ω: lifting points from the curve to Ω

Take $P = (x, y)$ in $X = \Omega/\Gamma$. Our goal is to compute a lift z of P in Ω.

Consider the commutative diagram

$$\begin{array}{ccc} \Omega & & \\ \downarrow & \searrow & \\ \Omega/\Gamma & \to & \Omega/\Gamma' \\ \downarrow & & \downarrow \\ X & \to & \mathbb{P}^1 \end{array}$$

where the isomorphism $\Omega/\Gamma' \simeq \mathbb{P}^1$ is induced by $F = F_{a,b} : \Omega \to \mathbb{P}^1$ for parameters $a, b \in \Omega$.

Using Newton iteration, we can find a $z \in \Omega$ such that $F(z) = x$. Then,

$$\text{the image of } z \text{ in } X \in \{(x, y), (x, -y)\}.$$

§4.2. Ω: lifting points from the curve to Ω

Take $P = (x, y)$ in $X = \Omega/\Gamma$. Our goal is to compute a lift z of P in Ω.

Consider the commutative diagram

$$\begin{array}{ccc} \Omega & & \\ \downarrow & \searrow & \\ \Omega/\Gamma & \to & \Omega/\Gamma' \\ \downarrow & & \downarrow \\ X & \to & \mathbb{P}^1 \end{array}$$

where the isomorphism $\Omega/\Gamma' \simeq \mathbb{P}^1$ is induced by $F = F_{a,b} : \Omega \to \mathbb{P}^1$ for parameters $a, b \in \Omega$.

Using Newton iteration, we can find a $z \in \Omega$ such that $F(z) = x$. Then,

$$\text{the image of } z \text{ in } X \in \{(x, y), (x, -y)\}.$$

Question: But... How do we distinguish?

§4.2. Ω: lifting points from the curve to Ω

Theorem (K.–Masdeu–Müller–van der Put)

Set $\gamma := \gamma_1 \cdots \gamma_g$, *and*

$$H(z) := \Theta(a, \gamma(a); z) \cdot \prod_{i=0}^{g} \Theta(a_i, b; z) \cdot \Theta(b_i, s_0(b); z), \quad z \in \Omega.$$

§4.2. Ω: lifting points from the curve to Ω

Theorem (K.–Masdeu–Müller–van der Put)

Set $\gamma := \gamma_1 \cdots \gamma_g$, *and*

$$H(z) := \Theta(a, \gamma(a); z) \cdot \prod_{i=0}^{g} \Theta(a_i, b; z) \cdot \Theta(b_i, s_0(b); z), \quad z \in \Omega.$$

Then

- *The function* H *is* Γ*-invariant, but not* Γ'*-invariant.*

§4.2. Ω: lifting points from the curve to Ω

Theorem (K.–Masdeu–Müller–van der Put)

Set $\gamma := \gamma_1 \cdots \gamma_g$, *and*

$$H(z) := \Theta(a, \gamma(a); z) \cdot \prod_{i=0}^{g} \Theta(a_i, b; z) \cdot \Theta(b_i, s_0(b); z), \quad z \in \Omega.$$

Then

- *The function* H *is* Γ*-invariant, but not* Γ'*-invariant.*
- *Let* H *also denote the induced element in the function field of* $X = \Omega/\Gamma$*. Then*

$$H^2 = \prod_{i=0}^{g} (x - F(a_i))(x - F(b_i)).$$

§4.2. Ω: lifting points from the curve to Ω

Theorem (K.–Masdeu–Müller–van der Put)

Set $\gamma := \gamma_1 \cdots \gamma_g$, *and*

$$H(z) := \Theta(a, \gamma(a); z) \cdot \prod_{i=0}^{g} \Theta(a_i, b; z) \cdot \Theta(b_i, s_0(b); z), \quad z \in \Omega.$$

Then

- *The function* H *is* Γ*-invariant, but not* Γ'*-invariant.*
- *Let* H *also denote the induced element in the function field of* $X = \Omega/\Gamma$. *Then*

$$H^2 = \prod_{i=0}^{g} (x - F(a_i))(x - F(b_i)).$$

- *The curve* $X = \Omega/\Gamma$ *is parametrized by* $z \in \Omega \mapsto (F(z), H(z))$.

§4.2. Ω: lifting points from the curve to Ω

Theorem (K.–Masdeu–Müller–van der Put)

Set $\gamma := \gamma_1 \cdots \gamma_g$, *and*

$$H(z) := \Theta(a, \gamma(a); z) \cdot \prod_{i=0}^{g} \Theta(a_i, b; z) \cdot \Theta(b_i, s_0(b); z), \quad z \in \Omega.$$

Then

- *The function* H *is* Γ*-invariant, but not* Γ'*-invariant.*
- *Let* H *also denote the induced element in the function field of* $X = \Omega/\Gamma$. *Then*

$$H^2 = \prod_{i=0}^{g} (x - F(a_i))(x - F(b_i)).$$

- *The curve* $X = \Omega/\Gamma$ *is parametrized by* $z \in \Omega \mapsto (F(z), H(z))$.

Corollary: If $H(z) = y$, then z is a lift of P. Else $s_0(z)$ is a lift of P.

§5. Numerical example

Consider the hyperelliptic curve $C/\mathbb{Q}$ given by

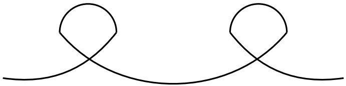
$$y^2 = x^5 - 326x^4 + 1052 \cdot 5^2 x^3 - 5914 \cdot 5^2 x^2 + 39 \cdot 5^5 x.$$

§5. Numerical example

Consider the hyperelliptic curve $C/\mathbb{Q}$ given by

$$y^2 = x^5 - 326x^4 + 1052 \cdot 5^2x^3 - 5914 \cdot 5^2x^2 + 39 \cdot 5^5x.$$

The prime $p = 5$ is a prime of bad reduction. Moreover, the corresponding (stable) reduction is a projective line with two ordinary double points:

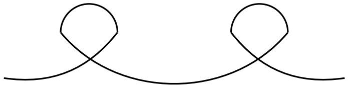


§5. Numerical example

Consider the hyperelliptic curve $C/\mathbb{Q}$ given by

$$y^2 = x^5 - 326x^4 + 1052 \cdot 5^2 x^3 - 5914 \cdot 5^2 x^2 + 39 \cdot 5^5 x.$$

The prime $p = 5$ is a prime of bad reduction. Moreover, the corresponding (stable) reduction is a projective line with two ordinary double points:



Set $D = (x) - (y)$ and $E = (z) - (w)$, where

$$x = (7,\ 1+3\cdot5+4\cdot5^2+5^5+5^6+O(5^7)), \qquad y = (12,\ 1+2\cdot5+3\cdot5^2+5^5+4\cdot5^6+O(5^7)),$$

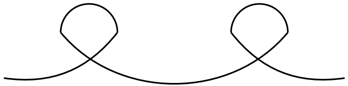
$$z = (-3,\ 1+2\cdot5^2+4\cdot5^4+2\cdot5^5+5^6+O(5^7)), \quad w = (-18,\ 1+3\cdot5+2\cdot5^3+5^4+5^5+2\cdot5^6+O(5^7)).$$

§5. Numerical example

Consider the hyperelliptic curve $C/\mathbb{Q}$ given by

$$y^2 = x^5 - 326x^4 + 1052 \cdot 5^2 x^3 - 5914 \cdot 5^2 x^2 + 39 \cdot 5^5 x.$$

The prime $p = 5$ is a prime of bad reduction. Moreover, the corresponding (stable) reduction is a projective line with two ordinary double points:



Set $D = (x) - (y)$ and $E = (z) - (w)$, where

$$x = (7,\ 1+3\cdot5+4\cdot5^2+5^5+5^6+O(5^7)), \qquad y = (12,\ 1+2\cdot5+3\cdot5^2+5^5+4\cdot5^6+O(5^7)),$$

$$z = (-3,\ 1+2\cdot5^2+4\cdot5^4+2\cdot5^5+5^6+O(5^7)), \qquad w = (-18,\ 1+3\cdot5+2\cdot5^3+5^4+5^5+2\cdot5^6+O(5^7)).$$

Goal

Compute the local height $(D, E)_p$.

§5. Numerical example

We have:

$$a_0 = 0, \qquad b_0 = 3 \cdot 5^3 + 3 \cdot 5^4 + 3 \cdot 5^5 + 3 \cdot 5^6 + O(5^7),$$
$$a_2 = 1, \qquad a_1 = 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 3 \cdot 5^4 + 5^6 + O(5^7),$$
$$b_2 = \infty, \qquad b_1 = 3 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 5^4 + 4 \cdot 5^5 + 3 \cdot 5^6 + O(5^7),$$

§5. Numerical example

We have:

$$\begin{aligned} a_0 &= 0, & b_0 &= 3\cdot 5^3 + 3\cdot 5^4 + 3\cdot 5^5 + 3\cdot 5^6 + O(5^7),\\ a_2 &= 1, & a_1 &= 5 + 2\cdot 5^2 + 2\cdot 5^3 + 3\cdot 5^4 + 5^6 + O(5^7),\\ b_2 &= \infty, & b_1 &= 3\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 5^4 + 4\cdot 5^5 + 3\cdot 5^6 + O(5^7), \end{aligned}$$

$$\gamma_1 = \begin{pmatrix} -375001\cdot 5 & 938432\cdot 5 \\ 2 & 78116 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 928593\cdot 5^3 & 95939\cdot 5^3 \\ 2 & 839746 \end{pmatrix},$$

We have:

$$\begin{aligned} a_0 &= 0, & b_0 &= 3\cdot 5^3 + 3\cdot 5^4 + 3\cdot 5^5 + 3\cdot 5^6 + O(5^7),\\ a_2 &= 1, & a_1 &= 5 + 2\cdot 5^2 + 2\cdot 5^3 + 3\cdot 5^4 + 5^6 + O(5^7),\\ b_2 &= \infty, & b_1 &= 3\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 5^4 + 4\cdot 5^5 + 3\cdot 5^6 + O(5^7), \end{aligned}$$

$$\gamma_1 = \begin{pmatrix} -375001\cdot 5 & 938432\cdot 5 \\ 2 & 78116 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 928593\cdot 5^3 & 95939\cdot 5^3 \\ 2 & 839746 \end{pmatrix},$$

$$(D, E)_5 = 3\cdot 5 + 2\cdot 5^2 + 4\cdot 5^3 + 2\cdot 5^5 + O(5^6).$$

§5. Numerical example

We have:

$$a_0 = 0, \qquad b_0 = 3\cdot 5^3 + 3\cdot 5^4 + 3\cdot 5^5 + 3\cdot 5^6 + O(5^7),$$
$$a_2 = 1, \qquad a_1 = 5 + 2\cdot 5^2 + 2\cdot 5^3 + 3\cdot 5^4 + 5^6 + O(5^7),$$
$$b_2 = \infty, \qquad b_1 = 3\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 5^4 + 4\cdot 5^5 + 3\cdot 5^6 + O(5^7),$$

$$\gamma_1 = \begin{pmatrix} -375001\cdot 5 & 938432\cdot 5 \\ 2 & 78116 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 928593\cdot 5^3 & 95939\cdot 5^3 \\ 2 & 839746 \end{pmatrix},$$

$$(D,E)_5 = 3\cdot 5 + 2\cdot 5^2 + 4\cdot 5^3 + 2\cdot 5^5 + O(5^6).$$

Question: How do we know that this is correct?

§5. Numerical example

We have:

$$a_0 = 0, \qquad b_0 = 3\cdot 5^3 + 3\cdot 5^4 + 3\cdot 5^5 + 3\cdot 5^6 + O(5^7),$$
$$a_2 = 1, \qquad a_1 = 5 + 2\cdot 5^2 + 2\cdot 5^3 + 3\cdot 5^4 + 5^6 + O(5^7),$$
$$b_2 = \infty, \qquad b_1 = 3\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 5^4 + 4\cdot 5^5 + 3\cdot 5^6 + O(5^7),$$

$$\gamma_1 = \begin{pmatrix} -375001\cdot 5 & 938432\cdot 5 \\ 2 & 78116 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 928593\cdot 5^3 & 95939\cdot 5^3 \\ 2 & 839746 \end{pmatrix},$$

$$(D,E)_5 = 3\cdot 5 + 2\cdot 5^2 + 4\cdot 5^3 + 2\cdot 5^5 + O(5^6).$$

Question: How do we know that this is correct?

The function $(\cdot,\cdot)_p$ is symmetric, and we have

$$(E,D)_5 = 3\cdot 5 + 2\cdot 5^2 + 4\cdot 5^3 + 2\cdot 5^5 + O(5^6). \quad :-)$$

From Marc's talk...

Danke Schön!

- *Basic Notions of Rigid Analytic Geometry* - Schneider
- *Non-archimedean Uniformization and Monodromy Pairing* - Papikian
- *Schottky Groups and Mumford Curves* - Gerritzen–van der Put
- *Rigid Geometry of Curves and Their Jacobians* - Lütkebbohmert

- *p-adic Height Pairings I* - Schneider
- *Local Heights on Mumford Curves* - Werner

- *Algorithms for Mumford Curves* - Morrison–Ren
- *Rigid Analytic Uniformization of Hyperelliptic Curves* - Kadziela
- *Algorithms for Heights On Mumford Curves* (to be modified) - K.–Masdeu–Müller–van der Put