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

Number Theory in Montserrat 2023
June 28, 2023

From Benasque...

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 consturcted by Coleman–Gross, Schneider, Mazur–Tate and Nekovář.

Introduction

In the literature, there are several p-adic height pairings. Some of them were consturcted 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 consturcted 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 consturcted 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.

Goal

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

Overview

1. p-adic numbers & rigid analytic geometry
2. Schneider p-adic heights
3. Mumford curves and their Jacobians
   - Mumford curves
   - Hyperelliptic Mumford curves
   - Jacobians of Mumford curves
4. Schneider heights on Mumford curves
   - Theta functions
   - Werner's formula
5. Computing Schneider heights on hyperelliptic Mumford curves
   - Setting
   - An algorithm for local components at p
6. Numerical example

Fix once and for all a prime number p.

§1. p-adic numbers & rigid analytic geometry

Fix once and for all a prime number p.

Let $|\cdot|_p$ denote the p-adic absolute value on $\mathbb{Q}$.

§1. p-adic numbers & rigid analytic geometry

Fix once and for all a prime number p.

Let $|\cdot|_p$ denote the p-adic absolute value on $\mathbb{Q}$.

$$\mathbb{Q}_p,\ \mathbb{C}_p \approx p\text{-adic analogues of } \mathbb{R},\ \mathbb{C}.$$

§1. p-adic numbers & rigid analytic geometry

Fix once and for all a prime number p.

Let $|\cdot|_p$ denote the p-adic absolute value on $\mathbb{Q}$.

$$\mathbb{Q}_p,\ \mathbb{C}_p \approx p\text{-adic analogues of } \mathbb{R},\ \mathbb{C}.$$

A **rigid analytic space** is an analogue of a complex analytic space over a non-archimedean field such as $\mathbb{Q}_p$ and $\mathbb{C}_p$. Rigid analytic spaces admit meaningful notions of analytic continuation and connectedness.

§1. p-adic numbers & rigid analytic geometry

Fix once and for all a prime number p.

Let $|\cdot|_p$ denote the p-adic absolute value on $\mathbb{Q}$.

$$\mathbb{Q}_p,\ \mathbb{C}_p \approx p\text{-adic analogues of } \mathbb{R},\ \mathbb{C}.$$

A **rigid analytic space** is an analogue of a complex analytic space over a non-archimedean field such as $\mathbb{Q}_p$ and $\mathbb{C}_p$. Rigid analytic spaces admit meaningful notions of analytic continuation and connectedness.

Warning: Formally, we need to use the language of rigid analytic spaces for what follows, but, for simplicity, we'll be sweeping things under the rug.

§2. Schneider p-adic heights

F	-	a number field
C	-	a projective, geometrically connected and smooth curve over F of genus $g \geq 1$
$\mathrm{Div}^0(C)$	-	the group of divisors of degree 0 on C

§2. Schneider p-adic heights

F	-	a number field
C	-	a projective, geometrically connected and smooth curve over F of genus $g \geq 1$
$\mathrm{Div}^0(C)$	-	the group of divisors of degree 0 on C

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

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

exists under a certain condition on the prime p; call this condition the **Schneider condition**.

§2. Schneider p-adic heights

F	-	a number field
C	-	a projective, geometrically connected and smooth curve over F of genus $g \geq 1$
$\mathrm{Div}^0(C)$	-	the group of divisors of degree 0 on C

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

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

exists under a certain condition on the prime p; call this condition the **Schneider condition**.

Schneider's pairing decomposes into local factors.

§2. Schneider p-adic heights

F	-	a number field
C	-	a projective, geometrically connected and smooth curve over F of genus $g \geq 1$
$\mathrm{Div}^0(C)$	-	the group of divisors of degree 0 on C

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

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

exists under a certain condition on the prime p; call this condition the **Schneider condition**.

Schneider's pairing decomposes into local factors. For a finite prime $\mathfrak{p}$ of F, set

$F_{\mathfrak{p}}$	-	the completion of F at $\mathfrak{p}$
$C_{\mathfrak{p}}$	-	$C \otimes F_{\mathfrak{p}}$
$\mathrm{Div}^0(C_{\mathfrak{p}})$	-	the group of divisors of degree 0 on $C_{\mathfrak{p}}$

Theorem (Schneider): For each finite prime $\mathfrak{p}$ of F, there exists a local pairing

$$(\cdot,\cdot)_{\mathfrak{p}} \colon \mathrm{Div}^0(C_{\mathfrak{p}}) \times \mathrm{Div}^0(C_{\mathfrak{p}}) \to \mathbb{Q}_p$$

such that,

Theorem (Schneider): For each finite prime $\mathfrak{p}$ of F, there exists a local pairing

$$(\cdot,\cdot)_{\mathfrak{p}} \colon \mathrm{Div}^0(C_{\mathfrak{p}}) \times \mathrm{Div}^0(C_{\mathfrak{p}}) \to \mathbb{Q}_p$$

such that, for all $D, E \in \mathrm{Div}^0(C)$, we have

$$(D,E)_{\mathrm{Sch}} = \sum_{\mathfrak{p}} (D,E)_{\mathfrak{p}}.$$

§2. Schneider p-adic heights

Theorem (Schneider): For each finite prime $\mathfrak{p}$ of F, there exists a local pairing

$$(\cdot,\cdot)_{\mathfrak{p}} \colon \mathrm{Div}^0(C_{\mathfrak{p}}) \times \mathrm{Div}^0(C_{\mathfrak{p}}) \to \mathbb{Q}_p$$

such that, for all $D, E \in \mathrm{Div}^0(C)$, we have

$$(D,E)_{\mathrm{Sch}} = \sum_{\mathfrak{p}} (D,E)_{\mathfrak{p}}.$$

Question: What is $(D,E)_{\mathfrak{p}}$?

§2. Schneider p-adic heights

Theorem (Schneider): For each finite prime $\mathfrak{p}$ of F, there exists a local pairing

$$(\cdot,\cdot)_{\mathfrak{p}} \colon \mathrm{Div}^0(C_{\mathfrak{p}}) \times \mathrm{Div}^0(C_{\mathfrak{p}}) \to \mathbb{Q}_p$$

such that, for all $D, E \in \mathrm{Div}^0(C)$, we have

$$(D,E)_{\mathrm{Sch}} = \sum_{\mathfrak{p}} (D,E)_{\mathfrak{p}}.$$

Question: What is $(D,E)_{\mathfrak{p}}$?

Local components away from p: If $\mathfrak{p}$ does not lie over p, then

$$(D,E)_{\mathfrak{p}} = \mathrm{constant} \cdot (D,E)_{\mathrm{IntMult}},$$

where $(D,E)_{\mathrm{IntMult}}$ denotes the intersection multiplicity of certain extensions of D and E to a regular model of $C_{\mathfrak{p}}$.

Theorem (Schneider): For each finite prime $\mathfrak{p}$ of F, there exists a local pairing

$$(\cdot,\cdot)_{\mathfrak{p}} \colon \mathrm{Div}^0(C_{\mathfrak{p}}) \times \mathrm{Div}^0(C_{\mathfrak{p}}) \to \mathbb{Q}_p$$

such that, for all $D, E \in \mathrm{Div}^0(C)$, we have

$$(D,E)_{\mathrm{Sch}} = \sum_{\mathfrak{p}} (D,E)_{\mathfrak{p}}.$$

Question: What is $(D,E)_{\mathfrak{p}}$?

Local components away from p: If $\mathfrak{p}$ does not lie over p, then

$$(D,E)_{\mathfrak{p}} = \text{constant} \cdot (D,E)_{\mathrm{IntMult}},$$

where $(D,E)_{\mathrm{IntMult}}$ denotes the intersection multiplicity of certain extensions of D and E to a regular model of $C_{\mathfrak{p}}$.

Local components at p: If $\mathfrak{p}$ lies over p, then a formula for $(D,E)_{\mathfrak{p}}$ was given by Werner in the case where $C_{\mathfrak{p}}$ is a *Mumford* curve.

§3.2. Mumford Curves

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

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

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

K - a finite extension of $\mathbb{Q}_p$
$|\cdot|$ - the 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.

§3.2. Mumford Curves

K	-	a finite extension of $\mathbb{Q}_p$
$\lvert \cdot \rvert$	-	the 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.

As $\mathrm{Aut}(\mathbb{P}^1_K) = \mathrm{PGL}_2(K)$, any subgroup Γ of $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$.

K - a finite extension of $\mathbb{Q}_p$
$|\cdot|$ - the 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.

As $\mathrm{Aut}(\mathbb{P}^1_K) = \mathrm{PGL}_2(K)$, any subgroup Γ of $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$. Set

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

§3.2. Mumford Curves

K - a finite extension of $\mathbb{Q}_p$
$|\cdot|$ - the 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.

As $\mathrm{Aut}(\mathbb{P}^1_K) = \mathrm{PGL}_2(K)$, any subgroup Γ of $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$. Set

$\mathcal{L}_\Gamma :=$ the set of **limit** points of Γ,

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

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

§3.2. Mumford Curves

K	-	a finite extension of $\mathbb{Q}_p$
$\lvert\cdot\rvert$	-	the 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.

As $\mathrm{Aut}(\mathbb{P}^1_K) = \mathrm{PGL}_2(K)$, any subgroup Γ of $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$. Set

$\mathcal{L}_\Gamma :=$ the set of **limit** points of Γ,

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

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?

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

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

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).

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:

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.

§3.2. Mumford Curves

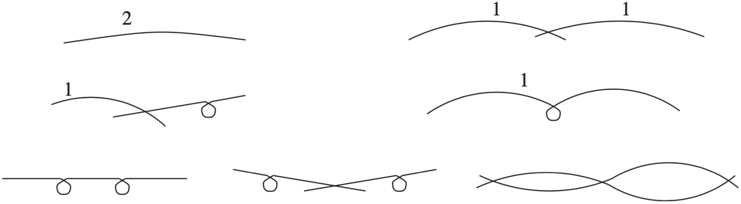
Example 1: If X_Γ has genus 1, then

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

Example 1: If X_Γ has genus 1, then

split degenerate reduction = split multiplicative reduction.

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

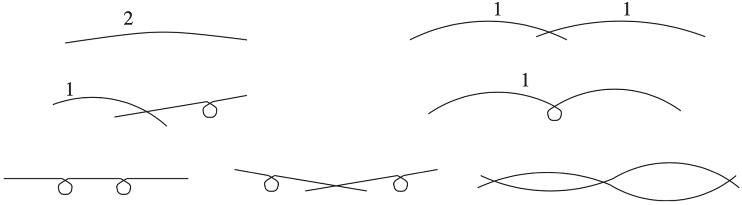


§3.2. Mumford Curves

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):



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).

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

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

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 $\mathrm{PGL}_2(K)$.

§3.2. 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.

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

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 $\langle s_0 \rangle * \cdots * \langle s_g \rangle$.

§3.3. 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.

§3.3. 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 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

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

§3.3. 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

§3.3. Hyperelliptic Mumford curves

- Γ is an index 2 subgroup of Γ'.

§3.3. Hyperelliptic Mumford curves

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

§3.3. 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.

§3.3. 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'.

§3.3. 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'?

§3.3. Hyperelliptic Mumford curves

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

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

§3.3. 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 a meromorphic function on Ω, and

§3.3. 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 a meromorphic function on Ω, and
- is Γ'-invariant and induces an isomorphism $\Omega/\Gamma' \simeq \mathbb{P}^1$.

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

§3.3. Hyperelliptic Mumford curves

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

Question: Can we be more precise?

§3.3. 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

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

§3.3. 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.

§3.3. 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.

§3.4. Jacobians of Mumford curves

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

§3.4. 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.

§3.4. 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.

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?

§3.4. 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.

§3.4. 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.

§4.1. Theta functions

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

§4.1. 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. $X \simeq \Omega/\Gamma$.

§4.1. 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:

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

§4.1. 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:

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

Properties:

- It's a meromorphic function.

§4.1. 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:

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

Properties:

- It's a meromorphic function.
- 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 $c(a, b, \gamma) \in K^{\times}$.

Let J/K be the Jacobian of X. Then there exists a lattice Λ such that

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

§4.1. Theta functions

Let J/K be the Jacobian of X. Then there exists a lattice Λ such that

$$J \simeq (K^\times)^g/\Lambda.$$

Question: What is Λ?

§4.1. Theta functions

Let J/K be the Jacobian of X. Then there exists a lattice Λ such that

$$J \simeq (K^\times)^g/\Lambda.$$

Question: What is Λ?

Set

$$H := \Gamma \Big/ \text{commutator subgroup of } \Gamma.$$

Then H is a free abelian group of rank g.

§4.1. Theta functions

Let J/K be the Jacobian of X. Then there exists a lattice Λ such that

$$J \simeq (K^\times)^g/\Lambda.$$

Question: What is Λ?

Set

$$H := \Gamma \Big/ \text{commutator subgroup of } \Gamma.$$

Then H is a free abelian group of rank g. Consider the pairing

$$\langle \cdot, \cdot \rangle \colon H \times H \to K^\times, \quad (\gamma, \gamma') \mapsto c(a, \gamma(a), \gamma')$$

for some $a \in \Omega$.

§4.1. Theta functions

Let J/K be the Jacobian of X. Then there exists a lattice Λ such that

$$J \simeq (K^\times)^g/\Lambda.$$

Question: What is Λ?

Set

$$H := {}^{\Gamma}\Big/_{\text{commutator subgroup of } \Gamma.}$$

Then H is a free abelian group of rank g. Consider the pairing

$$\langle \cdot, \cdot \rangle \colon H \times H \to K^\times, \quad (\gamma, \gamma') \mapsto c(a, \gamma(a), \gamma')$$

for some $a \in \Omega$. Fix a basis $\gamma_1, \ldots, \gamma_g$ of H, and set

$$\lambda_k := (\langle \gamma_k, \gamma_1 \rangle, \ldots, \langle \gamma_k, \gamma_g \rangle) \in (K^\times)^g, \quad k = 1, \ldots, g.$$

§4.1. Theta functions

Let J/K be the Jacobian of X. Then there exists a lattice Λ such that

$$J \simeq (K^\times)^g/\Lambda.$$

Question: What is Λ?

Set

$$H := \Gamma \Big/ \text{commutator subgroup of } \Gamma.$$

Then H is a free abelian group of rank g. Consider the pairing

$$\langle \cdot, \cdot \rangle \colon H \times H \to K^\times, \quad (\gamma, \gamma') \mapsto c(a, \gamma(a), \gamma')$$

for some $a \in \Omega$. Fix a basis $\gamma_1, \ldots, \gamma_g$ of H, and set

$$\lambda_k := (\langle \gamma_k, \gamma_1 \rangle, \ldots, \langle \gamma_k, \gamma_g \rangle) \in (K^\times)^g, \quad k = 1, \ldots, g.$$

Then $\lambda_1 \ldots, \lambda_g$ is a basis for the lattice Λ.

§4.2. Werner's formula for $(D, E)_{\mathfrak{p}}$

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.

§4.2. Werner's formula for $(D, E)_{\mathfrak{p}}$

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.

Definition: We say ρ is Λ-**invertible** if the matrix

$$\begin{pmatrix} \rho(\lambda_1) \\ \vdots \\ \rho(\lambda_g) \end{pmatrix} \in \mathbb{Q}_p^{g\times g}$$

has non-zero determinant.

§4.2. Werner's formula for $(D, E)_{\mathfrak{p}}$

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.

Definition: We say ρ is Λ-**invertible** if the matrix

$$\begin{pmatrix} \rho(\lambda_1) \\ \vdots \\ \rho(\lambda_g) \end{pmatrix} \in \mathbb{Q}_p^{g \times g}$$

has non-zero determinant.

Loosely speaking, this condition says that the image of the lattice Λ under the map ρ is a lattice of full rank in $\mathbb{Q}_p^g$.

§4.2. Werner's formula for $(D, E)_{\mathfrak{p}}$

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.

Definition: We say ρ is Λ-**invertible** if the matrix

$$\begin{pmatrix} \rho(\lambda_1) \\ \vdots \\ \rho(\lambda_g) \end{pmatrix} \in \mathbb{Q}_p^{g \times g}$$

has non-zero determinant.

Loosely speaking, this condition says that the image of the lattice Λ under the map ρ is a lattice of full rank in $\mathbb{Q}_p^g$.

Proposition (Werner): ρ is Λ-invertible $\Longleftrightarrow$ Schneider condition is fulfilled.

§4.2. Werner's formula for $(D, E)_{\mathfrak{p}}$

Now assume ρ is Λ-invertible, so that $(D, E)_{\mathfrak{p}}$ exists.

§4.2. Werner's formula for $(D, E)_{\mathfrak{p}}$

Now assume ρ is Λ-invertible, so that $(D, E)_{\mathfrak{p}}$ exists. 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 $x, y, z, w \in X = \Omega/\Gamma$.

§4.2. Werner's formula for $(D, E)_{\mathfrak{p}}$

Now assume ρ is Λ-invertible, so that $(D, E)_{\mathfrak{p}}$ exists. 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.

§4.2. Werner's formula for $(D, E)_\mathfrak{p}$

Now assume ρ is Λ-invertible, so that $(D, E)_\mathfrak{p}$ exists. 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. Let M denote the inverse of $(\rho(\lambda_k))_k$ and define

$$\big(\chi_1(z', w'), \dots, \chi_g(z', w')\big) := \big(\rho(c(z', w', \gamma_1)), \dots, \rho(c(z', w', \gamma_g))\big) \cdot M.$$

§4.2. Werner's formula for $(D, E)_{\mathfrak{p}}$

Now assume ρ is Λ-invertible, so that $(D, E)_{\mathfrak{p}}$ exists. 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. Let M denote the inverse of $(\rho(\lambda_k))_k$ and define

$$\big(\chi_1(z', w'), \ldots, \chi_g(z', w')\big) := \big(\rho(c(z', w', \gamma_1)), \ldots, \rho(c(z', w', \gamma_g))\big) \cdot M.$$

We then have

$$(D, E)_{\mathfrak{p}} = \rho\left(\frac{\Theta(x', y'; z')}{\Theta(x', y'; w')}\right) - \sum_{k=1}^{g} \chi_k(z', w')\rho(c(x', y', \gamma_k)).$$

§5.1. 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, $C \otimes F_{\mathfrak{p}}$ is a Mumford curve

§5.1. 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, $C \otimes F_{\mathfrak{p}}$ is a Mumford curve

Take $D, E \in \mathrm{Div}^0(C)$. We'd like to compute $(D, E)_{\mathrm{Sch}}$ (when it exists).

§5.1. 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, $C \otimes F_{\mathfrak{p}}$ is a Mumford curve

Take $D, E \in \mathrm{Div}^0(C)$. We'd like to compute $(D, E)_{\mathrm{Sch}}$ (when it exists).
Fix a finite prime $\mathfrak{p}$ of F.

§5.1. 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, $C \otimes F_{\mathfrak{p}}$ is a Mumford curve

Take $D, E \in \mathrm{Div}^0(C)$. We'd like to compute $(D, E)_{\mathrm{Sch}}$ (when it exists). Fix a finite prime $\mathfrak{p}$ of F.

Local components away from p: If $\mathfrak{p}$ does not lie over p, an algorithm to compute $(D, E)_{\mathfrak{p}}$ was provided by Müller in his PhD thesis.

§5.1. 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, $C \otimes F_{\mathfrak{p}}$ is a Mumford curve

Take $D, E \in \mathrm{Div}^0(C)$. We'd like to compute $(D, E)_{\mathrm{Sch}}$ (when it exists). Fix a finite prime $\mathfrak{p}$ of F.

Local components away from p: If $\mathfrak{p}$ does not lie over p, an algorithm to compute $(D, E)_{\mathfrak{p}}$ was provided by Müller in his PhD thesis. **Remark**. A different, but similar, algorithm was developed independently by Holmes.

§5.1. 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, $C \otimes F_{\mathfrak{p}}$ is a Mumford curve

Take $D, E \in \mathrm{Div}^0(C)$. We'd like to compute $(D, E)_{\mathrm{Sch}}$ (when it exists). Fix a finite prime $\mathfrak{p}$ of F.

Local components away from p: If $\mathfrak{p}$ does not lie over p, an algorithm to compute $(D, E)_{\mathfrak{p}}$ was provided by Müller in his PhD thesis. **Remark**. A different, but similar, algorithm was developed independently by Holmes.

Local components at p: If $\mathfrak{p}$ lies over p, we'll use Werner's formula for $(D, E)_{\mathfrak{p}}$.

§5.1. 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, $C \otimes F_{\mathfrak{p}}$ is a Mumford curve

Take $D, E \in \mathrm{Div}^0(C)$. We'd like to compute $(D, E)_{\mathrm{Sch}}$ (when it exists). Fix a finite prime $\mathfrak{p}$ of F.

Local components away from p: If $\mathfrak{p}$ does not lie over p, an algorithm to compute $(D, E)_{\mathfrak{p}}$ was provided by Müller in his PhD thesis. **Remark**. A different, but similar, algorithm was developed independently by Holmes.

Local components at p: If $\mathfrak{p}$ lies over p, we'll use Werner's formula for $(D, E)_{\mathfrak{p}}$. There are three main steps:

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

§5.1. Setting

K	-	$F_{\mathfrak{p}}$
$\lvert \cdot \rvert$	-	the absolute value on K
X	-	$C \otimes K$

K	-	$F_{\mathfrak{p}}$
$\lvert\cdot\rvert$	-	the absolute value on K
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 generators $\gamma_1, \dots, \gamma_g$

§5.1. Setting

K - $F_{\mathfrak{p}}$
$|\cdot|$ - the absolute value on K
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 generators $\gamma_1, \ldots, \gamma_g$
Γ' - discrete and free group containing Γ with generators $s_0, \ldots, s_g$

§5.1. Setting

K	-	$F_{\mathfrak{p}}$
$\lvert \cdot \rvert$	-	the absolute value on K
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 generators $\gamma_1, \ldots, \gamma_g$
Γ'	-	discrete and free group containing Γ with generators $s_0, \ldots, s_g$
a_i, b_i	-	fixed points of s_i

§5.2. Θ: computing theta functions

Recall that Γ is free.

§5.2. 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.

§5.2. 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

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

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

§5.2. 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

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

§5.2. 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 fast way.

To find Γ, it suffices to compute

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

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

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

§5.2. 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

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

§5.2. 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.

§5.2. 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?

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?

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

$$F(S) = R.$$

§5.2. 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.

§5.2. 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:

§5.2. 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* $F(\infty) = 1$.

§5.2. 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*

§5.2. 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

- *$F(z) \equiv 0 \mod \pi$,*

§5.2. 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

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

§5.2. 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.

§5.2. Γ: determining the Schottky group Γ

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

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

§5.2. 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 $F(z)$,

§5.2. 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.

§5.2. 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.

§5.2. 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.

§5.2. 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.

§5.2. 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 $a, b \in \Omega$.

§5.2. 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 $a, b \in \Omega$.

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

§5.2. 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 $F(z) = x$. Then,

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

§5.2. 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 $a, b \in \Omega$.

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?

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

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

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

§5.2. 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.*

§5.2. 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*

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

§5.2. 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* $z \in \Omega \mapsto (F(z), H(z))$.

§5.2. 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.

§6. Numerical example

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

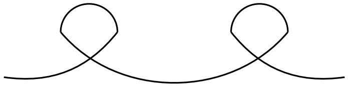
$$y^2 = x^5 - 326x^4 + 1052 \cdot 5^2 x^3 - 5914 \cdot 5^2 x^2 + 39 \cdot 5^5 x.$$

§6. 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:

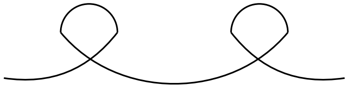


§6. Numerical example

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

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

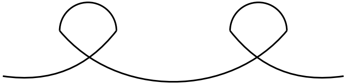
$$z = (-3,\ 1+2\cdot5^2+4\cdot5^4+2\cdot5^5+5^6+O(5^7)), \qquad w = (-18,\ 1+3\cdot5+2\cdot5^3+5^4+5^5+2\cdot5^6+O(5^7)).$$

§6. 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 $(D, E)_p$.

§6. Numerical example

We have:

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

§6. Numerical example

We have:

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

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

§6. Numerical example

We have:

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

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

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

§6. 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?

§6. 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

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

Gràcies!

- *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) - Kaya–Masdeu–Müller–van der Put