# A journey into the world of $p$-adic heights

**Enis Kaya** (KU Leuven)
*based on joint projects with*
Francesca Bianchi, Eric Katz, Marc Masdeu
Steffen Müller, Marius van der Put

Koç University
Math Seminar
December 19, 2023

# Introduction

In Diophantine geometry, *height* functions measure the “size” of rational points on algebraic varieties.

# Introduction

In Diophantine geometry, *height* functions measure the "size" of rational points on algebraic varieties. Such functions play a central role in defining and computing several interesting invariants in arithmetic geometry.

# Introduction

In Diophantine geometry, *height* functions measure the “size” of rational points on algebraic varieties. Such functions play a central role in defining and computing several interesting invariants in arithmetic geometry.

For a prime number $p$, a $p$-adic height function can be regarded as a local analogue of a classical height function.

# Introduction

In Diophantine geometry, *height* functions measure the “size” of rational points on algebraic varieties. Such functions play a central role in defining and computing several interesting invariants in arithmetic geometry.

For a prime number $p$, a $p$-adic height function can be regarded as a local analogue of a classical height function.

$\ltimes$ There are several $p$-adic height function constructions in the literature.

# Introduction

In Diophantine geometry, *height* functions measure the "size" of rational points on algebraic varieties. Such functions play a central role in defining and computing several interesting invariants in arithmetic geometry.

For a prime number $p$, a $p$-adic height function can be regarded as a local analogue of a classical height function.

- $\ltimes$ There are several $p$-adic height function constructions in the literature.
- $\ltimes$ **Question 1**. How are the different constructions related?

# Introduction

In Diophantine geometry, *height* functions measure the "size" of rational points on algebraic varieties. Such functions play a central role in defining and computing several interesting invariants in arithmetic geometry.

For a prime number $p$, a $p$-adic height function can be regarded as a local analogue of a classical height function.

$\ltimes$ There are several $p$-adic height function constructions in the literature.
$\ltimes$ **Question 1**. How are the different constructions related?

$\rtimes$ Algorithms for computing $p$-adic heights

- allow one to compute $p$-adic regulators, some of which fit into $p$-adic versions of Birch and Swinnerton–Dyer conjecture, and

# Introduction

In Diophantine geometry, *height* functions measure the "size" of rational points on algebraic varieties. Such functions play a central role in defining and computing several interesting invariants in arithmetic geometry.

For a prime number $p$, a $p$-adic height function can be regarded as a local analogue of a classical height function.

- $\ltimes$ There are several $p$-adic height function constructions in the literature.
- $\ltimes$ **Question 1**. How are the different constructions related?

- $\rtimes$ Algorithms for computing $p$-adic heights
  - allow one to compute $p$-adic regulators, some of which fit into $p$-adic versions of Birch and Swinnerton–Dyer conjecture, and
  - play a crucial role in carrying out the quadratic Chabauty method to determine rational points on curves of genus at least two.

# Introduction

In Diophantine geometry, *height* functions measure the "size" of rational points on algebraic varieties. Such functions play a central role in defining and computing several interesting invariants in arithmetic geometry.

For a prime number $p$, a $p$-adic height function can be regarded as a local analogue of a classical height function.

⋉ There are several $p$-adic height function constructions in the literature.
⋉ **Question 1**. How are the different constructions related?

⋊ Algorithms for computing $p$-adic heights

- allow one to compute $p$-adic regulators, some of which fit into $p$-adic versions of Birch and Swinnerton–Dyer conjecture, and
- play a crucial role in carrying out the quadratic Chabauty method to determine rational points on curves of genus at least two.

⋊ **Question 2**. How can one compute them numerically?

# Introduction

## Goal

Take you on a journey into the world of $p$-adic heights.

# Introduction

## Goal

Take you on a journey into the world of $p$-adic heights.

In particular, we will briefly discuss

- the relationships among some $p$-adic height constructions, and

# Introduction

## Goal

Take you on a journey into the world of $p$-adic heights.

In particular, we will briefly discuss

- the relationships among some $p$-adic height constructions, and
- algorithms to compute them numerically in special cases.

# Introduction

**Goal**

Take you on a journey into the world of $p$-adic heights.

In particular, we will briefly discuss

- the relationships among some $p$-adic height constructions, and
- algorithms to compute them numerically in special cases.

**Warning**. To make this talk less technical,

# Introduction

## Goal

Take you on a journey into the world of $p$-adic heights.

In particular, we will briefly discuss

- the relationships among some $p$-adic height constructions, and
- algorithms to compute them numerically in special cases.

**Warning**. To make this talk less technical,

- the base field will be $\mathbb{Q}$, though it could be any number field,

# Introduction

## Goal

Take you on a journey into the world of $p$-adic heights.

In particular, we will briefly discuss

- the relationships among some $p$-adic height constructions, and
- algorithms to compute them numerically in special cases.

**Warning**. To make this talk less technical,

- the base field will be $\mathbb{Q}$, though it could be any number field,
- we will give definitions and present results for Jacobian varieties, though most of them are valid for general abelian varieties, and

# Introduction

## Goal

Take you on a journey into the world of $p$-adic heights.

In particular, we will briefly discuss

- the relationships among some $p$-adic height constructions, and
- algorithms to compute them numerically in special cases.

**Warning**. To make this talk less technical,

- the base field will be $\mathbb{Q}$, though it could be any number field,
- we will give definitions and present results for Jacobian varieties, though most of them are valid for general abelian varieties, and
- time to time, I'll cheat a bit...

# Overview

1. Preliminaries
   - $p$-adic numbers
   - Elliptic curves and abelian varieties
   - Curves and their Jacobians
2. Classical Heights
   - Néron–Tate height pairing
   - Birch and Swinnerton–Dyer (BSD) conjecture
3. $p$-adic Heights & Our Results
   - Motivation: $p$-adic BSD and quadratic Chabauty
   - Coleman–Gross height pairing
   - Mazur–Tate height pairing
   - Schneider height pairing
4. Future Work
   - A dream: quadratic Chabauty at bad primes
   - $p$-adic BSD
5. Acknowledgements & References

# §1.1. $p$-adic numbers

*Kurt Hensel (1861-1941) discovered or invented the p-adic numbers around the end of the nineteenth century.* - A. M. Robert

# §1.1. $p$-adic numbers

*Kurt Hensel (1861-1941) discovered or invented the p-adic numbers around the end of the nineteenth century*. - A. M. Robert

The $p$-**adic valuation** of $r \in \mathbb{Q} \setminus \{0\}$ is defined as

$$v_p(r) = \begin{cases} \max\{k \in \mathbb{Z}_{\geq 0} : p^k \mid r\} & \text{if } r \in \mathbb{Z}, \\ \end{cases}$$

# §1.1. $p$-adic numbers

*Kurt Hensel (1861-1941) discovered or invented the p-adic numbers around the end of the nineteenth century.* - A. M. Robert

The $p$-**adic valuation** of $r \in \mathbb{Q} \setminus \{0\}$ is defined as

$$v_p(r) = \begin{cases} \max\{k \in \mathbb{Z}_{\geq 0} : p^k \mid r\} & \text{if } r \in \mathbb{Z}, \\ v_p(m) - v_p(n) & \text{if } r = m/n,\ m, n \in \mathbb{Z}. \end{cases}$$

*Kurt Hensel (1861-1941) discovered or invented the p-adic numbers around the end of the nineteenth century.* - A. M. Robert

The *p*-**adic valuation** of $r \in \mathbb{Q} \setminus \{0\}$ is defined as

$$v_p(r) = \begin{cases} \max\{k \in \mathbb{Z}_{\geq 0} : p^k \mid r\} & \text{if } r \in \mathbb{Z}, \\ v_p(m) - v_p(n) & \text{if } r = m/n, \ m, n \in \mathbb{Z}. \end{cases}$$

The *p*-**adic absolute value** of $r \in \mathbb{Q}$ is defined as

$$|r|_p = \begin{cases} 0 & \text{if } r = 0, \\ & \end{cases}$$

# §1.1. $p$-adic numbers

*Kurt Hensel (1861-1941) discovered or invented the p-adic numbers around the end of the nineteenth century.* - A. M. Robert

The $p$-**adic valuation** of $r \in \mathbb{Q} \setminus \{0\}$ is defined as

$$v_p(r) = \begin{cases} \max\{k \in \mathbb{Z}_{\geq 0} : p^k \mid r\} & \text{if } r \in \mathbb{Z}, \\ v_p(m) - v_p(n) & \text{if } r = m/n,\ m, n \in \mathbb{Z}. \end{cases}$$

The $p$-**adic absolute value** of $r \in \mathbb{Q}$ is defined as

$$|r|_p = \begin{cases} 0 & \text{if } r = 0, \\ p^{-v_p(r)} & \text{if } r \neq 0. \end{cases}$$

# §1.1. $p$-adic numbers

*Kurt Hensel (1861-1941) discovered or invented the p-adic numbers around the end of the nineteenth century.* - A. M. Robert

The $p$-**adic valuation** of $r \in \mathbb{Q} \setminus \{0\}$ is defined as

$$v_p(r) = \begin{cases} \max\{k \in \mathbb{Z}_{\geq 0} : p^k \mid r\} & \text{if } r \in \mathbb{Z}, \\ v_p(m) - v_p(n) & \text{if } r = m/n,\ m, n \in \mathbb{Z}. \end{cases}$$

The $p$-**adic absolute value** of $r \in \mathbb{Q}$ is defined as

$$|r|_p = \begin{cases} 0 & \text{if } r = 0, \\ p^{-v_p(r)} & \text{if } r \neq 0. \end{cases}$$

**Example**. For $n \in \mathbb{Z}$,

$$v_p(p^n) = n, \quad |p^n|_p = p^{-n}.$$

Then $|p^n|_p$ is small when $n$ is large; $p^n \to 0$ ($p$-adically!).

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Fact**: $\mathbb{Q}$ is **not** complete with respect to $|\cdot|_p$.

# §1.1. $p$-adic numbers

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Fact**: $\mathbb{Q}$ is **not** complete with respect to $|\cdot|_p$. The completion $\mathbb{Q}_p$ is called the field of $p$-**adic numbers**.

# §1.1. $p$-adic numbers

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Fact**: $\mathbb{Q}$ is **not** complete with respect to $|\cdot|_p$. The completion $\mathbb{Q}_p$ is called the field of $p$-**adic numbers**.

$$\mathbb{Q}_p \approx p\text{-adic analogue of } \mathbb{R}.$$

# §1.1. $p$-adic numbers

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Fact**: $\mathbb{Q}$ is **not** complete with respect to $|\cdot|_p$. The completion $\mathbb{Q}_p$ is called the field of $p$-**adic numbers**.

$$\mathbb{Q}_p \approx p\text{-adic analogue of } \mathbb{R}.$$

**Fact**: $\mathbb{Q}_p$ is **not** algebraically closed.

# §1.1. $p$-adic numbers

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Fact**: $\mathbb{Q}$ is **not** complete with respect to $|\cdot|_p$. The completion $\mathbb{Q}_p$ is called the field of $p$-**adic numbers**.

$$\mathbb{Q}_p \approx p\text{-adic analogue of } \mathbb{R}.$$

**Fact**: $\mathbb{Q}_p$ is **not** algebraically closed. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure. It is **not** complete.

# §1.1. $p$-adic numbers

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Fact**: $\mathbb{Q}$ is **not** complete with respect to $|\cdot|_p$. The completion $\mathbb{Q}_p$ is called the field of $p$-**adic numbers**.

$$\mathbb{Q}_p \approx p\text{-adic analogue of } \mathbb{R}.$$

**Fact**: $\mathbb{Q}_p$ is **not** algebraically closed. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure. It is **not** complete. The completion $\mathbb{C}_p$ is algebraically closed.

# §1.1. $p$-adic numbers

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Fact**: $\mathbb{Q}$ is **not** complete with respect to $|\cdot|_p$. The completion $\mathbb{Q}_p$ is called the field of $p$-**adic numbers**.

$$\mathbb{Q}_p \approx p\text{-adic analogue of } \mathbb{R}.$$

**Fact**: $\mathbb{Q}_p$ is **not** algebraically closed. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure. It is **not** complete. The completion $\mathbb{C}_p$ is algebraically closed.

$$\mathbb{C}_p \approx p\text{-adic analogue of } \mathbb{C}.$$

**Lemma**: $(\mathbb{Q}, |\cdot|_p)$ satisfies the following properties:

- $|r|_p = 0 \iff r = 0$,
- $|r \cdot s|_p = |r|_p \cdot |s|_p$, and
- $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

**Fact**: $\mathbb{Q}$ is **not** complete with respect to $|\cdot|_p$. The completion $\mathbb{Q}_p$ is called the field of $p$-**adic numbers**.

$$\mathbb{Q}_p \approx p\text{-adic analogue of } \mathbb{R}.$$

**Fact**: $\mathbb{Q}_p$ is **not** algebraically closed. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure. It is **not** complete. The completion $\mathbb{C}_p$ is algebraically closed.

$$\mathbb{C}_p \approx p\text{-adic analogue of } \mathbb{C}.$$

*There is a general philosophy in Number Theory that "all completions are created equal" and should have the same rights.* - M. Stoll

# §1.2. Elliptic curves

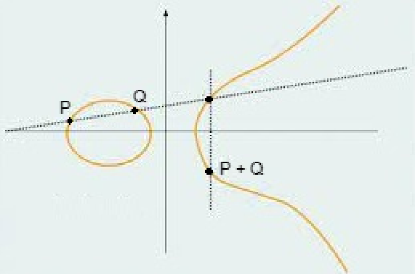
**Definition**. An **elliptic curve** is a curve of the form

$$y^2 = c_3x^3 + c_2x^2 + c_1x + c_0 \quad \text{(NO repeated roots).}$$

**Definition**. An **elliptic curve** is a curve of the form

$$y^2 = c_3x^3 + c_2x^2 + c_1x + c_0 \quad \text{(NO repeated roots).}$$

Such a curve admits the structure of an abelian group:

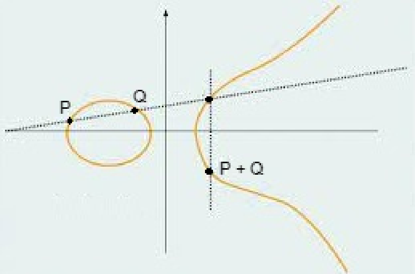


# §1.2. Elliptic curves

**Definition**. An **elliptic curve** is a curve of the form

$$y^2 = c_3x^3 + c_2x^2 + c_1x + c_0 \quad \text{(NO repeated roots)}.$$

Such a curve admits the structure of an abelian group:

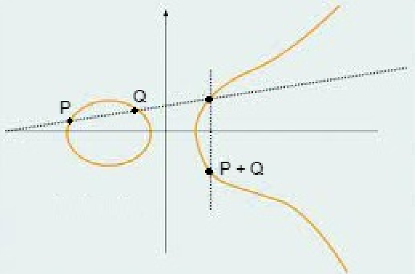



Elliptic curves are NOT just geometric objects, but also algebraic objects.

**Definition**. An **elliptic curve** is a curve of the form

$$y^2 = c_3x^3 + c_2x^2 + c_1x + c_0 \quad \text{(NO repeated roots).}$$

Such a curve admits the structure of an abelian group:




Elliptic curves are NOT just geometric objects, but also algebraic objects.

*It is possible to write endlessly on elliptic curves. (This is not a threat.)* - S. Lang

**Definition**.

**abelian varieties** = higher dimensional analogues of elliptic curves

# §1.2. Abelian varieties

**Definition.**

**abelian varieties** = higher dimensional analogues of elliptic curves

**Remarks.**

- Each abelian variety has a dimension, and

  abelian varietes of dimension 1 = elliptic curves.

# §1.2. Abelian varieties

**Definition**.

$$\textbf{abelian varieties} = \begin{array}{c}\text{higher dimensional analogues} \\ \text{of elliptic curves}\end{array}$$

**Remarks**.

- Each abelian variety has a dimension, and

$$\text{abelian varietes of dimension } 1 = \text{elliptic curves.}$$

- Abelian varieties carry the structure of an abelian group.

# §1.2. Abelian varieties

**Definition**.

$$\textbf{abelian varieties} = \begin{array}{c}\text{higher dimensional analogues} \\ \text{of elliptic curves}\end{array}$$

**Remarks**.

- Each abelian variety has a dimension, and

$$\text{abelian varietes of dimension } 1 = \text{elliptic curves.}$$

- Abelian varieties carry the structure of an abelian group.

**Theorem (Mordell–Weil)**. For an abelian variety $A/\mathbb{Q}$, the group $A(\mathbb{Q})$ of rational points of $A$

# §1.2. Abelian varieties

**Definition.**

$$\textbf{abelian varieties} = \begin{array}{c}\text{higher dimensional analogues}\\ \text{of elliptic curves}\end{array}$$

**Remarks.**

- Each abelian variety has a dimension, and

$$\text{abelian varietes of dimension } 1 = \text{elliptic curves.}$$

- Abelian varieties carry the structure of an abelian group.

**Theorem (Mordell–Weil).** For an abelian variety $A/\mathbb{Q}$, the group $A(\mathbb{Q})$ of rational points of $A$ is a finitely-generated abelian group;

**Definition**.

$$\textbf{abelian varieties} = \begin{array}{c}\text{higher dimensional analogues} \\ \text{of elliptic curves}\end{array}$$

**Remarks**.

- Each abelian variety has a dimension, and

  abelian varietes of dimension $1 =$ elliptic curves.

- Abelian varieties carry the structure of an abelian group.

**Theorem (Mordell–Weil)**. For an abelian variety $A/\mathbb{Q}$, the group $A(\mathbb{Q})$ of rational points of $A$ is a finitely-generated abelian group; that is,

$$A(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus A(\mathbb{Q})_{\mathrm{tors}}$$

for some $r \in \mathbb{Z}_{\geq 0}$, called the **algebraic rank** of $A/\mathbb{Q}$.

# §1.3. Curves

Let $C/\mathbb{Q}$ be a smooth curve of genus $g$.

Let $C/\mathbb{Q}$ be a smooth curve of genus $g$. Set

$$\mathrm{Div}^0(C) = \begin{array}{c}\text{formal integer combinations} \\ \text{of points in } C \text{ of degree } 0.\end{array}$$

# §1.3. Curves

Let $C/\mathbb{Q}$ be a smooth curve of genus $g$. Set

$$\mathrm{Div}^0(C) = \begin{array}{c}\text{formal integer combinations}\\ \text{of points in } C \text{ of degree } 0.\end{array}$$

**Example**. The curve

$$y^2 = c_{2g+1}x^{2g+1} + \cdots + c_1 x + c_0 \quad \text{(NO repeated roots)}$$

is a **hyperelliptic** curve of genus $g$.

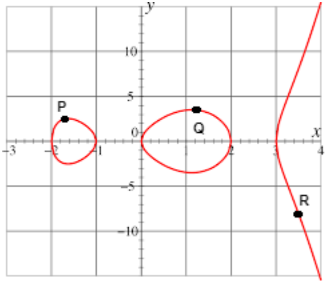
Let $C/\mathbb{Q}$ be a smooth curve of genus $g$. Set

$$\mathrm{Div}^0(C) = \begin{array}{c}\text{formal integer combinations}\\ \text{of points in } C \text{ of degree } 0.\end{array}$$

**Example**. The curve

$$y^2 = c_{2g+1}x^{2g+1} + \cdots + c_1 x + c_0 \quad \text{(NO repeated roots)}$$

is a **hyperelliptic** curve of genus $g$.




$$P - Q$$
$$P - 2Q + R$$
$$-P + 3Q - 2R$$
are in $\mathrm{Div}^0(C)$

## §1.3. Curves

We may assume that $C$ is defined by a polynomial with integer coefficients.

## §1.3. Curves

We may assume that $C$ is defined by a polynomial with integer coefficients. For a prime $p$, consider $C$ mod $\mathbb{F}_p$.

We may assume that $C$ is defined by a polynomial with integer coefficients. For a prime $p$, consider $C$ mod $\mathbb{F}_p$. If this curve is

- smooth, then $p$ is called a **good** prime;

We may assume that $C$ is defined by a polynomial with integer coefficients. For a prime $p$, consider $C \bmod \mathbb{F}_p$. If this curve is

- smooth, then $p$ is called a **good** prime;
- singular, then $p$ is called a **bad** prime.

# §1.3. Curves

We may assume that $C$ is defined by a polynomial with integer coefficients. For a prime $p$, consider $C$ mod $\mathbb{F}_p$. If this curve is

- smooth, then $p$ is called a **good** prime;
- singular, then $p$ is called a **bad** prime.

**Example**. If $C$ is given by

$$y^2 = x(x+1)(x+p)$$

# §1.3. Curves

We may assume that $C$ is defined by a polynomial with integer coefficients. For a prime $p$, consider $C$ mod $\mathbb{F}_p$. If this curve is

- smooth, then $p$ is called a **good** prime;
- singular, then $p$ is called a **bad** prime.

**Example**. If $C$ is given by

$$y^2 = x(x+1)(x+p)$$

then $C$ mod $\mathbb{F}_p$ is

$$y^2 = x^2(x+1)$$

*(repeated root!!!)*

# §1.3. Curves

We may assume that $C$ is defined by a polynomial with integer coefficients. For a prime $p$, consider $C$ mod $\mathbb{F}_p$. If this curve is

- smooth, then $p$ is called a **good** prime;
- singular, then $p$ is called a **bad** prime.

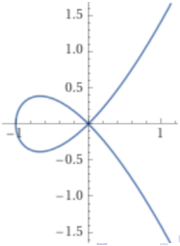
**Example**. If $C$ is given by

$$y^2 = x(x+1)(x+p)$$

then $C$ mod $\mathbb{F}_p$ is

$$y^2 = x^2(x+1)$$

*(repeated root!!!)*



**Example**. If $C$ is given by

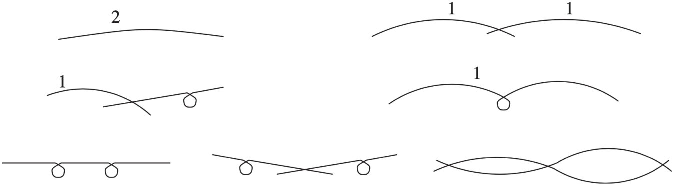
$$y^2 = c_5x^5 + \cdots + c_1x + c_0 \quad \text{(NO repeated roots)},$$

## §1.3. Curves

**Example**. If $C$ is given by

$$y^2 = c_5x^5 + \cdots + c_1x + c_0 \quad \text{(NO repeated roots)},$$

then $C$ mod $\mathbb{F}_p$ can be one of the following:



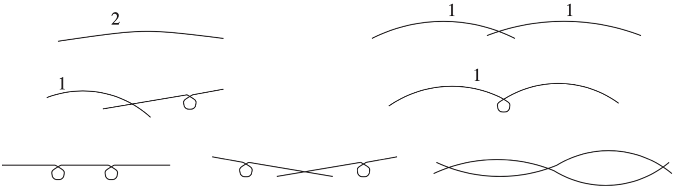

(picture taken from Liu's **Algebraic Geometry and Arithmetic Curves** book)

# §1.3. Curves

**Example**. If $C$ is given by

$$y^2 = c_5 x^5 + \cdots + c_1 x + c_0 \quad \text{(NO repeated roots)},$$

then $C$ mod $\mathbb{F}_p$ can be one of the following:




(picture taken from Liu's **Algebraic Geometry and Arithmetic Curves** book)

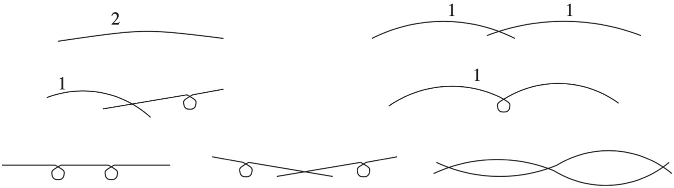
**Remark**. Instead of $C$ mod $\mathbb{F}_p$, we should say "the special fiber of its stable model".

# §1.3. Curves

**Example**. If $C$ is given by

$$y^2 = c_5x^5 + \cdots + c_1x + c_0 \quad \text{(NO repeated roots)},$$

then $C$ mod $\mathbb{F}_p$ can be one of the following:




(picture taken from Liu's **Algebraic Geometry and Arithmetic Curves** book)

**Remark**. Instead of $C$ mod $\mathbb{F}_p$, we should say "the special fiber of its stable model".

*Algebraic curves were created by God and algebraic surfaces by the Devil.*
- M. Noether

**Theorem (Faltings)**. The set $C(\mathbb{Q})$ is finite if $g \geq 2$.

**Theorem (Faltings)**. The set $C(\mathbb{Q})$ is finite if $g \geq 2$.

**Remark**. Finding these points is an industry in number theory...

**Theorem (Faltings).** The set $C(\mathbb{Q})$ is finite if $g \geq 2$.

**Remark.** Finding these points is an industry in number theory...

There exists an abelian variety $J/\mathbb{Q}$ of dimension $g$ such that

$$\text{points in J} \;=\; \mathrm{Div}^0(C)/\sim.$$

**Theorem (Faltings).** The set $C(\mathbb{Q})$ is finite if $g \geq 2$.

**Remark.** Finding these points is an industry in number theory...

There exists an abelian variety $J/\mathbb{Q}$ of dimension $g$ such that

$$\text{points in J} = \text{Div}^0(C)/\sim.$$

The variety $J$ is called the **Jacobian variety** of $C$. For a fixed point $O \in C$,

**Theorem (Faltings)**. The set $C(\mathbb{Q})$ is finite if $g \geq 2$.

**Remark**. Finding these points is an industry in number theory...

There exists an abelian variety $J/\mathbb{Q}$ of dimension $g$ such that

$$\text{points in J} \;=\; \text{Div}^0(C)/\sim .$$

The variety $J$ is called the **Jacobian variety** of $C$. For a fixed point $O \in C$, we have an embedding

$$\begin{aligned} \iota\colon C &\hookrightarrow J \\ P &\mapsto P - O \end{aligned}$$

# §1.3. Jacobians of curves

**Theorem (Faltings)**. The set $C(\mathbb{Q})$ is finite if $g \geq 2$.

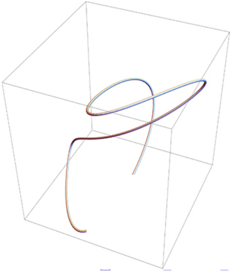
**Remark**. Finding these points is an industry in number theory...

There exists an abelian variety $J/\mathbb{Q}$ of dimension $g$ such that

$$\text{points in J} = \text{Div}^0(C)/\sim .$$

The variety $J$ is called the **Jacobian variety** of $C$. For a fixed point $O \in C$, we have an embedding

$$\begin{aligned} \iota \colon C &\hookrightarrow J \\ P &\mapsto P - O \end{aligned}$$



# §2.1. Size of points

*One of the fundamental tools required for the study of rational and integral points on an algebraic variety is a means of measuring the "size" of a point.* - Hindry–Silverman

# §2.1. Size of points

*One of the fundamental tools required for the study of rational and integral points on an algebraic variety is a means of measuring the "size" of a point.* - Hindry–Silverman

For $r = \frac{m}{n} \in \mathbb{Q}$ with $\gcd(m, n) = 1$, set

$$h(r) = \max\{|m|, |n|\}.$$

# §2.1. Size of points

*One of the fundamental tools required for the study of rational and integral points on an algebraic variety is a means of measuring the "size" of a point.* - Hindry–Silverman

For $r = \frac{m}{n} \in \mathbb{Q}$ with $\gcd(m, n) = 1$, set

$$h(r) = \max\{|m|, |n|\}.$$

**Example**. For the rational numbers,

$$r_1 = \frac{1}{2} \quad \text{and} \quad r_2 = \frac{10^{10000}}{2 \cdot 10^{10000} + 1},$$

# §2.1. Size of points

*One of the fundamental tools required for the study of rational and integral points on an algebraic variety is a means of measuring the "size" of a point.* - Hindry–Silverman

For $r = \frac{m}{n} \in \mathbb{Q}$ with $\gcd(m, n) = 1$, set

$$h(r) = \max\{|m|, |n|\}.$$

**Example**. For the rational numbers,

$$r_1 = \frac{1}{2} \quad \text{and} \quad r_2 = \frac{10^{10000}}{2 \cdot 10^{10000} + 1},$$

- $|r_1|$ and $|r_2|$ are very close, but

# §2.1. Size of points

*One of the fundamental tools required for the study of rational and integral points on an algebraic variety is a means of measuring the "size" of a point.* - Hindry–Silverman

For $r = \frac{m}{n} \in \mathbb{Q}$ with $\gcd(m, n) = 1$, set

$$h(r) = \max\{|m|, |n|\}.$$

**Example**. For the rational numbers,

$$r_1 = \frac{1}{2} \quad \text{and} \quad r_2 = \frac{10^{10000}}{2 \cdot 10^{10000} + 1},$$

- $|r_1|$ and $|r_2|$ are very close, but
- $h(r_1)$ and $h(r_2)$ are very far.

# §2.1. Néron–Tate height pairing

The naive height is

$$h_{\text{naive}} \colon \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}, \quad x \mapsto \log\Big(\max\big\{|x_0|, |x_1|, \ldots, |x_n|\big\}\Big)$$

where $x = (x_0 : x_1 : \cdots : x_n)$, $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$.

# §2.1. Néron–Tate height pairing

The naive height is

$$h_{\text{naive}} \colon \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}, \quad x \mapsto \log\Big(\max\big\{|x_0|, |x_1|, \dots, |x_n|\big\}\Big)$$

where $x = (x_0 : x_1 : \cdots : x_n)$, $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1, \dots, x_n) = 1$.

The Néron–Tate height is

$$h^{\text{NT}} \colon J(\mathbb{Q}) \to \mathbb{R}, \quad P \mapsto \lim_{n\to\infty} \frac{1}{n^2} h_{\text{naive}}(\iota(nP))$$

where $\iota \colon J/\pm \hookrightarrow \mathbb{P}^{2^g-1}$.

# §2.1. Néron–Tate height pairing

The naive height is

$$h_{\text{naive}} \colon \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}, \quad x \mapsto \log\left(\max\left\{|x_0|, |x_1|, \ldots, |x_n|\right\}\right)$$

where $x = (x_0 : x_1 : \cdots : x_n)$, $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$.

The Néron–Tate height is

$$h^{\text{NT}} \colon J(\mathbb{Q}) \to \mathbb{R}, \quad P \mapsto \lim_{n\to\infty} \frac{1}{n^2} h_{\text{naive}}(\iota(nP))$$

where $\iota \colon J/\pm \hookrightarrow \mathbb{P}^{2^g-1}$.

The Néron–Tate height pairing is

$$\langle \cdot, \cdot \rangle^{\text{NT}} \colon J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{R}, \quad (P, Q) \mapsto \frac{1}{2}\left(h^{\text{NT}}(P+Q) - h^{\text{NT}}(P) - h^{\text{NT}}(Q)\right).$$

# §2.2. BSD conjecture for abelian varieties

**Conjecture**. Let $r$ denote the algebraic rank of $J/\mathbb{Q}$.

# §2.2. BSD conjecture for abelian varieties

**Conjecture**. Let $r$ denote the algebraic rank of $J/\mathbb{Q}$. We have

$$r = \text{order of vanishing of the } L\text{-function } L(J, s) \text{ at } s = 1.$$

**Conjecture**. Let $r$ denote the algebraic rank of $J/\mathbb{Q}$. We have

$$r = \text{order of vanishing of the } L\text{-function } L(J,s) \text{ at } s = 1.$$

Moreover,

$$\lim_{s\to 1}(s-1)^{-r}L(J,s) = \frac{\Omega_J \cdot |\text{Ш}(J/\mathbb{Q})| \cdot \text{Reg}(J/\mathbb{Q}) \cdot \prod_v c_v}{|J(\mathbb{Q})_{\text{tors}}|^2}.$$

# §2.2. BSD conjecture for abelian varieties

**Conjecture**. Let $r$ denote the algebraic rank of $J/\mathbb{Q}$. We have

$$r = \text{order of vanishing of the } L\text{-function } L(J,s) \text{ at } s=1.$$

Moreover,

$$\lim_{s\to 1}(s-1)^{-r}L(J,s) = \frac{\Omega_J \cdot |\text{Ш}(J/\mathbb{Q})| \cdot \text{Reg}(J/\mathbb{Q}) \cdot \prod_v c_v}{|J(\mathbb{Q})_{\text{tors}}|^2}.$$

Here, $\text{Reg}(J/\mathbb{Q})$ is the canonical regulator, i.e.,

$$\text{Reg}(J/\mathbb{Q}) = \left| \det \begin{pmatrix} \langle P_1, P_1\rangle^{\text{NT}} & \langle P_1, P_2\rangle^{\text{NT}} & \cdots & \langle P_1, P_r\rangle^{\text{NT}} \\ \vdots & \vdots & \ddots & \vdots \\ \langle P_r, P_1\rangle^{\text{NT}} & \langle P_r, P_2\rangle^{\text{NT}} & \cdots & \langle P_r, P_r\rangle^{\text{NT}} \end{pmatrix} \right| \in \mathbb{R}$$

where $P_1, \ldots, P_r$ is a basis for $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$.

# §2.2. BSD conjecture for abelian varieties

**Conjecture**. Let $r$ denote the algebraic rank of $J/\mathbb{Q}$. We have

$$r = \text{order of vanishing of the } L\text{-function } L(J,s) \text{ at } s = 1.$$

Moreover,

$$\lim_{s\to 1}(s-1)^{-r}L(J,s) = \frac{\Omega_J \cdot |\text{Ш}(J/\mathbb{Q})| \cdot \text{Reg}(J/\mathbb{Q}) \cdot \prod_v c_v}{|J(\mathbb{Q})_{\text{tors}}|^2}.$$

Here, $\text{Reg}(J/\mathbb{Q})$ is the canonical regulator, i.e.,

$$\text{Reg}(J/\mathbb{Q}) = \left|\det \begin{pmatrix} \langle P_1, P_1\rangle^{\text{NT}} & \langle P_1, P_2\rangle^{\text{NT}} & \cdots & \langle P_1, P_r\rangle^{\text{NT}} \\ \vdots & \vdots & \ddots & \vdots \\ \langle P_r, P_1\rangle^{\text{NT}} & \langle P_r, P_2\rangle^{\text{NT}} & \cdots & \langle P_r, P_r\rangle^{\text{NT}} \end{pmatrix}\right| \in \mathbb{R}$$

where $P_1, \ldots, P_r$ is a basis for $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$.

*This remarkable conjecture relates the behavior of a function L, at a point where it is not at present known to be defined, to the order of a group Ш, which is not known to be finite.* - J. Tate

# §3.1. $p$-adic heights and motivation

Fix a prime number $p$. A $p$-adic height pairing is a function

$$\langle \cdot, \cdot \rangle \colon J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$$

# §3.1. $p$-adic heights and motivation

Fix a prime number $p$. A $p$-adic height pairing is a function

$$\langle \cdot, \cdot \rangle \colon J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$$

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

# §3.1. $p$-adic heights and motivation

Fix a prime number $p$. A $p$-adic height pairing is a function

$$\langle \cdot, \cdot \rangle \colon J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$$

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

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

# §3.1. $p$-adic heights and motivation

Fix a prime number $p$. A $p$-adic height pairing is a function

$$\langle \cdot, \cdot \rangle \colon J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$$

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

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

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 $\geq 2$.

# §3.1. *p*-adic heights and motivation

Fix a prime number $p$. A $p$-adic height pairing is a function

$$\langle \cdot , \cdot \rangle : J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$$

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

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

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 $\geq 2$.

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.

# §3.2. Coleman–Gross height pairing

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

$$\langle \cdot, \cdot \rangle^{\mathrm{CG}} = \sum_{q \in \{\text{prime numbers}\}} \langle \cdot, \cdot \rangle_q^{\mathrm{CG}}$$

# §3.2. Coleman–Gross height pairing

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

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

# §3.2. Coleman–Gross height pairing

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

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

The local components away from $p$ are described using “arithmetic intersection theory”,

# §3.2. Coleman–Gross height pairing

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

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

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

$$\langle D_1, D_2 \rangle_p^{\mathrm{CG}} := {}^{\mathrm{Vol}}\!\!\int_{D_2} \omega_{D_1}$$

where

- $\omega_{D_1}$ is a "canonical" differential form attached to $D_1$, and
- ${}^{\mathrm{Vol}}\!\!\int$ is the Vologodsky integration.

# §3.2. $p$-adic integration theories

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

# §3.2. $p$-adic integration theories

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

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

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

# §3.2. $p$-adic integration theories

Fix a smooth curve $X$ over $\mathbb{Q}_p$. Let $\omega$ 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 $X^{\mathrm{an}}$.

Fix a smooth curve $X$ over $\mathbb{Q}_p$. Let $\omega$ 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 $X^{\mathrm{an}}$. Pick a path $\gamma$ in $X^{\mathrm{an}}$ from $P$ to $Q$.

# §3.2. $p$-adic integration theories

Fix a smooth curve $X$ over $\mathbb{Q}_p$. Let $\omega$ 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 $X^{\mathrm{an}}$. Pick a path $\gamma$ in $X^{\mathrm{an}}$ 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.

# §3.2. $p$-adic integration theories

Fix a smooth curve $X$ over $\mathbb{Q}_p$. Let $\omega$ 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 $X^{\mathrm{an}}$. Pick a path $\gamma$ in $X^{\mathrm{an}}$ 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**.

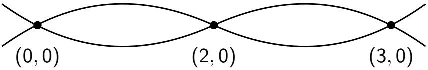
**Example**: Consider the hyperelliptic curve $X/\mathbb{Q}_5$ given by

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

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

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

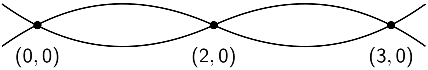
$p = 5$ is a prime of bad reduction for $X$, and $X$ mod $\mathbb{F}_5$ is as follows:

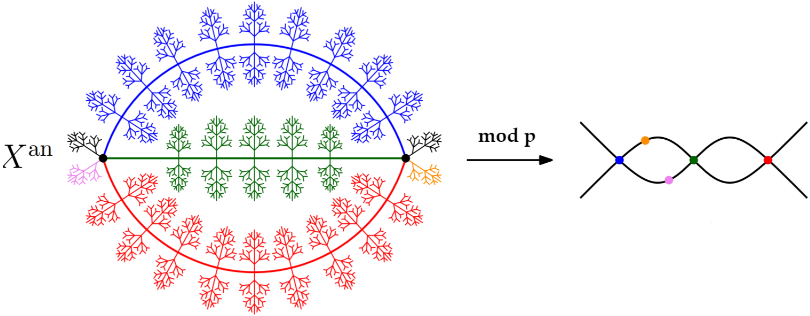


**Example**: Consider the hyperelliptic curve $X/\mathbb{Q}_5$ given by

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

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



**Remarks**

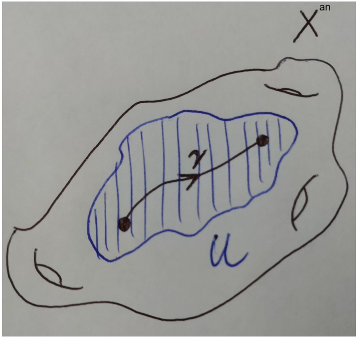
- If $X$ has good reduction, then ${}^{\mathrm{Vol}}\int_x^y \omega = {}^{\mathrm{BC}}\int_\gamma \omega$.

**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 $\gamma$, then the integral ${}^{\mathrm{BC}}\int_\gamma \omega$ can be computed from $U$, $\omega|_U$ and $\gamma$.

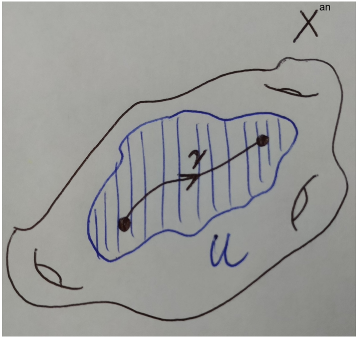
**Remarks**

- 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 $\gamma$, then the integral ${}^{\mathrm{BC}}\!\int_\gamma \omega$ can be computed from $U$, $\omega|_U$ and $\gamma$.



**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 $\gamma$, then the integral ${}^{\mathrm{BC}}\int_\gamma \omega$ can be computed from $U$, $\omega|_U$ and $\gamma$.




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

$$=$$

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

# §3.2. $p$-adic integration theories

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

# §3.2. *p*-adic integration theories

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

# §3.2. *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*

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

${}^{\mathrm{BC}}\!\int$ 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*

- $\gamma_i$*'s are the "loops" in* $X^{\mathrm{an}}$*, and*

# §3.2. $p$-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*

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

${}^{\mathrm{BC}}\!\int$ 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*

- $\gamma_i$*'s are the "loops" in* $X^{\mathrm{an}}$*, 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.*

# §3.2. Computing Coleman–Gross height pairing

An algorithm to compute the local heights away from $p$ was provided by Müller. **Remark**. A different, but similar, algorithm was developed independently by Holmes.

# §3.2. Computing Coleman–Gross height pairing

An algorithm to compute the local heights away from $p$ was provided by Müller. **Remark**. A different, but similar, algorithm was developed independently by Holmes.

An algorithm to compute the local height at $p$ in the case of good reduction was provided by Balakrishnan–Besser.

# §3.2. Computing Coleman–Gross height pairing

An algorithm to compute the local heights away from $p$ was provided by Müller. **Remark**. A different, but similar, algorithm was developed independently by Holmes.

An algorithm to compute the local height at $p$ in the case of good reduction was provided by Balakrishnan–Besser.

**Algorithm (Bianchi–K.–Müller)**

*Compute the Coleman–Gross p-adic height pairing on Jacobians of hyperelliptic curves of arbitrary reduction type.*

# §3.2. Computing Coleman–Gross height pairing

An algorithm to compute the local heights away from $p$ was provided by Müller. **Remark**. A different, but similar, algorithm was developed independently by Holmes.

An algorithm to compute the local height at $p$ in the case of good reduction was provided by Balakrishnan–Besser.

**Algorithm (Bianchi–K.–Müller)**

*Compute the Coleman–Gross p-adic height pairing on Jacobians of hyperelliptic curves of arbitrary reduction type.*

**Remark**. Recall that

$$\langle D_1, D_2 \rangle_p^{\mathrm{CG}} = {}^{\mathrm{Vol}}\!\!\int_{D_2} \omega_{D_1}.$$

# §3.2. Computing Coleman–Gross height pairing

An algorithm to compute the local heights away from $p$ was provided by Müller. **Remark**. A different, but similar, algorithm was developed independently by Holmes.

An algorithm to compute the local height at $p$ in the case of good reduction was provided by Balakrishnan–Besser.

### Algorithm (Bianchi–K.–Müller)

*Compute the Coleman–Gross p-adic height pairing on Jacobians of hyperelliptic curves of arbitrary reduction type.*

**Remark**. Recall that

$$\langle D_1, D_2 \rangle_p^{\mathrm{CG}} = {}^{\mathrm{Vol}}\!\!\int_{D_2} \omega_{D_1}.$$

Determining $\omega_{D_1}$ from $D_1$ is tricky...

# §3.3. Mazur–Tate height pairing

The pairing

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

is defined using the theory of "biextensions". Computing this pairing directly from the definition does NOT seem feasible...

# §3.3. Mazur–Tate height pairing

The pairing

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

is defined using the theory of "biextensions". Computing this pairing directly from the definition does NOT seem feasible... But, it is known that

$$\langle \cdot, \cdot \rangle^{\mathrm{CG}} = \langle \cdot, \cdot \rangle^{\mathrm{MT}}$$

so one can compute the global Mazur–Tate height pairing.

# §3.3. Mazur–Tate height pairing

The pairing

$$\langle \cdot, \cdot \rangle^{\mathrm{MT}} : \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p$$

is defined using the theory of "biextensions". Computing this pairing directly from the definition does NOT seem feasible... But, it is known that

$$\langle \cdot, \cdot \rangle^{\mathrm{CG}} = \langle \cdot, \cdot \rangle^{\mathrm{MT}}$$

so one can compute the global Mazur–Tate height pairing.

This height pairing is also sums of local pairings:

$$\langle \cdot, \cdot \rangle^{\mathrm{MT}} = \sum_{q \in \{\text{prime numbers}\}} \langle \cdot, \cdot \rangle_q^{\mathrm{MT}}.$$

# §3.3. Mazur–Tate height pairing

The pairing

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

is defined using the theory of "biextensions". Computing this pairing directly from the definition does NOT seem feasible... But, it is known that

$$\langle\cdot,\cdot\rangle^{\mathrm{CG}} = \langle\cdot,\cdot\rangle^{\mathrm{MT}}$$

so one can compute the global Mazur–Tate height pairing.

This height pairing is also sums of local pairings:

$$\langle\cdot,\cdot\rangle^{\mathrm{MT}} = \sum_{q \in \{\text{prime numbers}\}} \langle\cdot,\cdot\rangle_q^{\mathrm{MT}}.$$

The real-valued Néron–Tate height pairing $\langle\cdot,\cdot\rangle^{\mathrm{NT}}$ can be decomposed into a sum of "Néron" functions. Here is a $p$-adic analogue:

# §3.3. Mazur–Tate height pairing

**Theorem (Bianchi–K.–Müller)**

*For each q, there exists a p-adic "Néron function" $\lambda_q$ such that the local pairing $\langle \cdot, \cdot \rangle_q^{\mathrm{MT}}$ can be expressed in terms of $\lambda_q$.*

# §3.3. Mazur–Tate height pairing

**Theorem (Bianchi–K.–Müller)**

*For each $q$, there exists a $p$-adic "Néron function" $\lambda_q$ such that the local pairing $\langle\cdot,\cdot\rangle_q^{\mathrm{MT}}$ can be expressed in terms of $\lambda_q$.*

Here is a direct local comparison of Coleman–Gross and Mazur–Tate heights in a special case:

**Theorem (Bianchi–K.–Müller)**

*Let $C$ be a hyperelliptic curve of genus 2. For each prime $q$, we have $\langle\cdot,\cdot\rangle_q^{\mathrm{CG}} = \langle\cdot,\cdot\rangle_q^{\mathrm{MT}}$.*

# §3.3. Mazur–Tate height pairing

**Theorem (Bianchi–K.–Müller)**

*For each $q$, there exists a $p$-adic "Néron function" $\lambda_q$ such that the local pairing $\langle \cdot, \cdot \rangle_q^{\mathrm{MT}}$ can be expressed in terms of $\lambda_q$.*

Here is a direct local comparison of Coleman–Gross and Mazur–Tate heights in a special case:

**Theorem (Bianchi–K.–Müller)**

*Let $C$ be a hyperelliptic curve of genus 2. For each prime $q$, we have $\langle \cdot, \cdot \rangle_q^{\mathrm{CG}} = \langle \cdot, \cdot \rangle_q^{\mathrm{MT}}$. As a corollary, we get $\langle \cdot, \cdot \rangle^{\mathrm{CG}} = \langle \cdot, \cdot \rangle^{\mathrm{MT}}$.*

# §3.3. Mazur–Tate height pairing

**Theorem (Bianchi–K.–Müller)**

*For each q, there exists a p-adic "Néron function" $\lambda_q$ such that the local pairing $\langle \cdot, \cdot \rangle_q^{\mathrm{MT}}$ can be expressed in terms of $\lambda_q$.*

Here is a direct local comparison of Coleman–Gross and Mazur–Tate heights in a special case:

**Theorem (Bianchi–K.–Müller)**

*Let C be a hyperelliptic curve of genus 2. For each prime q, we have $\langle \cdot, \cdot \rangle_q^{\mathrm{CG}} = \langle \cdot, \cdot \rangle_q^{\mathrm{MT}}$. As a corollary, we get $\langle \cdot, \cdot \rangle^{\mathrm{CG}} = \langle \cdot, \cdot \rangle^{\mathrm{MT}}$.*

**Algorithm (Bianchi–K.–Müller)**

*Compute the Mazur–Tate p-adic height pairing on Jacobians of hyperelliptic curves of genus 2 using the "theta expression" of $\lambda_q$.*

# §3.4. Schneider height pairing

The pairing

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

exists under a certain condition on the prime $p$.

# §3.4. Schneider height pairing

The pairing

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

exists under a certain condition on the prime $p$.

**Remarks**.

- Recall that this pairing is particularly important as the corresponding regulator fits into $p$-adic versions of BSD conjecture.

# §3.4. Schneider height pairing

The pairing

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

exists under a certain condition on the prime $p$.

**Remarks**.

- Recall that this pairing is particularly important as the corresponding regulator fits into $p$-adic versions of BSD conjecture.
- In general, $\langle \cdot, \cdot \rangle^{\mathrm{Sch}} \neq \langle \cdot, \cdot \rangle^{\mathrm{CG}}$.

# §3.4. Schneider height pairing

The pairing

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

exists under a certain condition on the prime $p$.

**Remarks**.

- Recall that this pairing is particularly important as the corresponding regulator fits into $p$-adic versions of BSD conjecture.
- In general, $\langle \cdot, \cdot \rangle^{\mathrm{Sch}} \neq \langle \cdot, \cdot \rangle^{\mathrm{CG}}$.
- Computing $\langle \cdot, \cdot \rangle^{\mathrm{Sch}}$ directly from definition does NOT seem feasible...

# §3.4. Schneider height pairing

The pairing

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

exists under a certain condition on the prime $p$.

**Remarks**.

- Recall that this pairing is particularly important as the corresponding regulator fits into $p$-adic versions of BSD conjecture.
- In general, $\langle \cdot, \cdot \rangle^{\mathrm{Sch}} \neq \langle \cdot, \cdot \rangle^{\mathrm{CG}}$.
- Computing $\langle \cdot, \cdot \rangle^{\mathrm{Sch}}$ directly from definition does NOT seem feasible...

It can also be written as sums of local pairings:

$$\langle \cdot, \cdot \rangle^{\mathrm{Sch}} = \sum_{q \in \{\text{prime numbers}\}} \langle \cdot, \cdot \rangle_q^{\mathrm{Sch}}.$$

# §3.4. Schneider height pairing

The pairing

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

exists under a certain condition on the prime $p$.

**Remarks**.

- Recall that this pairing is particularly important as the corresponding regulator fits into $p$-adic versions of BSD conjecture.
- In general, $\langle \cdot, \cdot \rangle^{\mathrm{Sch}} \neq \langle \cdot, \cdot \rangle^{\mathrm{CG}}$.
- Computing $\langle \cdot, \cdot \rangle^{\mathrm{Sch}}$ directly from definition does NOT seem feasible...

It can also be written as sums of local pairings:

$$\langle \cdot, \cdot \rangle^{\mathrm{Sch}} = \sum_{q \in \{\text{prime numbers}\}} \langle \cdot, \cdot \rangle_q^{\mathrm{Sch}}.$$

As usual, the local pairing $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$ is more tricky to define...

# §3.4. Schneider height pairing

The pairing

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

exists under a certain condition on the prime $p$.

**Remarks**.

- Recall that this pairing is particularly important as the corresponding regulator fits into $p$-adic versions of BSD conjecture.
- In general, $\langle \cdot, \cdot \rangle^{\mathrm{Sch}} \neq \langle \cdot, \cdot \rangle^{\mathrm{CG}}$.
- Computing $\langle \cdot, \cdot \rangle^{\mathrm{Sch}}$ directly from definition does NOT seem feasible...

It can also be written as sums of local pairings:

$$\langle \cdot, \cdot \rangle^{\mathrm{Sch}} = \sum_{q \in \{\text{prime numbers}\}} \langle \cdot, \cdot \rangle_q^{\mathrm{Sch}}.$$

As usual, the local pairing $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$ is more tricky to define... But, a nice a formula was given by Werner in the case where $C/\mathbb{Q}_p$ is a *Mumford* curve.

# §3.4. Mumford curves

**Definition**. $C/\mathbb{Q}_p$ is called a **Mumford curve** if $C$ mod $\mathbb{F}_p$ is a union of curves of genus 0.

# §3.4. Mumford curves

**Definition**. $C/\mathbb{Q}_p$ is called a **Mumford curve** if $C$ mod $\mathbb{F}_p$ is a union of curves of genus 0.

**Example**. A curve $C$ of the form

$$y^2 = c_5x^5 + \cdots + c_1x + c_0 \quad \text{(NO repeated roots)}$$

is a Mumford curve if $C$ mod $\mathbb{F}_p$ is one of the following:

# §3.4. Mumford curves

**Definition**. $C/\mathbb{Q}_p$ is called a **Mumford curve** if $C$ mod $\mathbb{F}_p$ is a union of curves of genus 0.

**Example**. A curve $C$ of the form

$$y^2 = c_5x^5 + \cdots + c_1x + c_0 \quad \text{(NO repeated roots)}$$

is a Mumford curve if $C$ mod $\mathbb{F}_p$ is one of the following:

Assume from now on $C/\mathbb{Q}_p$ is a Mumford curve.

# §3.4. Mumford curves

**Definition**. $C/\mathbb{Q}_p$ is called a **Mumford curve** if $C$ mod $\mathbb{F}_p$ is a union of curves of genus 0.

**Example**. A curve $C$ of the form

$$y^2 = c_5x^5 + \cdots + c_1x + c_0 \quad \text{(NO repeated roots)}$$

is a Mumford curve if $C$ mod $\mathbb{F}_p$ is one of the following:

Assume from now on $C/\mathbb{Q}_p$ is a Mumford curve. Then it admits a $p$-adic uniformization:

# §3.4. Mumford curves

**Definition**. $C/\mathbb{Q}_p$ is called a **Mumford curve** if $C$ mod $\mathbb{F}_p$ is a union of curves of genus 0.

**Example**. A curve $C$ of the form

$$y^2 = c_5 x^5 + \cdots + c_1 x + c_0 \quad \text{(NO repeated roots)}$$

is a Mumford curve if $C$ mod $\mathbb{F}_p$ is one of the following:

Assume from now on $C/\mathbb{Q}_p$ is a Mumford curve. Then it admits a $p$-adic uniformization: there exists a $p$-adic "Schottky" group $\Gamma$ together with a "$p$-adic analytic" isomorphism

$$C \simeq \Omega/\Gamma$$

where $\Omega = \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p)$, the $p$**-adic upper half plane**.

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

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

This is a remarkable "automorphic" form.

# §3.4. Werner's formula for $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$

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

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

This is a remarkable "automorphic" form.

Now take $D, E \in \mathrm{Div}^0(C)$.

# §3.4. Werner's formula for $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$

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

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

This is a remarkable "automorphic" form.

Now take $D, E \in \mathrm{Div}^0(C)$. The pairing $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$ is additive in both arguments, so we can assume that

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

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

# §3.4. Werner's formula for $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$

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

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

This is a remarkable "automorphic" form.

Now take $D, E \in \mathrm{Div}^0(C)$. The pairing $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$ is additive in both arguments, so we can assume that

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

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

**Theorem (Werner)**. Choose preimages $x', y', z', w'$ in $\Omega$.

# §3.4. Werner's formula for $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$

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

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

This is a remarkable "automorphic" form.

Now take $D, E \in \mathrm{Div}^0(C)$. The pairing $\langle \cdot, \cdot \rangle_p^{\mathrm{Sch}}$ is additive in both arguments, so we can assume that

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

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

**Theorem (Werner).** Choose preimages $x', y', z', w'$ in $\Omega$. We then have

$$\langle D, E \rangle_p^{\mathrm{Sch}} = \log_p \left( \frac{\Theta(x', y'; z')}{\Theta(x', y'; w')} \right) - \begin{array}{c}\text{another function}\\ \text{in terms of } \Theta.\end{array}$$

# §3.4. Computing Schneider height pairing

**Algorithm (K.–Masdeu–Müller–van der Put (in progress))**

*Compute the Schneider $p$-adic height pairing on Jacobians of hyperelliptic Mumford curves.*

# §3.4. Computing Schneider height pairing

**Algorithm (K.–Masdeu–Müller–van der Put (in progress))**

*Compute the Schneider p-adic height pairing on Jacobians of hyperelliptic Mumford curves.*

There are three main steps:

- determining a Schottky group $\Gamma$ such that $C \simeq \Omega/\Gamma$:

# §3.4. Computing Schneider height pairing

**Algorithm (K.–Masdeu–Müller–van der Put (in progress))**

*Compute the Schneider p-adic height pairing on Jacobians of hyperelliptic Mumford curves.*

There are three main steps:

- determining a Schottky group $\Gamma$ such that $C \simeq \Omega/\Gamma$: a special case is due to Kadziela, we extended it.

# §3.4. Computing Schneider height pairing

**Algorithm (K.–Masdeu–Müller–van der Put (in progress))**

*Compute the Schneider p-adic height pairing on Jacobians of hyperelliptic Mumford curves.*

There are three main steps:

- determining a Schottky group $\Gamma$ such that $C \simeq \Omega/\Gamma$: a special case is due to Kadziela, we extended it.
- computing theta functions $\Theta$:

# §3.4. Computing Schneider height pairing

**Algorithm (K.–Masdeu–Müller–van der Put (in progress))**

*Compute the Schneider $p$-adic height pairing on Jacobians of hyperelliptic Mumford curves.*

There are three main steps:

- determining a Schottky group $\Gamma$ such that $C \simeq \Omega/\Gamma$: a special case is due to Kadziela, we extended it.
- computing theta functions $\Theta$: a special case is due to Morrison–Ren, we extended it.

# §3.4. Computing Schneider height pairing

**Algorithm (K.–Masdeu–Müller–van der Put (in progress))**

*Compute the Schneider p-adic height pairing on Jacobians of hyperelliptic Mumford curves.*

There are three main steps:

- determining a Schottky group $\Gamma$ such that $C \simeq \Omega/\Gamma$: a special case is due to Kadziela, we extended it.
- computing theta functions $\Theta$: a special case is due to Morrison–Ren, we extended it.
- lifting points from the curve $C$ to $\Omega$:

# §3.4. Computing Schneider height pairing

**Algorithm (K.–Masdeu–Müller–van der Put (in progress))**

*Compute the Schneider p-adic height pairing on Jacobians of hyperelliptic Mumford curves.*

There are three main steps:

- determining a Schottky group $\Gamma$ such that $C \simeq \Omega/\Gamma$: a special case is due to Kadziela, we extended it.
- computing theta functions $\Theta$: a special case is due to Morrison–Ren, we extended it.
- lifting points from the curve $C$ to $\Omega$: this requires, among other things, constructing a function which represent the "$y$-coordinate in the function field of the curve".

# §3.4. Computing Schneider height pairing

**Algorithm (K.–Masdeu–Müller–van der Put (in progress))**

*Compute the Schneider p-adic height pairing on Jacobians of hyperelliptic Mumford curves.*

There are three main steps:

- determining a Schottky group $\Gamma$ such that $C \simeq \Omega/\Gamma$: a special case is due to Kadziela, we extended it.
- computing theta functions $\Theta$: a special case is due to Morrison–Ren, we extended it.
- lifting points from the curve $C$ to $\Omega$: this requires, among other things, constructing a function which represent the "$y$-coordinate in the function field of the curve".

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

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

*is such a function.*

# §4.1. A dream: quadratic Chabauty at bad primes

If $g \geq 2$, then the set $C(\mathbb{Q})$ is known to be finite, however at present NO general algorithm for the computation of $X(\mathbb{Q})$ is known.

# §4.1. A dream: quadratic Chabauty at bad primes

If $g \geq 2$, then the set $C(\mathbb{Q})$ is known to be finite, however at present NO general algorithm for the computation of $X(\mathbb{Q})$ is known.

The abelian Chabauty method is a $p$-adic method that attempts to determine $C(\mathbb{Q})$ under the condition that $r < g$.

# §4.1. A dream: quadratic Chabauty at bad primes

If $g \geq 2$, then the set $C(\mathbb{Q})$ is known to be finite, however at present NO general algorithm for the computation of $X(\mathbb{Q})$ is known.

The abelian Chabauty method is a $p$-adic method that attempts to determine $C(\mathbb{Q})$ under the condition that $r < g$. An approach to circumvent this limitation is Kim's non-abelian Chabauty, of which quadratic Chabauty is a special case.

# §4.1. A dream: quadratic Chabauty at bad primes

If $g \geq 2$, then the set $C(\mathbb{Q})$ is known to be finite, however at present NO general algorithm for the computation of $X(\mathbb{Q})$ is known.

The abelian Chabauty method is a $p$-adic method that attempts to determine $C(\mathbb{Q})$ under the condition that $r < g$. An approach to circumvent this limitation is Kim's non-abelian Chabauty, of which quadratic Chabauty is a special case.

Working with primes of bad reduction for the abelian Chabauty method might have some practical advantages.

# §4.1. A dream: quadratic Chabauty at bad primes

If $g \geq 2$, then the set $C(\mathbb{Q})$ is known to be finite, however at present NO general algorithm for the computation of $X(\mathbb{Q})$ is known.

The abelian Chabauty method is a $p$-adic method that attempts to determine $C(\mathbb{Q})$ under the condition that $r < g$. An approach to circumvent this limitation is Kim's non-abelian Chabauty, of which quadratic Chabauty is a special case.

Working with primes of bad reduction for the abelian Chabauty method might have some practical advantages. It is a natural question whether this is also the case for quadratic Chabauty.

# §4.1. A dream: quadratic Chabauty at bad primes

If $g \geq 2$, then the set $C(\mathbb{Q})$ is known to be finite, however at present NO general algorithm for the computation of $X(\mathbb{Q})$ is known.

The abelian Chabauty method is a $p$-adic method that attempts to determine $C(\mathbb{Q})$ under the condition that $r < g$. An approach to circumvent this limitation is Kim's non-abelian Chabauty, of which quadratic Chabauty is a special case.

Working with primes of bad reduction for the abelian Chabauty method might have some practical advantages. It is a natural question whether this is also the case for quadratic Chabauty.

For some "modular" curves, the current quadratic Chabauty algorithms might need MONTHS to terminate.

# §4.1. A dream: quadratic Chabauty at bad primes

If $g \geq 2$, then the set $C(\mathbb{Q})$ is known to be finite, however at present NO general algorithm for the computation of $X(\mathbb{Q})$ is known.

The abelian Chabauty method is a $p$-adic method that attempts to determine $C(\mathbb{Q})$ under the condition that $r < g$. An approach to circumvent this limitation is Kim's non-abelian Chabauty, of which quadratic Chabauty is a special case.

Working with primes of bad reduction for the abelian Chabauty method might have some practical advantages. It is a natural question whether this is also the case for quadratic Chabauty.

For some "modular" curves, the current quadratic Chabauty algorithms might need MONTHS to terminate. I expect that working with primes of bad reduction makes the computations significantly faster.

# §4.1. A dream: quadratic Chabauty at bad primes

If $g \geq 2$, then the set $C(\mathbb{Q})$ is known to be finite, however at present NO general algorithm for the computation of $X(\mathbb{Q})$ is known.

The abelian Chabauty method is a $p$-adic method that attempts to determine $C(\mathbb{Q})$ under the condition that $r < g$. An approach to circumvent this limitation is Kim's non-abelian Chabauty, of which quadratic Chabauty is a special case.

Working with primes of bad reduction for the abelian Chabauty method might have some practical advantages. It is a natural question whether this is also the case for quadratic Chabauty.

For some "modular" curves, the current quadratic Chabauty algorithms might need MONTHS to terminate. I expect that working with primes of bad reduction makes the computations significantly faster.

*There are no bad primes, really.* - N. Dogra

# §4.2. $p$-adic BSD for abelian varieties

A $p$-adic analogue of the BSD conjecture for an elliptic curve over $\mathbb{Q}$ was given in Mazur–Tate–Teitelbaum (MTT) when $p$ is a prime of good “ordinary” or “multiplicative” reduction.

# §4.2. $p$-adic BSD for abelian varieties

A $p$-adic analogue of the BSD conjecture for an elliptic curve over $\mathbb{Q}$ was given in Mazur–Tate–Teitelbaum (MTT) when $p$ is a prime of good "ordinary" or "multiplicative" reduction.

*It also seemed, at the outset, that this would be a relatively routine project. The project has proved to be anything but routine, ...* - Mazur–Tate–Teitelbaum

# §4.2. *p*-adic BSD for abelian varieties

A $p$-adic analogue of the BSD conjecture for an elliptic curve over $\mathbb{Q}$ was given in Mazur–Tate–Teitelbaum (MTT) when $p$ is a prime of good "ordinary" or "multiplicative" reduction.

*It also seemed, at the outset, that this would be a relatively routine project. The project has proved to be anything but routine, ...* - Mazur–Tate–Teitelbaum

Balakrishnan–Müller–Stein formulated a generalization of the MTT conjecture in the good ordinary case to higher dimensional abelian varieties.

# §4.2. $p$-adic BSD for abelian varieties

A $p$-adic analogue of the BSD conjecture for an elliptic curve over $\mathbb{Q}$ was given in Mazur–Tate–Teitelbaum (MTT) when $p$ is a prime of good "ordinary" or "multiplicative" reduction.

*It also seemed, at the outset, that this would be a relatively routine project. The project has proved to be anything but routine, ...* - Mazur–Tate–Teitelbaum

Balakrishnan–Müller–Stein formulated a generalization of the MTT conjecture in the good ordinary case to higher dimensional abelian varieties.

On the other hand, the MTT conjecture in the case of split multiplicative reduction, the "exceptional" case, is of special interest.

# §4.2. *p*-adic BSD for abelian varieties

A $p$-adic analogue of the BSD conjecture for an elliptic curve over $\mathbb{Q}$ was given in Mazur–Tate–Teitelbaum (MTT) when $p$ is a prime of good "ordinary" or "multiplicative" reduction.

*It also seemed, at the outset, that this would be a relatively routine project. The project has proved to be anything but routine, ...* - Mazur–Tate–Teitelbaum

Balakrishnan–Müller–Stein formulated a generalization of the MTT conjecture in the good ordinary case to higher dimensional abelian varieties.

On the other hand, the MTT conjecture in the case of split multiplicative reduction, the "exceptional" case, is of special interest. One might expect that a generalization of this conjecture to higher dimensional abelian varieties in the case of "split purely toric" reduction can be formulated.

# with Katz, Columbus (2019)

# with Masdeu and Müller, Benasque (2022)

# with Bianchi and Müller, Groningen (2023)

# The journey has ended :-) Teşekkürler!

- *Diophantine Geometry: An Introduction* - Hindry–Silverman
- *Fundamentals of Diophantine Geometry* - Lang

- *p-adic heights on curves* - Coleman–Gross
- *Canonical height pairings via biextensions* - Mazur–Tate
- *p-adic height pairings I* - Schneider
- *Local Heights on Mumford Curves* - Werner
- *Computational tools for quadratic Chabauty* - Balakrishnan–Müller

- *Algorithms for Schneider heights on Mumford curves* (in progress) - K.–Masdeu–Müller–van der Put
- *Algorithms for Coleman–Gross Heights on Hyperelliptic Curves* (in preparation) - Bianchi–K.–Müller
- *Coleman–Gross heights and p-adic Néron functions on Jacobians of genus 2 curves* - Bianchi–K.–Müller
- *Explicit Vologodsky integration for hyperelliptic curves* - K.
- *p-adic Integration on bad reduction hyperelliptic curves* - Katz–K.