

Southwest Center
for Arithmetic Geometry

ARIZONA WINTER SCHOOL 2020

Department of Mathematics
The University of Arizona®

Deadline to apply for funding:
November 8, 2019

<http://swc.math.arizona.edu>

NONABELIAN CHABAUTY

Jennifer Balakrishnan

Computational tools for quadratic Chabauty

Bas Edixhoven

Geometric quadratic Chabauty

Minhyong Kim

Foundations of nonabelian Chabauty

David Zureick-Brown

Classical Chabauty

with **Bjorn Poonen**, Clay Lecturer

TUCSON, MARCH 7-11, 2020

Funded by the National Science Foundation
Supported by the National Security Agency
Organized in partnership
with the Clay Mathematics Institute



University of Arizona

Arizona Winter School 2020

Nonabelian Chabauty

Notes By: Caleb McWhorter

March 2020

Contents

I Talk Notes	5
1 Bjorn Poonen: Introduction to Chabauty's method and Kim's nonabelian generalization	1
1.1 Lecture 1	1
1.1.1 Rational points on Curves	1
1.1.2 Chabauty's Method	2
1.2 Lecture 2	4
1.2.1 Selmer Groups	4
1.2.2 Bloch-Kato Selmer Group	5
1.2.3 Global Galois Representations	5
1.2.4 Lower Central Series	6
1.2.5 Abelianized Fundamental Group	6
2 David Zureick-Brown: Effective Chabauty	8
2.1 Lecture 1	8
2.1.1 Effective Manin-Mumford	8
3 Minhyong Kim	10
3.1 Lectures 1–4	10
4 Jennifer Balakrishnan: Computational tools for quadratic Chabauty	11
4.1 Lecture 1	11
4.1.1 Coleman's Effective Chabauty	11
4.1.2 Explicit Coleman Integration	13
5 Bas Edixhoven: Geometric Quadratic Chabauty	15
5.1 Lecture 1	15
II Course/Project Outlines & Lecture Notes	16
6 Bjorn Poonen	17
6.1 Lecture Notes	17
7 David Zureick-Brown	36
7.1 Course & Project Outline	36
7.2 Lecture Notes	39
7.3 Project Description	57
8 Minhyong Kim	64
8.1 Course & Project Outline	64
8.2 Project Description	66
8.3 Lecture 1	68
8.4 Lecture 2	121
8.5 Lecture 3	172
8.6 Lecture 4	220

9 Jennifer Balakrishnan	253
9.1 Course & Project Outline	253
9.2 Lecture Notes & Project Descriptions (with J. Steffen Müller)	256
10 Bas Edixhoven	336
10.1 Course & Project Outline	336
10.2 Lecture Notes (Preprint of Edixhoven and Lido)	338
10.3 Project Description	342

Part I

Talk Notes

1 Bjorn Poonen: Introduction to Chabauty's method and Kim's non-abelian generalization

1.1 Lecture 1

1.1.1 Rational points on Curves

The starting point is Falting's Theorem, which was originally known as Mordell's conjecture.

Theorem 1.1 (Falting's, 1983). *Suppose $[K: \mathbb{Q}] < \infty$, and let X be a 'nice'¹ curve of genus g over K . If $g > 1$, then $X(K)$ is finite.*

There are several proofs now. The first was Falting's proof in 1983 based on Arakelov methods. The next was by Vojta 1991 and its variant (phrased in more elementary terms via Diophantine approximation) by Bombieri. But now there is a proof by Lawrence-Venkatesh in 2018 via p -adic period maps.

For integral points, the parallel to Falting's Theorem is Siegel's Theorem. Let $[K: \mathbb{Q}] < \infty$. Let $\mathcal{O} = \mathcal{O}_{K,S} = \{x \in K: \nu(x) \geq 0 \text{ for all } \nu \in S\}$, where S is a finite set of places, including all the archimedean places. Let $U := X \setminus Z$, where X is a nice curve of genus g and Z is a nonempty 0-dimensional subscheme. Now $\chi(U) := (2 - 2g) - r$, where $r = \#Z(\bar{K})$ and χ is the Euler characteristic. Suppose \mathcal{U} is a finite type \mathcal{O} -scheme with $\mathcal{U}_K = U$. If $\chi(U) < 0$. The condition that $\chi(U) < 0$ is sometimes phrased as that U is hyperbolic [over \mathbb{C} , $\tilde{U} \simeq b$].

Theorem 1.2 (Siegel's Theorem). *If $\chi(U) < 0$, then $\mathcal{U}(\mathcal{O})$ is finite.*

There is a proof, obviously, by Siegel. But there are also proofs by Baker-Coates (1970) when either $g \leq 1$ or when U is $y^2 = f(x)$ in \mathbb{A}^2 , and Lawrence-Venkatesh (2018) when $U = \mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Example 1.1. If $U = \mathbb{P} \setminus \{0, 1, \infty\}$, then $\mathcal{U} = \text{Spec } \mathcal{O}[x, \frac{1}{x}, \frac{1}{1-x}]$ and $\mathcal{U}(\mathcal{O})$ is the set of solutions to $x + y = 1$ with $x, y \in \mathcal{O}^\times$.

Remark. Falting's Theorem is strictly harder than Siegel's Theorem in that Falting's Theorem implies Siegel's Theorem. The key idea is that if $\chi(U) < 0$, then there is some finite étale cover of U is open in a nice curve of genus greater than 1.

In Siegel-Falting, $\chi(U) < 0$ means that

- $g = 0$, then $r \geq 3$
- $g = 1$, then $r \geq 1$
- $g \geq 2$, r arbitrary

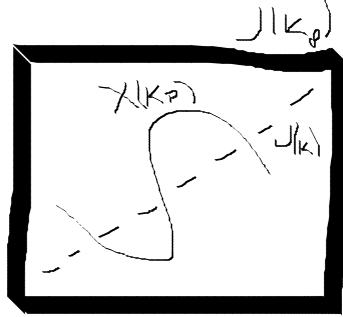
The problem with nearly all of these methods is that they are not effective. The goal is then to try to make them effective. This was exactly the hope of Chabauty.

¹smooth, projective, geometrically integral

1.1.2 Chabauty's Method

$$\begin{array}{ccc} K & & \mathfrak{p} \\ [K:\mathbb{Q}] = \dim_{\mathbb{Q}} K & \downarrow & \downarrow \\ \mathbb{Q} & & p \end{array}$$

Let X be a nice curve of genus g over K . Then X is a g -dimensional abelian variety. Let $J = \text{Jac } X$ and let $r = \text{rank } J(K)$. Choose $x \in X(K)$ to get $X \hookrightarrow J$.



$$\begin{array}{ccc} X(K) & \longrightarrow & X(K_p) \\ \downarrow & & \downarrow \\ J(K) & \longrightarrow & J(K_p) \xrightarrow{\log} \text{Lie } J_{K_p} \simeq K_p^g \end{array}$$

The kernel of the log map is finite and is a local diffeomorphism so the image will be open and compact (J is a compact group). Therefore, the image of log is an open compact subgroup of the Lie group $\text{Lie } J_{K_p}$. Moreover, the image of $J(K) \rightarrow K_p^g$ is generated by r elements. Then the dimension of K_p -span of the image is at most r . If $r < g$, there exists a nonzero linear $\lambda : \text{Lie } J_{K_p} \rightarrow K_p$ vanishing in $J(K)$, and λ pulls back to a nonzero locally analytic function on $X(K_p)$ vanishing on $X(K)$, so $X(K)$ is finite. But of course, this all requires what might be called Chabauty's condition: $r < g$.

How do we limit the role of the Jacobian in this to generalize? Rewriting

$$\begin{array}{ccccc} X(K) & \longrightarrow & X(K_p) & & \\ \downarrow & & \downarrow & & \\ J(K) & \longrightarrow & J(K_p) & \xrightarrow{\log} & \text{Lie } J_{K_p} \\ \downarrow & & \downarrow & & \nearrow \curvearrowright \\ \widehat{J(K)}[\frac{1}{p}] & \longrightarrow & \widehat{J(K_p)}[\frac{1}{p}] & & \end{array}$$

Given M , an abelian group, define $\widehat{M} := \varprojlim M/p^n M$, which is a \mathbb{Z}_p -module. Then $\widehat{M}[\frac{1}{p}] \simeq \widehat{M} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, which is a \mathbb{Q}_p vector space.

V is étale homology. As a motivation, if X is a curve over \mathbb{C} and J is its Jacobian. Then analytically, $J(\mathbb{C}) \simeq \mathbb{C}^g / \Lambda$, where $\Lambda = H_1(J(\mathbb{C}), \mathbb{Z})$. Using the right hand side, it is easy to see

that

$$J[p] \simeq \frac{1}{p} \Lambda / \Lambda \xrightarrow{p} \Lambda / p\Lambda = H_1(J(\mathbb{C}), \mathbb{Z}/p\mathbb{Z}) = H_1(X(\mathbb{C}), \mathbb{Z}/p\mathbb{Z})$$

If we are not using \mathbb{C} , we are going to have to switch to Étale (co)homology.

For X over K , $J[p] \simeq H_1^{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p\mathbb{Z}) := \mathbb{Z}/p\mathbb{Z}$ -dual of $H_1^{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p\mathbb{Z})$. Likewise, $J[p^n] \simeq H_1^{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p^n\mathbb{Z})$. Now \mathbb{Z}_p is the Tate module, where $T := \varprojlim J[p^n] \simeq H_1^{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_p)$. Tensoring with \mathbb{Q}_p , we obtain the \mathbb{Q}_p -Tate module $V := T[\frac{1}{p}] = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H_1^{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_p)$, which is a \mathbb{Q}_p -vector space of dimension $2g$.

Now write $\mathcal{V}(\mathbb{Q}_p)$ for a group variety $\mathcal{V} \simeq \mathbb{G}_a^{2g}$ over \mathbb{Q}_p . Note that \mathcal{V} is \mathbb{A}^{2g} with an additive group law. The group $G_K := \text{Gal}(\bar{K}/K)$ acts continuously on all of these, e.g. $G_K \rightarrow \text{Aut } \mathcal{V} \simeq \text{GL}_n(\mathbb{Q}_p)$, as a group variety.

1.2 Lecture 2

1.2.1 Selmer Groups

$$\begin{aligned} 0 &\longrightarrow J[p] \longrightarrow J \xrightarrow{p} J \longrightarrow 0 \\ J(K) &\xrightarrow{p} J(K) \longrightarrow H^1(K, J[p]) \\ \frac{J(K)}{pJ(K)} &\hookrightarrow H^1(K, J[p]) \end{aligned}$$

But the right side is an infinite dimensional \mathbb{F}_p -vector space if $\dim J \geq 0$.

$$\begin{array}{ccc} \frac{J(K)}{pJ(K)} & \hookrightarrow & \text{Sel}_p J \subseteq H^1(K, J[p]) \\ & & \downarrow \beta \\ \prod_v \frac{J(K_v)}{pJ(K_v)} & \xrightarrow{\alpha} & \prod_v H^1(K_v, J[p]) \end{array}$$

$\text{Sel}_p J := \{\xi \in H^1(K, J[p]): \beta(\xi) \in \text{im } \alpha\}$. This group is conjecturally finite and computable.
Similarly,

$$\frac{J(K)}{p^n J(K)} \hookrightarrow \text{Sel}_{p^n} J \subset H^1(K, J[p^n])$$

By taking inverse limits

$$\widehat{J(K)} \hookrightarrow \text{Sel}_{\mathbb{Z}_p} J \subset H^1(K, T)$$

then by inverting p

$$\widehat{J(K)}[\frac{1}{p}] \hookrightarrow \text{Sel}_{\mathbb{Q}_p} J \subset H^1(K, V)$$

Then we have

$$0 \longrightarrow \frac{J(K)}{pJ(K)} \longrightarrow \text{Sel}_p J \longrightarrow \text{III}[p] \longrightarrow 0$$

$$0 \longrightarrow$$

$$\begin{array}{ccccc} X(K) & \longrightarrow & X(K_{\mathfrak{p}}) & & \\ \downarrow & & \downarrow & & \\ J(K) & \longrightarrow & J(K_{\mathfrak{p}}) & \xrightarrow{\log} & \text{Lie } J_{K_{\mathfrak{p}}} \\ \downarrow & & \downarrow & \nearrow \curvearrowright & \\ \widehat{J(K)}[\frac{1}{p}] & \longrightarrow & \widehat{J(K_{\mathfrak{p}})}[\frac{1}{p}] & & \\ \downarrow & & \downarrow & & \\ \text{Sel}_{\mathbb{Q}_p} J & & & & \\ \downarrow & & & & \\ H^1(K, V) & \longrightarrow & H^1(K_{\mathfrak{p}}, V) & & \end{array}$$

1.2.2 Bloch-Kato Selmer Group

We examine the Bloch-Kato Selmer group in terms of V and not J . In the general setting (local Galois representations), let V be a finite dimensional \mathbb{Q}_p -vector space with continuous action— G_{K_v} -action.

$$D_{\text{cris}}(V) := (B_{\text{cris}} \otimes_{\mathbb{Q}_p} V)^{G_{K_v}}$$

where B_{cris} is a certain ring equipped with a G_{K_v} -action.

Remark. $\dim_{K_v} D_{\text{cris}}(V) \leq \dim_{\mathbb{Q}_p} V$

s

Definition (Crystalline). We call V crystalline if equality holds.

Remark. For v and an abelian variety J/K_v , then J has good reduction if and only if its \mathbb{Q}_p Tate module V is unramified if $v \nmid p$ and crystalline if $v \mid p$.

Now suppose $\xi \in H^1(K, V)$. Let

$$0 \longrightarrow V \longrightarrow E \longrightarrow \mathbb{Q}_p \longrightarrow 0$$

be the corresponding extension. Call ξ crystalline if E is crystalline.

$$H_f^1(K_v, V) := \{\text{crystalline classes in } H^1(K_v, V)\}$$

Remark. $\mathfrak{p} \mid p$. If J is an abelian variety with good reduction at \mathfrak{p} , and V is a \mathbb{Q}_p Tate module, then the image of

$$\widehat{J(K_{\mathfrak{p}})}[\frac{1}{p}] \rightarrow H^1(K_{\mathfrak{p}}, V)$$

equals $H_f^1(K_{\mathfrak{p}}, V)$. If $\mathfrak{p} \nmid p$, then $H^1(K_{\mathfrak{p}}, V) = 0$.

1.2.3 Global Galois Representations

Let V be a finite dimensional \mathbb{Q}_p -vector space with continuous G_K -action. Given $\xi \in H^1(K, V)$. Let ξ_v be its image in $H^1(K_v, V)$. The Bloch-Kato Selmer group of v is the group

$$H_f^1(K, V) := \{\xi \in H^1(K, V) : \xi_v \text{ is crystalline for all } v \mid p\}$$

Remark. If J is an abelian variety over K and V is a \mathbb{Q}_p Tate module, then $H_f^1(K, V) = \text{Sel}_{\mathbb{Q}_p} J$.

$$\begin{array}{ccccc}
X(K) & \longrightarrow & X(K_{\mathfrak{p}}) & & \\
\downarrow & & \downarrow & & \\
J(K) & \longrightarrow & J(K_{\mathfrak{p}}) & \xrightarrow{\log} & \text{Lie } J_{K_{\mathfrak{p}}} \\
\downarrow & & \downarrow & \nearrow \curvearrowright & \\
\widehat{J(K)}[\frac{1}{p}] & \longrightarrow & \widehat{J(K_{\mathfrak{p}})}[\frac{1}{p}] & & \\
\downarrow & & \downarrow & & \\
\text{Sel}_{\mathbb{Q}_p} J = H_f^1(K, V) & \longrightarrow & H_f^1(K_{\mathfrak{p}}, V) & & \\
\downarrow & & \downarrow & & \\
H^1(K, V) & \longrightarrow & H^1(K_{\mathfrak{p}}, V) & &
\end{array}$$

Algebraic de Rham Cohomology: $H_{\text{dr}}^1(X) := \mathbb{H}^1(X, \Omega^0)$ with Hodge filtration Fil^0 , where \mathbb{H} is hypercohomology. Define also $H_1^{\text{dr}}(X) :=$ dual of H_{dr}^1 with dual filtration.

$$\begin{array}{ccccc}
X(K) & \longrightarrow & X(K_{\mathfrak{p}}) & & \\
\downarrow & & \downarrow & & \\
J(K) & \longrightarrow & J(K_{\mathfrak{p}}) & \xrightarrow{\log} & \text{Lie } J_{K_{\mathfrak{p}}} \\
\downarrow & & \downarrow & \nearrow \curvearrowright & \\
\widehat{J(K)}[\frac{1}{p}] & \longrightarrow & \widehat{J(K_{\mathfrak{p}})}[\frac{1}{p}] & & \\
\downarrow & & \downarrow & & \\
\text{Sel}_{\mathbb{Q}_p} J = H_f^1(K, V) & \longrightarrow & H_f^1(K_{\mathfrak{p}}, V) & \xrightarrow{\log, \sim} & H_1^{\text{dr}}(K_{K_{\mathfrak{p}}}) / \text{Fil}^0 \\
\downarrow & & \downarrow & & \\
H^1(K, V) & \longrightarrow & H^1(K_{\mathfrak{p}}, V) & &
\end{array}$$

We get

$$\begin{array}{ccc}
X(K) & \longrightarrow & X(K_{\mathfrak{p}}) \\
\downarrow & & \downarrow \\
H_f^1(K, V) & \longrightarrow & H_f^1(K_{\mathfrak{p}}, V) \xrightarrow{\sim} H_1^{\text{dr}}(X_{K_{\mathfrak{p}}}) / \text{Fil}^0 \\
& & \searrow \text{p-adic integrals}
\end{array}$$

1.2.4 Lower Central Series

Let G be a (topological) group. For $A, B \leq g$, define $(A, B) := \overline{\langle aba^{-1}b^{-1} : a \in A, b \in B \rangle}$. Now define the lower central series by

$$\begin{aligned}
C^1 G &:= G \\
C^2 G &:= (G, C^1 G) = (G, G) \\
C^3 G &:= (G, C^2 G) \\
&\vdots
\end{aligned}$$

Finally, define $G_n := G/C^{n+1}G$. This is a n -step nilpotent group.

Example 1.2. $G_1 = G/(G, G) =: G^{ab}$, the abelianization of G , i.e. the largest abelian quotient.

This was just Group Theory. Now let's apply this to the fundamental group of the curve.

1.2.5 Abelianized Fundamental Group

Given M a connected real manifold, $m \in M$, we get $\pi_1(M, m)^{ab} \simeq H_1(M, \mathbb{Z})$, where π_1 is the fundamental group. What is the algebraic version? Given X , a 'nice' curve of genus g curve over K , $x \in X(K)$, we obtain

$$\pi_1^{\text{ét}}(X_{\bar{K}}, x)^{ab} \simeq H_1^{\text{ét}}(X_{\bar{K}}, \widehat{\mathbb{Z}})$$

But we have maps

$$\pi_1^{\text{ét}}(X_{\bar{K}}, x)_1 \xrightarrow{\sim} \pi_1^{\text{ét}}(X_{\bar{K}}, x)^a b \simeq H_1^{\text{ét}}(X_{\bar{K}}, \widehat{\mathbb{Z}}) \twoheadrightarrow H_1^{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_p) \subset H_1^{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_p) =: V = \mathcal{V}(\mathbb{Q}_p)$$

Kim obtains a generalization

$$\pi_1^{\text{ét}}(X_{\bar{K}}, x) \longrightarrow V_n = \mathcal{V}_n(\mathbb{Q}_p)$$

where \mathcal{V}_n is some unipotent algebraic group, and

$$\begin{array}{ccc} X(K) & \longrightarrow & X(K_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ H_f^1(K, V_n) & \longrightarrow & H_f^1(K_{\mathfrak{p}}, V_n) \xrightarrow{\sim} \pi_1^{\text{dr}}(X_{K_{\mathfrak{p}}}, x)_n / \text{Fil}^0 \end{array}$$

p-adic iterated integrals

and morphisms of \mathbb{Q}_p -varieties

$$\text{Sel}^{[n]} \longrightarrow J^{[n]} \longrightarrow L^{[n]}$$

which gives you the \mathbb{Q}_p points of $\pi_1^{\text{dr}}(X_{K_{\mathfrak{p}}}, x)_n / \text{Fil}^0$.

Theorem 1.3 (Kim). *If for some $n \geq 1$, $\dim \text{Sel}^{[n]} < \dim J^{[n]}$, then $X(K)$ is contained in the set of zeros of some nonzero locally analytic functions on the local points of the curve, which are given by some iterated integrals. Therefore, $X(K)$ is finite.*

2 David Zureick-Brown: Effective Chabauty

2.1 Lecture 1

Lorenzini-Tucker
McColm-Poonen
Stoll
Katz-ZB

Theorem 2.1 (K-ZB). *Let X/\mathbb{Q} be a ‘nice’ curve with $r = \text{rank } J(\mathbb{Q})$, and $p > 2r + 2$ a prime. Let \mathfrak{X} be a regular proper minimal model of X . Let $r < g$, then*

$$\#(X(\mathbb{Q})) \leq \#\mathfrak{X}_{\mathbb{F}_p}^?(\mathbb{F}_p) + 2r$$

Theorem 2.2 (Coleman, “rank favorable bound”). *In the situation above,*

$$\#(X(\mathbb{Q})) \leq \#\mathfrak{X}_{\mathbb{F}_p}^?(\mathbb{F}_p) + (2g - 2)$$

A question of Mazur is can we bound $\#X(K)$ using the rank of $J(K)$ and g ?

Conjecture 2.1 (Uniformity Conjecture). *There exists $B(K, g)$ such that for all nice X/K of genus g with*

$$\#X(K) \leq B(K, g)$$

Work of Poonen et al gives heuristics that, in the case of X an elliptic curve, imply r is bounded.

The Weak Lang Conjecture states that if X/K is a variety of general type, then there is $Z \subseteq X$ closed such that $Z(K) \subseteq X(K)$.

Theorem 2.3 (Caparso,Harris,Mazur). *The Weak Lang Conjecture implies the Uniformity Conjecture*

Example 2.1 (Gordon-Grant, '93). Let $X : y^2 = x(x-1)(x-2)(x-5)(x-6)$. This is a hyperelliptic curve with $g = 2$ and rank 1. But $r = 1 < 2$ so Coleman applies. Then $\#X(\mathbb{Q}) = 10$ GWP, 3 IG and IQ ± 120 . But mod 7, we have $\#X(\mathbb{F}_7) = 8$ gWP, $(3, \pm 6)$.

$$10 \leq \#X(\mathbb{Q}) \leq \#X(\mathbb{F}_7) + 2 = 8 + 2 = 10$$

Theorem 2.4 (Stoll). *Suppose that X is hyperelliptic, and suppose that $r \leq g - 3$. Then $\#X(\mathbb{Q}) \leq 3(r+4)(g-1) + \max\{1, 4r\} \cdot g$.*

Theorem 2.5 (Katz-Rabinoff-ZB). *Suppose $r \leq g - 3$. Then $\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28$.*

2.1.1 Effective Manin-Mumford

Let X be a curve and $X \xrightarrow{i} J$. Then $\#i(X) \cap J_{\text{tor}} < \infty$, proven by Raynaud, Buildum, Coleman.

$$X \hookrightarrow J \xrightarrow{\log} \text{Lie } J$$

Then the integrals vanish on $X \cap J_{\text{tors}}$. The nice thing here is that there is no necessary rank condition.

Theorem 2.6 (KRZB). $\bullet (X \cap J_{\text{tors}})(\mathbb{Q}) \leq (?)$

- I and X is very degenerate, e.g. totally degenerate
then we can bound $\#\cap J_{tors} \leq \dots$

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) \\ & \downarrow & \searrow \\ J(\mathbb{Q}) & \hookrightarrow & J(\mathbb{Q}_p) \xrightarrow{\log} \text{Lie } J \end{array}$$

'Black box Chabauty'.

- Setup
- local analysis
- global coordination

Setup

Let $r < g$. There exists $V \subseteq H^0(X_{\mathbb{Q}_p}, \Omega^1)$ such that for all $P, Q \in X(\mathbb{Q})$, $\int_P^Q \omega = 0$ for all $\omega \in V$ and $\dim V \geq g - r > 0$.

Local Analysis:

We can compute $\int_P^Q \omega$ locally and analyze with a Newton Polygon.

$[QI] := \{P \in X(\mathbb{Q}_p) \text{ such that } P \equiv Q \pmod{p}\} \simeq p\mathbb{Z}_p$, the p -adic disc. Where the map is $p \mapsto u(P)$, where u is a uniformizer at \tilde{Q} , a lift of Q .

Example 2.2 (HP survey). $X : y^2 = f(x) = x^6 + 8x^5 + \dots + 1 = xg(x) + 1$.

$(0, 1) \in X(\mathbb{F}_3)$.

$[(0, 1)] \xrightarrow{\sim} p\mathbb{Z}_p$ with map $p \mapsto X(P)$ forward and $t \mapsto (t, \sqrt{tg(t) + 1})$, which converges because t is small, $v_p(t) > 0$.

To compute $\int_P^Q \omega$, only compute "tiny" integrals, i.e. $P = Q \pmod{p}$. If $Q \in [P] \simeq p\mathbb{Z}_p \ni t$ with $\omega|_{[P]} = f(t) dt$ for some $f(t) \in \mathbb{Z}_p[1 + 1]$.

$$\int_P^Q \omega = \int_Q^t f(t) dt = I(t)$$

integrating formally.

3 Minhyong Kim

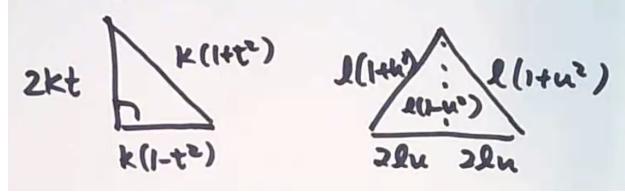
3.1 Lectures 1–4

Minhyong Kim's lectures were from his lecture note slides, please see those sections in Part II.

4 Jennifer Balakrishnan: Computational tools for quadratic Chabauty

4.1 Lecture 1

Question 1. Does there exist a pair of rational right triangles and a rational isosceles triangle that have the same area and the same perimeter?



We rescale $l = 1$, suppose $k, t, u \in \mathbb{Q}$, $0 < t, u < 1$, $k > 0$

Equate areas and perimeters:

{

After some algebra, we see there exists $x \in \mathbb{Q}$, $1 < x < 2$ such that $2xk^2 + (-3x^2 - 2x^2 + 6x - 4)k + x^5 = 0$. The discriminant of polynomial in k must be a rational square:

$$\begin{aligned} y^2 &= (-3x^2 - 2x^2 + 6x - 4)^2 - 4(2x)x^5 \\ &= x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16 \end{aligned}$$

This is a genus 2 curve, and we'd like to determine $X(\mathbb{Q})$. The Jacobian J of X has rank $\text{rank } J(\mathbb{Q}) = 1$. Also, Chabauty-Coleman bound gives $\#X(\mathbb{Q}) \leq 10$. We can find $\{\infty^\pm, (0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11)\} \subset X(\mathbb{Q})$. We've found no rational points!

The answer to the discriminant question:

Theorem 4.1 (Hirakawa-Matsumura, 2018). *Yes, there are exactly one pair of such triangles.*

4.1.1 Coleman's Effective Chabauty

Let X/\mathbb{Q} be a ‘nice’ curve with genus $g \geq 2$. Suppose that $\text{rank } J(\mathbb{Q}) < g$. If $p > 2g$ is good, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2$. This bound comes from bounding the number of zeros of a p -adic (Coleman) integral.

Coleman gave a theory of p -adic line integration in the 1980s.

Theorem 4.2 (Coleman). *Let X/\mathbb{Q}_p be a nice curve with good reduction at p . The p -adic integral $\int_P^Q \omega \in \overline{\mathbb{Q}}_p$, defined for $P, Q \in X(\overline{\mathbb{Q}}_p)$ and $\omega \in H^0(X, \Omega^1)$ satisfies the following:*

(i) *the integral is $\overline{\mathbb{Q}}_p$ linear in ω*

(ii) *if P, Q reduce to the same point $\bar{P} \in X(\mathbb{F}_p)$, then we call the integral a ‘tiny’ integral.*

(iii) *We have*

$$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^Q \omega + \int_{P'}^Q \omega$$

then we can define \int_D^ω for $D = \sum_{j=1}^n ((Q_j) - (P+j)) \in DN_K^0(\overline{\mathbb{Q}}_p)$ as $\int_P \omega = \sum_{j=1}^n \int_{P_j}^{Q_j} \omega$.

(iv) *if D is principal, then $\int_D \omega = 0$.*

(v) Integral compatibility with $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ -action.

(vi) Fix $P_0 \in X(\overline{\mathbb{Q}}_p)$. If $0 \neq \omega \in H^0(?, \Omega^1)$, then the set of points $P \in X(\overline{\mathbb{Q}}_p)$ reduces to a fixed point on $X(\mathbb{F}_p)$ such that $\int_{P_0}^P \omega = 0$ is finite.

This is the Coleman integral. Cont Given hypotheses of previous theorem, let $b \in X(\mathbb{Q}_p)$, $i : X \hookrightarrow J$ given by $P \mapsto [P - b]$. There is a map $J(\mathbb{Q}_p) \times H^0(X_{\mathbb{Q}_p}, \Omega^1) \rightarrow \mathbb{Q}_p$ given by $(Q, \omega) \mapsto \langle Q, \omega \rangle$ that's additive in Q , \mathbb{Q}_p -linear in ω , and given by $\langle [D], \omega \rangle = \int_D \omega$ for $D \in \text{Div}_X^0$.

For $P \in X(\mathbb{Q}_p)$, we have the Abel-Jacobi morphism AJ_b that takes P to

$$\langle i(P), \omega \rangle = \int_b^P \omega =: AJ_b(P)$$

The Chabauty-Coleman method uses a certain subspace of the space of regular 1-forms. Now assume $b \in X(\mathbb{Q})$, use it to embed $X \hookrightarrow J$.

Definition. Let $A = \{\omega \in H^0(X, \Omega^1) \text{ for all } P \in J(\mathbb{Q}), \langle P, \omega \rangle = 0\}$ be the subspace of annihilating differentials.

We have

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) \xrightarrow{\log} H^0(J_{\mathbb{Q}_p}, \Omega^1) \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1) \end{array}$$

By “computing rational points via Chabauty-Coleman: compute the finite set of p -adic points

$$X(\mathbb{Q}_p)_1 := \{z \in X(\mathbb{Q}_p) : \int_b^z \omega = 0 \text{ for all } \omega \in A\}$$

By construction, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$. How do we compute annihilating differ?

Example 4.1. Let $X : y^2 = x^5 - 2x^3 + x = 1$ (LMFBD: 971.4 971.1) Some facts about X :

(i) $X(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}$

(ii) J is simple, $J(\mathbb{Q}) \simeq \mathbb{Z}$, $[-1, -1/2] - (0, 1/2) \in J(\mathbb{Q})$ has infinite order.

(iii) X is good at $p = 3$, $\#X(\mathbb{F}_3) = 7$. Stoll's refinement of Chabauty-Coleman for $p = 3$:

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r + \frac{2r}{p-2} = 11$$

So need to do more work to determine $X(\mathbb{Q})$ here. We will construct a 3-adic annihilating differential η . Bases of $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ is $\left\{ \omega_i = \frac{x^i dx}{2y} \right\}_{i=0,1}$. So η is a \mathbb{Q}_3 -linear combination of ω_0, ω_1 . We will compute the values of $\alpha := \int_{(a,b)}^{1-\gamma_0} \omega_0$ and $\beta := \int_{(0,\gamma_0)}^{1-\gamma_0} \omega_1$ to compute η . SageMath can compute α, β

$$\alpha = 3 + 3^2 + 3^4 + \dots$$

$$\beta = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \dots$$

We take $\eta = \beta\omega_0 - \alpha\omega_1$ and run Chabauty-Coleman.

Where do these numbers come from?

4.1.2 Explicit Coleman Integration

Using the action of Frobenius on p -adic cohomology. (Sage for hyperelliptic curves or Magma for plane curves.) Let X^{an} denote the rigid analytic space over \mathbb{Q}_p associated to X/\mathbb{Q}_p . A wide open subspace of X^{an} , the complement in X^{an} of the union of a finite collection of disjoint closed disks of radius < 1 . Now for some more properties of the Coleman integral:

Theorem 4.3 (Coleman). *Let η, ξ be 1-forms on a wide open V of X^{an} , $P, Q, R \in V(\overline{\mathbb{Q}_p})$, let $a, b \in \overline{\mathbb{Q}_p}$. Then we have*

(i) *linearity in integrand:*

$$\int_P^Q a\eta + b\xi = a \int_P^Q \eta + b \int_P^Q \xi$$

(ii) *additivity in endpoints*

$$\int_P^R \eta + \int_R^Q \eta = \int_P^Q \eta$$

(iii) *change of variables under rigid analytic maps (Frobenius)*

(iv) *Fundamental Theorem of Calculus*

$$\int_P^Q df = f(Q) - f(P)$$

(v) *Galois compatibility*

We first integrate $\int_P^Q \omega$ for ω 1-form of the second kind, $P, Q \in V(\mathbb{Q}_p)$. Suppose X is a hyperelliptic curve. Sketch of explicit Coleman integration (B-Bradshaw-Kedlaya).

1. take a lift of p -power Frobenius
2. compute a basis $\{\omega_i\}$ of 1-forms of the second kind
3. compute $\phi^* \omega_i$ via Kedlaya's zeta function algorithm and use properties of Coleman integral to relate

$$\int_P^Q \phi^* \omega_i \text{ to } \int_P^Q \omega_i$$

as well as other easier terms.

4. solve for $\int_P^Q \omega_i$ using lth. algorithm.

We sketch Kedlaya's algorithm. Let X be the curve $y^2 = p(x)$. We work in an affine $Y \subset X$ given by defining Weierstrass points. Take ϕ to be $x \mapsto x^p$ and $y \mapsto y^p \sum_{j=0}^{\infty} \binom{1/2}{1} \left(\frac{p(x^p - p(x)^p)}{y^{2p}} \right)^j$.

Then we compute the action of ϕ on

$$\begin{aligned} \phi^* \left(\frac{x^i dx}{y} \right) &= \frac{x^{pi} d(x^p)}{\phi(y)} \\ &= \frac{x^{pi} p x^{p-1} dx}{\phi(y)} \\ &= p x^{pi+p-1} y^{-p} \sum_{j=0}^{\infty} \binom{1/2}{1} \left(\frac{p(x^p - p(x)^p)}{y^{2p}} \right)^j \end{aligned}$$

and reduce pole order of each resulting differential using relations in H^1 . Denote the basis by $\{\omega_i\}_{i=0,\dots,2g-1}$. Then Kedlaya's algorithm gives

$$\phi^* \omega_i = dh_o + \sum_{j=0}^{2g-1} \mu_{ji} \omega_j$$

If we can compute h_i and M , then

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i \\ \vdots \end{pmatrix} = (M^t - I)^{-1} \begin{pmatrix} \vdots \\ h_i(P) - h_i(Q) - \int_P^{\pi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i \\ \vdots \end{pmatrix}$$

Finishing the 3-adic integrals on $y^2 = x^5 - 2x^3 + x + 1/4$, we constructed $\eta = \beta\omega_0 - \alpha\omega_1$, where α, β are computed using (*). We want to compute $X(\mathbb{Q}_3)$. Compute power series expansions of

$$\left\{ \int_{(0,1/2)}^{P_t} \eta \right\}$$

where P_t ranges over all residue disks:

$$\int_{(0,1/2)}^{P_t} \eta = \underbrace{\int_{(0,1/2)}^{P_0} \eta}_{\text{Gives 3-adic}} + \underbrace{\int_{P_0}^{P_t} \eta}_{\text{Coleman 3-adic series}}$$

Lucky fact: For each residue disk, there exists $P_0 \in X(\mathbb{Q})$, the 3-adic number is 0. Compute the tiny integral in each residue disk, we find each just has a simple zero at known rational point. This proves that $\#X(\mathbb{Q}) = 7$.

5 Bas Edixhoven: Geometric Quadratic Chabauty

5.1 Lecture 1

Part II

Course/Project Outlines & Lecture Notes

p -ADIC APPROACHES TO RATIONAL AND INTEGRAL POINTS ON CURVES

BJORN POONEN

ABSTRACT. We give an introduction to two p -adic methods that aim to prove the finiteness of the set of rational or integral points on hyperbolic curves. The first is Kim’s method, generalizing Chabauty’s method, which in turn was inspired by a method of Skolem. The second is the method of Lawrence and Venkatesh, which uses p -adic period maps to give a new proof of the theorems of Siegel and Faltings.

1. THE THEOREMS OF SIEGEL AND FALTINGS

1.1. Rational points on projective curves. Let K be a number field. Call a curve over K nice if it is smooth, projective, and geometrically integral. The following theorem was originally conjectured by Mordell [Mor22].

Theorem 1.1 (Faltings). *Let X be a nice curve of genus g over K . If $g > 1$, then $X(K)$ is finite.*

There exist several proofs, all difficult:

- Faltings [Fal83], via Arakelov methods.
- Vojta [Voj91], via diophantine approximation. A more elementary variant of Vojta’s proof was given by Bombieri [Bom90].
- Lawrence–Venkatesh [LV18], via p -adic period maps.

There is also a much older result of Chabauty [Cha41], who adapted a p -adic method of Skolem to prove that if the Jacobian J of X satisfies $\text{rank } J(K) < g$, then $X(K)$ is finite.

1.2. Integral points on curves. Let S be a finite set of places of K containing all the archimedean places. Then the ring of S -integers in K is

$$\mathcal{O} = \mathcal{O}_{K,S} := \{x \in K : v(x) \geq 0 \text{ for all } v \notin S\}.$$

Date: March 7, 2020.

These are updated versions of notes for lectures given July 1–10, 2019 during the “Reinventing rational points” trimester at the Institut Henri Poincaré and on March 7, 2020 at the 2020 Arizona Winter School on “Nonabelian Chabauty”. The writing of these notes was supported in part by the Université de Paris-Sud, National Science Foundation grant DMS-1601946, and Simons Foundation grants #402472 (to Bjorn Poonen) and #550033.

Let X be a nice curve of genus g over K . Let Z be a nonempty 0-dimensional subscheme of X . Let $r = \#Z(\overline{K})$, where \overline{K} denotes an algebraic closure of K . Let $U = X - Z$. Then one may define the topological Euler characteristic $\chi(U) = \chi(X) - r = (2 - 2g) - r$.

Theorem 1.2 (Siegel). *Let $U = X - Z$ as above. Let \mathcal{U} be any finite-type \mathcal{O} -scheme such that $\mathcal{U}_K \simeq U$. If $\chi(U) < 0$, then $\mathcal{U}(\mathcal{O})$ is finite.*

Again there are a few proofs:

- Siegel [Sie29], via diophantine approximation.
- Baker–Coates [BC70] gave a proof when either $g \leq 1$ or X is hyperelliptic and Z contains a Weierstrass point, via linear forms in logarithms. This proof, when it applies, is the only one that is *effective*, giving a computable upper bound on the height of the integral points.
- Lawrence–Venkatesh [LV18], via p -adic period maps, gave a new proof of the case $U = \mathbb{P}^1 - \{0, 1, \infty\}$.

Also, Skolem [Sko34] invented a p -adic method that in some situations would determine $\mathcal{U}(\mathcal{O})$.

Remark 1.3. Theorem 1.1 implies Theorem 1.2, even if U has genus ≤ 1 , because one can use descent to replace U by a finite étale cover (and its twists) of genus > 1 .

Remark 1.4. If one allowed $Z = \emptyset$ in Theorem 1.2, then one would obtain a statement that included also Theorem 1.1: if $Z = \emptyset$, then the condition $\chi(U) < 0$ becomes $g > 1$ and the valuative criterion for properness yields $\mathcal{U}(\mathcal{O}) = X(K)$. In this combined statement, the hypothesis $\chi(U) < 0$ amounts to being in one of the following situations:

- $g = 0$ and $r \geq 3$ (e.g., $\mathbb{P}^1 - \{0, 1, \infty\}$);
- $g = 1$ and $r \geq 1$ (e.g., an elliptic curve with the point at infinity removed);
- $g \geq 2$ and r is arbitrary.

1.3. Goals of these lecture notes. Sections 2 and 3 give an introduction to Kim’s non-abelian generalization of Chabauty’s p -adic method.

The remaining sections give an introduction to the article by Lawrence and Venkatesh [LV18]. We present their general method, and sketch how they use it to prove Siegel’s theorem for $\mathbb{P}^1 - \{0, 1, \infty\}$, also known as the S -unit equation.

2. KIM’S REWRITING OF CHABAUTY IN TERMS OF ÉTALE HOMOLOGY OF THE CURVE

2.1. Chabauty’s method. Here we give only a quick review of Chabauty’s method; for more details, see [MP12], for example.

Let K be a number field. Let X be a nice (i.e., smooth, projective, and geometrically integral) curve of genus g over K . Let \mathfrak{p} be a prime of K at which X has good reduction. Let

p be the prime of \mathbb{Q} below \mathfrak{p} . Let $K_{\mathfrak{p}}$ be the completion of K at \mathfrak{p} . Let J be the Jacobian of X . Let r be the rank of $J(K)$. We have a commutative diagram

$$(1) \quad \begin{array}{ccc} X(K) & \longrightarrow & X(K_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ J(K) & \longrightarrow & J(K_{\mathfrak{p}}) \xrightarrow{\log} \text{Lie } J_{K_{\mathfrak{p}}}. \end{array}$$

Chabauty's approach is to understand the images of $J(K)$ and $X(K_{\mathfrak{p}})$ in $\text{Lie } J_{K_{\mathfrak{p}}}$. Specifically, the image of $J(K)$ in the g -dimensional space $\text{Lie } J_{K_{\mathfrak{p}}}$ spans a $K_{\mathfrak{p}}$ -subspace of dimension at most r , so if $r < g$, then there is a nonzero $K_{\mathfrak{p}}$ -linear functional on $\text{Lie } J_{K_{\mathfrak{p}}}$ vanishing on the image of $J(K)$, and one shows that it pulls back to a nonzero locally analytic function on $X(K_{\mathfrak{p}})$ vanishing on $X(K)$, which proves that $X(K)$ is finite.

2.2. Summary of the rewriting. Minhyong Kim found a way to rewrite (1) so that all references to J are replaced by references to X and its various homology groups. This enabled him to generalize, by replacing homology by deeper quotients of the fundamental group of X . Our exposition of this mainly follows [Cor19], but without going into as much detail.

The rewriting can be summarized by the following diagram, which will be explained in later sections; the red items are to be replaced by the green ones.

$$(2) \quad \begin{array}{ccccccc} X(K) & \longrightarrow & X(K_{\mathfrak{p}}) & & & & \\ \downarrow & & \downarrow & & & & \\ \color{red}J(K) & \longrightarrow & \color{red}J(K_{\mathfrak{p}}) & \xrightarrow{\log} & \color{red}\text{Lie } J_{K_{\mathfrak{p}}} & & \\ \downarrow & & \downarrow & & \nearrow \simeq & & \uparrow \simeq \\ \widehat{J(K)} \left[\frac{1}{p} \right] & \longrightarrow & \widehat{J(K_{\mathfrak{p}})} \left[\frac{1}{p} \right] & & & & \\ \simeq ? \downarrow & & \downarrow & & & & \\ \text{Sel}_{\mathbb{Q}_p} J = \color{green}H^1_f(K, V) & \longrightarrow & \color{green}H^1_f(K_{\mathfrak{p}}, V) & \xrightarrow[\simeq]{\log_{BK}} & \color{green}H_1^{\text{dR}}(X_{K_{\mathfrak{p}}}) / \text{Fil}^0 & & \\ \downarrow & & \downarrow & & & & \\ H^1(K, V) & \longrightarrow & H^1(K_{\mathfrak{p}}, V). & & & & \end{array}$$

2.3. p -adic completions. Let M be an abelian group. We can form a \mathbb{Z}_p -module by taking the p -adic completion $\widehat{M} := \varprojlim_n M/p^n M$. Next, we can form a \mathbb{Q}_p -vector space by localizing the module by inverting p , to obtain $\widehat{M} \left[\frac{1}{p} \right] \simeq M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. These constructions are functorial in M .

The group $J(K_{\mathfrak{p}})$ is compact, so the images of $p^n J(K_{\mathfrak{p}})$ in $\text{Lie } J_{K_{\mathfrak{p}}}$ tend to 0 p -adically as $n \rightarrow \infty$. Therefore the homomorphism $J(K_{\mathfrak{p}}) \rightarrow \text{Lie } J_{K_{\mathfrak{p}}}$ factors through $\widehat{J(K_{\mathfrak{p}})}$ and hence

also through $\widehat{J(K_p)} \left[\frac{1}{p} \right]$. Using that \log is a local diffeomorphism with finite kernel, one can prove that the \mathbb{Q}_p -linear map $\widehat{J(K_p)} \left[\frac{1}{p} \right] \rightarrow \text{Lie } K_p$ is an isomorphism.

This explains up to the third row of (2).

2.4. Étale homology. If $J = \text{Jac } X$ for some curve X over \mathbb{C} , then $J(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ for some lattice $\Lambda \simeq H_1(J(\mathbb{C}), \mathbb{Z})$, and

$$J[p] \simeq \frac{p^{-1}\Lambda}{\Lambda} \simeq \frac{\Lambda}{p\Lambda} \simeq H_1(J(\mathbb{C}), \mathbb{Z}/p\mathbb{Z}) \simeq H_1(X(\mathbb{C}), \mathbb{Z}/p\mathbb{Z}).$$

Similarly, for our curve X over K , one can define $H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p\mathbb{Z})$ as the $\mathbb{Z}/p\mathbb{Z}$ -dual of the étale cohomology group $H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p\mathbb{Z})$, and then

$$J[p] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p\mathbb{Z})$$

as \mathfrak{G}_K -modules, where $\mathfrak{G}_K := \text{Gal}(\overline{K}/K)$. Likewise, for $n \geq 1$ one has

$$J[p^n] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p^n\mathbb{Z}).$$

Take inverse limits to define the \mathbb{Z}_p and \mathbb{Q}_p Tate modules

$$\begin{aligned} T &:= \varprojlim_n J[p^n] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \\ V &:= T \left[\frac{1}{p} \right] = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \end{aligned}$$

in terms of X . We have $\dim_{\mathbb{Q}_p} V = 2g$.

Finally, let us associate to V an algebraic group \mathcal{V} . Over any field F , the additive group variety \mathbb{G}_a , defined as $\mathbb{A}_F^1 := \text{Spec } F[t]$ equipped with the group law given by addition, is such that $\mathbb{G}_a(F) = F$. More generally, any finite-dimensional F -vector space W can be viewed as $\mathcal{W}(F)$ for a canonically-associated group variety \mathcal{W} isomorphic to a power of \mathbb{G}_a . In particular, V is $\mathcal{V}(\mathbb{Q}_p)$ for some \mathcal{V} isomorphic to \mathbb{G}_a^{2g} .

2.5. Selmer groups. Taking cohomology of the Kummer sequence

$$0 \longrightarrow J[p] \longrightarrow J \xrightarrow{p} J \longrightarrow 0$$

yields an injection

$$\frac{J(K)}{pJ(K)} \hookrightarrow H^1(K, J[p]).$$

(Note: Before we were using étale cohomology of a variety, but now we are using Galois cohomology.) The \mathbb{F}_p -vector space $H^1(K, J[p])$ is infinite-dimensional if $\dim J > 0$, but $J(K)/pJ(K)$ injects into a finite-dimensional subspace $\text{Sel}_p J$ defined as the set of classes that are “locally in the image”; more precisely, if α and β are the homomorphisms in the

diagram

$$\begin{array}{ccc} \frac{J(K)}{pJ(K)} & \hookrightarrow & H^1(K, J[p]) \\ \downarrow & & \beta \downarrow \\ \prod_v \frac{J(K_v)}{pJ(K_v)} & \xhookrightarrow{\alpha} & \prod_v H^1(K_v, J[p]), \end{array}$$

then $\text{Sel}_p J := \beta^{-1}(\text{im } \alpha)$.

A similar square with p^n in place of p yields

$$\frac{J(K)}{p^n J(K)} \hookrightarrow \text{Sel}_{p^n} J \subset H^1(K, J[p^n]).$$

The inverse limit of these square diagrams yields

$$\widehat{J(K)} \hookrightarrow \text{Sel}_{\mathbb{Z}_p} J \subset H^1(K, T),$$

and inverting p yields

$$\widehat{J(K)} \left[\frac{1}{p} \right] \hookrightarrow \text{Sel}_{\mathbb{Q}_p} J \subset H^1(K, V).$$

Let III be the Shafarevich–Tate group of J . The standard exact sequence

$$0 \longrightarrow \frac{J(K)}{pJ(K)} \longrightarrow \text{Sel}_p J \longrightarrow \text{III}[p] \longrightarrow 0$$

and its analogue for p^n lead to the exact sequence

$$0 \longrightarrow \widehat{J(K)} \left[\frac{1}{p} \right] \longrightarrow \text{Sel}_{\mathbb{Q}_p} J \longrightarrow (\varprojlim \text{III}[p^n]) \left[\frac{1}{p} \right] \longrightarrow 0.$$

If $\text{III}[p^\infty]$ is finite, as is conjectured, then $\varprojlim \text{III}[p^n] = 0$, so $\widehat{J(K)} \left[\frac{1}{p} \right] \simeq \text{Sel}_{\mathbb{Q}_p} J$.

We have now explained all of (2) except for the green terms and homomorphisms involving them.

2.6. The Bloch–Kato Selmer group. Let V be a local Galois representation: more precisely, a finite-dimensional \mathbb{Q}_p -vector space with a continuous action of a local Galois group \mathfrak{G}_{K_v} . Fontaine defined $D_{\text{cris}}(V) := (B_{\text{cris}} \otimes_{\mathbb{Q}_p} V)^{\mathfrak{G}_{K_v}}$ for a certain ring B_{cris} equipped with a \mathfrak{G}_{K_v} -action; see [BC09] for an extended exposition. Then $\dim_{K_v} D_{\text{cris}}(V) \leq \dim_{\mathbb{Q}_p} V$, and V is called **crystalline** if equality holds. The notion of crystalline can be extended to cohomology classes $\xi \in H^1(K_v, V)$: namely, ξ corresponds to an isomorphism class of extensions $0 \rightarrow V \rightarrow E \rightarrow \mathbb{Q}_p \rightarrow 0$, and ξ is called **crystalline** if the Galois representation E is. Let $H_f^1(K_v, V)$ be the set of crystalline classes in $H^1(K_v, V)$.

Now let V be a global Galois representation: a finite-dimensional \mathbb{Q}_p -vector space with a continuous action of a global Galois group \mathfrak{G}_K . Given $\xi \in H^1(K, V)$, let ξ_v be its

image in $H^1(K_v, V)$. Finally, the Bloch–Kato Selmer group $H_f^1(K, V)$ is $\{\xi \in H^1(K, V) : \xi_v \text{ is crystalline for every } v|p\}$.

Bloch and Kato proved that $H_f^1(K, V)$ coincides with $\text{Sel}_{\mathbb{Q}_p} J$ in $H^1(K, V)$, and hence gives a Jacobian-free way to define the Selmer group. They also proved that the image of the injection $\widehat{J(K_p)} \left[\frac{1}{p} \right] \rightarrow H^1(K_p, V)$ equals $H_f^1(K_p, V)$.

Let $H_{\text{dR}}^1(X_{K_p})$ be the (algebraic) de Rham cohomology group; it is a finite-dimensional K_p -vector space equipped with a descending chain Fil^\bullet of subspaces called the Hodge filtration. Define the de Rham homology group $H_1^{\text{dR}}(X_{K_p})$ as the dual vector space with the dual filtration. Bloch and Kato showed that the \mathbb{Q}_p -linear isomorphism $\widehat{J(K_p)} \left[\frac{1}{p} \right] \rightarrow \text{Lie } J_{K_p}$ induced by \log is isomorphic to a \mathbb{Q}_p -linear isomorphism $H_f^1(K_p, V) \rightarrow H_1^{\text{dR}}(X_{K_p}) / \text{Fil}^0$ that can be defined without reference to J .

This completes the explanation of the diagram (2).

2.7. Conclusion. The upshot is that we obtain a diagram

$$(3) \quad \begin{array}{ccc} X(K) & \longrightarrow & X(K_p) \\ \downarrow & & \downarrow \\ H_f^1(K, V) & \longrightarrow & H_f^1(K_p, V) \xrightarrow{\cong} H_1^{\text{dR}}(X_{K_p}) / \text{Fil}^0 \end{array}$$

p-adic integrals

that contains the same information as Chabauty’s diagram (1) (at least if $\text{III}[p^\infty]$ is finite) and that is expressed purely in terms of X and its homology group V .

3. KIM’S NONABELIAN GENERALIZATION OF CHABAUTY’S METHOD

3.1. Lower central series. Let G be a group (resp., topological group). For subgroups $A, B \subset G$, let (A, B) denote (the closure of) the subgroup generated by the elements $aba^{-1}b^{-1}$ for $a \in A$ and $b \in B$.

Define $C^1G := G$ and $C^nG := (G, C^{n-1}G)$ for $n \geq 2$, where Then (C^nG) is a descending chain of normal subgroups of G called the lower central series of G . Define the quotient $G_n = G/C^{n+1}G$. For example, $G_1 = G/C^2G = G/(G, G)$ is the abelianization G^{ab} of G . For $n \geq 2$, the group G_n is an n -step nilpotent group that is typically nonabelian.

3.2. The abelianized fundamental group. A connected real manifold M equipped with a basepoint m has a fundamental group $\pi_1(M, m)$ and homology group $H_1(M, \mathbb{Z})$, which are canonically related as follows: $\pi_1(M, m)^{\text{ab}} \simeq H_1(M, \mathbb{Z})$.

Now let us return to our genus g curve X over K , and assume that X is equipped with a K -point x . Then one can define the geometric étale fundamental group $\pi_1^{\text{et}}(X_{\overline{K}}, x)$, a profinite group such that $\pi_1^{\text{et}}(X_{\overline{K}}, x)^{\text{ab}} \simeq H_1^{\text{et}}(X_{\overline{K}}, \widehat{\mathbb{Z}})$. Then

$$(4) \quad \pi_1^{\text{et}}(X_{\overline{K}}, x)_1 = \pi_1^{\text{et}}(X_{\overline{K}}, x)^{\text{ab}} \simeq H_1^{\text{et}}(X_{\overline{K}}, \widehat{\mathbb{Z}}) \twoheadrightarrow H_1^{\text{et}}(X_{\overline{K}}, \mathbb{Z}_p) \subseteq H_1^{\text{et}}(X_{\overline{K}}, \mathbb{Q}_p) =: V = \mathcal{V}(\mathbb{Q}_p),$$

6

and \mathfrak{G}_K acts continuously on all these groups; in particular, it acts via \mathbb{Q}_p -linear automorphisms on $\mathcal{V} \simeq \mathbb{G}_a^{2g}$.

3.3. Deeper quotients of the fundamental group. For $n \geq 2$, there is a construction analogous to that embodied in (4) that maps $\pi_1^{\text{et}}(X_{\overline{K}}, x)_n$ to a topological group V_n that is the group of \mathbb{Q}_p -points of a unipotent algebraic group \mathcal{V}_n over \mathbb{Q}_p equipped with a \mathfrak{G}_K -action.

Kim generalized (3) to a diagram

$$(5) \quad \begin{array}{ccc} X(K) & \longrightarrow & X(K_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ H_f^1(K, V_n) & \longrightarrow & H_f^1(K_{\mathfrak{p}}, V_n) \xrightarrow{\simeq} \pi_1^{\text{dR}}(X_{K_{\mathfrak{p}}}, x)_n / \text{Fil}^0 \end{array}$$

p-adic iterated integrals

and interpreted the bottom row as being the maps on \mathbb{Q}_p -points for morphisms of \mathbb{Q}_p -varieties $\text{Sel}^{[n]} \rightarrow J^{[n]} \xrightarrow{\sim} L^{[n]}$ (not group varieties for $n > 1$). For example, $\text{Sel}^{[1]} \rightarrow J^{[1]}$ is simply a linear morphism between affine spaces over \mathbb{Q}_p .

Finally, $X(K_{\mathfrak{p}}) \rightarrow \pi_1^{\text{dR}}(X_{K_{\mathfrak{p}}}, x)_n / \text{Fil}^0$ is an analytic map whose image turns out to be Zariski dense in $L^{[n]}$; this implies the following generalization of Chabauty's theorem:

Theorem 3.1 (Kim). *If for some $n \geq 1$ we have*

$$\dim \text{Sel}^{[n]} < \dim J^{[n]},$$

then $X(K)$ is contained in the set of zeros of some nonzero locally analytic function on $X(K_{\mathfrak{p}})$, so $X(K)$ is finite.

Various conjectures would imply that $\dim \text{Sel}^{[n]} < \dim J^{[n]}$ holds for sufficiently large n , but this is not yet known in general.

This ends our introduction to Kim's nonabelian Chabauty method.

4. FALTINGS'S FINITENESS THEOREM FOR GALOIS REPRESENTATIONS

We now begin assembling the ingredients needed for the method of Lawrence and Venkatesh.

Let K be a number field. Fix an algebraic closure \overline{K} of K , and let $\mathfrak{G}_K := \text{Gal}(\overline{K}/K)$. Let S be a finite set of places of K containing all archimedean places.

Theorem 4.1 (Hermite [Ser97, §4.1]). *Fix a number field K , a finite set of places S of K , and a positive integer d . Then the set of isomorphism classes of degree d field extensions of K unramified outside S is finite.*

For each nonarchimedean place v of K , let $\text{Frob}_v \in \mathfrak{G}_K$ be a Frobenius automorphism, and let $I_v \subseteq \mathfrak{G}_K$ be the inertia subgroup associated to an extension of v to \overline{K} . Call a homomorphism h from \mathfrak{G}_K to a group G **unramified outside S** if $h(I_v) = 1$ for all $v \notin S$.

Lemma 4.2 (Weak Chebotarev). *Given a number field K and a finite set of places S of K , for any discrete finite group G and continuous homomorphism $h: \mathfrak{G}_K \rightarrow G$ unramified outside S , there exists a finite set T of primes of K disjoint from S such that $\{\text{Frob}_v : v \in T\}$ has the same image under h as the whole group \mathfrak{G}_K .*

Proof. Factor h as $\mathfrak{G}_K \twoheadrightarrow \text{Gal}(L/K) \hookrightarrow G$, and apply the Chebotarev density theorem to the finite Galois extension $L \supseteq K$. \square

Lemma 4.3 (Uniform weak Chebotarev). *Given a number field K , a finite set S of places of K , and a positive integer n , there exists a finite set T of primes of K disjoint from S such that for any discrete group G of order $\leq n$ and any continuous homomorphism $h: \mathfrak{G}_K \rightarrow G$ unramified outside S , the subset $\{\text{Frob}_v : v \in T\}$ has the same image under h as the whole group \mathfrak{G}_K .*

Proof. By Theorem 4.1, there are only finitely many possible h up to isomorphism, say $h_i: \mathfrak{G}_K \rightarrow G_i$. Let T be as in Lemma 4.2 for the product $\prod h_i: \mathfrak{G}_K \rightarrow \prod G_i$. \square

A \mathbb{Z}_ℓ -lattice is a finite-dimensional \mathbb{Q}_ℓ -vector space V is a finitely generated (hence free) \mathbb{Z}_ℓ -submodule L such that $\mathbb{Q}_\ell L = V$.

Lemma 4.4. *Let \mathfrak{G} be a compact topological group (e.g., any Galois group). Any finite dimensional \mathbb{Q}_ℓ -representation V of \mathfrak{G} contains a \mathfrak{G} -stable \mathbb{Z}_ℓ -lattice.*

Proof. Let L_0 be any \mathbb{Z}_ℓ -lattice in V . Let L be the \mathbb{Z}_ℓ -span of the lattices gL_0 for all $g \in \mathfrak{G}$, so L is \mathfrak{G} -stable and $\mathbb{Q}_\ell L = V$.

The image of the compact space $\mathfrak{G} \times L_0$ under the action map $\mathfrak{G} \times V \rightarrow V$ is compact, hence contained in a finitely generated \mathbb{Z}_ℓ -submodule M of V . By construction, $L \subseteq M$, so L is finitely generated too. \square

Lemma 4.5. *Given a number field K , a finite set of places S of K , a rational prime ℓ , and a nonnegative integer d , there exists a finite set of primes T of K disjoint from S such that if ρ and ρ' are d -dimensional \mathbb{Q}_ℓ -representations of \mathfrak{G}_K unramified outside S and $\text{tr } \rho(\text{Frob}_v) = \text{tr } \rho'(\text{Frob}_v)$ for all $v \in T$, then $\text{tr } \rho(g) = \text{tr } \rho'(g)$ for all $g \in \mathfrak{G}_K$.*

Proof. Let T be as in Lemma 4.3 with $n := \ell^{2d^2}$. Suppose that ρ and ρ' are d -dimensional \mathbb{Q}_ℓ -representations of \mathfrak{G}_K unramified outside S such that $\text{tr } \rho(\text{Frob}_v) = \text{tr } \rho'(\text{Frob}_v)$ for all $v \in T$.

By Lemma 4.4, we may assume that ρ and ρ' take values in $\text{GL}_d(\mathbb{Z}_\ell)$. Let $R \subseteq \text{M}_d(\mathbb{Z}_\ell) \times \text{M}_d(\mathbb{Z}_\ell)$ be the \mathbb{Z}_ℓ -module spanned by $\{(\rho(g), \rho'(g)) : g \in \mathfrak{G}_K\}$; in fact, R is a \mathbb{Z}_ℓ -subalgebra. Let h be the composition

$$\mathfrak{G}_K \longrightarrow R^\times \longrightarrow (R/\ell R)^\times,$$

and for each $v \in T$, let $r_v \in R^\times$ and $r_{v,\ell} \in (R/\ell R)^\times$ denote the images of Frob_v :

$$\text{Frob}_v \longmapsto r_v \longmapsto r_{v,\ell}.$$

- (i) We have $\#(R/\ell R)^\times \leq n$. (Proof: As a \mathbb{Z}_ℓ -module, $M_d(\mathbb{Z}_\ell) \times M_d(\mathbb{Z}_\ell)$ is free of rank $2d^2$, so R is free of rank $\leq 2d^2$, so $\#(R/\ell R)^\times \leq \#(R/\ell R) \leq \ell^{2d^2} = n$.)
- (ii) The homomorphism h is unramified outside S . (Proof: $(\rho, \rho') : \mathfrak{G}_K \rightarrow R^\times$ is unramified outside S .)
- (iii) The set $\{r_{v,\ell} : v \in T\}$ equals $h(\mathfrak{G}_K)$, which spans $R/\ell R$ as an \mathbb{F}_ℓ -vector space. (Proof: By (i) and (ii), the T in Lemma 4.3 is such that $\{r_{v,\ell} : v \in T\} = h(\mathfrak{G}_K)$. The image of $\mathfrak{G}_K \rightarrow R^\times$ spans R as a \mathbb{Z}_ℓ -module by construction, so the image $h(\mathfrak{G}_K)$ of $\mathfrak{G}_K \rightarrow (R/\ell R)^\times$ spans $R/\ell R$ as an \mathbb{F}_ℓ -vector space.)
- (iv) The set $\{r_v : v \in T\}$ spans R as a \mathbb{Z}_ℓ -module. (Proof: Combine (iii) with Nakayama's lemma.)

By hypothesis on ρ and ρ' , each r_v has the property that its two projections in $M_d(\mathbb{Z}_\ell)$ have the same trace. Since the r_v span R , every element of R has this property. In particular, if $g \in \mathfrak{G}_K$, then $(\rho(g), \rho'(g))$ has the property; i.e., $\text{tr } \rho(g) = \text{tr } \rho'(g)$. \square

Corollary 4.6. *In the setting of Lemma 4.5, if in addition ρ and ρ' are semisimple, then $\rho \simeq \rho'$.*

Proof. Over a characteristic 0 field, such as \mathbb{Q}_ℓ , a semisimple representation is determined by its trace. \square

Let ρ be a \mathbb{Q}_ℓ -representation of \mathfrak{G}_K unramified outside S . Call ρ **pure of weight i** if for every $v \notin S$, every eigenvalue of $\rho(\text{Frob}_v)$ is an algebraic integer all of whose conjugates have complex absolute value $q_v^{i/2}$, where q_v is the size of the residue field at v .

Theorem 4.7 (Faltings). *Fix a number field K , a finite set S of places of K , a rational prime ℓ , a nonnegative integer d , and an integer i . Then the set of equivalence classes of semisimple d -dimensional \mathbb{Q}_ℓ -representations ρ of \mathfrak{G}_K that are unramified outside S and pure of weight i is finite.*

Proof. Let T be as in Lemma 4.5. If ρ is pure of weight i and $v \notin S$, then there are only finitely many possibilities for the eigenvalues of $\rho(\text{Frob}_v)$, so there is a finite set $Z_v \subseteq \mathbb{Q}_\ell$ that contains all possibilities for $\text{tr } \rho(\text{Frob}_v)$. By Corollary 4.6, $\rho \mapsto (\text{tr } \rho(\text{Frob}_v))_{v \in T}$ defines an injection from the set of classes of representations in question to the finite set $\prod_{v \in T} Z_v$. \square

5. COHOMOLOGY THEORIES

Let K be any field. Let X be a smooth proper variety over K . Let i be a nonnegative integer.

5.1. Betti cohomology. If $K = \mathbb{C}$, one has the **Betti cohomology group** (also called **singular cohomology group**) $H_B^i(X(\mathbb{C}), \mathbb{Z})$. It is a finitely generated \mathbb{Z} -module.

5.2. Étale cohomology. Choose a prime $\ell \neq \text{char } K$. After base changing X to \overline{K} (to have a geometric object more analogous to a variety over \mathbb{C}), one forms the **étale cohomology group** (also called ℓ -adic cohomology group) $H_{\text{ét}}^i(X_{\overline{K}}, \mathbb{Z}_{\ell})$. It is a finitely generated \mathbb{Z}_{ℓ} -module equipped with a continuous \mathfrak{G}_K -action.

5.3. De Rham cohomology. Define $H_{\text{dR}}^i(X) := \mathbb{H}^i(X, \Omega^{\bullet})$ (hypercohomology of the algebraic de Rham complex). This is a finite-dimensional K -vector space equipped with a descending filtration

$$\text{Fil}^0 H_{\text{dR}}^i(X) \supseteq \text{Fil}^1 H_{\text{dR}}^i(X) \supseteq \text{Fil}^2 H_{\text{dR}}^i(X) \supseteq \dots$$

of subspaces called the **Hodge filtration**. We have $\text{Fil}^0 H_{\text{dR}}^i(X) = H_{\text{dR}}^i(X)$, and $\text{Fil}^p H_{\text{dR}}^i(X) = 0$ if p is sufficiently large.

5.4. Crystalline cohomology. Suppose that K is a perfect field of characteristic p . Let $W := W(K)$ be the ring of Witt vectors, which is the unique complete discrete valuation ring with residue field K and maximal ideal (p) . There is a **Frobenius automorphism** $F: W \rightarrow W$, but it is not the p th power map. For example, if $K = \mathbb{F}_{p^n}$, and L_n is the degree n unramified extension of \mathbb{Q}_p , and σ is the automorphism in $\text{Gal}(L_n/\mathbb{Q}_p)$ inducing the p th power map on the residue field \mathbb{F}_{p^n} , then W is the valuation ring of L_n and $F = \sigma|_W$. A **semilinear operator** ϕ on a W -module H is a homomorphism of abelian groups $\phi: H \rightarrow H$ such that $\phi(av) = F(a)\phi(v)$ for all $a \in W$ and $v \in H$. (Linear would mean $\phi(av) = a\phi(v)$ instead.)

Sheaf cohomology on the crystalline site lets one define $H_{\text{cris}}^i(X/W)$. This is a finitely generated W -module equipped with a semilinear operator ϕ called **Frobenius** (because it is induced by the absolute Frobenius morphism of X).

6. COMPARISONS

Remark 6.1 (Changing the coefficient ring). If a cohomology theory $H_{\bullet}^i(X, R)$ above produces an R -module, and R' is a flat R -algebra (e.g., a field extension of $\text{Frac } R$), then it is reasonable to define $H_{\bullet}^i(X, R')$ as $R' \otimes_R H_{\bullet}^i(X, R)$ if it is not already defined directly.

6.1. Étale and Betti. If $K = \mathbb{C}$, then $H_{\text{ét}}^i(X, \mathbb{Z}_{\ell}) \simeq H_B^i(X(\mathbb{C}), \mathbb{Z}_{\ell})$. (As explained above, $H_B^i(X(\mathbb{C}), \mathbb{Z}_{\ell}) = \mathbb{Z}_{\ell} \otimes H_B^i(X(\mathbb{C}), \mathbb{Z})$.)

6.2. De Rham and Betti. If $K = \mathbb{C}$, then integration of differential forms defines an isomorphism $H_{\text{dR}}^i(X) \xrightarrow{\sim} H_B^i(X(\mathbb{C}), \mathbb{C})$.

6.3. Étale, de Rham, and crystalline. Let K be a finite unramified extension of \mathbb{Q}_p . Let \mathcal{O} be its valuation ring. Let k be its residue field. Thus k is a finite field, and $\mathcal{O} \simeq W(k)$.

A filtered ϕ -module over K is a triple $(D, \phi, \text{Fil}^\bullet)$, consisting of a finite-dimensional K -vector space D , a semilinear map $\phi: D \rightarrow D$ and a descending filtration Fil^\bullet of subspaces of D indexed by integers such that $\text{Fil}^i = D$ for $i \ll 0$ and $\text{Fil}^i = 0$ for $i \gg 0$.

Let $\text{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ be the category of finite-dimensional \mathbb{Q}_p -vector spaces equipped with a continuous \mathfrak{G}_K -action. Let MF_K^ϕ denote the category of filtered ϕ -modules. Then there exists a functor

$$\begin{aligned} D_{\text{cris}}: \text{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K) &\rightarrow \text{MF}_K^\phi \\ V &\mapsto (B_{\text{cris}} \otimes_{\mathbb{Q}_p} V)^{\mathfrak{G}_K}. \end{aligned}$$

(This is the same functor as in Section 2.6, although there we were not concerned with the semilinear operator and filtration on the output.) Recall that $\dim_K D_{\text{cris}}(V) \leq \dim_{\mathbb{Q}_p} V$, and that V is called crystalline if equality holds. Let $\text{Rep}_{\mathbb{Q}_p}^{\text{cris}}(\mathfrak{G}_K) \subseteq \text{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ denote the full subcategory of crystalline representations.

Theorem 6.2.

- (a) *The functor D_{cris} restricts to a fully faithful functor $\text{Rep}_{\mathbb{Q}_p}^{\text{cris}}(\mathfrak{G}_K) \hookrightarrow \text{MF}_K^\phi$.*
- (b) *If X is a smooth proper \mathcal{O} -scheme, then*
 - (i) *The representation $H_{\text{et}}^i(X_{\bar{K}}, \mathbb{Q}_p)$ is crystalline.*
 - (ii) *There is a canonical isomorphism $H_{\text{dR}}^i(X_K) \simeq H_{\text{cris}}^i(X_k/K)$ of K -vector spaces, making either vector space into a filtered ϕ -module (the filtration is the Hodge filtration on $H_{\text{dR}}^i(X_K)$, and the ϕ is the Frobenius on $H_{\text{cris}}^i(X_k/K)$).*
 - (iii) *The functor D_{cris} maps $H_{\text{et}}^i(X_{\bar{K}}, \mathbb{Q}_p)$ to $H_{\text{dR}}^i(X_K) \simeq H_{\text{cris}}^i(X_k/K)$.*

7. COHOMOLOGY IN A FAMILY; PERIOD MAPS

Let B be a smooth variety over a field K . Let $f: X \rightarrow B$ be a smooth proper morphism. For each $b \in B$, the fiber $X_b := f^{-1}(b)$ is a smooth proper variety (over the residue field of b).

In the following table, each entry in the first column refers to a single variety Z , and each entry in the second column is the analogue for a family $f: X \rightarrow B$.

$\Gamma(Z, -)$	f_*
$H^i(Z, -)$	$R^i f_*$
$\mathbb{H}^i(Z, -)$	$\mathbb{R}^i f_*$
$H_{\text{dR}}^i(Z)$	$\mathbb{R}^i f_* \Omega_{X/B}^\bullet$

The relative de Rham cohomology $\mathbb{R}^i f_* \Omega_{X/B}^\bullet$ is a vector bundle on B whose fiber above each point b is the de Rham cohomology group $H_{\text{dR}}^i(X_b)$.

7.1. Complex setting. Let $K = \mathbb{C}$. Let $\Omega \subset B(\mathbb{C})$ be a simply connected open subset. Normally, given a vector bundle on B , there is no canonical way to identify the nearby fibers (fibers above points of Ω). But for $\mathbb{R}^i f_* \Omega_{X/B}^\bullet$ there is a way, which admits two descriptions:

7.1.1. *Description 1.* Ehresmann's theorem says that $f^{-1}\Omega \rightarrow \Omega$ viewed as a map of C^∞ manifolds is diffeomorphic to a constant family $X_0 \times \Omega \rightarrow \Omega$, so the spaces $H_B^i(X_b(\mathbb{C}), \mathbb{C})$ for $b \in \Omega$ are canonically identified — the fancy way to say this is to say that $Rf_* \underline{\mathbb{C}}$ is a local system of \mathbb{C} -vector spaces on B . By comparison, it follows that $H_{dR}^i(X_b)$ for $b \in \Omega$ are canonically identified as vector spaces (without filtration).

7.1.2. *Description 2.* The operator d on differential forms induces a rule for taking directional derivatives of sections of $\mathbb{R}^i f_* \Omega_{X/B}^\bullet$. The fancy way to say this is to say that the vector bundle $\mathbb{R}^i f_* \Omega_{X/B}^\bullet$ comes equipped with a connection ∇ , called the **Gauss–Manin connection** — this connection is algebraic, defined over K ; it is also integrable (i.e., flat): see [KO68]. A section s of $\mathbb{R}^i f_* \Omega_{X/B}^\bullet$ is called **horizontal** if $\nabla s = 0$. If a local basis of the vector bundle is chosen, then $\nabla s = 0$ amounts to a system of linear differential equations whose coefficients are algebraic functions on B ; because the connection is integrable, there exists a basis of *analytic* solutions on Ω . Fibers above points of Ω can be identified by following these horizontal sections.

7.1.3. *Equality of descriptions.* It turns out that the two descriptions give the *same* identification of fibers.

7.1.4. *Period map.* As hinted above, the identification does not respect the fiberwise Hodge filtrations Fil^\bullet . To measure the variation of the Hodge filtration, fix a point $0 \in \Omega$, let \mathcal{F} be the **flag variety** parametrizing chains of subspaces in $H_{dR}^i(X_0)$ of dimensions agreeing with the spaces in $\text{Fil}^\bullet H_{dR}^i(X_0)$, and define the **complex period map**

$$\begin{aligned} \Omega &\xrightarrow{\text{Period}_\mathbb{C}} \mathcal{F}(\mathbb{C}) \\ b &\longmapsto (\text{Fil}^\bullet H_{dR}^i(X_b) \text{ transported to } H_{dR}^i(X_0)). \end{aligned}$$

This is an analytic map.

Remark 7.1. If $X \rightarrow B$ is defined over a subfield of $K \subseteq \mathbb{C}$ and $0 \in B(K)$, then \mathcal{F} is a K -variety and $\text{Period}_\mathbb{C}$ near 0 is given by power series with coefficients in K , because ∇ is defined over K .

7.2. p -adic setting. Let K_v be a finite unramified extension of \mathbb{Q}_p . Let \mathcal{O}_v be its valuation ring. Let k_v be its residue field. Let B be a smooth scheme over \mathcal{O}_v . Let $\bar{0} \in B(k_v)$. Let $\Omega_v = \{b \in B(\mathcal{O}_v) \text{ reducing to } \bar{0}\}$. Fix $0 \in \Omega_v$. Again we have a canonical identification of the fibers of $\mathbb{R}^i f_* \Omega_{X/B}^\bullet$ above K -points in Ω_v , as we now explain.

7.2.1. *Description 1.* The K_v -vector spaces $H_{dR}^i(X_b)$ for $b \in \Omega_v$ are canonically identified since they are all canonically isomorphic to $H_{\text{cris}}^i(X_{\bar{0}}/K_v)$.

7.2.2. *Description 2.* Use p -adic analytic solutions to $\nabla s = 0$.

7.2.3. *Equality of descriptions.* Again it turns out that the two descriptions give the *same* identification of fibers.

7.2.4. *Period map.* Define the p -adic period map

$$\begin{aligned} \Omega_v &\xrightarrow{\text{Period}_v} \mathcal{F}(K_v) \\ b &\longmapsto (\text{Fil}^\bullet H_{\text{dR}}^i(X_b) \text{ transported to } H_{\text{dR}}^i(X_0)). \end{aligned}$$

This is a p -adic analytic map.

7.3. Comparison. If $X \rightarrow B$ is over a ring of S -integers $\mathcal{O}_{K,S}$ in a number field K , then $\text{Period}_{\mathbb{C}}$ and Period_v both come from the formal solutions to $\nabla s = 0$, so they are given by the same power series with coefficients in K . It follows that the Zariski closures $(\text{im } \text{Period}_{\mathbb{C}})^{\text{Zar}}$ and $(\text{im } \text{Period}_v)^{\text{Zar}}$ in \mathcal{F} are equal.

8. RATIONAL/INTEGRAL POINTS AND PERIOD MAPS

8.1. General setup. Let K be a number field. Let S be a finite set of places of K containing all archimedean places and all ramified places. Let $\mathcal{O} := \mathcal{O}_{K,S}$, the ring of S -integers in K . Let $v \notin S$. Let K_v be the completion of K at v . Let \mathcal{O}_v be the valuation ring in K_v . Let k_v be the residue field of \mathcal{O}_v . Let Y be a smooth separated finite-type \mathcal{O} -scheme such that Y_K is a smooth geometrically integral curve that is **hyperbolic**, meaning that $\chi(Y_K) < 0$ (if $Y_{\overline{K}}$ is expressed as a smooth projective curve of genus g minus r points, then $\chi(Y_K) := 2 - 2g - r$).

The goal is to prove that $Y(\mathcal{O})$ is finite. It suffices to consider one residue disk in $Y(\mathcal{O}_v)$ at a time, so without loss of generality, remove all but one k_v -point from Y ; now $Y(\mathcal{O}_v)$ is a single residue disk. Assume that $y_0 \in Y(\mathcal{O})$.

8.2. Rough strategy.

1. Choose a smooth proper family $f: X \rightarrow Y$ and a nonnegative integer i .
2. For each $y \in Y(\mathcal{O})$, we get $V_y := H_{\text{et}}^i((X_y)_{\overline{K}}, \mathbb{Q}_p) \in \text{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K)$.
3. Use Faltings's finiteness theorem for semisimple Galois representations to prove that there are only finitely many possibilities for the isomorphic type of V_y . (One challenge here is that we do not know a priori that the V_y are semisimple.)
4. Prove that V_y varies enough with y (even when restricted to a representation of \mathfrak{G}_{K_v}) that each isomorphism type arises from only finitely many y .

8.3. Additional notation. Let $V := H_{\text{dR}}^i((X_{y_0})_{K_v})$; this is a finite-dimensional K_v -vector space, and it has a Frobenius operator ϕ and Hodge filtration Fil^\bullet . Let $d := \dim_{K_v} V$, which also equals $\dim_{\mathbb{Q}_p} V_y$ for any $y \in Y(\mathcal{O}_v)$.

Let $Y(\mathcal{O})^{\text{ss}} := \{y \in Y(\mathcal{O}) : V_y \text{ is semisimple}\}$.

Let $\text{Rep}_{\mathbb{Q}_p}^{\text{cris at } v}(\mathfrak{G}_K)$ be the category of \mathbb{Q}_p -representations of \mathfrak{G}_K that are crystalline at v (i.e., the restriction to \mathfrak{G}_{K_v} is crystalline). Let $\text{Rep}_{\mathbb{Q}_p}^{\text{Faltings}}(\mathfrak{G}_K)$ be the category of semisimple d -dimensional \mathbb{Q}_p -representations of \mathfrak{G}_K that are unramified and pure of weight i outside S and crystalline at v .

Let $\text{MF}_{K_v}^{\phi, \text{framed}}$ be the category of tuples $(D, \varphi, \text{Fil}^\bullet, \iota)$ where $(D, \varphi, \text{Fil}^\bullet) \in \text{MF}_{K_v}^\phi$ and the “framing” $\iota: (D, \varphi) \xrightarrow{\sim} (V, \phi)$ is a K_v -linear isomorphism $D \rightarrow V$ under which φ and ϕ correspond.

8.4. The big diagram. One should interpret each category in the following commutative diagram as its set of isomorphism classes.

(6)

$$\begin{array}{ccccccc}
 Y(\mathcal{O})^{\text{ss}} & \hookrightarrow & Y(\mathcal{O})^c & \longrightarrow & Y(\mathcal{O}_v) & \xrightarrow{\text{Period}_v} & \\
 \downarrow H_{\text{et}}^i & & \downarrow H_{\text{et}}^i & & \downarrow H_{\text{dR}}^i + \text{GM} & & \\
 \text{Rep}_{\mathbb{Q}_p}^{\text{Faltings}}(\mathfrak{G}_K) & \hookrightarrow & \text{Rep}_{\mathbb{Q}_p}^{\text{cris at } v}(\mathfrak{G}_K) & \longrightarrow & \text{Rep}_{\mathbb{Q}_p}^{\text{cris}}(\mathfrak{G}_{K_v}) & \xleftarrow{D_{\text{cris}}} & \text{MF}_{K_v}^\phi \\
 & & & \searrow H_{\text{et}}^i & & \downarrow \text{forget frame} & \\
 & & & & \text{MF}_{K_v}^{\phi, \text{framed}} & \longrightarrow & \mathcal{F}(K_v)
 \end{array}$$

The first two maps labelled H_{et}^i send y to $H_{\text{et}}^i((X_y)_{\overline{K}}, \mathbb{Q}_p)$; the third sends y to $H_{\text{et}}^i((X_y)_{\overline{K}_v}, \mathbb{Q}_p)$. The map $H_{\text{dR}}^i + \text{GM}$ sends y to $(H_{\text{dR}}^i(X_y), \varphi, \text{Fil}^\bullet, \text{GM})$, where φ is the Frobenius operator coming from comparison with $H_{\text{cris}}^i((X_y)_{k_v}/K_v)$, and Fil^\bullet is the Hodge filtration, and GM is the isomorphism $H_{\text{dR}}^i(X_y) \rightarrow V = H_{\text{dR}}^i((X_{y_0})_{K_v})$ coming from the Gauss–Manin connection. The map $\text{MF}_{K_v}^{\phi, \text{framed}} \rightarrow \mathcal{F}(K_v)$ takes $(D, \varphi, \text{Fil}^\bullet, \iota)$ to the filtration $\iota(\text{Fil}^\bullet)$ of V .

Let $\text{Aut}(V, \phi)$ be the set of K_v -linear automorphisms of V that commute with the operator ϕ . Let $\Phi = \phi^{[K_v : \mathbb{Q}_p]}$, so $\text{Aut}(V, \phi) \subseteq \text{Aut}(V, \Phi)$. Then Φ is K_v -linear, so $\text{Aut}(V, \Phi)$ is (the set of K_v -points of) an algebraic subgroup of $\text{GL}(V)$.

The group $\text{Aut}(V, \phi)$ acts on $\text{MF}_{K_v}^{\phi, \text{framed}}$; namely, α maps $(D, \varphi, \text{Fil}^\bullet, \iota)$ to $(D, \varphi, \text{Fil}^\bullet, \alpha\iota)$. The group $\text{GL}(V)$ acts on $\mathcal{F}(K_v)$; namely $g \in \text{GL}(V)$ maps $(\text{Fil}^j)_{j \in \mathbb{Z}}$ to $(g\text{Fil}^j)_{j \in \mathbb{Z}}$. These two actions are compatible with respect to the map $\text{MF}_{K_v}^{\phi, \text{framed}} \rightarrow \mathcal{F}(K_v)$ and inclusion $\text{Aut}(V, \phi) \subseteq \text{GL}(V)$.

Each nonempty fiber of the “forget frame” map is an $\text{Aut}(V, \phi)$ -orbit in $\text{MF}_{K_v}^{\phi, \text{framed}}$, and such an orbit maps into an $\text{Aut}(V, \Phi)$ -orbit in $\mathcal{F}(K_v)$. Thus the diagram shows

Proposition 8.1. *The set $Y(\mathcal{O})^{\text{ss}}$ is mapped by Period_v into finitely many $\text{Aut}(V, \Phi)$ -orbits in $\mathcal{F}(K_v)$.*

Proof. By Theorem 4.7, $\text{Rep}_{\mathbb{Q}_p}^{\text{Faltings}}(\mathfrak{G}_K)$ has only finitely many isomorphism classes. The diagram (6) then shows that the image of $Y(\mathcal{O})^{\text{ss}}$ in $\text{MF}_{K_v}^\phi$ is finite, so the image of $Y(\mathcal{O})^{\text{ss}}$

in $\text{MF}_{K_v}^{\phi, \text{framed}}$ is contained in finitely many $\text{Aut}(V, \phi)$ -orbits, and these map into finitely many $\text{Aut}(V, \Phi)$ -orbits in $\mathcal{F}(K_v)$. \square

Corollary 8.2. *If $\dim_{K_v} \text{Aut}(V, \Phi) < \dim \text{im}(\text{Period}_v)^{\text{Zar}}$, then $Y(\mathcal{O})^{\text{ss}}$ is contained in the set of zeros of some nonzero analytic function on $Y(\mathcal{O}_v)$, and hence is finite.*

8.5. Period maps and the monodromy group. Let $\widetilde{Y(\mathbb{C})}$ be the universal cover of $Y(\mathbb{C})$. Analytically continue $\text{Period}_{\mathbb{C}}: \Omega \rightarrow \mathcal{F}(\mathbb{C})$ to obtain $\widetilde{\text{Period}}_{\mathbb{C}}: \widetilde{Y(\mathbb{C})} \rightarrow \mathcal{F}(\mathbb{C})$. Let $V_{\mathbb{C}} = H_B^i(X_{y_0}(\mathbb{C}), \mathbb{C}) \simeq H_{\text{dR}}^i(X_{y_0, \mathbb{C}})$. If γ is a loop in $Y(\mathbb{C})$ based at y_0 , then following horizontal sections above γ gives a \mathbb{C} -linear identification of $V_{\mathbb{C}}$ with itself, i.e., an element of $\text{GL}(V_{\mathbb{C}})$, and this defines the **monodromy representation** $\pi_1(Y, y_0) \rightarrow \text{GL}(V_{\mathbb{C}})$. The Zariski closure of the image of this representation is called the **monodromy group** Γ . We obtain a commutative diagram

$$\begin{array}{ccc} \pi_1(Y, y_0) & \longrightarrow & \Gamma \subseteq \text{GL}(V_{\mathbb{C}}) \\ \downarrow & & \downarrow \\ \widetilde{Y(\mathbb{C})} & \xrightarrow{\widetilde{\text{Period}}_{\mathbb{C}}} & \mathcal{F}(\mathbb{C}), \end{array}$$

in which the right vertical map sends $g \in \text{GL}(V_{\mathbb{C}})$ to $g(\text{Fil}^\bullet V_{\mathbb{C}})$.

Now

$$\text{im}(\text{Period}_v)^{\text{Zar}} = \text{im}(\text{Period}_{\mathbb{C}})^{\text{Zar}} = \text{im}(\widetilde{\text{Period}}_{\mathbb{C}})^{\text{Zar}} \supseteq (\Gamma \cdot \text{Fil}^\bullet V_{\mathbb{C}})^{\text{Zar}}.$$

Combining this with Corollary 8.2 yields

Corollary 8.3. *If $\dim_{K_v} \text{Aut}(V, \Phi) < \dim (\Gamma \cdot \text{Fil}^\bullet V_{\mathbb{C}})^{\text{Zar}}$, then $Y(\mathcal{O})^{\text{ss}}$ is finite.*

9. THE S -UNIT EQUATION

9.1. Setup. Now we specialize to the case $Y = \mathbb{P}^1 - \{0, 1, \infty\}$, which is isomorphic to the curve $t + u = 1$ in $\mathbb{G}_m \times \mathbb{G}_m$. (More formally, $Y = \text{Spec } \mathcal{O}[t, 1/t, 1/(t-1)]$.) The goal is the following:

Theorem 9.1. *The set $Y(\mathcal{O}) = \{t \in \mathcal{O}^\times : 1-t \in \mathcal{O}^\times\}$ is finite.*

We may assume that $y_0 \in Y(\mathcal{O})$; identify this point with a number $t_0 \in \mathcal{O}^\times$.

9.2. First attempt. Let $X \rightarrow Y$ be the Legendre family of elliptic curves, whose fiber above t is the elliptic curve $E_t: y^2 = x(x-1)(x-t)$ (i.e., the smooth projective model of this affine curve). Let $i = 1$. Then $\dim V = 2$.

9.2.1. Left hand side. On the left of the inequality in Corollary 8.3 is $\dim \text{Aut}(V, \Phi)$, which could be as large as 4 (e.g., if $\Phi = -p$, which could happen if the mod p reduction of E_{t_0} is a supersingular elliptic curve over \mathbb{F}_{p^2}).

9.2.2. *Right hand side.* On the right is $\dim(\Gamma \cdot \text{Fil}^\bullet V_{\mathbb{C}})^{\text{Zar}}$, which is at most 1, since the Zariski closure is taken inside $\mathcal{F} = \{1\text{-dimensional subspaces of } V\} \simeq \mathbb{P}^1$. In fact, the image of the monodromy representation $\pi_1(Y(\mathbb{C}), t_0) \rightarrow \text{GL}(V_{\mathbb{C}}) = \text{GL}_2(\mathbb{C})$ is a finite-index subgroup of $\text{SL}_2(\mathbb{Z})$, so $\Gamma = \text{SL}_2$ and $\dim(\Gamma \cdot \text{Fil}^\bullet V_{\mathbb{C}})^{\text{Zar}} = 1$.

9.2.3. *Conclusion.* The inequality $4 < 1$ does not hold, so we cannot apply Corollary 8.3 to deduce finiteness. We need to start over with a different family $X \rightarrow Y$.

9.3. **Second attempt.** Choose $m \geq 1$, and let $Y' = \mathbb{P}^1 - \{0, \mu_m, \infty\}$ be the inverse image of Y under the m th power map $\mathbb{P}^1 \rightarrow \mathbb{P}^1$. Let z be the coordinate on Y' , so $z^m = t$. Let $X \rightarrow Y'$ be the family whose fiber above $z \in Y'$ is E_z . Thus the fiber X_t of the composition $X \rightarrow Y' \rightarrow Y$ above t is a smooth proper geometrically *disconnected* curve with $(X_t)_{\overline{K}} = \coprod_{z^m=t} E_z$.

The group $\mu_{2^\infty}(K)$ of roots of unity of 2-power order in K is a finite cyclic group. Let m be its order, and let ζ be a generator. Without loss of generality, enlarge K and S (this only makes $Y(\mathcal{O})$ larger) so that $m \geq 8$ and S contains all the places above 2 and ∞ , and all the places ramified in K/\mathbb{Q} .

Let $U := \{t \in Y(\mathcal{O}) : t \notin K^{\times 2}\}$.

Lemma 9.2. *We have $Y(\mathcal{O}) = U \cup U^2 \cup U^4 \cup \dots \cup U^m$.*

Proof. First, if $t, 1-t \in \mathcal{O}^\times$ and $\sqrt{t} \in K$, then $\sqrt{t}, 1-\sqrt{t} \in \mathcal{O}^\times$ too, because $1-t = (1+\sqrt{t})(1-\sqrt{t})$. Let $t \in Y(\mathcal{O})$.

- If $t^{1/m} \notin K$, then repeatedly taking square roots until no longer possible shows that $t \in U \cup U^2 \cup \dots \cup U^{m/2}$.
- If $t^{1/m} \in K$, then $t = (t^{1/m})^m = (\zeta t^{1/m})^m$, and either $t^{1/m}$ or $\zeta t^{1/m}$ is in U (since $\zeta \notin K^{\times 2}$). \square

By Lemma 9.2, it will suffice to prove that U is finite. We may also assume that U is nonempty, so assume $t_0 \in U$.

By Hermite's theorem (Theorem 4.1), there are only finitely many possibilities for the field $K(t^{1/m})$ as t ranges over U . Therefore it will suffice to fix one of them, say L , and prove that the set of $t \in U$ such that $K(t^{1/m}) \simeq L$ is finite. Since $t \notin K^{\times 2}$, the field L is a Kummer extension of K , with $\text{Gal}(L/K) \simeq \mathbb{Z}/m\mathbb{Z}$.

Choose a place $v \notin S$ such that Frob_v is a generator of $\text{Gal}(L/K)$. Then v is inert in L/K , and the completion L_v at the place of L above v is a $\mathbb{Z}/m\mathbb{Z}$ -extension of K_v .

9.3.1. *Left hand side.* Let $V = H_{\text{dR}}^1((X_{t_0})_{K_v})$. Then V is a $2m$ -dimensional K_v -vector space with K_v -linear operator Φ , but $(X_{t_0})_{K_v}$ can also be viewed as an elliptic curve over L_v , so V can also be viewed as a 2 -dimensional L_v -vector space \mathcal{V} with L_v -linear operator Φ^m .

An elementary linear algebra lemma (Lemma 2.1 in [LV18]) shows that $\dim_{K_v} \text{Aut}(V, \Phi) = \dim_{L_v} \text{Aut}(\mathcal{V}, \Phi^m)$, and the latter is at most $\dim_{L_v} \text{GL}_2(L_v) = 4$.

9.3.2. Right hand side. A monodromy calculation (Lemma 4.3 in [LV18]) shows that the image of the monodromy representation contains a finite index subgroup of $\prod_{z^m=t_0} \text{SL}_2(\mathbb{Z}) \subseteq \text{GL}(\bigoplus_{z^m=t_0} H^1(E_z(\mathbb{C}), \mathbb{C}))$, so Γ contains $\prod_{z^m=t_0} \text{SL}_2$. Thus $(\Gamma \cdot \text{Fil}^\bullet V_{\mathbb{C}})^{\text{Zar}} = \prod_{z^m=t_0} \mathbb{P}^1$, so $\dim(\Gamma \cdot \text{Fil}^\bullet V_{\mathbb{C}})^{\text{Zar}} = m \geq 8$.

9.3.3. Conclusion. We have $\dim_{K_v} \text{Aut}(V, \Phi) \leq 4 < 8 \leq m = \dim(\Gamma \cdot \text{Fil}^\bullet V_{\mathbb{C}})^{\text{Zar}}$, so Corollary 8.3 shows that the set $U^{\text{ss}} := U \cap Y(\mathcal{O})^{\text{ss}}$ is finite.

9.3.4. Handling points with non-semisimple representations. It remains to show that the set $U^{\text{non-ss}} := U - U^{\text{ss}}$ is finite. In fact, we will prove that $Y(\mathcal{O})^{\text{non-ss}} := Y(\mathcal{O}) - Y(\mathcal{O})^{\text{ss}}$ is finite.

Recall that an elliptic curve E over a field L is called **non-CM** if $\text{End } E_{\overline{L}} = \mathbb{Z}$.

We use Serre's open image theorem:

Theorem 9.3 ([Ser72, statement (2)]). *If E is a non-CM elliptic curve over a number field L , then the image of $\mathfrak{G}_L \rightarrow \text{Aut } H^1_{\text{et}}(E_{\overline{L}}, \mathbb{Z}_p) \simeq \text{GL}_2(\mathbb{Z}_p)$ is an open subgroup of finite index.*

Corollary 9.4. *Under the hypotheses of Theorem 9.3, the 2-dimensional representation $H^1_{\text{et}}(E_{\overline{L}}, \mathbb{Q}_p) \in \text{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_L)$ is simple.*

Proof. A finite-index subgroup of $\text{GL}_2(\mathbb{Z}_p)$ does not stabilize any 1-dimensional subspace of \mathbb{Q}_p^2 . \square

Corollary 9.5. *Let $t \in Y(\mathcal{O})$. Suppose that for all $z \in \overline{K}$ with $z^m = t$, the elliptic curve E_z is non-CM. Then the representation $V_t \in \text{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ is semisimple.*

Proof. For a representation over a field of characteristic 0, semisimplicity is unaffected by restricting to a finite index subgroup. The restriction of V_t to a representation of $\mathfrak{G}_{K(z)}$ is a direct sum of m simple representations of the type in Corollary 9.4. \square

Corollary 9.6. *The set $Y(\mathcal{O})^{\text{non-ss}}$ is finite.*

Proof. There are only finitely many CM j -invariants of any fixed degree, and the j -invariant of E_z is a rational function of z , so there are only finitely many $z \in \overline{K}$ of degree $\leq m[K : \mathbb{Q}]$ such that E_z has CM, and hence there are only finitely many t that violate the hypothesis of Corollary 9.5. \square

This completes the proof of Theorem 9.1.

Remark 9.7. One can prove Corollary 9.6 without using Serre's open image theorem, by using Hodge–Tate weights: see [LV18, Lemma 4.2]. This is important for the application of the method in other situations where the analogue of Serre's theorem is unknown or false.

10. THE MORDELL CONJECTURE

The proof of the Mordell conjecture in [LV18] follows similar lines, but everything is more complicated, especially the method for handling non-semisimple representations and the computation of the monodromy group.

ACKNOWLEDGMENTS

I thank David Corwin, Olivier Wittenberg, and Zijian Yao for sharing their notes on these subjects. Part of the present exposition is adapted from their presentations. I also thank Zhiyu Zhang for spotting some typos.

REFERENCES

- [BC70] A. Baker and J. Coates, *Integer points on curves of genus 1*, Proc. Cambridge Philos. Soc. **67** (1970), 595–602, DOI 10.1017/s0305004100045904. MR256983 ↑1.2
- [Bom90] Enrico Bombieri, *The Mordell conjecture revisited*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, 615–640. MR1093712 (92a:11072) ↑1.1
- [BC09] Oliver Brinon and Brian Conrad, *CMI Summer School notes on p-adic Hodge theory (preliminary version)*, June 24, 2009. Preprint, <http://math.stanford.edu/~conrad/papers/notes.pdf>. ↑2.6
- [Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French). MR0004484 (3,14d) ↑1.1
- [Cor19] David Corwin, *From Chabauty's method to Kim's non-abelian Chabauty method*, July 4, 2019. Preprint, <https://math.berkeley.edu/~dcorwin/files/ChabautytoKim.pdf>. ↑2.2
- [Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German). English translation: Finiteness theorems for abelian varieties over number fields, 9–27 in *Arithmetic Geometry (Storrs, Conn., 1984)*, Springer, New York, 1986. Erratum in: Invent. Math. **75** (1984), 381. MR718935 (85g:11026a) ↑1.1
- [KO68] Nicholas M. Katz and Tadao Oda, *On the differentiation of de Rham cohomology classes with respect to parameters*, J. Math. Kyoto Univ. **8** (1968), 199–213, DOI 10.1215/kjm/1250524135. MR0237510 ↑7.1.2
- [LV18] Brian Lawrence and Akshay Venkatesh, *Diophantine problems and p-adic period mappings*, August 30, 2018. Preprint, [arXiv:1807.02721v2](https://arxiv.org/abs/1807.02721v2). ↑1.1, 1.2, 1.3, 9.3.1, 9.3.2, 9.7, 10
- [MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit Methods in Number Theory: Rational Points and Diophantine Equations, Panoramas et Synthèses, vol. 36, Société Mathématique de France, Paris, 2012, pp. 99–117. ↑2.1
- [Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Phil. Soc. **21** (1922), 179–192. ↑1.1
- [Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331 (French). MR0387283 (52 #8126) ↑9.3
- [Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. MR1757192 (2000m:11049) ↑4.1

- [Sie29] Carl Ludwig Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuß. Akad. Wissen. Phys.-math. Klasse (1929), 41–69. English translation: *On some applications of diophantine approximations*, edited by Umberto Zannier, Scuola Normale Superiore Pisa, 2014. ↑1.2
- [Sko34] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8. Skand. Mat.-Kongr., Stockholm, 1934, pp. 163–188 (German). ↑1.2
- [Voj91] Paul Vojta, *Siegel's theorem in the compact case*, Ann. of Math. (2) **133** (1991), no. 3, 509–548. MR1109352 (93d:11065) ↑1.1

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139-4307, USA

Email address: poonen@math.mit.edu

URL: <http://math.mit.edu/~poonen/>

2020 ARIZONA WINTER SCHOOL COURSE AND PROJECT OUTLINE: “ABELIAN CHABAUTY”

DAVID ZUREICK-BROWN

1. COURSE OUTLINE

Let X be a “nice”¹ curve over a number field K . This course will discuss the method of Chabauty and Coleman (alternatively, “Abelian Chabauty”), which is a p -adic technique that often allows one to provably compute the (finite, by Faltings’ theorem) set $X(K)$ of K -rational points on X , and which is an essential part of the “explicit approaches to rational points” toolbox.

Abelian Chabauty. We will start with a detailed discussion of the method of Chabauty and Coleman, and will address every point of view (theoretical, practical, computational). We will include some discussion of how abelian Chabauty is a special case of non-abelian Chabauty. Poonen will address some subset of this material in his plenary lecture.

Uniform Bounds. The *uniformity conjecture* is one of the outstanding open conjectures in arithmetic and diophantine geometry, and asserts that, for a number field K , there exists a constant $B(g, K)$ such that every smooth curve X over K of genus $g \geq 2$ has at most $B(g, K)$ many K -rational points. The uniformity conjecture famously follows from the conjecture of Lang–Vojta (the higher dimension analogue of Faltings’ theorem). We will discuss techniques for using p -adic methods to obtain uniform bounds on small rank curves, including Coleman’s “Effective Chabauty” [Col85].

Bad reduction. One avenue to improve on Coleman’s bound is to generalize the Chabauty framework and Coleman’s arguments to the case of bad reduction. We will discuss the advantage of working at bad primes and the difficulties that arise, starting with the work of Lorenzini–Tucker [LT02].

Rank favorable bounds. Stoll [Sto06] was the first to discover “rank favorable” bounds: when the rank is strictly smaller than $g - 1$, there are more “inputs” to Chabauty’s method and one expects this extra flexibility to lead to improvements in the method. The “geometric input” that allows Stoll to convert this intuition into a theorem is the (classical) notion of “rank of a divisor”, and after translating his setup into this language, improved bounds follow from Clifford’s Theorem. I’ll discuss my work with Eric Katz [KZB12] which generalizes Stoll’s theorem to the bad reduction setting, and which exploits recent ideas from tropical geometry (in particular “chip-firing”, the “discrete case” of tropical geometry).

Date: September 16, 2019.

¹i.e., smooth projective geometrically integral

Tropical Geometry. For a curve with bad reduction at a prime p , it had been well understood that “monodromy” and “analytic continuation” of p -adic integrals was an issue. Coleman proved that in the case of good reduction, there is no “monodromy” and the various ways of analytically continuing p -adic integrals all coincide. In the case of bad reduction, they generally do not coincide (we will discuss a simple example which illustrates this).

Stoll [Sto19] discovered that, while choices of analytic continuation genuinely do differ, they do so in a fairly controlled manner (linear, even), and was able to exploit this to prove a uniformity result for *hyperelliptic* curves of small rank.

These results all argue in the framework of rigid geometry (in the sense of Tate). Enter Berkovich spaces, which fill in the “missing” points of rigid spaces and which, at least in the case of curves, are fairly concrete and manageable topological spaces (they’re even Hausdorff). I’ll discuss Chabauty in the setting of Berkovich and tropical geometry and explain how modern tools (e.g., Berkovich’s contraction theorem and Thuillier’s slope formula, expository in [BPR13]) give a clean explanation of Coleman’s “good reduction” theorem, and will discuss my work with Katz and Rabinoff [KRZB] which give uniform bounds for arbitrary (but still small rank) curves.

Background reading. I recommend McCallum and Poonen’s survey [MP12] as a great starting point for the method of Chabauty and Coleman, and my survey with Katz and Rabinoff [KRZB16] for tropical techniques.

2. PROJECTS

- (1) Find every rational point on every (symmetric power of every) modular curve. More seriously: there are several interesting examples of modular (in some appropriate sense) curves, and one collection of projects is to study, via Chabauty and other explicit methods, the rational points on these curves.

As an example: there are several composite, but non prime power, level modular curves that arise naturally in “Mazur’s program B” for which the determination of rational points has some particular challenging aspect.

- (2) Similarly, one could compute specific quadratic points on certain modular curves using a modified Chabauty. More precisely, there is a heuristic of Siksek and Wetherell saying that for a nice curve X/\mathbb{Q} , a Chabauty-type method could bound the number of K -rational points on a curve X of genus g under the weaker assumption that $J_X(K)$ has rank $r \leq d(g - 1)$ where $d = [K : \mathbb{Q}]$.
- (3) Improve the “rank favorable” bounds on the rank functions that arise in Stoll’s work and in my work with Eric Katz for special curves (e.g., trigonal). This project would involve very little p -adic analysis; the techniques are more akin to the geometry of curves and combinatorics.
- (4) Uniform bounds for d th symmetric products of curves with small rank.
- (5) Rank favorable, uniform bounds for projective plane curves (e.g., non-hyperelliptic genus 3 curves) with small rank. For many “special” families of curves one has an explicit description of differentials, which helps with the “ p -adic analysis” part of the arguments.

REFERENCES

- [BPR13] Matthew Baker, Sam Payne, and Joseph Rabinoff, *On the structure of nonarchimedean analytic curves*, Tropical and Non-Archimedean Geometry, 2013, pp. 93–121. ↑2
- [Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR808103 (87f:11043) ↑1
- [KRZB16] Eric Katz, Joseph Rabinoff, and David Zureick-Brown, *Diophantine and tropical geometry, and uniformity of rational points on curves*, Survey article for the 2015 Summer Research Institute on Algebraic Geometry Proceedings (in review) (2016). ↑2
- [KRZB] _____, *Uniform bounds for the number of rational points on curves of small mordell–weil rank*, to appear in Duke Mathematical Journal. ↑2
- [KZB12] Eric Katz and David Zureick-Brown, *The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions* (2012). ↑1
- [LT02] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77. MR1892843 (2003d:11088) ↑1
- [MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, 2012, pp. 99–117. MR3098132 ↑2
- [Sto06] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661 (2007m:14025) ↑1
- [Sto19] _____, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell–Weil rank*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 3, 923–956. MR3908770 ↑2

DEPT. OF MATHEMATICS, EMORY UNIVERSITY, ATLANTA, GA 30322 USA
E-mail address: dzb@mathcs.emory.edu

ABELIAN CHABAUTY

DAVID ZUREICK-BROWN

ABSTRACT. These are expanded lecture notes for a series of four lectures at the Arizona Winter School on “Nonabelian Chabauty”, held March 7-11, 2020 in Tucson, Arizona.

Last update: March 4, 2020

CONTENTS

1. Introduction	1
1.1. Course outline, and how to read these notes	2
1.2. Acknowledgements	4
2. Abelian Chabauty	4
2.2. Computational aspects: an exercise	5
3. The uniformity conjecture	6
3.5. Evidence and records	6
3.6. Chabauty–Coleman bounds	7
3.8. A new hope	7
4. Bad Reduction	7
4.2. A few examples	8
5. Rank Favorable bounds	9
5.3. Stoll’s proof of Theorem 5.1	10
5.4. The rank of a divisor	12
5.6. Chip firing and the rank of a divisor on a graph	13
5.12. Semicontinuity of specialization	14
5.14. Rank favorable bounds for curves with totally degenerate reduction	15
5.15. Refined ranks	16
6. Tropical Geometry, Berkovich spaces, and Chabauty	16
References	16

1. INTRODUCTION

Let K be a number field and let X/K be a nice¹ curve of genus $g > 1$ whose Jacobian has rank $r := \text{rank } \text{Jac}_X(K)$.

The *Method of Chabauty–Coleman* (alternatively: “Chabauty’s method”, “Abelian Chabauty”, or just plain, vanilla, “Chabauty”) is among the most successful and widely

Date: March 4, 2020.

¹smooth, projective, and geometrically integral

applicable techniques for analyzing (either theoretically or explicitly) the set $X(K)$ of K -points of a low rank ($r < g$) curve X , and is an essential part of the “explicit approaches to rational points” toolbox. In particular, with some luck, Chabauty’s method allows one to

- explicitly determine, with proof, the set $X(K)$, or
- determine an upper bound on $\#X(K)$.

Mordell conjectured in the 20’s that the set $X(K)$ of K -points of X was finite. This was famously proved in the 80’s by Faltings [Fal86] (for which he was awarded a Fields medal), with subsequent independent proofs by Vojta and Bombieri [Voj91, Bom90].

Chabauty [Cha41], building on a idea of Skolem [Sko34], gave the first substantial progress toward Mordell’s conjecture. Chabauty’s method, which used p -adic techniques to produce p -adic “locally analytic” functions, relies on the hypothesis that $r < g$. This technique sat somewhat dormant until the 80’s, when Coleman’s seminal paper [Col85] resurrected and improved Chabauty’s idea.

Machine Computation. Computer aided computational tools took some time to catch up. The first big bottleneck was to improve the techniques for compute ranks of Jacobians of curves. To execute Chabauty’s method for a particular, explicit curve, one needs to know the rank r of its Jacobian (to check the $r < g$ condition), and a basis for the Mordell–Weil group of $\text{Jac}(K)$ (or at least a finite index subgroup). An early highlight is due to Gordon and Grant [GG93]; building on work of Cassels and Flynn [Fly90, Cas89, Cas83] they work out the special case of two-descent on the Jacobian of a genus 2 hyperelliptic curve with rational Weierstrass points, and (with the help of a SUN Sparcstation) provably compute the rank of a couple examples.

This ushered in a golden era of computer assisted approaches to rational points on curves (and higher dimensional varieties). Even today there are substantial conceptual and practical improvements; one recent highlight is [BPS16], which greatly expands our abilities to compute ranks of Jacobians of non-hyperelliptic curves.

Applications. It is worth highlighting a few of the numerous applications of Chabauty’s method.

- McCallum made substantial progress towards a proof of Fermat’s Last Theorem, via a careful study of certain quotients of the Fermat curve $x^p + y^p = z^p$; for instance, [McC94] proves the “second case” of Fermat’s Last Theorem for regular primes;
- arithmetic statistics: Poonen and Stoll use Chabauty’s method to prove that 100% of odd degree hyperelliptic curves have only one rational point [PS14];
- analysis of rational points on modular curves, and Mazur’s “Program B” [RZB15];
- resolution of various generalized Fermat equations [PSS07].

1.1. Course outline, and how to read these notes. There is already an excellent survey by McCallum and Poonen [MP12]. This is short (16 pages) and a great entry point. I recommend my survey with Katz and Rabinoff [KRZB16] for the connections between p -adic and tropical techniques, and the survey [BJ15] by Baker and Jensen for a more geometric and combinatorial perspective. I also recommend attempting the computational Exercise 2.3 below (even if one is ultimately most interested in theory).

These notes will focus on the ideas from [KZB13] and [KRZB], and the papers [LT02, Sto06, Sto19, Bak08] which inspired our work. In particular, my discussion of the foundations of Abelian Chabauty, and discussion of tropical techniques, will be abridged, and these notes are somewhat of an advertisement for [MP12] and [KRZB16].

Additionally, while reading these notes, we also recommend attempting Exercise 2.3 from Subsection 2.2, which will help to quickly come up with speed with how to perform Chabauty's method in Magma.

Abelian Chabauty. We will start with a ‘black box’ discussion of the method of Chabauty and Coleman, addressing various points of view; this section is mostly an abridged version of [MP12], and it is recommended to read their survey alongside this section and before reading future sections.

Exhibiting Abelian Chabauty as a special case of Nonabelian Chabauty is not completely straightforward. These notes do not address this, and we instead recommend Poonen’s excellent set of notes available at

http://www-math.mit.edu/~poonen/papers/p-adic_approach.pdf.

Bad reduction. One avenue to improve on Coleman’s bound is to generalize the framework of Chabauty and Coleman’ arguments to the case of bad reduction. We will discuss the advantage of working at bad primes and the difficulties and tradeoffs that arise, starting with the work of Lorenzini–Tucker [LT02].

Rank favorable bounds. When the rank is strictly smaller than $g - 1$, there are more “inputs” to Chabauty’s method and one expects this extra flexibility to lead to improvements to the method, giving rise to “rank favorable” bounds. We’ll discuss the setup, and the translation to the notion of a “rank” of a divisor (due to Stoll [Sto06]). For a curve with good reduction, this notion of rank will be the classical one, and the improved bounds will follow from Clifford’s Theorem [Har77, Theorem IV.5.4]. In the case of bad reduction, reducible reduction, ranks are no longer as well behaved; instead, we introduce Baker’s notion of “numerical rank” [Bak08] and explain how to repair Stoll’s argument in the special case of a curve with totally degenerate reduction.

Tropical Geometry and Berkovich spaces. For a curve with bad reduction at a prime p , it had been well understood that “monodromy” and “analytic continuation” of p -adic integrals was an issue. Coleman proved that in the case of good reduction, there is no “monodromy” and the various ways of analytically continuing p -adic integrals all coincide. In the case of bad reduction, they generally do not coincide (we will discuss a simple example which illustrates this).

Stoll [Sto19] discovered that, while choices of analytic continuation genuinely do differ, they do so in a fairly controlled manner (linear, even), and was able to exploit this to prove a uniformity result for *hyperelliptic* curves of small rank.

These results all argue in the framework of rigid geometry (in the sense of Tate). Great clarification arose from the systematic reformulation via Berkovich spaces, which fill in the “missing” points of rigid spaces and which, at least in the case of curves, are fairly concrete and manageable topological spaces (they’re even Hausdorff). I’ll discuss Chabauty in the setting of Berkovich and tropical geometry and explain how modern tools (e.g., Berkovich’s

contraction theorem and Thuillier’s slope formula, exposited in [BPR13]) give a clean explanation of Coleman’s “good reduction” theorem, and will discuss my work with Katz and Rabinoff [KRZB] which give uniform bounds for arbitrary (but still small rank) curves.

1.2. Acknowledgements. The author would like to thank Enis Kaya, Jackson Morrow, Dino Lorenzini, and John Voight for useful comments and/or discussions. The author was supported by National Science Foundation CAREER award DMS-1555048.

2. ABELIAN CHABAUTY

We give here a quick “black box” version of Chabauty’s method, broken into 3 parts: setup, local analysis, and global coordination. We refer the reader to the excellent survey [MP12] for a more detailed introduction.

As before, let K be a number field with ring of integers \mathcal{O}_K and let X/K be a nice curve of genus $g > 1$. Let $r := \text{rank } \text{Jac}_X(K)$ be the rank of the Jacobian of X . Fix a prime p and a prime \mathfrak{p} of \mathcal{O}_K above p .

Setup. Under the assumption $r < g$, there exist **locally analytic** functions f_ω on $X(K_{\mathfrak{p}})$ (arising as a p -adic integral of a differential ω) which vanish on $X(K)$, but not on $X(K_{\mathfrak{p}})$. More precisely, there exists a subspace $V \subset H^0(X_{K_{\mathfrak{p}}}, \Omega_X^1)$ such that $\dim_{K_{\mathfrak{p}}} V \geq g - r$, and with the property that the p -adic integral

$$\int_P^Q \omega$$

vanishes for all $P, Q \in X(K)$ and for all $\omega \in V$. We will frequently refer to V as V_{chab} . This is (more or less) enough to conclude finiteness (and is roughly the original argument of Chabauty [Cha41]). See [MP12, Section 4 and Subsection 5.4] for proofs of these statements (culminating in [MP12, Theorem 4.4]).

Local analysis. On (residue) discs, the integrals f_ω are “locally analytic”: they have (p -adic) power series expansions, a discrete set of zeroes, and are amenable to fairly explicit study via tools from p -adic analysis (Newton polygons, or in more complicated situations, tropical geometry). In Coleman’s original analysis ([Col85, Lemma 3] or [MP12, Lemma 5.1]), one can bound the number zeros of f_ω in a residue disc in terms of the zeroes of its “derivative”, which we summarize as a ‘ p -adic Rolle’s theorem’ (in the sense of freshman calculus). In the simplest case one gets Rolle’s theorem on the nose: for $K = \mathbb{Q}$ and $p > 2$, Coleman proves [MP12, Theorem 5.3(1)] that the number of zeroes of f_ω in a residue disc D_P is at most $1 + n_P$, where

$$n_P = \#(\text{div } \omega \cap D_P). \quad (2.0.1)$$

See [MP12, Section 5] for proofs of these statements (culminating in [MP12, Theorem 5.5]).

Remark 2.1. An exciting “modern” version of this argument is [BD19, Section 4], where they compare the divisor of a locally analytic function F to the divisor of $\mathcal{D}(F)$, where \mathcal{D} is a “nice” differential operator \mathcal{D} .

Global coordination. One needs some way to coordinate the different, a priori independent, local bounds (as in Equation 2.0.1), and typically exploits some type of “global”

theorem from the geometry of curves. In Coleman’s proof, Riemann–Roch [Har77, Theorem IV.1.3] suffices; the local bounds (under the $K = \mathbb{Q}$ and $p > 2$ hypotheses) are $1 + n_P$; by Equation 2.0.1 we have that

$$\sum_{P \in X(\mathbb{F}_p)} n_P = \sum_{P \in X(\mathbb{F}_p)} \#(\operatorname{div} \omega \cap D_P) \leq \deg \operatorname{div} \omega = 2g - 2,$$

which suffices to prove Coleman’s theorem:

$$\#X(\mathbb{Q}) \leq \sum_{P \in X(\mathbb{F}_p)} (1 + n_P) = \sum_{P \in X(\mathbb{F}_p)} 1 + \sum_{P \in X(\mathbb{F}_p)} n_P \leq X(\mathbb{F}_p) + 2g - 2.$$

In the “improvements” to this theorem that we discuss in these notes, one instead needs some other global theorem, e.g., Clifford’s theorem (or Riemann–Roch and Clifford’s theorem for graphs, or for arithmetic curves, or for other refined rank functions). In [KRZB], which uses (in a sense) the full power of the tools from tropical geometry, this step relies global information about sections of the “tropical canonical bundle” (see [KRZB, Lemma 4.15]).

Again, please see [MP12] (especially the detailed examples in Section 8) for a survey and a more thorough introduction. It is also very useful to attempt the Magma exercise (Exercise 2.3) described in the “Computational aspects” part of Subsection 1.1.

2.2. Computational aspects: an exercise. While reading these notes, we also recommend attempting Exercise 2.3 below, which will help to quickly come up with speed with how to perform Chabauty’s method in Magma.

Magma has a free, limited use online calculator here

<http://magma.maths.usyd.edu.au/calc/>,

and a thoroughly documented implementation of Chabauty’s method

<http://magma.maths.usyd.edu.au/magma/handbook/text/1533>.

Even better is to obtain a copy for your laptop, or ssh access to a departmental server with a copy of Magma. The Simons Foundation has graciously made Magma freely available to mathematicians working in the US

<http://magma.maths.usyd.edu.au/magma/ordering/>;

your department’s tech staff should be able to help you obtain a copy of Magma through this agreement.

Exercise 2.3. Take Smart’s list (from [Sma97]) of the 427 genus 2 curves with good reduction away from 2, and provably find all of the rational points on them. A temporary folder containing several references, and containing a subfolder titled “preparatory-Magma-exercise” with instructions for this exercise, is available at

<http://www.math.emory.edu/~dzb/AWS2020>.

As an entry point to some of the additional computational techniques one might need (such as étale descent), we recommend Poonen’s surveys [Poo96] and [Poo02].

3. THE UNIFORMITY CONJECTURE

The *uniformity conjecture* is one of the outstanding open conjectures in arithmetic and diophantine geometry. Initially, Mazur asked whether one can bound $\#X(K)$ purely in terms of the rank of the Jacobian of X (see [Maz00, Page 223] [Maz86, Page 234]). This was later promoted to the following stronger conjecture.

Conjecture 3.1 ([CHM97]). Let K be a number field and let $g \geq 2$ be an integer. There exists a constant $B_g(K)$ such that for every smooth curve X over K of genus g , the number $\#X(K)$ of K -rational points is at most $B_g(K)$.

The uniformity conjecture famously follows [CHM97, Theorem 1.1] from the Weak Lang conjecture (a higher dimension analogue of the Mordell conjecture), which is the following.

Conjecture 3.2 ([Lan74], 1.3; see also [Lan86]). Let X be a smooth proper variety of general type over a number field K . Then there exists a proper closed subscheme Z of X such that $X(K) = Z(K)$.

Alternatively, there are the following stronger pair of conjectures.

Conjecture 3.3 (Generic Uniform Boundedness [CHM97]). Let $g \geq 2$ be an integer. There exists a constant B_g such that for number field K , there exist only finitely many isomorphism classes of curves of genus g and over K such that $\#X(K) > B_g$.

This follows from the Strong Lang Conjecture.

Conjecture 3.4 ([Lan74], 1.3; see also [Lan86]). Let X be a smooth proper variety of general type over a number field K . Then there exists a proper closed subscheme Z of X such that for every finite extension $K \subset L$, the complement $X(L) - Z(L)$ is finite.

In [CHM97], one applies the Weak (or Strong) Lang Conjecture to symmetric powers of the universal curve $\mathcal{C} \rightarrow \overline{M_{g,n}}$. A major aspect of their proof is to show that large enough symmetric powers of \mathcal{C} are of general type (or at least dominate a variety of general type); this is a special case of their “correlation” theorem [CHM97, Theorem 1.2]. See the papers [Pac97, Pac99, Abr97, Abr95, Cap95, CHM95] for improvements, variants and a lot of additional discussion, and the slides

<http://www-math.mit.edu/~poonen/slides/uniformboundedness.pdf>

for a fairly recent discussion and some additional motivation.

3.5. Evidence and records. The following table (taken from [Cap95, Section 4] gives the best known lower bounds on the constant $B_g(\mathbb{Q})$.

g	2	3	4	5	10	45	g
$B_g(\mathbb{Q}) \geq$	642	112	126	132	192	781	$16(g+1)$

The record so far is due to Michael Stoll, who found (searching systematically through several families of curves constructed by Noam Elkies) the following:

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

It has at least 642 rational points, and rank at most 22. See

<http://www.mathe2.uni-bayreuth.de/stoll/recordcurve.html>

for a full list of the known points.

The families constructed by Elkies arise in the following way: he studied K3 surfaces of the form

$$y^2 = S(t, u, v)$$

with lots of rational lines, such that S restricted to such a line is a perfect square.

3.6. Chabauty–Coleman bounds. The proofs of Mordell due to Faltings, Vojta, and Bombieri [Fal97, Voj91, Bom90] give upper bounds on $\#X(K)$. These bounds tend to be astronomical, and are not explicit in their original proofs; moreover, it is unclear (to me) how they depend on X and K .

One application of Chabauty’s method is to give uniform bounds on small rank curves. Coleman’s original theorem is the following.

Theorem 3.7 (Coleman, [Col85]). *Let X/\mathbb{Q} be a curve of genus g and let $r = \text{rank}_{\mathbb{Z}} \text{Jac}_X(\mathbb{Q})$. Suppose $p > 2g$ is a prime of **good reduction**. Suppose $r < g$. Then*

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2.$$

See [Col85, Lemma 3] or [MP12, Theorem 5.3] for a proof.

Various authors have worked to weaken Coleman’s hypotheses and to improve the bound; see Theorems 4.1, 5.1, 5.2, 6.1, and 6.2 below and the surrounding discussion.

3.8. A new hope. The recent work of Dimitrov, Gao and Habegger [DGH19, DGH20] give bounds on $\#X(K)$ which only depend on $g(X)$, $\deg K$, and $\text{rank Jac}_X(K)$. Combined with the conjectural boundedness of ranks of Jacobians of curves of fixed genus over a fixed number field (as predicted by [PPVW19] and [Poo18, Section 4.2]) this would prove uniformity. Their approach is in the spirit of Vojta’s original proof [Voj91], and relies on their recent other work on improved height bounds.

4. BAD REDUCTION

One avenue to improve on Coleman’s bound is to generalize the Chabauty framework and Coleman’s arguments to the case of bad reduction. We will discuss the advantage of working at bad primes and the difficulties that arise, starting with the work of Lorenzini–Tucker [LT02].

Coleman’s original bound (3.7) relies on an initial choice of a prime of good reduction. The first such prime could be arbitrarily large (e.g., consider a hyperelliptic curve $y^2 = f(x)$, and twist it by d , where d is the product of the first million primes; or, pick singular curves X_p over \mathbb{F}_p , for the first million primes p , and use the Chinese Remainder Theorem to construct a curve X over \mathbb{Q} that $X_{\mathbb{F}_p} \cong X_p$ for each such prime p). The problem with this is that the Hasse bound only provides that $\#X(\mathbb{F}_p) \leq 2g\sqrt{p} + p + 1$; so as p increases, Coleman’s bound becomes increasingly worse, and in particular is not uniform.

Whence the appeal of the following theorem of Lorenzini and Tucker.

Theorem 4.1 (Lorenzini, Tucker, [LT02], Corollary 1.11). *Suppose $p > 2g$ and let \mathcal{X} be a proper regular model of X over \mathbb{Z}_p . Suppose $r < g$. Then*

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}_{\mathbb{F}_p}^{\text{sm}} + 2g - 2$$

where $\mathcal{X}_{\mathbb{F}_p}^{\text{sm}}$ is the smooth locus of the special fiber $\mathcal{X}_{\mathbb{F}_p}$.

Recall that a scheme X is **regular** if for every point $x \in X$, with corresponding maximal ideal \mathfrak{m} and residue field $k(x)$,

$$\dim_{k(x)} \mathfrak{m}/\mathfrak{m}^2 = \dim X.$$

If R is a DVR with uniformizer π and residue field k and $X \rightarrow \text{Spec } R$ is a relative curve, then a point $x \in X_k$ is regular if and only if the local equation at x is $yz = \pi$. (By “local equation” we mean the equation for the completion of the étale local ring $\mathcal{O}_{X,x}$.) See the examples in Subsection 4.2, and see [Sil94, Chapter IV] for a leisurely treatment.

The utility of the proper regular model \mathcal{X} of X is that the reduction map

$$r: \mathcal{X}(\mathbb{Q}) \rightarrow \mathcal{X}(\mathbb{F}_p)$$

takes values in the smooth locus $\mathcal{X}^{\text{sm}}(\mathbb{F}_p)$. In Chabauty’s method, one thus only needs to consider residue classes $r^{-1}(Q)$ of points $Q \in \mathcal{X}^{\text{sm}}(\mathbb{F}_p)$. Such residue classes are (p -adically analytically) isomorphic to discs; this makes the setup of Chabauty easier, and makes the “local analysis” much easier.

The “ $2g - 2$ ” term in Coleman’s bound (3.7) is derived from Riemann–Roch on $X_{\mathbb{F}_p}$, and is the rationale for the “good reduction” hypothesis. Lorenzini and Tucker recover the $2g - 2$ term via Riemann–Roch on $X_{\mathbb{Q}_p}$ and a more involved p -adic analytic argument. A later, alternative proof [MP12, Theorem A.5] instead recovers the $2g - 2$ term via arithmetic intersection theory on \mathcal{X} and adjunction.

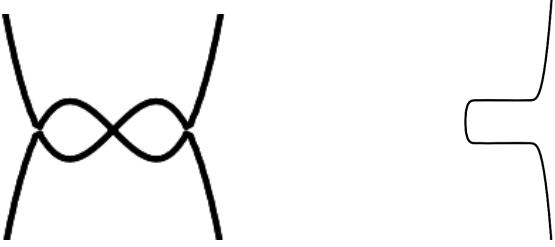
The drawback is that $\mathcal{X}_{\mathbb{F}_p}$ could contain an arbitrarily long chain of \mathbb{P}^1 ’s. (For example, if X is an elliptic curve with semistable reduction at p and $v_p(j(X)) = -n$, then $\mathcal{X}_{\mathbb{F}_p}$ is an n -gon of \mathbb{P}^1 ’s.) Once again, the size of $\mathcal{X}^{\text{sm}}(\mathbb{F}_p)$ could be arbitrarily large, giving non-uniform bounds.

Stoll [Sto19] had the bold idea to work with a *non-regular, minimal* model: one contacts each chain of \mathbb{P}^1 ’s into a single node. Such a model is no longer regular, but the number of components is bounded, and the genus of each component is bounded (exercise: verify this). Since the model is no longer regular, rational points no longer reduce to smooth points (exercise: give an example), and might reduce to a node. The residue class of a node is now an annulus (explain in an example). This creates multiple problems: an annulus admits “monodromy” and integrals no longer admit a unique analytic continuation, and local expansions are now laurent, rather than power, series. See Theorem 6.1 below and the surrounding discussion.

4.2. A few examples.

Example 4.3 (A regular model). The relative curve

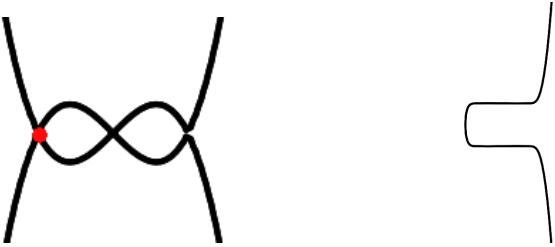
$$\begin{aligned} y^2 &= (x(x-1)(x-2))^3 - 5 \\ &= (x(x-1)(x-2))^3 \pmod{5}. \end{aligned}$$



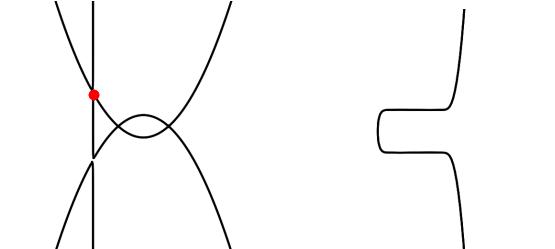
is regular at the point $(0, 0)$. The local equation at $(0, 0)$ analytically looks like $xy = 5$. One can see by elementary number theory that no rational point can reduce to $(0, 0)$.

Example 4.4 (Resolving a semistable, but not regular, model).

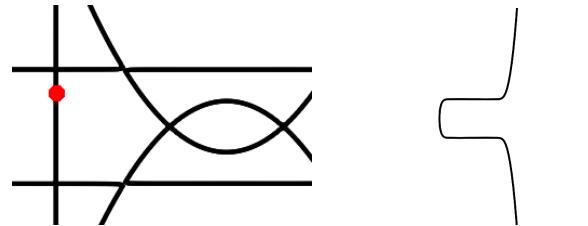
$$\begin{aligned} y^2 &= (x(x-1)(x-2))^3 - 5^4 \\ &= (x(x-1)(x-2))^3 \pmod{5} \end{aligned}$$



Now, the local equation at $(0, 0)$ looks like $xy = 5^4$, and $(0, 5^2)$ reduces to $(0, 0)$. Blowing up along the ideal $(x, y, 5)$ gives



and the local equations now look like $xy = 5^3$ and $xy = 5$. One of the 2 points is still not regular. After 2 more blowups we get



and now all of the local equations look like $xy = 5$, giving a regular model.

5. RANK FAVORABLE BOUNDS

Lorenzini and Tucker [LT02] ask if one can refine Coleman's bound (Theorem 3.7) when the rank r is small (i.e., $r \leq g - 2$). This was subsequently answered by Stoll.

Theorem 5.1 (Stoll, [Sto06], Corollary 6.7). *With the hypothesis of Theorem 3.7,*

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r.$$

The space of differentials “suitable” for Chabauty’s method has dimension at least $g - r$. When $r < g - 1$, there are thus more “inputs” to Chabauty’s method and this extra flexibility can be exploited to improve the p -adic analysis. Indeed, Stoll’s idea is: instead of using a single integral, to taylor the choice of integral to each residue class. The additional “global geometric input” is the (classical) notion of “rank of a divisor”, and after translating his setup into this language, improved bounds follow from Clifford’s Theorem.

The application of Clifford’s theorem is also the source of the “good reduction” hypothesis. Using ideas from the “discrete case” of tropical geometry (in particular “chip-firing”), Eric Katz and I generalized Stoll’s theorem to arbitrary reduction types.

Theorem 5.2 (Katz, Zureick-Brown, [KZB13]). *Let X/\mathbb{Q} be a curve of genus g and let $r = \text{rank } \text{Jac}_X(\mathbb{Q})$. Suppose $p > 2r + 2$ is a prime, that $r < g$, and let \mathcal{X} be a proper regular model of X over \mathbb{Z}_p . Then*

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}_{\mathbb{F}_p}^{\text{sm}}(\mathbb{F}_p) + 2r.$$

Unlike Lorenzini and Tucker’s generalization of Coleman’s theorem, where they replace Coleman’s use of Riemann–Roch on $X_{\mathbb{F}_p}$ with Riemann–Roch on $X_{\mathbb{Q}_p}$, it does not seem possible to replace Stoll’s use of Clifford’s theorem on $X_{\mathbb{F}_p}$ with Clifford’s theorem on $X_{\mathbb{Q}_p}$. Matt Baker suggested that it might be possible to generalize Stoll’s theorem to curves with bad, *totally degenerate* reduction (i.e., $X_{\mathbb{F}_p}$ is a union of rational curves meeting transversely) using ideas from tropical geometry (see the recent survey [BJ15] on tropical geometry and applications), in particular the notion of “chip firing”, Baker’s combinatorial definition of rank, and Baker–Norine’s [BN07] combinatorial Riemann–Roch and Clifford theorems. Baker was correct, and in fact an enrichment of his theory led to the following common generalization of Stoll’s and Lorenzini and Tucker’s theorems.

Baker’s recent work [Bak08] clarifies the relationship between *linear systems* on curves and on finite graphs. Highlights include a semicontinuity theorem for ranks of linear systems (as one passes from the curve to its dual graph), and graph theoretic analogues of Riemann–Roch and Clifford’s theorem. Baker’s theory works best with totally degenerate curves (i.e. each component is a \mathbb{P}^1). Theorem 5.2 requires an enrichment of Baker’s theory if the irreducible components of the reduction have higher genus.

5.3. Stoll’s proof of Theorem 5.1. Let $p > 2$. Denote by V_{chab} the vector space of all $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1_{X_{\mathbb{Q}_p}/\mathbb{Q}_p})$ such that $\int_{P_1}^{P_2} \omega = 0$ for all $P_1, P_2 \in X(\mathbb{Q})$. Then $\dim V_{\text{chab}} \geq g - r$. For each $\omega \in V_{\text{chab}}$, scale ω by a power of p so that the reduction $\tilde{\omega}$ of ω is non zero, and denote by \tilde{V}_{chab} the set of all such reductions; we note that $\dim_{\mathbb{F}_p} \tilde{V}_{\text{chab}} = \dim_{\mathbb{Q}_p} V_{\text{chab}}$.

For each $Q \in X(\mathbb{F}_p)$ and $\omega \in \tilde{V}_{\text{chab}}$, set

$$n_Q(\omega) := \deg (\text{div } \omega|_{]Q[}) \text{ and } n_Q := \min_{\omega \in \tilde{V}_{\text{chab}}} n_Q(\omega)$$

(where we recall that $]Q[$ denotes the *tube* or *residue class* of Q , that is, the set of all points of $X(\mathbb{Q}_p)$ which reduce to Q). Since div is compatible with reduction mod p , $n_Q(\omega)$ is equal to the valuation $v_Q(\tilde{\omega})$ (i.e., the order of vanishing of $\tilde{\omega}$ at Q).

By the “ p -adic Rolle’s theorem”, the number of zeroes of $\int \omega$ in $]Q[$ is at most $1 + n_Q(\omega)$, so

$$X(\mathbb{Q}) \leq \sum_{Q \in X(\mathbb{F}_p)} (1 + n_Q) = \sum_{Q \in X(\mathbb{F}_p)} 1 + \sum_{Q \in X(\mathbb{F}_p)} n_Q = X(\mathbb{F}_p) + \deg(D_{\text{chab}}),$$

where we define D_{chab} to be the divisor

$$D_{\text{chab}} := \sum_{Q \in X(\mathbb{F}_p)} n_Q Q \in \text{Div } X_{\mathbb{F}_p}.$$

By Riemann–Roch, $\deg D_{\text{chab}} \leq 2g - 2$, recovering the bound

$$X(\mathbb{Q}) \leq X(\mathbb{F}_p) + 2g - 2.$$

We claim that, in fact, $\deg D \leq 2r$, which suffices to prove Theorem 5.1. (When $r = g - 1$, $2r = 2g - 2$.) Stoll’s main observation is that

$$\tilde{V}_{\text{chab}} \subset H^0(X_{\mathbb{F}_p}, \Omega_{X_{\mathbb{F}_p}}^1(-D_{\text{chab}})), \quad (5.3.1)$$

and in particular,

$$\dim H^0(X_{\mathbb{F}_p}, \Omega_{X_{\mathbb{F}_p}}^1(-D_{\text{chab}})) \geq \dim \tilde{V}_{\text{chab}} \geq g - r. \quad (5.3.2)$$

To justify Equation 5.3.1, given an effective divisor $E = \sum n_P P$ and a line bundle \mathcal{L} on a curve X , recall that $H^0(X, \mathcal{L}(-E))$ is the subspace of sections of $H^0(X, \mathcal{L})$ that have at least a zero of order n_p at P . A differential $\tilde{\omega} \in \tilde{V}_{\text{chab}}$ thus satisfies $v_P(\tilde{\omega}) \geq n_P$ by definition of n_p !

On the other hand, Clifford’s Theorem [Har77, Theorem IV.5.4] implies that

$$\dim H^0(X_{\mathbb{F}_p}, \Omega_{X_{\mathbb{F}_p}}^1(-D_{\text{chab}})) \leq \frac{1}{2} \deg(\Omega_{X_{\mathbb{F}_p}}^1(-D_{\text{chab}})) + 1. \quad (5.3.3)$$

Combining equations 5.3.2 and 5.3.3 gives

$$g - r \leq \frac{1}{2} \deg(\Omega_{X_{\mathbb{F}_p}/\mathbb{Q}_p}^1(-D_{\text{chab}})) + 1 = g - 1 - \frac{1}{2} \deg D_{\text{chab}} + 1$$

and simplifying gives

$$\deg D_{\text{chab}} \leq 2r.$$

To justify Equation 5.3.3, we switch to the language of divisors. Recall that a divisor is *special* if $\dim H^0(X, K - D) > 0$, where K is a canonical divisor. (Equivalently, D is special if and only if it is a subdivider of some canonical divisor.) For context: Riemann–Roch reads:

$$H^0(X, D) = \dim H^0(X, K - D) + \deg D + 1 - g.$$

This gives a formula for $H^0(X, D)$ when the degree of D is large; indeed when $\deg D > \deg K = 2g - 2$, $\deg K - D < 0$, therefore $\dim H^0(X, K - D) = 0$ and $H^0(X, D) = \deg D + 1 - g$. At the other extreme: if $\deg D \leq 2g - 2$, then it is still possible that $\dim H^0(X, K - D) = 0$, in which case, again, $H^0(X, D) = \deg D + 1 - g$. If D is special, i.e., $\dim H^0(X, K - D) > 0$, then by Riemann–Roch, $H^0(X, D) < \deg D + 1 - g$; in this case, Clifford’s Theorem gives the much stronger bound

$$H^0(X, D) \leq \frac{1}{2} (\deg D) + 1.$$

Let $K = \text{div } \tilde{\omega}$. Then, by definition of n_Q , D_{chab} is a subdivider of the canonical divisor K (since $v_Q(D_{\text{chab}}) := v_Q(\tilde{\omega}) = n_Q(\tilde{\omega}) \geq n_Q$); in particular, D_{chab} is special.

5.4. The rank of a divisor. In the proof of Stoll's theorem, we implicitly used the notion of *rank of a line bundle* (or divisor). One can simply define the rank $r(\mathcal{L})$ of a divisor $\mathcal{L} \in \text{Pic}(X)$ to be

$$r(\mathcal{L}) := \dim H^0(X, \mathcal{L}) - 1.$$

This has the following alternative interpretation over an algebraically closed field: $r(\mathcal{L})$ is the largest number of independent and generic “vanishing conditions” one can impose on sections of \mathcal{L} . Recall that for a closed point P , $H^0(X, \mathcal{L}(-P))$ is the subspace of sections of $H^0(X, \mathcal{L})$ that have at least a simple zero at the point P . More generally, for an effective divisor $E = \sum n_P P$, $H^0(X, \mathcal{L}(-E))$ is the subspace of sections of $H^0(X, \mathcal{L})$ that have at least a zero of order n_p at P . By [Har77, Proof of Theorem IV.1.3],

$$\dim H^0(X, \mathcal{L}(-P)) \geq \dim H^0(X, \mathcal{L}) - 1,$$

and in particular,

$$\dim H^0(X, \mathcal{L}(-E)) \geq \dim H^0(X, \mathcal{L}) - \deg E. \quad (5.4.1)$$

Similarly, one can define the rank $r(D)$ of a divisor $D \in \text{Div}(X)$ to be

$$r(D) := \dim H^0(X, D) - 1.$$

This has the following alternative interpretation over an algebraically closed field: $r(D)$ is the largest number of points of $X_{\bar{k}}$ (allowing for multiplicity) one can remove from D before D is no longer equivalent to some effective divisor. Equivalently, the rank is the largest number of points (allowing for multiplicity) that you can demand occurs as a subdivisor of some effective divisor D' equivalent to D .

More formally, we make the following definitions.

Definition 5.5. Let $D \in \text{Div } X$ be a divisor. The **linear system** associated to D is the collection $|D|$ of effective divisors linearly equivalent to D . We define the **rank** $r(D)$ of D to be -1 if $|D|$ is empty (i.e., if D is not equivalent to an effective divisor). Otherwise, we define

$$r(D) := \max\{n \in \mathbb{Z}_{\geq 0} : |D - E| \neq \emptyset, \forall E \in \text{Div}_{\geq 0}^n(X_{\bar{k}})\},$$

where $\text{Div}_{\geq 0}^n(X_{\bar{k}})$ is the subset of $\text{Div}(X_{\bar{k}})$ of effective divisors of degree n .

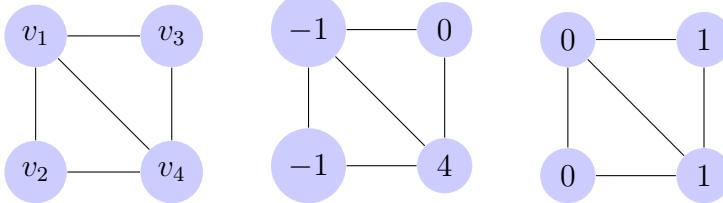
The linear system $|D|$ is naturally isomorphic to the projective space $\text{Proj } H^0(X, D) \cong \mathbb{P}^{r-1}$, where $r = \dim H^0(X, D)$.

By Equation 5.4.1,

$$r(D) \geq \dim H^0(X, D) - 1.$$

The converse follows from the observation (exercise!) that if $r(D) = n$, then there exists $P \in X_{\bar{k}}$ such that $r(D - P) = n - 1$. Note that one must take \bar{k} in the definition of rank. Indeed, consider a non hyperelliptic curve X with $X(k) = \emptyset$, but $X(k') \neq \emptyset$ for some quadratic extension k' of k . Then for $P \in X(k')$ with conjugate point Q , $D := P + Q \in \text{Div}^2 X$. Then $r(D) = 1$; but, $\text{Div}_{\geq 0}^1 X$ is empty, so

$$\max\{n \in \mathbb{Z}_{\geq 0} : |D - E| \neq \emptyset, \forall E \in \text{Div}_{\geq 0}^n(X)\} = 1$$

FIGURE 1. The effect of firing once at v_4

5.6. Chip firing and the rank of a divisor on a graph. I recommend taking a quick look at Matt Baker's short expository article available at

<http://people.math.gatech.edu/~mbaker/pdf/g4g9.pdf>.

For a short selection of other references: the papers [Bak08, BN07] by Baker and collaborators are my preferred starting point; [BJ15] is also a great survey.

Let Γ be a connected graph, with vertex set $V(\Gamma)$ and edge set $E(\Gamma)$. We define $\text{Div } \Gamma$ to be the set of maps from the vertices of $V(\Gamma)$ to \mathbb{Z} ; this is isomorphic to the free group $\mathbb{Z}[V(\Gamma)]$ generated by the set of vertices of Γ , and will sometimes write $D = \sum_v n_v(v)$ for the function that has value n_v at v . The degree of D is $\deg D = \sum_v D(v)$. We'll refer to an element $D \in \text{Div } \Gamma$ as a **divisor** or **configuration**, and will typically represent them visually as in Figure 5.6, and refer to $D(v)$ as the “number of chips” or “dollars” at the vertex v .

The goal of the “dollar game” or “chip firing” is to get a divisor out of debt. We say that a divisor D is **effective**, and write $D \geq 0$, if $D(v) \geq 0$ for all vertices v of Γ .

One formalizes lending and borrowing as follows: given $f \in \text{Div } \Gamma$, we define the principal divisor associated to f to be

$$\text{div } f = \sum_{v \in \Gamma} D(v) \cdot \left(-(\deg v)(v) + \sum_{w \neq v} \#\{\text{edges between } w \text{ and } v\}(w) \right).$$

In particular, $\text{div } \delta_v$ is

$$-(\deg v)(v) + \sum_{w \neq v} \#\{\text{edges between } w \text{ and } v\}(w)$$

which has the effect of the vertex v “lending” one chip to each adjacent vertex (see Figure 5.6). We say that two divisors D and D' are **equivalent** if there is a sequence of lends and borrows which transforms D into D' , and we define the **Jacobian** or **Picard group** $\text{Pic } \Gamma$ to be the abelian group of equivalence classes of divisors on Γ . more formally, there is an exact sequence

$$0 \rightarrow \mathbb{Z} \rightarrow \text{Div } \Gamma \xrightarrow{\text{div}} \text{Div } \Gamma \rightarrow \text{Pic } \Gamma \rightarrow 0,$$

where the first map sends 1 to the function $\sum_v \delta_v$ (i.e., every vertex lends, which has no effect).

The vector space $H^0(\Gamma, D)$ doesn't make sense for a graph. Baker's insight from [Bak08] is that the “practical” definition of rank (Definition 5.5) *does* generalize nicely to divisors on graphs.

Definition 5.7. Let $D \in \text{Div } \Gamma$ be a divisor. The **linear system** associated to D is the collection $|D|$ of effective divisors linearly equivalent to D . We define the **rank** $r(D)$ of D to be -1 if $|D|$ is empty (i.e., if D is not equivalent to an effective divisor). Otherwise, we define

$$r(D) := \max\{n \in \mathbb{Z}_{\geq 0} : |D - E| \neq \emptyset, \forall E \in \text{Div}_{\geq 0}^n(\Gamma)\},$$

where $\text{Div}_{\geq 0}^n(X_{\bar{k}})$ is the subset of $\text{Div}(X_{\bar{k}})$ of effective divisors of degree n .

Equivalently, the rank is the largest number of points (allowing for multiplicity) that you can demand occurs as a subdivisor of some effective divisor D' equivalent to D . In other words, the rank of a divisor D is the “amount of damage” necessary to make the chip firing game unwinnable.

Definition 5.8. Let Γ be a graph. We define the **canonical divisor** on K to be the divisor

$$K_{\Gamma} := \sum_{v \in V(\Gamma)} (\deg v - 2)(v).$$

The **genus** $g(\Gamma)$ (alternatively **first Betti number** $h^1(\Gamma)$) of Γ is the number of edges minus the number of vertices; note that $\deg K_{\Gamma} = 2g(\Gamma) - 2$. We say that a divisor D is **special** if D is effective and $|K - D|$ is non empty.

This definition is motivated by adjunction.

Theorem 5.9 ([BN07], Theorem 1.12 and Corollary 3.5). *Let $D \in \text{Div } \Gamma$. Then the following are true.*

- (1) *Riemann–Roch:* $r(D) - r(K - D) = \deg D + 1 - g$.
- (2) *Clifford’s Theorem:* if D is special, then $r(D) \leq \frac{1}{2} \deg D$.

Corollary 5.10 ([BN07], Theorem 1.9). *The chip firing game is winnable for the configuration D if $\deg D \geq g$.*

Remark 5.11. It is unknown whether one can deduce these from the analogous theorems from the geometry of curves.

5.12. Semicontinuity of specialization. Let R be a complete discrete valuation ring with maximal ideal π , residue field k , and fraction field K . Denote by η the generic point of $\text{Spec } R$, and by b the closed point. (Most of what we say below works just as well if we replace $\text{Spec } R$ by an integral scheme B .) Let $C \rightarrow B$ be a relative curve of genus g (i.e., a smooth proper morphism such that for every $x \in \text{Spec } R$, the fiber C_x is a smooth proper curve of genus g over the residue field $k(x)$).

Let $D = \sum n_P P \in \text{Div } C_{\eta}$. The dimension of C is 2, and we can extend D to a divisor \mathcal{D} on C by taking the closure of its support; in other words, $\mathcal{D} := \sum n_P \bar{P} \in \text{Div } C_{\eta}$, where \bar{P} is the closure of P . Intersecting \mathcal{D} with the special fiber C_b thus gives a **specialization map**

$$\text{sp}: \text{Div } C_{\eta} \rightarrow \text{Div } C_b.$$

Proposition 5.13. *Let $D \in \text{Div } C_{\eta}$. Then $r(\text{sp}(D)) \geq r(D)$.*

The inequality can certainly be strict. Indeed, consider \mathcal{C} with hyperelliptic special fiber and non-hyperelliptic generic fiber, and let $D = P + Q$ where $P, Q \in \mathcal{C}(K)$ are points whose reductions are hyperelliptic conjugate. Then $r(D) = 1$ but $r(\text{sp}(D)) = 2$.



FIGURE 2. A curve and its dual graph.

More generally, if L is a line bundle on C_η , there is a unique (up to isomorphism) extension of L to a line bundle \mathcal{L} on C (i.e., a line bundle \mathcal{L} on C such that \mathcal{L}_η is isomorphic to L . (Indeed, let $s \in L(U)$ be a section over some non empty open set $U \subset C_\eta$; then $\mathcal{L} = \mathcal{O}_C(\bar{(\div s)})$ extends L .)

There is thus an analogous **specialization map**

$$\text{sp}: \text{Pic } C_\eta \rightarrow \text{Pic } C_b,$$

and (since $r(D) = r(\mathcal{O}(D))$), Proposition 5.13 equivalently implies that $r(\text{sp}(L)) \geq r(L)$.

Proposition 5.13 is a special case of Semicontinuity of Cohomology [Har77, Theorem III.12.8] (taking $i = 0$ and $\mathcal{F} = \mathcal{O}_C(D)$). Unsurprisingly, this is overkill; we sketch a direct proof that will generalize to the “discrete” case.

Proof of Proposition 5.13. First, note that a section $s \in H^0(C_\eta, D)$ can be scaled by a power of the uniformizer π to a section of $H^0(C, \mathcal{O}(\bar{D}))$. There are a few ways to see this: if we think of s as a function

Conversely, Since $C_\eta \subset C$ is open, and since the vanishing locus of a section of a line bundle is closed, the map

$$H^0(C, \mathcal{O}(\bar{D})) \rightarrow H^0(C_\eta, D)$$

is injective. In particular,

$$\text{rank}_R H^0(C, \mathcal{O}(\bar{D})) = \text{rank}_K H^0(C_\eta, D).$$

Alternatively, it follows directly from flatness that

$$H^0(C, \mathcal{O}(\bar{D})) \otimes_R K \cong H^0(C_\eta, D).$$

One can then show that the dimension of the reduction map

$$H^0(C, \mathcal{O}(\bar{D})) \rightarrow H^0(C_b, \mathcal{O}(D_b))$$

is $\dim H^0(C_\eta, D)$, so in particular

$$\dim H^0(C_b, \mathcal{O}(D_b)) \geq \dim H^0(C_\eta, D).$$

□

5.14. Rank favorable bounds for curves with totally degenerate reduction. One can associate to such a singular curve with transverse crossings its dual graph as in Figure 1. Component curves become nodes, and intersections correspond to edges.

In this lectures, I'll discuss the special case of a “Mumford curve” (i.e., a curve with “totally degenerate” reduction, in that the reduction is a collection of \mathbb{P}^1 's meeting transversely, and in particular represents an isolated point on the moduli space of curves); for such curves, one

only needs Baker’s original notion of rank (which we call “numerical rank”); for a discussion of the “abelian rank”, and a detailed proof in this case, see our paper [KZB13]. The main point is that there is also a specialization map for the numerical (i.e., “chip firing”) rank, and once one sets things up properly, the proof is similar to Stoll’s proof.

5.15. Refined ranks. In a certain sense, the numerical rank only “sees” the component group of the Néron model. The enriched notion of abelian rank from [KZB13] and [AB15] sees the abelian part of the Néron model. One can ask if there is a corresponding notion of “toric” or “unipotent” rank. In [KZB13, Subsection 3.3], we define a “toric” rank, and in [KZB13, Example 5.5] demonstrate that these ranks differ; we have yet to find a useful application.

6. TROPICAL GEOMETRY, BERKOVICH SPACES, AND CHABAUTY

A recent breakthrough [Sto19] fully removed, in the special case of hyperelliptic curves, the dependence on a *regular* model and derived a *uniform* bound on $\#X(\mathbb{Q})$ for small ($r \leq g-3$) rank curves.

Theorem 6.1 (Stoll, [Sto19]). *Let X be a hyperelliptic curve of genus g and let $r = \text{rank}_{\mathbb{Z}} \text{Jac}_X(\mathbb{Q})$. Suppose $r \leq g-3$. Then*

$$\#X(\mathbb{Q}) \leq 8(r+4)(g-1) + \max\{1, 4r\} \cdot g.$$

A main ingredient in Stoll’s proof is to understand the discrepancy between the different flavors of integration. Eric Katz noticed that this discrepancy “factored through the tropicalization of the torus part of the Berkovich uniformization of X ”. After a thorough reinterpretation of the method of Chabauty and Coleman via Berkovich spaces, and harnessing the full catalogue of tropical and non-Archimedean analytic tools, we were able to improve Stoll’s result to *arbitrary* curves of small rank.

Theorem 6.2 (Katz–Rabinoff–Zureick-Brown, [KRZB]). *Let X be **any** curve of genus g and let $r = \text{rank}_{\mathbb{Z}} \text{Jac}_X(\mathbb{Q})$. Suppose $r \leq g-3$. Then*

$$\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28.$$

For more details, see our survey [KRZB16].

REFERENCES

- [AB15] Omid Amini and Matthew Baker, *Linear series on metrized complexes of algebraic curves*, Math. Ann. **362** (2015), no. 1-2, 55–106. MR3343870 ↑16
- [Abr95] Dan Abramovich, *Uniformité des points rationnels des courbes algébriques sur les extensions quadratiques et cubiques*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 6, 755–758. MR1354720 ↑6
- [Abr97] ———, *Uniformity of stably integral points on elliptic curves*, Invent. Math. **127** (1997), no. 2, 307–317. MR1427620 ↑6
- [Bak08] Matthew Baker, *Specialization of linear systems from curves to graphs*, Algebra Number Theory **2** (2008), no. 6, 613–653. With an appendix by Brian Conrad. MR2448666 (2010a:14012) ↑3, 10, 13
- [BD19] Jennifer S. Balakrishnan and Netan Dogra, *An effective Chabauty-Kim theorem*, Compos. Math. **155** (2019), no. 6, 1057–1075. MR3949926 ↑4
- [BJ15] Matthew Baker and David Jensen, *Degeneration of linear series from the tropical point of view and applications*, arXiv preprint arXiv:1504.05544 (2015). ↑2, 10, 13

- [BN07] M. Baker and S. Norine, *Riemann-Roch and Abel-Jacobi theory on a finite graph*, Adv. Math. **215** (2007), no. 2, 766–788. MR2355607 (2008m:05167) ↑10, 13, 14
- [Bom90] E. Bombieri, *The Mordell conjecture revisited*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, 615–640. MR1093712 (92a:11072) ↑2, 7
- [BPR13] Matthew Baker, Sam Payne, and Joseph Rabinoff, *On the structure of nonarchimedean analytic curves*, Tropical and Non-Archimedean Geometry, 2013, pp. 93–121. ↑4
- [BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), e6, 80. MR3482281 ↑2
- [Cap95] L. Caporaso, *Counting rational points on algebraic curves*, Rend. Sem. Mat. Univ. Politec. Torino **53** (1995), no. 3, 223–229. Number theory, I (Rome, 1995). MR1452380 (98i:11041) ↑6
- [Cas83] J. W. S. Cassels, *The Mordell-Weil group of curves of genus 2*, Arithmetic and geometry, Vol. I, 1983, pp. 27–60. MR717589 ↑2
- [Cas89] ———, *Arithmetic of curves of genus 2*, Number theory and applications (Banff, AB, 1988), 1989, pp. 27–35. MR1123068 ↑2
- [Cha41] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l’unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885. ↑2, 4
- [CHM95] Lucia Caporaso, Joe Harris, and Barry Mazur, *How many rational points can a curve have?*, The moduli space of curves (Texel Island, 1994), 1995, pp. 13–31. MR1363052 (97d:11099) ↑6
- [CHM97] ———, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35. MR1325796 (97d:14033) ↑6
- [Col85] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. ↑2, 4, 7
- [DGH19] Vesselin Dimitrov, Ziyang Gao, and Philipp Habegger, *Uniform bound for the number of rational points on a pencil of curves*, arXiv preprint arXiv:1904.07268 (2019). ↑7
- [DGH20] ———, *Uniformity in mordell-lang for curves*, arXiv preprint arXiv:2001.10276 (2020). ↑7
- [Fal86] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields* (1986), 9–27. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. MRFaltings:bookArithmeticGeometry ↑2
- [Fal97] ———, *The determinant of cohomology in etale topology*, Arithmetic geometry (Cortona, 1994), 1997, pp. 157–168. MRFaltings:bookArithmeticGeometry (98k:14023) ↑7
- [Fly90] Eugene Victor Flynn, *The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field*, Math. Proc. Cambridge Philos. Soc. **107** (1990), no. 3, 425–441. MR1041476 ↑2
- [GG93] Daniel M. Gordon and David Grant, *Computing the Mordell-Weil rank of Jacobians of curves of genus two*, Trans. Amer. Math. Soc. **337** (1993), no. 2, 807–824. MR1094558 ↑2
- [Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116) ↑3, 5, 11, 12, 15
- [KRZB16] Eric Katz, Joseph Rabinoff, and David Zureick-Brown, *Diophantine and tropical geometry, and uniformity of rational points on curves*, Survey article for the 2015 Summer Research Institute on Algebraic Geometry Proceedings (in review) (2016). ↑2, 3, 16
- [KRZB] ———, *Uniform bounds for the number of rational points on curves of small mordell-weil rank*, to appear in Duke Mathematical Journal. ↑3, 4, 5, 16
- [KZB13] Eric Katz and David Zureick-Brown, *The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions*, Compos. Math. **149** (2013), no. 11, 1818–1838. MR3133294 ↑3, 10, 16
- [Lan74] Serge Lang, *Higher dimensional diophantine problems*, Bull. Amer. Math. Soc. **80** (1974), 779–787. MR360464 ↑6
- [Lan86] ———, *Hyperbolic and Diophantine analysis*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), no. 2, 159–205. MR828820 ↑6
- [LT02] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77. ↑3, 7, 8, 9
- [Maz00] Barry Mazur, *Abelian varieties and the Mordell-Lang conjecture*, Model theory, algebra, and geometry, 2000, pp. 199–227. MR1773708 (2001e:11061) ↑6
- [Maz86] B. Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), no. 2, 207–259. MR828821 (88e:11050) ↑6

- [McC94] William G. McCallum, *On the method of Coleman and Chabauty*, Math. Ann. **299** (1994), no. 3, 565–596. MR1282232 ↑2
- [MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, 2012, pp. 99–117. MR3098132 ↑2, 3, 4, 5, 7, 8
- [Pac97] Patricia L. Pacelli, *Uniform boundedness for rational points*, Duke Math. J. **88** (1997), no. 1, 77–102. MR1448017 ↑6
- [Pac99] ———, *Uniform bounds for stably integral points on elliptic curves*, Proc. Amer. Math. Soc. **127** (1999), no. 9, 2535–2546. MR1676288 ↑6
- [Poo02] Bjorn Poonen, *Computing rational points on curves*, Number theory for the millennium, III (Urbana, IL, 2000), 2002, pp. 149–172. ↑5
- [Poo18] ———, *Heuristics for the arithmetic of elliptic curves*, Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. II. Invited lectures, 2018, pp. 399–414. MR3966772 ↑7
- [Poo96] ———, *Computational aspects of curves of genus at least 2*, Algorithmic number theory (Talence, 1996), 1996, pp. 283–306. MR1446520 (98c:11059) ↑5
- [PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903. MR3985613 ↑7
- [PS14] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166. MR3245014 ↑2
- [PSS07] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$* , Duke Math. J. **137** (2007), no. 1, 103–158. MR2309145 (2008i:11085) ↑2
- [RZB15] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over \mathbb{Q} and 2-adic images of Galois representations*, Research in Number Theory, Accepted (2015). ↑2
- [Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. ↑8
- [Sko34] Thoralf Skolem, *Ein verfahren zur behandlung gewisser exponentialer gleichungen und diophantischer gleichungen*, C. r **8** (1934), 163–188. ↑2
- [Sma97] N. P. Smart, *S-unit equations, binary forms and curves of genus 2*, Proc. London Math. Soc. (3) **75** (1997), no. 2, 271–307. MR1455857 ↑5
- [Sto06] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661 (2007m:14025) ↑3, 10
- [Sto19] ———, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 3, 923–956. MR3908770 ↑3, 8, 16
- [Voj91] P. Vojta, *Siegel’s theorem in the compact case*, Ann. of Math. (2) **133** (1991), no. 3, 509–548. MR1109352 (93d:11065) ↑2, 7

DEPT. OF MATHEMATICS, EMORY UNIVERSITY, ATLANTA, GA 30322 USA

E-mail address: dzb@mathcs.emory.edu

2020 ARIZONA WINTER SCHOOL PROJECT NOTES: “ABELIAN CHABAUTY”

DAVID ZUREICK-BROWN AND JACKSON MORROW

Last update: March 3, 2020

1. SUGGESTIONS FOR PREPARATION

For almost all of our proposed projects, it is essential to have a working knowledge of Chabauty’s method. In addition to the “Abelian Chabauty” course notes, we recommend starting with McCallum and Poonen’s survey [MP12].

For the more computational projects, we recommend Poonen’s surveys [Poo96] and [Poo02]. More importantly, it is important to quickly come up with speed with how to perform Chabauty’s method in Magma. Magma has a free, limited use online calculator here

<http://magma.maths.usyd.edu.au/calc/>,

and a thoroughly documented implementation of Chabauty’s method

<http://magma.maths.usyd.edu.au/magma/handbook/text/1533>.

Even better is to obtain a copy for your laptop, or ssh access to a departmental server with a copy of Magma. The Simons Foundation has graciously made Magma freely available to mathematicians working in the US

<http://magma.maths.usyd.edu.au/magma/ordering/>;

please contact your department’s tech staff, who should be able to help you obtain a copy of Magma through this agreement.

Finally a very useful exercise is to take Smart’s list of the 427 genus 2 curves with good reduction away from 2, and provably find all of the rational points on them. I have set up a temporary folder at my web page

<http://www.math.emory.edu/~dzb/AWS2020>

containing several references, and containing a subfolder titled “preparatory-Magma-exercise” with instructions for this exercise.

2. PROJECT DESCRIPTIONS

Project 1. Quadratic points on modular curves. The goal is of this project is to determine the K -rational points on certain modular curves using a modification of Chabauty’s method, where K is a quadratic number field. More precisely, there is a heuristic of Siksek and Wetherell [Sik13] saying that for a nice curve X/\mathbb{Q} , a Chabauty-type method could bound the number of K -rational points on a curve X of genus g under the weaker assumption that $J_X(K)$ has rank $r \leq d(g - 1)$ where $d = [K : \mathbb{Q}]$.

Date: March 3, 2020.

The works of [BN15, OS19] focused on determining the quadratic points on the modular curves $X_0(N)$ of genus ≤ 5 with Mordell–Weil rank 0, and the work of [Box19] studied the cases when the Mordell–Weil rank is positive. The modular curve $X_0(37)$ stands out because it has genus 2, positive Mordell–Weil rank, and two sources of infinitely many quadratic points: one coming from the hyperelliptic map $X_0(37) \rightarrow \mathbb{P}^1$ and one coming from the quotient by the Atkin–Lehner involution $X_0(37) \rightarrow X_0(37)^+$ [Box19, Section 5].

While the project heading is quite broad, it would be interesting to start with a study of the quadratic points on $X_0(37)$ and to see when the heuristic of Siksek and Wetherell can be applied. More precisely:

- (1) For $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}),$ and $\mathbb{Q}(\sqrt{-3})$, can one provably determine $X_0(37)(K)$ using the heuristic of Siksek and Wetherell? Are there other quadratic fields K (perhaps real quadratic field) where $X_0(37)(K)$ can be provably determined?
- (2) For the above mentioned fields K , can one determine where the quadratic points come from using the geometry of $X_0(37)$?
- (3) For $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}),$ and $\mathbb{Q}(\sqrt{-3})$, can one provably determine $X_0(43)(K)$ using the heuristic of Siksek and Wetherell?

Recommended reading. A discussion of the heuristic of Siksek and Wetherell can be found at [Sik13], and for a detailed example of the heuristic of Siksek and Wetherell, we recommend reading [Doy18, Appendix A]. We also recommend the works [BN15, OS19, Box19] for thorough discussions of quadratic points on modular curves.

Project 2. Rank functions for special families of curves. The goal of this project is to improve the “rank favorable” bounds on the rank functions that arise in [Sto06] and [KZB13] for special curves (e.g., trigonal). This project would involve very little p -adic analysis; the techniques are more akin to the geometry of curves and combinatorics.

Recommended reading. We recommend reading [Sto06] and [KZB13] to get an understanding for the rank functions involved in their work.

Project 3. Rank favorable bounds for special families of curves. In [Sto13], Stoll proved uniform bounds on rational points of hyperelliptic curves over \mathbb{Q} with low Mordell–Weil, where the bounds incorporate the Mordell–Weil rank of the curve (i.e., the lower the Mordell–Weil rank of the hyperelliptic curve is the better the bound becomes). A key ingredient in getting rank favorable uniform bounds is that one has an explicit description of the differentials on a hyperelliptic curve which helps with the “ p -adic analysis” part of the arguments. Moreover, one can hope to find rank favorable uniform bounds for special families of curves where one has an explicit description of differentials. In [Kan17], Kantor accomplished this by determining rank favorable uniform bounds for superelliptic curves.

The goal of this project is to determine rank favorable uniform bounds for “special” families of curves, where one has an explicit description of differentials. Here is a guideline:

- (1) Determine uniform bounds for non-hyperelliptic genus 3 curves (i.e., plane quartics) of Mordell–Weil rank 0.
- (2) Determine uniform bounds for plane curves of low Mordell–Weil rank.

The main theorem of [KRZB15] gives uniform bounds in both of these cases, but we anticipate that one can obtain much better bounds in both cases.

Recommended reading. We recommend [KRZB18] for a survey of the techniques involved in determining uniform bounds for curves of low Mordell–Weil rank. Also, we recommend the original works of Stoll [Sto13] and Katz–Rabinoff–Zureick–Brown [KRZB15].

Project 4. Uniform bounds for the d th symmetric products of curves with small rank. The goal of this project is to combine works on symmetric power Chabauty and on uniform bounds for curves of low Mordell–Weil rank to obtain uniform bounds for the d th symmetric products of curves with low Mordell–Weil rank. In [VW17], Vemulapalli–Wang determined uniform bounds for symmetric squares of curves of low Mordell–Weil rank, which also satisfy another technical assumption (cf. [GM17, Assumption 5.7(†)]).

Once participants have an understanding of the tools involved in symmetric power Chabauty and in the works on uniform bounds for curves of low Mordell–Weil rank (e.g., p -adic analysis, non-Archimedean geometry, and some tropical geometry), the project boils down to a problem in combinatorics. Here is a guideline:

- (1) Determine how small the Mordell–Weil rank of a curve needs to be in order to incorporate the symmetric power Chabauty and uniform bound techniques.
- (2) Find uniform bounds for the d th symmetric product of curves with the above rank condition.

Recommended reading. We recommend [Sik09] for the foundations of symmetric power Chabauty and [GM17] for how to use tropical techniques to make symmetric power Chabauty explicit. Also, the work [VW17] illustrates the combinatorial nature of the project.

Project 5. Avoiding d th symmetric powers in a $d+1$ st symmetric power. It would be interesting, but possibly substantial, to improve the work of Siksek and Box to the case where $\text{Sym}^d X(\mathbb{Q})$ is infinite, and to find the points of $\text{Sym}^{d+1} X(\mathbb{Q})$ which are not in the image of $X(\mathbb{Q}) \times \text{Sym}^d X(\mathbb{Q}) \rightarrow \text{Sym}^{d+1} X(\mathbb{Q})$.

As an example: there are several composite, but non prime power, level modular curves that arise naturally in “Mazur’s program B” for which the determination of rational points has some particular challenging aspect. The example that inspired this is the following. The modular curve $X_0(65)$ is genus 5, and not trigonal; there are finitely many cubic points on $X_0(65)$. However, $\text{Sym}^3 X_0(65)(\mathbb{Q})$ is not finite. The Jacobian $J_0(65)$ decomposes as $E \times A_1 \times A_2$, where E is a rank 1 elliptic curve, and both A_i are geometrically simple rank 0 abelian surfaces; moreover, the optimal map $X_0(65) \rightarrow E$ has degree 2. Since $X_0(65)$ has rational points (the 4 cusps), there are 4 “copies” of $\text{Sym}^2 X_0(65)(\mathbb{Q})$ lying on $\text{Sym}^3 X_0(65)(\mathbb{Q})$. In particular, $\text{Sym}^3 X_0(65)(\mathbb{Q})$ is infinite, but only finitely many rational points of $\text{Sym}^3 X_0(65)$ do not lie on one of the copies of $\text{Sym}^2 X_0(65)(\mathbb{Q})$.

Recommended reading. Suppose that X is a curve and $f: X \rightarrow C$ is a degree d map. This gives rise to a map $C \rightarrow \text{Sym}^d X$. When $C(\mathbb{Q})$ is infinite (e.g., C is \mathbb{P}^1 or a positive rank elliptic curve), this gives rise to infinitely many degree d points on X .

The papers [Sik09] and [Box19] explain how to determine the degree d points of X which do not arise from C . We are hopeful that a modification of their argument will work.

Project 6. Improved rank favorable bounds. This project is recommended for anyone who is looking for a purely combinatorial project.

The “rank favorable bounds” part of my lecture notes discusses the following theorem.

Theorem 2.1 (Stoll [Sto06]; Katz, Zureick-Brown, [KZB13]). *Let X/\mathbb{Q} be a curve of genus g and let $r = \text{rank } \text{Jac}_X(\mathbb{Q})$. Suppose $p > 2r + 2$ is a prime, that $r < g$, and let \mathcal{X} be a proper regular model of X over \mathbb{Z}_p . Then*

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}_{\mathbb{F}_p}^{\text{sm}}(\mathbb{F}_p) + 2r.$$

Actually, Stoll observed that if X is not hyperelliptic, then one can further improve the $2r$ term in the bound. Define

$$f_X(r) = \max \{ \deg(D) \mid D \geq 0 \text{ and } \dim H^0(X, \Omega^1(-D)) \geq g - r \};$$

then $f(r) \leq 2r$ (for $0 \leq r < g$), with equality if and only if X is hyperelliptic, and the bound in Stoll's theorem is actually

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + f(r).$$

See [Sto06, Section 3].

The bound in the bad reduction case can be similarly improved, if one instead defines

$$f_{\Gamma}(r) = \max \{ \deg(D) \mid D \geq 0, \text{ and } \dim r(K - D) \geq g - r - 1 \}$$

for a graph Γ with canonical divisor K . Here, one can work with either the “numerical rank” (i.e., the notion of rank from [Bak08, 1.3]), or the “abelian rank” (from [KZB13, 3.3]).

Problem: Understand $f(r)$ for non-hyperelliptic graphs. (See [BN09] for the notion of hyperelliptic graph.) For example:

- We know that if $f(r) = 2r$, then Γ is hyperelliptic. Contrapositively, if Γ is not hyperelliptic, then $f(r) < 2r$. Can we characterize graphs such that $f(r) < 2r - 1$?
- Find interesting families for which $f(r)$ is small. (For example: what happens for trigonal graphs, or for graphs with extra automorphisms?)

Project 7. A curve with many rational points. The “Elkies–Stoll” curve

$$\begin{aligned} X : y^2 &= 82342800x^6 - 470135160x^5 + 52485681x^4 + \\ &2396040466x^3 + 567207969x^2 - 985905640x + 247747600 \end{aligned}$$

has at least 642 rational points, and its Jacobian has rank 22. See

<http://www.mathe2.uni-bayreuth.de/stoll/recordcurve.html>

for a full list of the known points.

It would be interesting to prove that $\#X(\mathbb{Q})$ is **exactly** 642. Reducing mod a few primes of good reduction verifies that $\text{Jac}_X(\mathbb{Q})_{\text{tors}}$ is trivial. Magma's RankBound command computes that the rank is at most 22, and differences of known points generate a subgroup of rank 22; [MS16, Proposition 19.1] proves that the subgroup generated by the known points is the full group, and exhibits explicit generators.

Problem: Prove that $\#X(\mathbb{Q}) = 642$.

Chabauty's method is clearly not applicable (since $22 \geq 2$). One untested idea is to pass to a field extension where X attains a 2-torsion point and to attempt a combination of étale descent and elliptic Chabauty. (Of course, there are a few things that need to go right, and it is possible that this approach won't work; but, if it doesn't work, it would be useful to

know that! There is a longer interesting list of curves at [Sto09, Figure 5] for which it would be interesting to provably compute $X(\mathbb{Q})$.)

Update, added March 2. The field one would need to work over for this problem has degree 15, which is probably too large to do computations with, even assuming GRH (though I would prefer to be proven wrong!). There are a few simpler, but still interesting, curves with many points that are easier to study. In the document

http://www.math.harvard.edu/~elkies/many_pts.pdf

Elkies discusses several examples. The record before the Elkies–Stoll curve above was due to Keller-Kulesz; the curve

$$X_2: y^2 = 278271081x^2(x^2 - 9)^2 - 229833600(x^2 - 1)^2$$

has 588 rational points, and it obtains a 2-torsion point over a quadratic extension. Moreover, its Jacobian is isogenous to the square of an elliptic curve of rank at least 12. It would be interesting to determine $X_2(\mathbb{Q})$ explicitly.

See also [Poo96, Section 8] for a discussion of other interesting examples.

Recommended reading. Poonen’s surveys [Poo96] and [Poo02] are a good start. The paper [RZB15] has several examples of similar (but easier) computations (for example Subsections 8.3 and 9.2; see also the accompanying transcript of computations [RZB]).

Poonen’s notes “Lectures on rational points on curves”, available at

<http://www-math.mit.edu/~poonen/papers/curves.pdf>

are also a great resource.; see for example Section 7 on étale descent.

Project 8. Point Count Records. The uniformity conjecture is the following.

Conjecture 2.2 ([CHM97]). Let K be a number field and let $g \geq 2$ be an integer. There exists a constant $B_g(K)$ such that for every smooth curve X over K of genus g , the number $\#X(K)$ of K -rational points is at most $B_g(K)$.

This famously follows from Lang’s conjecture, and inspired a large effort to compute lower bounds on the constants $B_g(K)$. It would be interesting to take another look at the literature, starting with [Poo96, Section 8],

http://www.math.harvard.edu/~elkies/many_pts.pdf,

[Sto09] (and possibly some of the papers discussed there, such as [Kul98, Kul95, KK95]), and to see if the methods there can be improved (especially for fields $K \neq \mathbb{Q}$). For example: it would be really interesting to generate examples of genus 2 curves over \mathbb{Q} with a very large number of quadratic points; such a curve would likely have very large rank (and as of now, we have better records for ranks of elliptic curves (28) than ranks of simple abelian surfaces (22, I think)).

Project ∞ . Rational points on (symmetric powers of) modular curves. Find every rational point on every (symmetric power of every) modular curve. More seriously: there are several interesting examples of modular (in some appropriate sense) curves, and one collection of projects is to study, via Chabauty and other explicit methods, the rational points on these curves.

Recommended reading. We recommend taking a look at [RZB15] and [Poo02].

REFERENCES

- [Bak08] Matthew Baker, *Specialization of linear systems from curves to graphs*, Algebra Number Theory **2** (2008), no. 6, 613–653. With an appendix by Brian Conrad. MR2448666 (2010a:14012) ↑4
- [BN09] M. Baker and S. Norine, *Harmonic morphisms and hyperelliptic graphs*, Int. Math. Res. Not. IMRN **15** (2009), 2914–2955. MR2525845 (2010e:14031) ↑4
- [BN15] Peter Bruin and Filip Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS Journal of Computation and Mathematics **18** (2015), no. 1, 578–602. ↑2
- [Box19] Joshua Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Preprint arXiv:1906.05206 (2019). ↑2, 3
- [CHM97] Lucia Caporaso, Joe Harris, and Barry Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35. MR1325796 (97d:14033) ↑5
- [Doy18] John R Doyle, *Preperiodic points for quadratic polynomials over cyclotomic quadratic fields*, Preprint arXiv:1801.09003 (2018). ↑2
- [GM17] Joseph Gunther and Jackson S Morrow, *Irrational points on random hyperelliptic curves*, Preprint arXiv:1709.02041 (2017). ↑3
- [Kan17] Noam Kantor, *Rank-favorable bounds for rational points on superelliptic curves of small rank*, Preprint arXiv:1708.09120 (2017). ↑2
- [KK95] Wilfrid Keller and Leopoldo Kulesz, *Courbes algébriques de genre 2 et 3 possédant de nombreux points rationnels*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 11, 1469–1472. MR1366103 ↑5
- [KRZB15] Eric Katz, Joseph Rabinoff, and David Zureick-Brown, *Uniform bounds for the number of rational points on curves of small mordell–weil rank*, preprint arXiv:1504.00694 (2015). ↑2, 3
- [KRZB18] ———, *Diophantine and tropical geometry, and uniformity of rational points on curves*, Algebraic geometry: Salt Lake City 2015, 2018, pp. 231–279. MR3821174 ↑3
- [Kul95] Leopoldo Kulesz, *Courbes algébriques de genre 2 possédant de nombreux points rationnels*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 1, 91–94. MR1340089 ↑5
- [Kul98] ———, *Courbes algébriques de genre ≥ 2 possédant de nombreux points rationnels*, Acta Arith. **87** (1998), no. 2, 103–120. MR1665199 ↑5
- [KZB13] Eric Katz and David Zureick-Brown, *The Chabauty–Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions*, Compos. Math. **149** (2013), no. 11, 1818–1838. MR3133294 ↑2, 4
- [MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, 2012, pp. 99–117. MR3098132 ↑1
- [MS16] Jan Steffen Müller and Michael Stoll, *Canonical heights on genus-2 Jacobians*, Algebra Number Theory **10** (2016), no. 10, 2153–2234. MR3582017 ↑4
- [OS19] Ekin Ozman and Samir Siksek, *Quadratic points on modular curves*, Math. Comp. **88** (2019), no. 319, 2461–2484. MR3957901 ↑2
- [Poo02] Bjorn Poonen, *Computing rational points on curves*, Number theory for the millennium, III (Urbana, IL, 2000), 2002, pp. 149–172. ↑1, 5, 6
- [Poo96] ———, *Computational aspects of curves of genus at least 2*, Algorithmic number theory (Talence, 1996), 1996, pp. 283–306. MR1446520 (98c:11059) ↑1, 5
- [RZB15] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over \mathbb{Q} and 2-adic images of Galois*, Res. Number Theory **1** (2015), Art. 12, 34. MR3500996 ↑5, 6
- [RZB] ———, *Electronic transcript of computations for the paper ‘Elliptic curves over \mathbb{Q} and 2-adic images of Galois’*. Available at <http://users.wfu.edu/rouseja/2adic/>. (Also attached at the end of the tex file.) ↑5
- [Sik09] Samir Siksek, *Chabauty for symmetric powers of curves*, Algebra Number Theory **3** (2009), no. 2, 209–236. ↑3

- [Sik13] ———, *Explicit Chabauty over number fields*, Algebra Number Theory **7** (2013), no. 4, 765–793. MR3095226 ↑1, 2
- [Sto06] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661 (2007m:14025) ↑2, 4
- [Sto09] ———, *On the average number of rational points on curves of genus 2*, arXiv preprint arXiv:0902.4165 (2009). ↑5
- [Sto13] ———, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell–Weil rank*, arXiv preprint arXiv:1307.1773 (2013). ↑2, 3
- [VW17] Sameera Vemulapalli and Danielle Wang, *Uniform bounds for the number of rational points on symmetric squares of curves with low Mordell–Weil rank*, Preprint arXiv:1708.07057 (2017). ↑3

DEPT. OF MATHEMATICS, EMORY UNIVERSITY, ATLANTA, GA 30322 USA

Email address: dzb@mathcs.emory.edu

DEPT. OF MATHEMATICS, EMORY UNIVERSITY, ATLANTA, GA 30322 USA

AWS 2020: Selmer varieties and non-abelian descent

Minhyong Kim

This course will outline the theory of Selmer varieties. We will describe their construction, some known properties, associated reciprocity laws and their application to Diophantine problems. A rough course outline might look like this:

- I. Motivational introduction: a review of elliptic curves, descent, and the conjectures of Birch and Swinnerton-Dyer. Brief overview of the Diophantine geometry of curves of higher genus. Arithmetic fundamental groups of elliptic curves.
- II. Arithmetic fundamental groups in general. Unipotent completions. Galois actions on fundamental groups. Some preliminary work on the projective line minus three points. De Rham and crystalline fundamental groups. A brief overview of Deligne's long paper on this topic.
- III. Non-abelian cohomology. Construction of local and global moduli spaces of principal bundles. p -adic Hodge theory and iterated integrals. Another view of Deligne. Applications to Siegel's theorem.
- IV. Finiteness theorems and connections to mixed motives. Grothendieck's section conjecture and effective computation of rational points. Non-abelian reciprocity.
- V. Some speculation on effective computation of Selmer varieties. A return to the projective line minus three points. Punctured elliptic curves with complex multiplication and p -adic L-functions.

A project might involve going through some of the existing papers on effective computations of rational or integral points and making precise the equations for Selmer varieties contained therein. If things go well, we can try to compute some Selmer varieties for punctured elliptic curves with CM. This project will be suitable for students with some background in algebraic and arithmetic geometry including some familiarity with elliptic curves, Galois representations, and knowledge of arithmetic cohomologies or a willingness to work with them as a blackbox that gradually lights up. Some knowledge of the algebraic number theory of local and global fields will also be helpful.

References

- [1] Balakrishnan, Jennifer; Dogra, Netan; Mller, J. Steffen; Tuitman, Jan; Vonk, Jan Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math.* (2) 189 (2019), no. 3, 885–944.
- [2] Balakrishnan, Jennifer S.; Dan-Cohen, Ishai; Kim, Minhyong; Wewers, Stefan A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. *Math. Ann.* 372 (2018), no. 1-2, 369–428.
- [3] Balakrishnan, Jennifer S.; Dogra, Netan An effective Chabauty-Kim theorem. *Compos. Math.* 155 (2019), no. 6, 1057–1075.
- [4] Balakrishnan, Jennifer S.; Dogra, Netan Quadratic Chabauty and rational points, I: p -adic heights. With an appendix by J. Steffen Mller. *Duke Math. J.* 167 (2018), no. 11, 1981–2038.
- [5] Balakrishnan, Jennifer S.; Besser, Amnon; Mller, J. Steffen Quadratic Chabauty: p -adic heights and integral points on hyperelliptic curves. *J. Reine Angew. Math.* 720 (2016), 51–79.
- [6] Betts, Luke Alexander The motivic anabelian geometry of local heights on abelian varieties. arXiv:1706.04850

- [7] Dan-Cohen, Ishai; Wewers, Stefan Mixed Tate motives and the unit equation. *Int. Math. Res. Not.* IMRN 2016, no. 17, 5291–5354.
- [8] Le groupe fondamental de la droite projective moins trois points. Galois groups over \mathbb{Q} (Berkeley, CA, 1987), 79–297, *Math. Sci. Res. Inst. Publ.*, 16, Springer, New York, 1989.
- [9] Arithmetic Gauge Theory: A Brief Introduction *Modern Physics Letters A*. Volume 33, Issue 29 (2018).
- [10] Kim, Minhyong The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.* 161 (2005), no. 3, 629–656.
- [11] Kim, Minhyong p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication. *Ann. of Math.* (2) 172 (2010), no. 1, 751–759.
- [12] Kim, Minhyong Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.* 23 (2010), no. 3, 725–747.
- [13] Kim, Minhyong Tangential localization for Selmer varieties. *Duke Math. J.* 161 (2012), no. 2, 173199.
- [14] Kim, Minhyong Remark on fundamental groups and effective Diophantine methods for hyperbolic curves. *Number theory, analysis and geometry*, 355–368, Springer, New York, 2012.
- [15] Kim, Minhyong Diophantine geometry and non-abelian reciprocity laws I. Elliptic curves, modular forms and Iwasawa theory, 311–334, *Springer Proc. Math. Stat.*, 188, Springer, Cham, 2016.
- [16] Kim, Minhyong Kim, Minhyong Principal bundles and reciprocity laws in number theory. *Algebraic geometry: Salt Lake City 2015*, 305–318, *Proc. Sympos. Pure Math.*, 97.2, Amer. Math. Soc., Providence, RI, 2018.
- [17] Kim, Minhyong The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.* 45 (2009), no. 1, 89–133.
- [18] Kim, Minhyong; Tamagawa, A. The l-component of the unipotent albanese map. *Math. Ann.* 340 (2008), no. 1, 223–235.
- [19] Pridham, Jonathan Non-abelian reciprocity laws and higher Brauer-Manin obstructions. arXiv:1704.03021.

Equations for Selmer varieties: project brief

February 4, 2020

Let S be a finite set of (rational) primes and \mathcal{X}/\mathbb{Z}_S a suitable model of a hyperbolic curve X/\mathbb{Q} . A central role in the non-abelian Chabauty method is played by the (global) *Selmer variety* $\text{Sel}_{S,U}(\mathcal{X})$ [1, §2 & §8] corresponding to a suitable quotient U of the \mathbb{Q}_p -pro-unipotent étale fundamental group of X (at a rational basepoint). Whenever the localisation map $\text{loc}: \text{Sel}_{S,U}(\mathcal{X}) \rightarrow H_f^1(G_p, U)$ is non-dominant – for instance for dimension reasons – the set $\mathcal{X}(\mathbb{Z}_S)$ of S -integral points is finite. More precisely, each defining equation of the (scheme-theoretic) image of the localisation map gives rise to a p -adic analytic function on $\mathcal{X}(\mathbb{Z}_p)$ vanishing on $\mathcal{X}(\mathbb{Z}_S)$, and by understanding these functions one can often compute the set $\mathcal{X}(\mathbb{Z}_S)$ in practice.

The broad aim of this project is to understand the equations cutting out the image of the localisation map. There are several key examples in the literature where the non-abelian Chabauty method has been made explicit (to varying extents), including:

1. the quadratic Chabauty method [2, 3];
2. explicit Chabauty–Kim for $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ [4, 5]; and
3. the contributions from places $\ell \in S$ [6].

The first part of this project will consist of collating these examples and recasting them in the language of equations for Selmer images.

Once these examples have been collated, the second part of the project will be to explore several new examples where explicit equations for Selmer varieties can be found, and then to use these to determine rational or S -integral points. The main example we will consider is determining S -integral points on $\mathcal{X} = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ for $\#S = 2$. Using the refined Selmer varieties of [6], one expects the Selmer image to be cut out by quadratic relations in depth 2 (i.e. for the 2-step unipotent quotient U_2), and we will identify exactly what these relations are. Using this, we will compute $\mathcal{X}(\mathbb{Z}_p)_{S,U_2}$ in small cases (esp. $S = \{2, 3\}$), and compare it to $\mathcal{X}(\mathbb{Z}_S)$.

Project requirements

You should already have a basic understanding of the workings of non-abelian Chabauty and the theory of Selmer varieties: what they are and how one controls

their dimension. An understanding of iterated Coleman integration is helpful for the latter parts of the project, but not necessary. You should be willing to familiarise yourself with the contents of at least one of the papers [2, 3, 4, 5, 6] before the winter school and present the main results to the rest of the group.

References

- [1] J. Balakrishnan, I. Dan-Cohen, M. Kim, S. Wewers: *A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves*, Mathematische Annalen, 372(2018), no. 1-2, 369–428. arXiv:1209.0640 (v4)
- [2] J. Balakrishnan, N. Dogra: *Quadratic Chabauty and rational points I: p-adic heights* (with appendix by J.S. Müller), Duke Mathematical Journal, 167(2018), no. 11, 1981–2038. arXiv:1601.00388 (v2)
- [3] J. Balakrishnan, N. Dogra: *Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties*, International Mathematics Research Notices (to appear). arXiv:1705.00401 (v2)
- [4] I. Dan-Cohen, S. Wewers: *Mixed Tate motives and the unit equation*, International Mathematics Research Notices, (2016), no. 17, 5291–5354. arXiv:1311.7008 (v3)
- [5] I. Dan-Cohen: *Mixed Tate motives and the unit equation II*, Algebra and Number Theory (to appear). arXiv:1510.01362 (v2)
- [6] L.A. Betts, N. Dogra: *The local theory of unipotent Kummer maps and refined Selmer varieties*. arXiv:1909.05734 (v2)

Selmer Schemes I

Minhyong Kim

Tucson, March, 2019

Disclaimer

These lecture slides come with a bibliography at the end. However, there has been no attempt at accurate attribution of mathematical results. Rather, the list mostly contains works the lecturer has consulted during preparation, which he hopes will be helpful for users.

I. Background: Arithmetic of Algebraic Curves

Arithmetic of algebraic curves

X : a smooth algebraic curve of genus g defined over \mathbb{Q} .

For example, given by a polynomial equation

$$f(x, y) = 0$$

of degree d with rational coefficients, where

$$g = (d - 1)(d - 2)/2.$$

Diophantine geometry is concerned with the set $X(\mathbb{Q})$ of rational solutions.

Structure is quite different in the three cases:

$g = 0$, spherical geometry (positive curvature);

$g = 1$, flat geometry (zero curvature);

$g \geq 2$, hyperbolic geometry (negative curvature).

Arithmetic of algebraic curves: $g = 0, d \leq 2$

Even now (after millennia of studying these problems), $g = 0$ is the only case that is completely understood.

For $g = 0$, techniques reduce to class field theory and algebraic geometry: local-to-global methods, generation of solutions via sweeping lines, etc.

Idea is to study \mathbb{Q} -solutions by considering the geometry of solutions in various completions, the local fields

$$\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \dots, \mathbb{Q}_{691}, \dots,$$

Arithmetic of algebraic curves: $g = 0$

Local-to-global methods sometimes allow us to ‘globalise’. For example [Serre],

$$37x^2 + 59y^2 - 67 = 0$$

has a \mathbb{Q} -solution if and only if it has a solution in each of $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_{37}, \mathbb{Q}_{59}, \mathbb{Q}_{67}$, (Hasse principle) a criterion that can be effectively implemented.

If the existence of a solution is guaranteed, it can be found by an exhaustive search. From one solution, there is a method for parametrising all others: From $(0, -1)$, generate solutions

$$\left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right)$$

to $x^2 + y^2 = 1$.

Arithmetic of algebraic curves: $g = 0$

In other words, there is a successful study of the inclusion

$$X(\mathbb{Q}) \subset X(\mathbb{A}_{\mathbb{Q}}) = \prod' X(\mathbb{Q}_p)$$

coming from **reciprocity laws**.

Arithmetic of algebraic curves: $g = 1$ ($d = 3$)

$X(\mathbb{Q}) = \phi$, non-empty finite, infinite, all are possible.

Hasse principle fails:

$$3x^3 + 4y^3 + 5 = 0$$

has points in \mathbb{Q}_v for all v , but no rational points.

If $X(\mathbb{Q}) \neq \phi$, then fixing an origin $O \in X(\mathbb{Q})$ gives $X(\mathbb{Q})$ the structure of a finitely-generated abelian group via the chord-and-tangent method:

$$X(\mathbb{Q}) \simeq X(\mathbb{Q})_{tor} \times \mathbb{Z}^r.$$

Here, r is called the rank of the curve and $X(\mathbb{Q})_{tor}$ is a finite effectively computable abelian group.

Arithmetic of algebraic curves: $g = 1$

To compute $X(\mathbb{Q})_{tor}$, write

$$X := \{y^2 = x^3 + ax + b\} \cup \{\infty\}$$

$(a, b \in \mathbb{Z})$.

Then $(x, y) \in X(\mathbb{Q})_{tor} \Rightarrow x, y$ are integral and

$$y^2 | (4a^3 + 27b^2).$$

Arithmetic of algebraic curves: $g = 1$

However, the algorithmic computation of the rank and a full set of generators for $X(\mathbb{Q})$ is very difficult, and is the subject of the conjecture of Birch and Swinnerton-Dyer.

In practice, it is often possible to compute these. For example, for

$$y^2 = x^3 - 2,$$

Sage will give you $r = 1$ and the point $(3, 5)$ as generator.

Note that

$$2(3, 5) = (129/100, -383/1000)$$

$$3(3, 5) = (164323/29241, -66234835/5000211)$$

$$4(3, 5) = (2340922881/58675600, 113259286337279/449455096000)$$

Arithmetic of algebraic curves: $g = 1$

3
 100
 2041
 125723613593509407457
 51127310073606144900
 34851910470516704471441
 3010634928798730717842957991799140
 125723613593509407457
 13295632536 19216306163748139417326301623493250
 91020566473629269393925903734818516645916463953957939242680660
 4768082743467146765704014395717230915147490143279572579397894415975440
 51295669917125723613593509407457
 1651577320861379566324940545 563518273093891402467184930993112202652114149838004
 204793813598781472909886793492114001051957932299875760421630264817744645832023274147545169954197412293264949521
 32794043552793040445148512435165242491609971746164948163059123161951672205452666649935343035751773594913804394492172900
 10767534976491822164163534909444958052248794 220498497400772288710005462345971749416191922075936327070747700891430932980095951689712053310641
 977049679725746792194695 477264545604441339239212943971349492121294871895489979491181948861590970725597580707176161259016310149624476561485485493113676168100
 168361217610197531956910907035338767344071314094931010201389274146251616471423176877541411217923100091543490490086465314902151515761612301880091551344419951121574499801
 107054832149735913613553242598601191465271630 2873476194914101493790703418140571833102035772021582670542566917851162949489498189212707174880819399516954701765212759337637875277292168364292129690000
 114844192354910916517044015305461244162716494787346 16964545922115539706712467800514747273243175 65626862416761768481697324671413574310295141826499774412257649 215562727326217049940144407617358672139322022793978891046143215342
 2057527711799122845452159786442932925898740997534412045414571397155861765108524025245252510721761635634997158017130171293226511913237789944691513152378389440974335220141792426691
 13898570167075952411447490004005234 202544888323892900781058054291829046912793102576716889396599649358097463 149992948671448451036197631068577766559495288194475483444411303462379678676870169412566114495794319421607450213217903197320144951631221043
 1766627813621492727445727675791609446757519724337147712254813151793281604163910454756868442926272645144948347472422716072880876460578939314073045351515163124046221254793211226552268691686359215293623467315624893402291517937529592100716953537446052478784015462445459157429169913240160
 6147432071086841653688113679164143357766130913856935879545153954317021785407190572412036261447703935776642929176492092120039210515256647429092305369569747454257452774073751790863277714929521364237521
 45194363797225458163510227363464997071714481255212025891247767615212676408914048944064573201330789531407202346779585045907881171651684939712244425737034910083567102474623714476461676957710494916517457845245214989717801106596648142772624293012593853119887725242164576912998867912954483500642620900
 4244993224391194251749893442563920571863553249535355579466611572179138586726158263520753374316430441563239301972908043187723202383140818397591511777202470769134945994466342598975161932991349271924724971793967313367345011534119157422416168882427516877293910690539997254616837331334611594468712667395186556425541232363917029951227571610227341

Figure: Denominators of $N(3, 5)$

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

$X(\mathbb{Q})$ is always finite (Mordell conjecture [Faltings])

However, *very* difficult to compute: consider

$$x^n + y^n = 1$$

for $n \geq 4$.

Sometime easy, such as

$$x^4 + y^4 = -1.$$

However, when there isn't an obvious reason for non-existence, e.g., there already is one solution, then it's hard to know when you have the full list. For example,

$$y^3 = x^6 + 23x^5 + 37x^4 + 691x^3 - 631204x^2 + 5168743489$$

obviously has the solution $(0, 1729)$, but are there any others?

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

Effective Mordell problem:

Find a terminating algorithm: $X \mapsto X(\mathbb{Q})$

The **Effective Mordell conjecture** (Szpiro, Vojta, ABC, ...) makes this precise using height inequalities.

Will describe an approach to this problem using the arithmetic geometry of principal bundles.

II. Arithmetic Principal Bundles

Arithmetic principal bundles: (G_K, R, P)

K : field of characteristic zero.

$G_K = \text{Gal}(\bar{K}/K)$: absolute Galois group of K .

A group over K is a topological group R with a continuous action of G_K by group automorphisms:

$$G_K \times R \longrightarrow R.$$

A principal R -bundle over K is a topological space P with compatible continuous actions of G_K (left) and R (right, simply transitive):

$$P \times R \longrightarrow P;$$

$$G_K \times P \longrightarrow P;$$

$$g(zr) = g(z)g(r)$$

for $g \in G_K$, $z \in P$, $r \in R$.

Arithmetic principal bundles: (G_K, R, P)

Note that P is *trivial*, i.e., $\cong R$, exactly when there is a fixed point $z \in P^{G_K}$:

$$R \cong z \times R \cong P.$$

Arithmetic principal bundles

Example:

$$R = \mathbb{Z}_p(1) := \varprojlim \mu_{p^n},$$

where $\mu_{p^n} \subset \bar{K}$ is the group of p^n -th roots of 1.

Thus,

$$\mathbb{Z}_p(1) = \{(\zeta_n)_n\},$$

where

$$\zeta_n^{p^n} = 1; \quad \zeta_{nm}^{p^m} = \zeta_n.$$

As a group,

$$\mathbb{Z}_p(1) \simeq \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n,$$

but there is a continuous action of G_K .

Arithmetic principal bundles

Given any $x \in K^*$, get principal $\mathbb{Z}_p(1)$ -bundle

$$P(x) := \{(y_n)_n \mid y_n^{p^n} = x, \quad y_{nm}^{p^m} = y_n\}$$

over K .

$P(x)$ is trivial iff x admits a p^n -th root in K for all n .

For example, when $K = \mathbb{C}$, $P(x)$ is always trivial.

When $K = \mathbb{Q}$, $P(x)$ is trivial iff $x = 1$ or p is odd and $x = -1$.

For $K = \mathbb{R}$, and p odd, $P(x)$ is trivial for all x .

For $K = \mathbb{R}$ and $p = 2$, $P(x)$ is trivial iff $x > 0$.

Arithmetic principal bundles: moduli spaces

Given a principal R -bundle P over K , choose $z \in P$. This determines a continuous function $c_P : G_K \longrightarrow R$ via

$$g(z) = z c_P(g).$$

It satisfies the condition

$$c_P(g_1 g_2) = c_P(g_1) g_1(c_P(g_2)),$$

defining the set $Z^1(G, R)$. If we choose $z' = zr^{-1}$, then

$$g(z') = g(z)g(r^{-1}) = z c_P(g)g(r^{-1}) = z' r c_P(g)g(r^{-1}).$$

Thus, we get a well-defined class

$$[c_P] \in R \setminus Z^1(G_K, R) =: H^1(G_K, R)$$

where the R -action is defined by

$$c^r(g) = r c(g)g(r^{-1}).$$

Arithmetic principal bundles: moduli spaces

This induces a bijection

$$\{\text{Isomorphism classes of principal } R\text{-bundles over } K\} \cong H^1(G_K, R).$$

Our main concern is the geometry of non-abelian cohomology spaces in various forms.

For these lectures, R will mostly be a unipotent fundamental group of an algebraic curve with a very complicated K -structure.

Two more classes of important examples:

– R is the monodromy group of a specific local system on a curve.
(Lawrence and Venkatesh [LV])

– R is a reductive group with a trivial K -structure:

$$H^1(G_K, R) = R \backslash \text{Hom}(G_K, R).$$

These are analytic moduli spaces of Galois representations
[Chenevier].

Arithmetic principal bundles: moduli spaces

When K is a number field, there are completions K_v and injections

$$G_v = \text{Gal}(\bar{K}_v/K_v) \hookrightarrow G = \text{Gal}(\bar{K}/K).$$

giving rise to the localisation map

$$\text{loc} : H^1(K, R) \longrightarrow \prod_v H^1(K_v, R).$$

A wide range of problems in number theory rely on the study of its image. The general principle is that the local-to-global problem is easier to study for principal bundles than for points.

III. Diophantine principal bundles: elliptic curves

Diophantine principal bundles: elliptic curves

[Silverman]

E : elliptic curve over \mathbb{Q} .

We let $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ act on the exact sequence

$$0 \longrightarrow E[p](\bar{\mathbb{Q}}) \longrightarrow E(\bar{\mathbb{Q}}) \xrightarrow{p} E(\bar{\mathbb{Q}}) \longrightarrow 0$$

to generate the long exact sequence

$$\begin{aligned} 0 &\longrightarrow E(\mathbb{Q})[p] \longrightarrow E(\mathbb{Q}) \xrightarrow{p} E(\mathbb{Q}) \\ &\longrightarrow H^1(\mathbb{Q}, E[p]) \longrightarrow H^1(\mathbb{Q}, E) \xrightarrow{p} H^1(\mathbb{Q}, E), \end{aligned}$$

from which we get the inclusion (Kummer map)

$$0 \longrightarrow E(\mathbb{Q})/pE(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, E[p])$$

Diophantine principal bundles: elliptic curves

The central problem in the theory of elliptic curves is the identification of the image

$$\text{Im}(E(\mathbb{Q})/pE(\mathbb{Q})) \subset H^1(G, E[p]).$$

To this end, define the p -Selmer group

$$\text{Sel}(\mathbb{Q}, E[p]) \subset H^1(\mathbb{Q}, E[p])$$

to be the classes in $H^1(\mathbb{Q}, E[p])$ that locally come from points. This is useful because the local version of this problem can be solved.

Diophantine principal bundles: elliptic curves

$$\begin{array}{ccccccc}
 0 & \longrightarrow & E(\mathbb{Q})/pE(\mathbb{Q}) & \hookrightarrow & H^1(\mathbb{Q}, E[p]) \\
 & & \downarrow loc_v & & \downarrow loc_v \\
 0 & \longrightarrow & E(\mathbb{Q}_v)/pE(\mathbb{Q}_v) & \hookrightarrow & H^1(\mathbb{Q}_v, E[p])
 \end{array}$$

Then

$$Sel(\mathbb{Q}, E[p]) := \cap_v loc_v^{-1}(Im(E(\mathbb{Q}_v)/pE(\mathbb{Q}_v))).$$

Diophantine principal bundles: elliptic curves

The key point is that the **p -Selmer group is a finite-dimensional \mathbb{F}_p -vector space that is effectively computable** and this already gives us a bound on the Mordell-Weil group of E :

$$E(\mathbb{Q})/pE(\mathbb{Q}) \subset Sel(\mathbb{Q}, E[p]).$$

This is then refined by way of the diagram

$$\begin{array}{ccc} 0 & \longrightarrow & E(\mathbb{Q})/p^n E(\mathbb{Q}) \longrightarrow Sel(\mathbb{Q}, E[p^n]) \\ & & \downarrow \\ 0 & \longrightarrow & E(\mathbb{Q})/pE(\mathbb{Q}) \longrightarrow Sel(\mathbb{Q}, E[p]) \end{array}$$

for increasing values of n .

Diophantine principal bundles: elliptic curves

Conjecture: (BSD, Tate-Shafarevich)

$$\text{Im}(E(\mathbb{Q})/pE(\mathbb{Q})) = \cap_{n=1}^{\infty} \text{Im}[Sel(\mathbb{Q}, E[p^n])] \subset Sel(\mathbb{Q}, E[p]).$$

Of course this implies that

$$\text{Im}(E(\mathbb{Q})/pE(\mathbb{Q})) = \text{Im}[Sel(\mathbb{Q}, E[p^N])] \subset Sel(\mathbb{Q}, E[p])$$

at some finite level p^N , and there is a conditional algorithm for verifying this. A main goal of BSD is to remove the conditional aspect.

IV. Diophantine principal bundles II: The non-abelian case

Diophantine principal bundles II: The non-abelian case

To generalise, focus on the sequence of maps

$$\cdots \longrightarrow E[p^3] \xrightarrow{p} E[p^2] \xrightarrow{p} E[p]$$

of which we take the inverse limit to get the p -adic Tate module of E :

$$T_p E := \varprojlim E[p^n].$$

This is a free \mathbb{Z}_p -module of rank 2.

The previous finite boundary maps can be packaged into

$$j : E(\mathbb{Q}) \longrightarrow \varprojlim H^1(\mathbb{Q}, E[p^n]) = H^1(\mathbb{Q}, T_p E).$$

Diophantine principal bundles II: The non-abelian case

The key point is that

$$T_p E \simeq \pi_1^p(\bar{E}, O),$$

where $\pi_1^p(\bar{X}, b)$ refers to the pro- p completion of the fundamental group $\pi_1(X(\mathbb{C}), b)$ of a variety X .

The map j can be thought of as

$$x \mapsto \pi^p(\bar{E}; O, x).$$

Diophantine principal bundles II: The non-abelian case

Fundamental fact of arithmetic homotopy:

If X is a variety defined over \mathbb{Q} and $b, x \in X(\mathbb{Q})$, then

$$\pi_1^p(\bar{X}, b), \quad \pi_1^p(\bar{X}; b, x)$$

admit compatible actions of $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The triples

$$(G_{\mathbb{Q}}, \pi_1^p(\bar{X}, b), \pi_1^p(\bar{X}; b, x))$$

are important concrete examples of (G_K, R, P) from the general definitions.

Diophantine principal bundles II: The non-abelian case

This formulation then extends to general X , whereby we get a map

$$j : X(\mathbb{Q}) \longrightarrow H^1(G, \pi_1^p(\bar{X}, b))$$

given by

$$x \mapsto [\pi_1^p(\bar{X}; b, x)]$$

For each prime v , have local versions

$$j_v : X(\mathbb{Q}_v) \longrightarrow H^1(G_v, \pi_1^p(\bar{X}, b))$$

given by

$$x \mapsto [\pi_1^p(\bar{X}; b, x)]$$

which turn out to be far more computable than the global map.

Diophantine principal bundles II: The non-abelian case

Localization diagram:

$$\begin{array}{ccc}
 X(\mathbb{Q}) & \longrightarrow & \prod_v X(\mathbb{Q}_v) \\
 j \downarrow & & \downarrow \prod_v j_v \\
 H^1(G, \pi_1^p(\bar{X}, b)) & \xrightarrow{\text{loc}} & \prod_v H^1(G_v, \pi_1^p(\bar{X}, b))
 \end{array}$$

As in the elliptic curve case, our interest is in the interaction between the images of loc and $\prod_v j_v$.

Diophantine principal bundles II: The non-abelian case

Actual applications use

$$\begin{array}{ccc}
 X(\mathbb{Q}) & \longrightarrow & \prod_v X(\mathbb{Q}_v) \\
 j \downarrow & & \downarrow \prod_v j_v \\
 H^1(G, U(\bar{X}, b)) & \rightarrow & \prod_v H^1(G_v, U(\bar{X}, b))
 \end{array}$$

where

$$U(\bar{X}, b) = ' \pi_1^p(X, b) \otimes \mathbb{Q}_p '$$

is the \mathbb{Q}_p -pro-unipotent completion of $\pi_1^p(\bar{X}, b)$ [Deligne].

The effect is that the moduli spaces become pro-algebraic schemes over \mathbb{Q}_p and the lower row of this diagram an algebraic map.

Diophantine principal bundles II: The non-abelian case

That is, the key object of study is

$$H_f^1(G, U(\bar{X}, b))$$

the **Selmer scheme** of X , defined to be the subfunctor of $H^1(G, U(\bar{X}, b))$ satisfying local conditions at all (or most) v .

These are conditions like ‘unramified at most primes’, ‘crystalline at p ’, and often a few extra conditions [BD, Fontaine].

Diophantine principal bundles II: The non-abelian case

$$\begin{array}{ccc}
 X(\mathbb{Q}) & \longrightarrow & \prod_{\nu} X(\mathbb{Q}_{\nu}) \\
 j \downarrow & & \downarrow \prod_{\nu} j_{\nu} \\
 H_f^1(G, U(\bar{X}, b)) & \rightarrow & \prod_{\nu} H_f^1(G_{\nu}, U(\bar{X}, b)) \xrightarrow{\alpha} \mathbb{Q}_p
 \end{array}$$

If α is an algebraic function vanishing on the image, then

$$\alpha \circ \prod_{\nu} j_{\nu}$$

gives a defining equation for $X(\mathbb{Q})$ inside $\prod_{\nu} X(\mathbb{Q}_{\nu})$.

Diophantine principal bundles II: The non-abelian case

To make this concretely computable, we take the projection

$$pr_p : \prod_v X(\mathbb{Q}_v) \longrightarrow X(\mathbb{Q}_p)$$

and try to compute

$$\cap_{\alpha} pr_p(Z(\alpha \circ \prod_v j_v)) \subset X(\mathbb{Q}_p).$$

Non-Archimedean effective Mordell Conjecture:

- I. $\cap_{\alpha} pr_p(Z(\alpha \circ \prod_v j_v)) = X(\mathbb{Q})$
- II. This set is effectively computable.

Diophantine principal bundles II: The non-abelian case

Two remarks:

1. As soon as there is one α with α_p non-trivial, $pr_p(Z(\alpha \circ \prod_v j_v))$ is finite.
2. There is a (highly reliable) conjectural mechanism for producing infinitely many algebraically independent α .

V. Computing Rational Points

Computing rational points

[DW1, DW2]

For $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$,

$$X(\mathbb{Z}[1/2]) = \{2, -1, 1/2\} \subset \{D_2(z) = 0\} \cap \{D_4(z) = 0\},$$

where

$$D_2(z) = \ell_2(z) + (1/2) \log(z) \log(1-z),$$

$$\begin{aligned} D_4(z) &= \zeta(3)\ell_4(z) + (8/7)[\log^3 2/24 + \ell_4(1/2)/\log 2] \log(z) \ell_3(z) \\ &+ [(4/21)(\log^3 2/24 + \ell_4(1/2)/\log 2) + \zeta(3)/24] \log^3(z) \log(1-z), \end{aligned}$$

and

$$\ell_k(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^k}.$$

Numerically, the inclusion appears to be an equality.

Computing rational points

Some qualitative results:

(Coates and Kim [CK])

$$ax^n + by^n = c$$

for $n \geq 4$ has only finitely many rational points.

Standard structural conjectures on mixed motives (generalised BSD)

- ⇒ There exist (many) non-zero α as above
- ⇒ Faltings's theorem over \mathbb{Q} .

Recently, Lawrence and Venkatesh [LV] have succeeded in giving an unconditional new proof of Faltings's theorem using the same diagram with U replaced by (the vector bundle associated to a representation of) the monodromy group of π_1 with respect to a semi-simple representation

$$\rho : \pi_1 \longrightarrow \text{Aut}(V).$$

Computing rational points

A recent result on modular curves by Balakrishnan, Dogra, Mueller, Tuitmann, Vonk [BDMTV]

$$X_s^+(N) = X(N)/C_s^+(N),$$

where $X(N)$ the the compactification of the moduli space of pairs

$$(E, \phi : E[N] \simeq (\mathbb{Z}/N)^2),$$

and $C_s^+(N) \subset GL_2(\mathbb{Z}/N)$ is the normaliser of a split Cartan subgroup.

Bilu-Parent-Rebolledo [BP, BPR] had shown that $X_s^+(p)(\mathbb{Q})$ consists entirely of cusps and CM points for all primes $p > 7$, $p \neq 13$. They called $p = 13$ the ‘cursed level’.

Computing rational points

Theorem (BDMTV)

The modular curve

$$X_s^+(13)$$

has exactly 7 rational points, consisting of the cusp and 6 CM points.

This concludes an important chapter of a conjecture of Serre:

There is an absolute constant A such that

$$G \longrightarrow \text{Aut}(E[p])$$

is surjective for all non-CM elliptic curves E/\mathbb{Q} and primes $p > A$.

Computing rational points

[Burcu Baran]

$$\begin{aligned}y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z \\ - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0\end{aligned}$$



Figure: The cursed curve

$$\{(1:1:1), (1:1:2), (0:0:1), (-3:3:2), (1:1:0), (0,2:1), (-1:1:0) \}$$

VI. Some speculations on rational points and critical points

Some speculations on rational points and critical points

Would like to think of

$$H^1(G, U(\bar{X}, b)) \longrightarrow \prod_v H^1(G_v, U(\bar{X}, b))$$

as being like

$$\mathbb{S}(M, G) \subset \mathcal{A}(M, G)$$

the space of solutions to a set of Euler-Lagrange equations on a space of connections.

In particular, functions cutting out the image of localisation should be thought of as ‘classical equations of motion’ for gauge fields.

Some speculations on rational points and critical points

When X is smooth and projective, $X(\mathbb{Q}) = X(\mathbb{Z})$, and we are actually interested in

$$\text{Im}(H^1(G_S, U)) \cap \prod_{v \in S} H_f^1(G_v, U) \subset \prod_{v \in S} H^1(G_v, U),$$

where

$$H_f^1(G_v, U) \subset H^1(G_v, U)$$

is a subvariety defined by some integral or Hodge-theoretic conditions.

In order to apply symplectic techniques, replace U by

$$T^*(1)U := (\text{Lie } U)^*(1) \rtimes U.$$

Some speculations on rational points and critical points

Then

$$\prod_{v \in S} H^1(G_v, T^*(1)U)$$

is a symplectic variety and

$$Im(H^1(G_S, T^*(1)U)), \quad \prod_{v \in S} H_f^1(G_v, T^*(1)U)$$

are Lagrangian subvarieties.

Thus, the (derived) intersection

$$\mathcal{D}_S(X) := Im(H^1(G_S, T^*(1)U)) \cap \prod_{v \in S} H_f^1(G_v, T^*(1)U)$$

has a $[-1]$ -shifted symplectic structure.

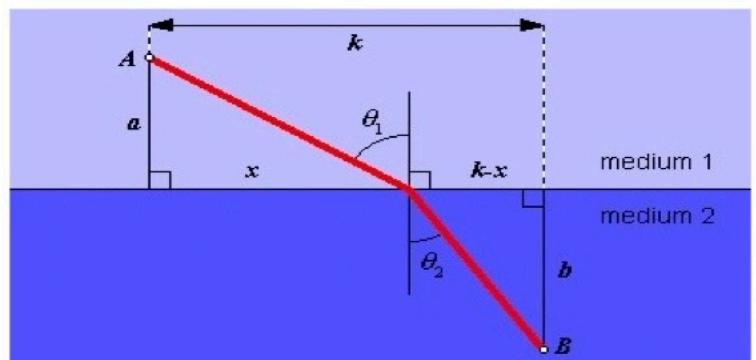
Zariski-locally the critical set of a function. (Brav, Bussi, Joyce [BBJ])

Some speculations on rational points and critical points

$$\begin{array}{ccccc}
 X(\mathbb{Z}) & \longrightarrow & j_S^{-1}(\mathcal{D}_S(X)) & \hookrightarrow & \prod_{v \in S} X(\mathbb{Q}_v) \\
 j^g \downarrow & & j_S \downarrow & & j_S \downarrow \\
 H_f^1(G_S, T^*(1)U) & \xrightarrow{\text{loc}_S} & \mathcal{D}_S(X) & \hookrightarrow & \prod_{v \in S} H^1(G_v, T^*(1)U_n)
 \end{array}$$

From this view, the global points can be obtained by pulling back ‘Euler-Lagrange equations’ via a period map.

Some speculations on rational points and critical points



For integers $n > 2$ the equation

$$a^n + b^n = c^n$$

cannot be solved with positive integers a, b, c .

Figure: Pierre de Fermat (1607-1665)

Bibliography

-  J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, J. Vonk
Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Annals of Math.* 189 (2019), Issue 3, pp. 888-944
-  Betts, L. Alexander, Dogra, Netan The local theory of unipotent Kummer maps and refined Selmer schemes.
[arXiv:1909.05734](https://arxiv.org/abs/1909.05734)
-  Bilu, Yuri; Parent, Pierre Serre's uniformity problem in the split Cartan case. *Ann. of Math.* (2) 173 (2011), no. 1, 569–584.
-  Bilu, Yuri; Parent, Pierre; Rebolledo, Marusia Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)* 63 (2013), no. 3, 957–984.
-  Brav, Christopher; Bussi, Vittoria; Joyce, Dominic A ‘Darboux theorem’ for derived schemes with shifted symplectic structure.
[arXiv:1305.6302v3](https://arxiv.org/abs/1305.6302v3)

Bibliography

-  Chenevier, Gaëtan The p -adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings. Automorphic forms and Galois representations. Vol. 1, 221–285, London Math. Soc. Lecture Note Ser., 414, Cambridge Univ. Press, Cambridge, 2014.
-  Coates, John; Kim, Minhyong Selmer varieties for curves with CM Jacobians. Kyoto J. Math. 50 (2010), no. 4, 827–852.
-  Dan-Cohen, Ishai; Wewers, Stefan Mixed Tate motives and the unit equation. <https://arxiv.org/abs/1311.7008>
-  Dan-Cohen, Ishai; Wewers, Stefan Mixed Tate motives and the unit equation II. <https://arxiv.org/abs/1510.01362>

Bibliography

-  Deligne, Pierre Le groupe fondamental de la droite projective moins trois points. Galois groups over \mathbb{Q} (Berkeley, CA, 1987), 79–297, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.
-  Faltings, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. 73 (1983), no. 3, 349–366.
-  Fontaine, Jean-Marc (ed.) *Périodes p -adiques*. Astérisque, 223, Paris: Société Mathématique de France (1994)
-  Lawrence, Brian, Venkatesh, Akshay Diophantine problems and p -adic period mappings
-  Serre, J.-P. A course in arithmetic. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.
-  Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

Selmer Schemes II

Minhyong Kim

Tucson, March, 2019

Disclaimer

These lecture slides come with a bibliography at the end. However, there has been no attempt at accurate attribution of mathematical results. Rather, the list mostly contains works the lecturer has consulted during preparation, which he hopes will be helpful for users.

I. Preliminaries on covering spaces and fundamental groups

Universal Covering Spaces

M : a locally contractible connected topological space.

A covering space

$$M' \longrightarrow M$$

is a locally trivial fibre bundle with discrete fibres:

There is a discrete set F and an open covering $M = \cup U_i$ such that

$$M'_{U_i} \simeq F \times U_i$$

for each i .

Universal Covering Spaces

A universal covering space

$$\pi : \tilde{M} \longrightarrow M$$

is a covering space with \tilde{M} connected and simply connected.

It is not universal in a categorical sense: For any other covering space $M' \longrightarrow M$, there is a commutative diagram

$$\begin{array}{ccc} \tilde{M} & \longrightarrow & M' \\ & \searrow & \downarrow \\ & & M \end{array}$$

However, the diagram is *not unique*: There is no initial object in the category of covering spaces.

Universal Covering Spaces

Consider instead *pointed* covering spaces.

Having chosen a point $b \in M$, a pointed covering space is a map

$$(M', b') \longrightarrow (M, b).$$

Now we choose a point $\tilde{b} \in \tilde{M}_b$. Then the pair (\tilde{M}, \tilde{b}) is indeed an initial object in the category of pointed universal covering spaces:

$$\begin{array}{ccc} (\tilde{M}, \tilde{b}) & \xrightarrow{\exists!} & (M', b') \\ & \searrow & \downarrow \\ & & (M, b) \end{array}$$

Note that the choice of a different $\tilde{c} \in \tilde{M}_b$ will give another initial object (\tilde{M}, \tilde{c}) which is uniquely isomorphic to (\tilde{M}, \tilde{b}) .

Fibre Functors

Now consider the functor

$$F_b : \text{Cov}(M) \longrightarrow \text{Sets}$$

$$M' \mapsto M'_b,$$

and its automorphism group

$$\text{Aut}(F_b).$$

By the definition of a natural transformation, an element γ of this group is a compatible sequence of bijections

$$\gamma_{M'} : M'_b \cong M'_b.$$

Fibre Functors

Compatibility here is with respect to maps of covering spaces:

If $f : M'_1 \longrightarrow M'_2$ is a map of covering spaces, then

$$\begin{array}{ccc} M'_{1,b} & \xrightarrow{\gamma_{M_1}} & M'_{1,b} \\ f \downarrow & & \downarrow f \\ M'_{2,b} & \xrightarrow{\gamma_{M_2}} & M'_{2,b} \end{array}$$

$$f \circ \gamma_{M'_1} = \gamma_{M'_2} \circ f.$$

Fibre Functors

Define a map

$$\text{Aut}(F_b) \longrightarrow \tilde{M}_b$$

by

$$\gamma \mapsto \gamma_{\tilde{M}}(\tilde{b}) \in \tilde{M}_b.$$

Proposition

This map induces a bijection

$$\text{Aut}(F_b) \cong \tilde{M}_b.$$

Fibre Functors

Injectivity:

Given any $b' \in M'_b$, there is a unique map $f : (\tilde{M}, \tilde{b}) \longrightarrow (M', b')$.
Thus

$$\gamma_{M'}(b') = \gamma_{M'}(f(\tilde{b})) = f(\gamma_{\tilde{M}}(\tilde{b})),$$

and the action of γ on M'_b is determined by $\gamma_{\tilde{M}}(\tilde{b})$.

On the other hand, given $y \in \tilde{M}_b$, we would like to define γ such that $\gamma_{\tilde{M}}(\tilde{b}) = y$.

The point is that there is only one way to do it in a way that's compatible with maps of covering spaces and this gives us $\gamma_{M'}$ for every $M' \longrightarrow M$.

Fibre Functors

Given $b' \in M'_b$, there is a unique $f_{b'} : (\tilde{M}, \tilde{b}) \longrightarrow (M', b')$. Define

$$\gamma_{M'}(b') = \gamma_{M'}(f_{b'}(\tilde{b})) (= f_{b'}(\gamma_{\tilde{M}}(\tilde{b}))) := f_{b'}(y).$$

Compatibility comes from commutative triangles

$$\begin{array}{ccc}
 (\tilde{M}, \tilde{b}) & \xrightarrow{f_{b'}} & (M', b') \\
 & \searrow f_{h(b')} & \downarrow h \\
 & & (M'', h(b''))
 \end{array}$$

that imply

$$h(\gamma_{M'}(b')) = h(f_{b'}(y)) = f_{h(b')}(y) = \gamma_{M''}(h(b')).$$

Fibre Functors

An identical proof gives us:

Proposition

For two points $b, x \in M$,

$$\text{Isom}(F_b, F_x) \simeq \tilde{M}_x.$$

That is, an element $p \in \text{Isom}(F_b, F_x)$ is determined by $p_{\tilde{M}}(\tilde{b})$, and any $y \in \tilde{M}_x$ determines such a p .

Note that $\text{Isom}(F_b, F_x)$ is a principal bundle for $\text{Aut}(F_b)$. As an exercise, try to describe for yourself the action of \tilde{M}_b on \tilde{M}_x .

Homotopy classes of paths

Consider the usual definition of $\pi_1(M; b, x)$ using homotopy classes of paths. There is a classical isomorphism

$$\pi_1(M; b, x) \cong \text{Isom}(F_b, F_x)$$

defined via path lifting.

That is, a path $p : I = [0, 1] \longrightarrow M$ such that $p(0) = b$ and $p(1) = x$ acts on the fibres of a covering $M' \longrightarrow M$ via the unique lifting diagram:

$$\begin{array}{ccc} & (M', b') & \\ p \swarrow & & \downarrow \\ (I, 0) & \xrightarrow{p} & (M, b) \end{array}$$

That is $p \cdot b' = p'(1)$.

Homotopy classes of paths

The endpoint $p'(1)$ depends only on the homotopy class of p because of the discreteness of the fibres.

If $f : (M'_1, b'_1) \longrightarrow (M'_2, b'_2)$ is a map of pointed covering spaces, then $f \circ p'_1 = p'_2$ by uniqueness.

Thus, path lifting defines a compatible collection of isomorphisms

$$p_{M'} : M'_b \cong M'_x.$$

In particular, loops based at b will act compatibly on all fibres M'_b .

Homotopy classes of paths

The easiest way to see that this gives an isomorphism

$$\pi_1(M; b, x) \cong \text{Isom}(F_b, F_x)$$

uses \tilde{M}_b again.

That is, denote by \tilde{p} the lifting of p to \tilde{M} such that $\tilde{p}(0) = \tilde{b}$. In that case, we get that

Proposition

The map $p \mapsto \tilde{p}(1)$ defines a bijection

$$\pi_1(M; b, x) \cong \tilde{M}_x.$$

Homotopy classes of paths

The inverse is given by mapping $y \in \tilde{M}_x$ to the homotopy class $[\pi \circ q]$, where q is any path in \tilde{M} from \tilde{b} to y . The homotopy class is independent of q since \tilde{M} is simply connected.

However, this map clearly factors through

$$\pi_1(M; b, x) \longrightarrow \text{Isom}(F_b, F_x) \cong \tilde{M}_b,$$

proving that the first map is also an isomorphism.

In other words, the choice of base-points gives us an expression

$$\tilde{M} = \cup_{x \in M} \pi_1(M; b, x).$$

The fibers of \tilde{M} give us a concrete model of path spaces, which generalises to situations where physical paths are missing.

Homotopy classes of paths

To summarise, we have the bijections

$$\pi_1(M; b, x) \cong \text{Isom}(F_b, F_x) \cong \tilde{M}_x.$$

The second two objects generalise to other settings.

II. Preliminaries on Tannakian formalism

Tannakian formalism

G : finite group;

Rep_k^G : category of finite-dimensional representations of G on k -vector space.

A pointed representation is a representation V together with a vector $v \in V$.

Proposition

The left-regular pointed representation

$$(k[G], 1)$$

is the universal pointed representation of G .

Given any pointed representation (V, v) , we get a unique map $(k[G], 1) \longrightarrow (V, v)$ that sends g to gv .

Tannakian formalism

Let

$$F : \text{Rep}_k^G \longrightarrow \text{Vect}_k$$

be the forgetful functor to k -vector spaces.

Consider the endomorphisms

$$\text{End}(F)$$

of F .

Thus, an element $a \in \text{End}(F)$ is a compatible sequence of linear transformations $a_V : V \longrightarrow V$ as V runs over representations of G :

$$\begin{array}{ccc} V & \xrightarrow{a_V} & V \\ \phi \downarrow & & \downarrow \phi \\ W & \xrightarrow{a_W} & W \end{array}$$

Tannakian formalism

Proposition

The map

$$a \mapsto a_{k[G]}(1)$$

defines an isomorphism $\text{End}(F) \cong k[G]$.

Tannakian formalism

There is an augmentation map $e^* : k[G] \longrightarrow k$ and the map $G \longrightarrow G \times G$, $g \mapsto (g, g)$ induces the comultiplication map

$$\Delta : k[G] \longrightarrow k[G \times G] \simeq k[G] \otimes k[G].$$

Given representations V and W , $V \otimes_k W$ is initially a representation of $k[G] \otimes k[G]$ which is turned into a representation of $k[G]$ and G via Δ .

Proposition

G itself can be recovered as the group-like elements of $k[G]$, i.e., $a \in k[G]$ such that $e^*(a) = 1$ and

$$\Delta(a) = a \otimes a.$$

Tannakian formalism

Proposition

G is isomorphic to $\text{Aut}^{\otimes} F$, the tensor-compatible automorphisms of the forgetful functor F from Rep_G^k to Vect_k

Here, an element $f \in \text{Aut}(F)$ is tensor-compatible if $f_{V \otimes W} = f_V \otimes f_W$.

If we let

$$A = \text{Hom}_k(k[G], k),$$

$$\Delta^* : A \otimes A \cong \text{Hom}(k[G] \otimes k[G], k) \longrightarrow A$$

gives it the structure of a commutative k -algebra. Of course,

$$G \hookrightarrow \text{Hom}_k(A, k).$$

Corollary

$$G = \text{Spec}(A)(k) = \text{Hom}_{k\text{-alg}}(A, k).$$

III. Return to arithmetic fundamental groups

Arithmetic setting

K : a number field or a finite extension of \mathbb{Q}_p .

X : a smooth curve over K

\bar{X} : the basechange of X to \bar{K} .

$b, x \in X(K)$ viewed sometimes as geometric points:

$$\text{Spec}(\bar{K}) \longrightarrow \bar{X} \longrightarrow X.$$

In the local case, let \mathcal{X} be a smooth scheme over \mathcal{O}_K with good compactification and generic fiber X . and let Y be the special fiber of \mathcal{X} over $k = \mathcal{O}_K/m_K$.

Profinite étale fundamental group

[Szamuely] $\text{Cov}(\bar{X})$: category of finite étale covering spaces of \bar{X} .

There is a fibre functor

$$F_b : \text{Cov}(\bar{X}) \longrightarrow \text{FinSet};$$

$$(Y \longrightarrow \bar{X}) \mapsto Y_b.$$

Define

$$\hat{\pi}_1(\bar{X}; b, x) := \text{Isom}(F_b, F_x).$$

Profinite étale fundamental group

Proposition

There is a ‘universal’ pro-étale cover

$$\tilde{\bar{X}} = (\bar{X}_i) \longrightarrow \bar{X}$$

with the property that we get a diagram

$$\begin{array}{ccc} \tilde{\bar{X}} & \longrightarrow & Y \\ & \searrow & \downarrow \\ & & \bar{X} \end{array}$$

for any finite étale cover $Y \longrightarrow \bar{X}$.

The arrow $\tilde{\bar{X}} \longrightarrow Y$ is an element of $\varprojlim \text{Hom}(\bar{X}_i, Y)$.

Profinite étale fundamental group

Pick a ‘point’ $\tilde{b} \in \tilde{\bar{X}}$, by which we mean a compatible sequence of points $b_i \in \bar{X}_{i,b}$. Then $(\tilde{\bar{X}}, \tilde{b})$ is a universal pointed pro-étale cover:

Proposition

We get a diagram

$$\begin{array}{ccc} (\tilde{\bar{X}}, \tilde{b}) & \xrightarrow{\exists!} & (Y, b_Y) \\ & \searrow & \downarrow \\ & & (\bar{X}, b) \end{array}$$

for any finite étale cover $(Y, b_Y) \longrightarrow (\bar{X}, b)$.

Profinite étale fundamental group

Furthermore,

Proposition

The cover (\tilde{X}, \tilde{b}) is defined over K . That is, there is a cover

$$(\tilde{X}, \tilde{b}) \longrightarrow (X, b)$$

with \tilde{b} rational, whose base change to \bar{K} is $(\tilde{\bar{X}}, \tilde{\bar{b}})$.

Be warned that in spite of the notation, $\tilde{X} \longrightarrow X$ is not the universal cover of X . The universal cover of X is

$$\tilde{\bar{X}} \longrightarrow \bar{X} \longrightarrow X.$$

The cover $\tilde{X} \longrightarrow X$ is a K -model of the universal cover of \bar{X} .

Profinite étale fundamental group

Examples:

$$(\mathbb{G}_m, 1)$$

Then

$$\widetilde{\mathbb{G}_m} = (\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m)_n$$

with basepoint 1.

E an elliptic curve over K with basepoint $O \in E(K)$.

Then

$$\tilde{E} = (E \xrightarrow{n} E)_n$$

with basepoint (O) .

Profinite étale fundamental group

Theorem

The map

$$\gamma \mapsto (\gamma_{\bar{X}_i}(b_i)) \in \tilde{\bar{X}}_x = \tilde{X}_b(\bar{K})$$

induces a G_K -equivariant isomorphism

$$\hat{\pi}_1(\bar{X}; b, x) \simeq \tilde{\bar{X}}_x = \tilde{X}_x(\bar{K})$$

This isomorphism gives a concrete way of ‘computing’ the action of $\text{Gal}(\bar{K}/K)$ on $\hat{\pi}_1(\bar{X}; b, x)$.

Profinite étale fundamental group

The formal definition of the action on the left is given as follows.

For $g \in G_K$ and $p \in \hat{\pi}_1(\bar{X}; b, x)$, $g(p)$ associates to $X' \rightarrow X$ the lower arrow that makes the diagram commute:

$$\begin{array}{ccc}
 g^*(X')_b & \xrightarrow{p_{g^*(X')}} & g^*(X')_x \\
 g \downarrow & & \downarrow g \\
 X_b & \xrightarrow{g(p)} & X_x
 \end{array}$$

$$g(p)_x = g \circ p_{g^*(X')} g^{-1}.$$

Profinite étale fundamental group

$$\hat{\pi}_1(\bar{\mathbb{G}}_m, 1) = (\widetilde{\mathbb{G}_m})_1 = \hat{\mathbb{Z}}(1).$$

$$\hat{\pi}_1(\bar{E}, O) = \tilde{E}_1 = \hat{T}(E).$$

$$\hat{\pi}_1(\bar{\mathbb{G}}_m; 1, x) = (\widetilde{\mathbb{G}_m})_x = (x^{1/n}).$$

$$\hat{\pi}_1(\bar{E}; O, x) = \tilde{E}_x = (\frac{1}{n}x).$$

Profinite étale fundamental group

General construction:

If $P \longrightarrow M$ is a principal G -bundle and G (left-)acts continuously on a set A , then can form associated bundle

$$P \times_G A := [P \times A]/G,$$

where G acts on the product as $(p, a)g = (pg, g^{-1}a)$.

This is a fibre bundle over M with fibre A which varies according to the variation of P .

When $\rho : G \longrightarrow H$ is a group homomorphism, this construction $P \times_G H$ gives a principal H -bundle.

Profinite étale fundamental group

The cover

$$\tilde{\bar{X}} \longrightarrow \bar{X}$$

is a principal $\hat{\pi}_1(\bar{X}, b)$ -bundle.

$$\tilde{\bar{X}}^{(p)} = \tilde{\bar{X}} \times_{\hat{\pi}_1(\bar{X}, b)} \hat{\pi}_1^{(p)}(\bar{X}, b),$$

which is a principal $\hat{\pi}_1^{(p)}(\bar{X}, b)$ -bundle, is the universal pro- p étale cover.

In general, we might try to study the G_K -action on $\hat{\pi}_1(\bar{X}; b, x)$ via fibres of suitable quotient coverings like this.

For example, if X is a modular curve, then the tower

$$X_{\text{Mod}} \longrightarrow X$$

of modular curves, corresponds to the ‘modular quotient group’ of $\hat{\pi}_1(\bar{X}, b)$.

Profinite étale fundamental group

Given a continuous \mathbb{Q}_p -representation V of $\hat{\pi}_1(\bar{X}, b)$, we get a locally constant sheaf of \mathbb{Q}_p -vector spaces

$$\tilde{\bar{X}} \times_{\hat{\pi}_1(\bar{X}, b)} V,$$

giving a functor

$$Rep_{\hat{\pi}_1(\bar{X}, b)}^{\mathbb{Q}_p} \longrightarrow Loc^{\mathbb{Q}_p}(\bar{X})$$

which is inverse to the fibre functor

$$F_b : \mathcal{L} \mapsto \mathcal{L}_b.$$

This is a version of the ‘vector bundle associated to a principal G -bundle and a linear representation of G ,’ familiar from usual geometry. However, to do this carefully in this case, you need to construct the correspondence with finite coefficients first and then consider projective systems. (This is where you need the continuity.)

III. Unipotent fundamental groups

Unipotent fundamental groups

[Deligne]

We linearise categories.

$\text{Un}(\bar{X}, \mathbb{Q}_p)$: The category of unipotent \mathbb{Q}_p -locally constant sheaves on the étale site of \bar{X} .

A local system \mathcal{F} is unipotent if it admits a filtration

$$\mathcal{F} = \mathcal{F}^0 \supset \mathcal{F}^1 \supset \cdots \supset \mathcal{F}^n = 0$$

such that

$$\mathcal{F}^i / \mathcal{F}^{i+1} \simeq (\mathbb{Q}_p)_{\bar{X}}^{r_i}$$

for each i . With this notation, we say \mathcal{F} has index of unipotency $\leq n$.

Unipotent fundamental groups

Theorem

There is a universal pointed pro-object in $Un(\bar{X}, \mathbb{Q}_p)$. This is a projective system

$$(\mathcal{E}, v) = ((\mathcal{E}_n, v_n))_n$$

with $v_n \in (\mathcal{E}_n)_b$ such that for any $\mathcal{F} \in Un(\bar{X}, \mathbb{Q}_p)$ and $w \in \mathcal{F}_b$, there is a unique map

$$f : (\mathcal{E}, v) \longrightarrow (\mathcal{F}, w).$$

Again,

$$\text{Hom}(\mathcal{E}, \mathcal{F}) = \varinjlim \text{Hom}(\mathcal{E}_n, \mathcal{F}).$$

Unipotent fundamental groups

The \mathcal{E}_n as above corresponds to the representation

$$\mathcal{E}_{n,b} = E_n := (\mathbb{Z}_p[[\hat{\pi}_1(\bar{X}, b)]]/I^{n+1}) \otimes \mathbb{Q}_p,$$

where $I \subset \mathbb{Z}_p[[\hat{\pi}_1(\bar{X}, b)]]$ is the augmentation ideal, and $v_n = 1$.

We put

$$E = \varprojlim E_n = \varprojlim (\mathbb{Z}_p[[\hat{\pi}_1(\bar{X}, b)]]/I^{n+1}) \otimes \mathbb{Q}_p.$$

We think of this as non-commutative power series in $\gamma - 1$, where γ are topological generators of $\hat{\pi}_1(\bar{X}, b)$. Contains elements like

$$\gamma^a = \exp(a \log(\gamma))$$

for $a \in \mathbb{Q}_p$.

Unipotent fundamental groups

The pointed local system (\mathcal{E}_n, v_n) is universal among unipotent local systems of index of unipotency $\leq n$. Thus we get unique maps

$$\mathcal{E}_{m+n} \mapsto \mathcal{E}_m \otimes \mathcal{E}_n$$

that send v_{m+n} to $v_m \otimes v_n$. These come together to a map

$$\Delta : \mathcal{E} \longrightarrow \mathcal{E} \hat{\otimes} \mathcal{E}.$$

Using the fibre functor

$$F_b : \text{Un}(\bar{X}, \mathbb{Q}_p) \longrightarrow \text{Vect}_{\mathbb{Q}_p}.$$

we now define

$$U(\bar{X}, b) := \text{Aut}^{\otimes}(F_b);$$

$$P(\bar{X}; b, x) := \text{Isom}^{\otimes}(F_b, F_x).$$

Unipotent fundamental groups

Lemma

$$\text{End}(F_b) \cong \mathcal{E}_b.$$

Theorem

The pro-algebraic group $U(\bar{X}, b)$ is isomorphic to the group-like elements in \mathcal{E}_b , while $P(\bar{X}; b, x)$ is given by the group-like elements in \mathcal{E}_x .

In fact, the lower central series

$$U = U^1 \supset U^2 \supset U^3 \dots$$

is compatible with the filtration by I^n , so that $U_n = U/U^{n+1}$ are the group-like elements in E_n .

Unipotent fundamental groups

Put

$$\mathcal{A} = \text{Hom}(\mathcal{E}, \mathbb{Q}_p) = \varinjlim \text{Hom}(\mathcal{E}_n, \mathbb{Q}_p).$$

Then \mathcal{A} is a sheaf of \mathbb{Q}_p -algebras via Δ^* .

Corollary

$$U(\bar{X}, b) = \text{Spec}(\mathcal{A}_b).$$

$$P(\bar{X}; b, x) = \text{Spec}(\mathcal{A}_x).$$

Unipotent fundamental groups

Some remarks on Galois actions.

- (1) The action on $P(\bar{X}; b, x)$ is induced by the action on \mathcal{E}_x .
- (2) The action on \mathcal{E}_x uses $\tilde{\bar{X}}_x \times_{\hat{\pi}_1(\bar{X}, b)} E$.
- (3) The action on $\tilde{\bar{X}}_x$ is given by a cocycle

$$c_x : G_K \longrightarrow \hat{\pi}_1(\bar{X}, b).$$

That is, choose $\tilde{x} \in \tilde{\bar{X}}$. Then c_x is defined by

$$g(\tilde{x}) = \tilde{x} c_x(g)$$

and satisfies $c_x(g_1 g_2) = c(g_1) g_1 c(g_2)$.

Then \mathcal{E}_x can be identified with E where the action is twisted:

$$g_x v = c_x(g) g v.$$

Unipotent fundamental groups

Some basic structural facts.

The map

$$g \mapsto [g - 1]$$

induces an isomorphism

$$H_1(\bar{X}, \mathbb{Q}_p) = \hat{\pi}_1(\bar{X}, b)^{ab} \otimes \mathbb{Q}_p \cong I/I^2.$$

The multiplication map

$$(I/I^2)^{\otimes n} \longrightarrow I^n/I^{n+1}$$

includes an isomorphism

$$H_1^{\otimes n}/K_n \simeq I^n/I^{n+1}$$

where $T_n := H_1^{\otimes n}/K_n \simeq (R^n)^*$ and $R^n \subset (H^1)^{\otimes n}$ is defined inductively as follows.

Unipotent fundamental groups

$$R^0 = \mathbb{Q}_p, \quad R^1 = H^1,$$

$$R^2 = \text{Ker}(H^1 \otimes H^1 \xrightarrow{\gamma_1 := \cup} H^2).$$

We will have $R^{n+1} \subset R^n \otimes H^1$. Define the map γ_n inductively as

$$\gamma_n : R^n \otimes H^1 \longrightarrow R^{n-1} \otimes H^1 \otimes H^1 \longrightarrow R^{n-1} \otimes H^2,$$

and define

$$R^{n+1} = \text{Ker}(\gamma_n).$$

Unipotent fundamental groups

This comes from a different tautological construction [AIK, Faltings1, Faltings2].

$$\mathrm{Ext}_{\bar{X}}^1((\mathbb{Q}_p)_{\bar{X}}, (H_1(\bar{X}))_{\bar{X}}) \simeq H^1(\bar{X}) \otimes H_1(\bar{X}) = \mathrm{Hom}(H_1, H_1).$$

So there is an extension

$$0 \longrightarrow H_1(\bar{X}) \longrightarrow \mathcal{E}_1 \longrightarrow \mathbb{Q}_p \longrightarrow 0$$

corresponding to the identity map on the right.

Now we get an exact sequence

$$\begin{aligned} & \mathrm{Hom}_{\bar{X}}(H_1, \mathbb{Q}_p) \\ \xrightarrow{\delta} & \mathrm{Ext}_{\bar{X}}^1(\mathbb{Q}_p, \mathbb{Q}_p) \longrightarrow \mathrm{Ext}_{\bar{X}}^1(\mathcal{E}_1, \mathbb{Q}_p) \longrightarrow \mathrm{Ext}_{\bar{X}}^1(H_1, \mathbb{Q}_p) \\ \xrightarrow{\delta} & \mathrm{Ext}_{\bar{X}}^2(\mathbb{Q}_p, \mathbb{Q}_p) \end{aligned}$$

Unipotent fundamental groups

This can be written as

$$H^1 \xrightarrow{\delta} H^1 \longrightarrow \mathrm{Ext}_{\bar{X}}^1(\mathcal{E}_1, \mathbb{Q}_p) \longrightarrow H^1 \otimes H^1 \xrightarrow{\delta} H^2.$$

which induces the isomorphism

$$\mathrm{Ext}_{\bar{X}}^1(\mathcal{E}_1, \mathbb{Q}_p) \cong R^2 \cong T_2^*.$$

Hence,

$$\mathrm{Ext}_{\bar{X}}^1(\mathcal{E}_1, T_2) \cong \mathrm{Hom}(T_2, T_2),$$

so that there is an extension

$$0 \longrightarrow T_2 \longrightarrow \mathcal{E}_2 \longrightarrow \mathcal{E}_1 \longrightarrow 0$$

corresponding to the identity on the right.

One continues in this way and the universal property can also be proved in a tautological manner.

Unipotent fundamental groups

Idea: When the index of unipotency is 1 we have a constant sheaf $V_{\bar{X}} \longrightarrow \bar{X}$. Of course there is a unique map

$$f_1 : [\mathbb{Q}_p]_{\bar{X}} \longrightarrow V_{\bar{X}}$$

that takes $1 \in \mathbb{Q}_p = [\mathbb{Q}_p]_{\bar{X}, b}$ to any fixed $v \in V = V_{\bar{X}, b}$.

Now suppose you have

$$0 \longrightarrow W \longrightarrow \mathcal{F} \longrightarrow V \longrightarrow 0$$

with V and \mathcal{F}^1 constant. We would like to construct a lift f_2 as below

$$\begin{array}{ccccccc} 0 & \longrightarrow & T_1 & \longrightarrow & \mathcal{E}_1 & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\ & & \downarrow & & f_2 \downarrow & & f_1 \downarrow & & \\ 0 & \longrightarrow & W & \longrightarrow & \mathcal{F} & \longrightarrow & V & \longrightarrow & 0 \end{array}$$

Unipotent fundamental groups

The idea is to pull back by f_1 to get

$$0 \longrightarrow W \longrightarrow f_1^* \mathcal{F} \longrightarrow \mathbb{Q}_p \longrightarrow 0.$$

We would like to show this comes from \mathcal{E}_1 via a push-out along a map $\phi : T_1 \longrightarrow W$. But this extension is a class

$$c \in \text{Ext}_{\bar{X}}^1(\mathbb{Q}_p, W) = H^1 \otimes W.$$

Meanwhile, \mathcal{E}_1 corresponds to the class

$$I = \sum_i b^i \otimes b_i \in \text{Ext}^1(\mathbb{Q}_p, H_1) = H^1 \otimes H_1,$$

where $\{b_i\}$ is a basis for H_1 and $\{b^i\}$ the dual basis.

Write $c = \sum_i b^i \otimes w_i$, and define ϕ to be the linear map that takes b_i to w_i .

Bibliography

-  Andreatta, Fabrizio; Iovita, Adrian; Kim, Minhyong A p-adic nonabelian criterion for good reduction of curves. *Duke Math. J.* 164 (2015), no. 13, 2597–2642.
-  Deligne, Pierre Le groupe fondamental de la droite projective moins trois points. Galois groups over \mathbb{Q} (Berkeley, CA, 1987), 79–297, *Math. Sci. Res. Inst. Publ.*, 16, Springer, New York, 1989.
-  Faltings, Gerd Mathematics around Kim's new proof of Siegel's theorem. *Diophantine geometry*, 173?188, CRM Series, 4, Ed. Norm., Pisa, 2007.
-  Faltings, Gerd The motivic logarithm for curves. The arithmetic of fundamental groups, PIA 2010, 107-125, *Contrib. Math. Comput. Sci.*, 2, Springer, Heidelberg, 2012.
-  Szamuely, Tamás Galois groups and fundamental groups. Cambridge Studies in Advanced Mathematics, 117. Cambridge University Press, Cambridge, 2009. x+270 pp.

Selmer Schemes II, III

Minhyong Kim

Tucson, March, 2019

Disclaimer

These lecture slides come with a bibliography at the end. However, there has been no attempt at accurate attribution of mathematical results. Rather, the list mostly contains works the lecturer has consulted during preparation, which he hopes will be helpful for users.

I. De Rham fundamental groups

De Rham fundamental groups

F : a finite extension of \mathbb{Q}_p .

X : a smooth curve over F

\bar{X} : the basechange of X to \bar{F} .

$b, x \in X(F)$ viewed sometimes as geometric points:

$$\text{Spec}(\bar{K}) \longrightarrow \bar{X} \longrightarrow X.$$

\mathcal{X} : a smooth scheme over \mathcal{O}_F , the valuation ring of F , with good compactification and generic fiber X .

Y : special fiber of \mathcal{X} over $k = \mathcal{O}_F/m_F$.

De Rham fundamental groups

The De Rham version is similar to the etale case [Hain, AIK, Kim3]. The relevant category is

$$\text{Un}^{DR}(X) \subset \text{Loc}^{DR}(X)$$

the category of unipotent vector bundles with (flat) connections, a full subcategory of all bundles with flat connections.

There are fibre functors

$$F_b : \text{Un}^{DR}(X) \longrightarrow \text{Vect}_F,$$

$$(V, \nabla) \mapsto V_x$$

and the objects of interest are

$$U^{DR} = U^{DR}(X, b) = \text{Aut}^{\otimes}(F_b)$$

and

$$P^{DR}(x) = P^{DR}(X; b, x) = \text{Isom}^{\otimes}(F_b, F_x)$$

De Rham fundamental groups

They can be constructed using universal objects which in turn admit a tautological construction [AIK] using

$$\mathrm{Ext}_{\mathrm{Loc}^{DR}(X)}^i((V, \nabla), (V', \nabla')) \simeq H_{DR}^i(X, (V, \nabla)^* \otimes (W, \nabla)),$$

where

$$H_{DR}^i(X, (V, \nabla)) = H^i(X_{Zar}, V \longrightarrow V \otimes_{\mathcal{O}_X} \Omega_X)$$

In particular, it is a projective system

$$(\mathcal{E}_n^{DR}, \nabla_n),$$

which fit together as

$$0 \longrightarrow T_n^{DR} \otimes \mathcal{O}_X \longrightarrow \mathcal{E}_n^{DR} \longrightarrow \mathcal{E}_{n-1}^{DR} \longrightarrow 0.$$

Here, T_n^{DR} is a quotient of $(H_1^{DR})^{\otimes n}$ as in the étale case.

De Rham fundamental groups

After choosing an element $1 \in \mathcal{E}_b^{DR}$ we get the universal property:

Given any object (V, ∇_V) in $Un^{DR}(X)$ together with an element $v \in V_b$ (the fiber at b), there exists a unique morphism $\phi : (\mathcal{E}^{DR}, \nabla) \rightarrow (V, \nabla_V)$ such that $1 \in \mathcal{E}_b^{DR} \mapsto v$.

Corollary

$$End(F_b) \cong \mathcal{E}_b^{DR}.$$

De Rham fundamental groups

Theorem

The pro-algebraic group $U^{DR}(X, b)$ is isomorphic to the group-like elements in \mathcal{E}_b , while $P^{DR}(X; b, x)$ is isomorphic to the group-like elements in \mathcal{E}_x .

The universal property gives rise to a map in $\text{Un}(X)$:

$$\Delta : (\mathcal{E}^{DR}, \nabla) \longrightarrow (\mathcal{E}^{DR}, \nabla) \hat{\otimes} (\mathcal{E}^{DR}, \nabla)$$

that takes 1 to $1 \otimes 1$.

Let $\mathcal{A}^{DR} = \mathcal{E}^{DR}$ be the dual (ind-)bundle. Then Δ^* gives

$$\mathcal{A}_x^{DR} = \text{Hom}(\mathcal{E}_x^{DR}, K)$$

the structure of a commutative algebra, and

$$P^{DR}(x) = \text{Spec}(\mathcal{A}_x^{DR}).$$

De Rham fundamental groups: Hodge filtration

[Hain, Wojtkowiak, Vologodsky, Hadian, Kim3]

There is a unique decreasing filtration \mathcal{F}^i , $i \leq 0$, of \mathcal{E}^{DR} satisfying the following conditions.

- (1) Griffiths transversality $\nabla(\mathcal{F}^i) \subset \mathcal{F}^{i-1} \otimes \Omega_X$;
- (2) The induced filtration on T_n coincides with the constant one coming from (co)homology;
- (3) $1 \in F^0 \mathcal{E}_b^{DR}$.

This is the Hodge filtration on \mathcal{E}^{DR} .

There is an induced Hodge filtration with non-negative degrees on \mathcal{A}^{DR} and $F^1 \mathcal{A}^{DR}$ is an ideal. $F^0 P^{DR}(x)$ is defined to be the zero set of $F^1 \mathcal{A}_x^{DR}$. It is a torsor for $F^0 U^{DR}$, which is a subgroup of U^{DR} .

De Rham fundamental groups: Hodge filtration

This is an aspect of the fact that the action of U^{DR} on $P^{DR}(x)$ is compatible with the Hodge filtration. The action map

$$P^{DR}(x) \times U^{DR} \longrightarrow P^{DR}(x)$$

corresponds to a co-action map

$$\mathcal{A}_x^{DR} \longrightarrow \mathcal{A}_x^{DR} \otimes \mathcal{A}_b^{DR}$$

This is compatible with the Hodge filtration.

The choice of a point $p \in F^0 P^{DR}(x)$ gives an algebra homomorphism $\mathcal{A}_x^{DR} \longrightarrow F$ which kills $F^1 \mathcal{A}_x^{DR}$, which is hence a map of Hodge structures.

De Rham fundamental groups: Hodge filtration

Thus, we get an isomorphism

$$\mathcal{A}_x^{DR} \cong \mathcal{A}_b^{DR}$$

that is compatible with the Hodge filtration. A dimension count then shows that

$$F^1 \mathcal{A}_x^{DR} \cong F^1 \mathcal{A}_b^{DR},$$

and hence,

$$\mathcal{A}_x^{DR} / F^1 \mathcal{A}_x^{DR} \cong \mathcal{A}_b^{DR} / F^1 \mathcal{A}_b^{DR},$$

giving us

$$F^0 U^{DR} \cong F^0 P^{DR}(x).$$

De Rham fundamental groups: crystalline structures

In the local case, the (k -linear) Frobenius ϕ of the special fibre Y acts on the category $\text{Un}^{DR}(X)$ [Deligne, Besser].

Write $\mathcal{X} = \cup_i U_i$ so that U_i is a smooth lift of $U_i \otimes k$. Choose local lifts ϕ_i on U_i of the Frobenius on $U_i \otimes k$.

Then given a bundle with connection (V, ∇) , we consider the local pull-backs $(\phi_i^*(V|_{U_i}), \phi_i^*(\nabla))$. The connection allows us to patch these together canonically to give us $\phi^*(V, \nabla)$.

In particular,

$$(\mathcal{E}^{DR}, \nabla, 1) \longrightarrow (\phi^*\mathcal{E}^{DR}, \phi^*\nabla, \phi^*1),$$

Get compatible actions on $U^{DR}(V, b)$ and $P^{DR}(X; b, x)$.

De Rham fundamental groups: crystalline structures

On T_n , agrees with the action induced by the isomorphism

$$H_{DR}^1(X) \cong H_{\text{crys}}^1(Y).$$

Hence, the eigenvalues are the same as the ones coming from étale cohomology.

Theorem

There is a unique Frobenius invariant element $p_{b,x}^{cr}$ in $P^{DR}(X, b, x)$.

De Rham fundamental groups: crystalline structures

Lemma

The Lang map $L(\phi) : U^{DR} \longrightarrow U^{DR}$ that sends u to $u\phi^{-1}(u)$ is a bijection.

In particular, the identity is the only element fixed by ϕ .

Proof.

The eigenvalues of ϕ on $T_n^{DR} = U^{DR,n}/U^{DR,n+1}$ are all different from 1. □

Proof of theorem.

Choose $p \in P^{DR}$. Then there is a unique $u \in U^{DR}$ such that $\phi(p) = pu$. Write $u = v\phi(v^{-1})$. Then

$$\phi(pv) = pv.$$

Uniqueness comes from the fact that if p is fixed, no pu will be fixed for $u \neq e$. □

De Rham fundamental groups: crystalline structures

Better to think in terms of *crystalline fundamental groups*: Given a point $y \in Y(k)$, define on $\mathrm{Un}(X)^{DR}$ the fibre functor

$$(V, \nabla) \mapsto V([y])^{\nabla=0},$$

the flat sections of V over the tube $[y]$ of y , the analytic space of points that reduce to y .

Then for $x, x' \in [y]$, $p_{x,x'}^{cr}$ is given by the diagram

$$\begin{array}{ccc} & V([y])^{\nabla=0} & \\ \swarrow \cong & & \searrow \cong \\ V_x & & V_{x'} \end{array}$$

De Rham fundamental groups: crystalline structures

This is supplemented by an isomorphism

$$p_{yy'}^{cr} : V([y])^{\nabla=0} \cong V([y'])^{\nabla=0}$$

for $y, y' \in Y(k)$ called Coleman integration [Besser]. The computation of this is Kedlaya's theory.

De Rham moduli spaces

The space of torsors for U^{DR} that have compatible Frobenius and Hodge filtration are classified by

$$U^{DR}/F^0.$$

Given a torsor T , choose elements $t^{cr} \in T$ and $t^H \in F^0 T$. Then

$$t^H = t^{cr} u_T^{cr}.$$

The element u_T^{cr} is independent of the choice of t^H up to multiplication by $F^0 U^{DR}$ on the right, giving us a well-defined element

$$[u_T^{cr}] \in U^{DR}/F^0.$$

De Rham fundamental groups

We will give an explicit description for X affine [Kim3].

We first choose

$$\alpha_1, \alpha_2, \dots, \alpha_m,$$

global algebraic differential forms representing a basis of $H_{DR}^1(X)$.

Thus, $m = 2g + s - 1$, where s is the number of missing points.

De Rham fundamental groups

Consider the algebra

$$F\langle A_1, \dots, A_m \rangle$$

generated by the symbols A_1, A_2, \dots, A_m . Thus, it is the tensor algebra of the F -vector space generated by the A_i . Let I be the augmentation ideal.

The algebra $F\langle A_1, \dots, A_m \rangle$ has a natural comultiplication map Δ with values $\Delta(A_i) = A_i \otimes 1 + 1 \otimes A_i$.

Now let

$$E_n = F\langle A_1, \dots, A_m \rangle / I^{n+1}$$

and take the completion

$$E := \varprojlim F\langle A_1, \dots, A_m \rangle / I^n$$

Δ extends naturally to a comultiplication $E \rightarrow E \hat{\otimes} E$.

De Rham fundamental groups

\mathcal{E} : pro-unipotent pro-vector bundle $E \otimes \mathcal{O}_X$ with the connection ∇ determined by

$$\nabla_{\mathcal{E}} f = df - \sum_i A_i f \alpha_i$$

for sections $f : X \longrightarrow E$.

There is an element $1 \in \mathcal{E}_b = E$.

Theorem

There is a unique isomorphism

$$(\mathcal{E}, \nabla_{\mathcal{E}}, 1) \cong (\mathcal{E}^{DR}, \nabla, 1)$$

It is compatible with the comultiplication on either side.

De Rham fundamental groups

The theorem is an easy consequence of

Lemma

Let (V, ∇) be a unipotent bundle with flat connection on X of rank r . Then there exist strictly upper-triangular matrices N_i such that

$$(V, \nabla) \simeq (\mathcal{O}_X^r, d + \sum_i \alpha_i N_i)$$

De Rham fundamental groups

The isomorphism

$$\begin{array}{ccc}
 \mathcal{E}^{DR}(]y[)^{\nabla=0} & & \\
 \searrow \approx & & \swarrow \approx \\
 \mathcal{E}_b^{DR} & & \mathcal{E}_x^{DR}
 \end{array}$$

can be constructed locally by solving differential equations.

Let

$$f = \sum_w f_w [w]$$

be a section of \mathcal{E} , where the $[w]$ are words in the A_i , and $f(b) = 1$.

Then the flatness condition is

$$df = \sum_w \sum_i f_w \alpha_i [A_i w],$$

De Rham fundamental groups

This is

$$df_{A_i w} = f_w \alpha_i$$

for all w and i .

We solve this iteratively:

$$f_{A_i}(z) = \int_b^z \alpha_i.$$

This can be constructed as a power series with initial condition $f_{A_i}(x) = 0$.

We continue

$$f_{A_j A_i}(z) = \int_b^z f_{A_i} \alpha_j,$$

and so on. Thus, the components of f become iterated integrals.

De Rham fundamental groups

Having solved the equation with initial condition 1, get p_{bx}^{cr} for $v \in \mathcal{E}_b^{DR}$ by

$$p_{bx}^{cr}(v) = f(x)v.$$

For general x , the components of p_{bx}^{cr} give the *definition* of iterated integrals.

The shuffle identities for iterated integrals

$$\int_b^z \alpha_1 \alpha_2 \cdots \alpha_k \int_b^z \alpha_{k+1} \alpha_{k+2} \cdots \alpha_n = \sum_{\sigma} \int_b^z \alpha_{\sigma(1)} \alpha_{\sigma(2)} \cdots \alpha_{\sigma(n)}$$

with the sum running over $(k, n - k)$ shuffles of $\{1, 2, \dots, n\}$ follow from the group-like nature of $p_{b,z}^{cr}$.

De Rham fundamental groups

Another way to say this is that

$$\mathcal{A}_z^{DR} = F[\phi_w]$$

the vector space generated by ϕ_w such that $\phi_w[w'] = \delta_{ww'}$. The algebra structure is given by

$$\phi_w \phi_{w'} = \sum_{\sigma} \phi_{\sigma(ww')},$$

where again the σ run over shuffles. The iterated integral identity is the fact that

$$p_{b,z}^{cr} : \mathcal{A}_z^{DR} \longrightarrow F$$

is an algebra homomorphism.

De Rham fundamental groups

Theorem

The map

$$j^{DR} : X(F) \longrightarrow U^{DR}/F^0$$

has the property that $j^{DR}(]y[)$ is Zariski dense for each $y \in Y$.

The idea is to show that all iterated integrals are algebraically independent using transcendental methods.

Hence, as we increase n , the coordinates of the map

$$j^{DR} : X(F) \longrightarrow U_n^{DR}/F^0$$

keep giving genuinely new analytic functions.

Selmer schemes III

I. Preliminary remarks on gauge theory

Gauge theory

M : connected orientable manifold.

G : Lie group.

$\mathcal{A}(M, G)$: the space of principal G -bundles with connections.

In gauge theory, study various functions on $\mathcal{A}(M, G)$, for example,

$$YM(P, \nabla) = \int_M \|F_\nabla \wedge *F_\nabla\|^2$$

on a four-manifold, or

$$CS(P, \nabla) = \int_M Tr(A \wedge dA + (2/3)A \wedge A \wedge A).$$

on a three-manifold.

Gauge theory

The critical points of such functions will form moduli spaces

$$\mathbb{S}(M, G)$$

of classical solutions.

These can be studied for their own sake, or via the analogy

$$\mathbb{S}(M, G) \sim H^1(M, G)$$

as non-abelian cohomological invariants of M .

These have seen spectacular applications in geometry, Donaldson theory, Simpson theory, Seiberg-Witten theory, TQFT, ... (e.g. [Donaldson, Witten])

Gauge theory

In recent decades, geometers have become interested in formal integrals like

$$\int_{\mathcal{A}/\mathcal{G}} e^{-kCS(A)} dA$$

or

$$\int_{\mathcal{A}/\mathcal{G}} \text{Hol}_{K_1, R_1}(A) \text{Hol}_{K_2, R_2}(A) \cdots \text{Hol}_{K_m, R_m}(A) e^{-kCS(A)} dA,$$

where the K_i are closed curves in M and $\text{Hol}_{K_i, R_i}(A)$ denotes the holonomy in some representation R_i of G .

Would like to develop such tools for the geometric study of arithmetic schemes.

II. Geometry of non-abelian cohomology

Non-abelian cohomology functors

X/\mathbb{Q} : a smooth curve and $p > 2$ a place of good reduction.

$U = U(\bar{X}, b)$, the \mathbb{Q}_p -prounipotent étale fundamental group.

$U_n = U/U^{n+1}$.

G : either the group $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ or $G_T = \text{Gal}(\mathbb{Q}_T/\mathbb{Q})$, where \mathbb{Q}_T is the maximal extension of \mathbb{Q} unramified outside a finite set T of primes. We assume that T contains $\infty, 2, p$ and all primes of bad reduction.

Non-abelian cohomology functors

[Kim1]

We define a functor of \mathbb{Q}_p -algebras

$$R \mapsto H^1(G, U_n(R)) := U_n(R) \setminus Z^1(G, U_n(R)).$$

The H^1 refers to continuous cohomology: Z^1 denotes the continuous functions

$$f : G \longrightarrow U(R)$$

such that $f(g_1g_2) = f(g_1)g_1(f(g_2))$ on which $U_n(R)$ acts via

$$f^u(g) = uf(g)g(u^{-1}).$$

Non-abelian cohomology functors

The G -action on $U_n(R)$ is defined by identifying

$$U_n \cong^{\log} L_n := \text{Lie}(U_n).$$

In fact, it is often good to think of U_n as being L_n with group law defined by the BCH formula:

$$X \cdot Y = X + Y + (1/2)[X, Y] + (1/12)[X, [X, Y]] - (1/12)[Y, [Y, X]] + \dots$$

(Formula for $\log(\exp(X) \exp(Y))$.)

Then $U_n(R) = L_n \otimes R$.

Non-abelian cohomology functors

The topology in $U_n(R)$ is defined by using

$$U_n \cong \mathbb{A}^N,$$

which gives

$$U_n(R) \cong R^N.$$

We give R^N the inductive limit topology of finite-dimensional \mathbb{Q}_p -subspaces. (This definition works also for all affine schemes.)

On the abelian pieces U^n/U^{n+1} , the same definition of H^1 applies, but we can also define H^2 .

Proposition

$$H^i(G, U^n/U^{n+1}(R)) \cong H^i(G, U^n(\mathbb{Q}_p)/U^{n+1}(\mathbb{Q}_p)) \otimes R.$$

That is, the functor of R can be represented by the finite-dimensional \mathbb{Q}_p -vector space $H^i(G, U^n(\mathbb{Q}_p)/U^{n+1}(\mathbb{Q}_p))$.

Non-abelian cohomology functors

Theorem

The functor

$$R \mapsto H^1(G, U_n(R))$$

is represented by an affine \mathbb{Q}_p -scheme of finite type.

The scheme represents principal U_n -bundles with continuous G action:

The R -points are principal $(U_n)_R$ bundles

$$P \longrightarrow \text{Spec}(R),$$

with functorial continuous action of G on $P(S)$ for any R -algebra S .

Non-abelian cohomology functors

The proof is by induction on n using the exact sequence

$$\begin{aligned} 0 \longrightarrow H^1(G, U^n/U^{n+1}(R)) &\longrightarrow H^1(G, U_n(R)) \longrightarrow H^1(G, U_{n-1}(R)) \\ &\xrightarrow{\delta} H^2(G, U^n/U^{n+1}(R)). \end{aligned}$$

That is, once $H^1(G, U_{n-1})$ is representable, δ is a map of schemes. The exact sequence means that $H^1(G, U_n)$ defines a $H^1(G, U^n/U^{n+1})$ -torsor over $\text{Ker}(\delta)$, which then must be represented by

$$\text{Ker}(\delta) \times H^1(G, U^n/U^{n+1}).$$

Non-abelian cohomology functors

In the local case, define also

$$R \mapsto H^1(G, U_n(B_{\text{cris}} \otimes R)),$$

and

$$H_f^1(G, U_n) = \text{Ker}(H^1(G, U_n) \longrightarrow H^1(G, U_n(B_{\text{cris}}))),$$

which is a subscheme by induction on n :

$$\begin{array}{ccccccc}
 0 & \longrightarrow & H^1(G, U^n/U^{n+1}) & \longrightarrow & H^1(G, U_n) & \longrightarrow & H^1(G, U_{n-1}) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \rightarrow & H^1(G, U^n/U^{n+1}(B_{\text{cris}})) & \rightarrow & H^1(G, U_n(B_{\text{cris}})) & \rightarrow & H^1(G, U_{n-1}(B_{\text{cris}}))
 \end{array}$$

Non-abelian cohomology functors

$H_f^1(G_p, U_n)$ represents torsors that have a G_p -invariant point in $U_n(B_{\text{cris}})$.

We have the localisation

$$H^1(G_T, U_n) \longrightarrow H^1(G_p, U_n)$$

using which we define $H_f^1(G_T, U_n) = \text{loc}_p^{-1}(H_f^1(G_p, U_n))$.

Thus, we get a diagram

$$\begin{array}{ccc} X(\mathbb{Z}) & \longrightarrow & X(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ H_f^1(G_T, U_n) & \longrightarrow & H_f^1(G_p, U_n) \end{array}$$

The bottom arrow is a map of schemes since it represents a map of functors. It is a *computable replacement* for $X(\mathbb{Z}) \subset X(\mathbb{Z}_p)$,

De Rham moduli spaces

The reason $X(\mathbb{Z}_p)$ maps to H_f^1 is because of the non-abelian p -adic Hodge theory isomorphism:

$$P_n^{et}(x)(B_{cr}) \cong P_n^{DR}(x)(B_{cr}) \cong B_{cr}^N.$$

The first isomorphism respects all structures, while the second is Galois equivariant, showing the existence of an invariant point.

II. The fundamental diagram

The fundamental diagram

[Kim1, Kim2, Kim3]

Given T a crystalline torsor for U , the trivialisations of $T(B_{cr})$ form a torsor $D(T)$ for U^{DR} .

Lemma

$$T \mapsto D(T)$$

defines an isomorphism

$$H_f^1(G_p, U_n) \cong U_n^{DR}/F^0.$$

The fundamental diagram

$$\begin{array}{ccc}
 X(\mathbb{Z}) & \longrightarrow & X(\mathbb{Z}_p) \\
 \downarrow & & \downarrow \searrow \\
 H_f^1(G_T, U_n) & \longrightarrow & H_f^1(G_p, U_n) \cong U_n^{DR}/F^0
 \end{array}$$

The isomorphism on the right comes from the construction of an inverse using the fundamental exact sequence of p -adic Hodge theory:

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_{cr}^{\phi=1} \oplus B_{DR}^+ \longrightarrow B_{DR} \longrightarrow 0.$$

The fundamental diagram

From this, we get

$$U(B_{DR})/U(B_{DR}^+) \longrightarrow H^1(G, U) \longrightarrow H^1(G, U(B_{cr}^\phi)).$$

For U , we get an equality between

$$H_e^1(G, U) = \text{Ker}[H^1(G, U) \longrightarrow H^1(G, U(B_{cr}^\phi))]$$

and

$$H_f^1(G, U) = \text{Ker}[H^1(G, U) \longrightarrow H^1(G, U(B_{cr}))]$$

Bibliography

-  Andreatta, Fabrizio; Iovita, Adrian; Kim, Minhyong A p-adic nonabelian criterion for good reduction of curves. Duke Math. J. 164 (2015), no. 13, 2597–2642.
-  Besser, Amnon Coleman integration using the Tannakian formalism. Math. Ann. 322 (2002), no. 1, 19?48.
-  Donaldson, S. K. An application of gauge theory to four-dimensional topology. J. Differential Geom. 18 (1983), no. 2, 279–315.
-  Deligne, Pierre Le groupe fondamental de la droite projective moins trois points. Galois groups over \mathbb{Q} (Berkeley, CA, 1987), 79–297, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.
-  M. Hadian: *Motivic Fundamental Groups and Integral Points*. Duke Math. J. **160** (2011), 503 V565

Bibliography

-  Hain, Richard M. The de Rham homotopy theory of complex algebraic varieties. I, K-Theory 1 (1987), no. 3, 271–324.
-  Kim, Minhyong The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. Invent. Math. 161 (2005), no. 3, 629–656.
-  Kim, Minhyong Tangential localization for Selmer varieties. Duke Math. J. 161 (2012), no. 2, 173–199.
-  Kim, Minhyong The unipotent Albanese map and Selmer varieties for curves. Publ. Res. Inst. Math. Sci. 45 (2009), no. 1, 89–133.
-  V. Vologodsky, *Hodge structures on the fundamental group and its applications to p-adic integration*. Mosc. Math. J. 3 (2003), 205–247.

Bibliography

-  Witten, Edward Quantum field theory and the Jones polynomial. *Comm. Math. Phys.* 121 (1989), no. 3, 351–399.
-  Wojtkowiak, Z. Cosimplicial objects in algebraic geometry, in Algebraic K-theory and algebraic topology (Lake Louise, AB, 1991), 287-327, Kluwer Acad. Publ., Dordrecht,

Selmer Schemes IV

Minhyong Kim

Tucson, March, 2020

Disclaimer

These lecture slides come with a bibliography at the end. However, there has been no attempt at accurate attribution of mathematical results. Rather, the list mostly contains works the lecturer has consulted during preparation, which he hopes will be helpful for users.

Non-abelian descent?

[Kim1]

From here on, we assume that X is a smooth proper curve of genus ≥ 2 . We will focus on the base field \mathbb{Q} , even though Netan Dogra has generalised all the arguments to number fields [1].

$$\begin{array}{ccc}
 X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\
 \downarrow & & \downarrow \\
 H_f^1(G_T, U_n) & \xrightarrow{\text{loc}_p} & H_f^1(G_p, U_n) \xrightarrow{\cong^D} U_n^{DR} / F^0
 \end{array}$$

Conjecture (A)

The image of loc_p is non-dense for $n \gg 0$.

Theorem

Assuming the conjecture, $X(\mathbb{Q})$ is finite.

Non-abelian descent?

Proof.

By assumption, there is an algebraic function $\alpha \neq 0$ that vanishes on $D(\text{loc}_p(H_f^1(G_T, U_n)))$. Hence,

$$\alpha \circ j^{DR} | X(\mathbb{Q}) = 0.$$

But $\alpha \circ j^{DR}$ is a non-zero convergent power series on each $]y[$, $y \in Y(\mathbb{F}_p)$. So the zero set is finite. □

Define

$$\begin{aligned} X(\mathbb{Q}_p)_n &:= \cap_{\alpha \circ D \circ \text{loc}_p=0} Z(\alpha \circ j^{DR}) \\ &= (j^{DR})^{-1}(\overline{D(\text{loc}_p(H_f^1(G_T, U_n)))}). \end{aligned}$$

Non-abelian descent?

[BDKW]

Since the diagrams are compatible over n , we get a decreasing filtration:

$$X(\mathbb{Q}_p) \supset X(\mathbb{Q}_p)_1 \supset X(\mathbb{Q}_p)_2 \supset X(\mathbb{Q}_p)_3 \supset \dots$$

Note that the conjecture actually implies that $X(\mathbb{Q}_p)_n$ is finite for $n \gg 0$.

Conjecture (B)

$$\cap_n X(\mathbb{Q}_p)_n = X(\mathbb{Q})$$

Conjecture (C)

$\cap_n X(\mathbb{Q}_p)_n$ is computable and conjecture (B) is computationally verifiable.

Non-abelian descent?

Key problem:

Find defining equations for

$$\text{loc}_p(H_f^1(G_T, U_n)) \subset H_f^1(G_p, U_n).$$

Are there *canonical* equations related to non-abelian L -functions?

A canonical trivialisation

$$R\Gamma(G_T, U) \sim^{\mathcal{L}} 0$$

in a suitable homotopy category?

Should be similar to the annihilation of Selmer groups by p -adic L -functions [CK] or Iwasawa's theorem on the image of cyclotomic units in local units [1].

II. Effectivity and the section conjecture

Effectivity and the section conjecture

[Kim2]

Assumptions:

(1) The map

$$H_f^1(G, U_n) \longrightarrow U_n^{DR}/F^0$$

can be effectively computed.

(2) Using (1), we can compute an effective lower bound for the p -adic distances between the points in $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$.

Effectivity and the section conjecture

(3) Thus, we get an effective M such that $X(\mathbb{Q}) \longrightarrow X(\mathbb{Z}/p^M)$ is injective.

(4) Using this, we get effective N , for example, $N = |J_X(\mathbb{Z}/p^M)|$, such that

$$X(\mathbb{Q}) \subset J(\mathbb{Q}) \subset J(\mathbb{Z})/NJ(\mathbb{Q}) \hookrightarrow H^1(G_S, J[N])$$

is injective, where S is the set of all places of bad reduction, and the primes dividing pN .

Effectivity and the section conjecture

(5) Grothendieck's section conjecture [Grothendieck]:

$$X(F) \cong H^1(G_F, \hat{\pi}_1(\bar{X}, b)).$$

Note that for elliptic curves, one conjectures

$$E(F) \otimes \mathbb{Z}_p \cong H_f^1(G_F, \hat{\pi}_1(\bar{E}, b)^{(p)}).$$

Effectivity and the section conjecture

Let n be larger than N and all the primes in S .

- $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $G_n = \pi_1(\text{Spec}(\mathbb{Z}[1/n!]))$.
- $\Delta = \hat{\pi}_1(\bar{X}, b)$ and K_n the intersection of all open subgroups of index $\leq n$. (There are finitely many, and K is normal.)
- $\Delta(n) = \Delta/K_n$. Thus the prime divisors of the order of any element in $\Delta(n)$ is $\leq n$.
- Denote by $\pi(n)$ the quotient of $\hat{\pi}(X, b)$ by K_n , so that we have a pushout diagram:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \Delta & \longrightarrow & \hat{\pi}(X, b) & \longrightarrow & G & \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow & \\
 0 & \rightarrow & \Delta(n) & \longrightarrow & \pi(n) & \longrightarrow & G & \longrightarrow 0.
 \end{array}$$

Effectivity and the section conjecture

There is a pull-back diagram

$$\begin{array}{ccccccc}
 0 & \rightarrow & \Delta(n) & \longrightarrow & \pi(n) & \longrightarrow & G & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \rightarrow & \Delta(n) & \longrightarrow & \pi_1(\mathfrak{X}_n, b)/K_n & \longrightarrow & G_n & \longrightarrow & 0
 \end{array}$$

where \mathfrak{X}_n is a smooth projective model for X over $\text{Spec}(\mathbb{Z}[1/n!])$.

Hence, any point $x \in X(\mathbb{Q})$ defines a class in $H^1(G_n, \Delta(n))$.

Effectivity and the section conjecture

We have a commutative diagram

$$\begin{array}{ccc}
 X(\mathbb{Q}) & \hookrightarrow & H^1(G, \Delta) \\
 \downarrow & & \downarrow \\
 H^1(G_n, \Delta(n)) & \hookrightarrow & H^1(G, \Delta(n))
 \end{array}$$

and hence, a sequence of subsets $H^i(G, \Delta)_n$ consisting of classes whose images in $H^1(G, \Delta(n))$ come from $H^1(G_n, \Delta(n))$.

Effectivity and the section conjecture

Thus we have diagrams

$$\begin{array}{ccc}
 H^1(G, \Delta)_n & \hookrightarrow & H^1(G, \Delta) \\
 \downarrow & & \downarrow \\
 H^1(G_n, \Delta(n)) & \hookrightarrow & H^1(G, \Delta(n)) \\
 \downarrow & & \downarrow \\
 H^1(G_S, J[N]) & \hookrightarrow & H^1(G_n, J[N])
 \end{array}$$

Effectivity and the section conjecture

and

$$\begin{array}{ccccc}
 & & H^1(G_{n+1}, \Delta(n+1)) & & \\
 & & \downarrow & & \\
 H^1(G_n, \Delta(n)) & \hookrightarrow & H^1(G_{n+1}, \Delta(n)) & & \\
 \downarrow & & \downarrow & & \\
 H^1(G_S, J[N]) & \hookrightarrow & H^1(G_n, J[N]) & \hookrightarrow & H^1(G_{n+1}, J[N])
 \end{array}$$

Effectivity and the section conjecture

Using this, we can define a decreasing sequence of subsets

$$H^1(G_S, J[N])_{n+1} \subset H^1(G_S, J[N])_n$$

consisting of those classes whose images in $H^1(G_i, J[N])$ lift to $H^1(G_i, \Delta(i))$ for all $i \leq n$, i larger than $n_0 = \sup(N, p \in S)$.

Meanwhile, there is an increasing sequence of subsets $X(\mathbb{Q})_n$ of points whose heights are $\leq n$, all of which occur in the ‘non-abelian descent sequence’:

$$\cdots X(\mathbb{Q})_n \subset X(\mathbb{Q})_{n+1} \subset X(\mathbb{Q})_{n+2} \subset \cdots$$

$$\cdots \subset H^1(G_S, J[N])_{n+2} \subset H^1(G_S, J[N])_{n+1} \subset H^1(G_S, J[N])_n \subset \cdots$$

Effectivity and the section conjecture

Using the section conjecture,

$$X(\mathbb{Q})_n = H^1(G_S, J[N])_n$$

for n sufficiently large, and $X(\mathbb{Q})_n = X(\mathbb{Q})$ at that point.

Effectivity and the section conjecture

To check this, note that the section conjecture implies that the inclusions

$$X(\mathbb{Q}) \subset H^1(G, \Delta)_n \subset H^1(G, \Delta),$$

are all equalities.

From the diagrams

$$\begin{array}{ccc} H^1(G, \Delta)_n & \xrightarrow{=} & H^1(G, \Delta) \\ \downarrow & & \downarrow \\ H^1(G_n, \Delta(n)) & \hookrightarrow & H^1(G, \Delta(n)) \end{array}$$

we have maps

$$H^1(G, \Delta) \longrightarrow H^1(G_n, \Delta(n))$$

and

$$H^1(G, \Delta) = \varprojlim H^1(G, \Delta(n)) = \varprojlim H^1(G_n, \Delta(n)).$$

Effectivity and the section conjecture

Suppose

$$c \in H^1(G_S, J[N])_n$$

for all n . Then the set

$$H^1(\Gamma_n, \Delta(n))_c$$

of classes that lift c is non-empty for all n , and hence,

$$X(\mathbb{Q})_c = H^1(\Gamma, \Delta)_c = \varprojlim H^1(\Gamma_n, \Delta(n))_c$$

is non-empty.

This shows that

$$\cap_n H^1(G_S, J[N])_n = X(\mathbb{Q}).$$

Since all sets are finite, we must have

$$X(\mathbb{Q}) = H^1(G_S, J[N])_n$$

for some n .

III. Remark on non-abelian reciprocity

Diophantine geometry: remark on non-abelian reciprocity

[Kim3]

Given a variety X over a number field F , can one describe the inclusion

$$X(F) \subset X(\mathbb{A}_F)$$

?

For \mathbb{G}_m , this is partially achieved by the reciprocity map

$$\mathbb{G}_m(F) \hookrightarrow \mathbb{G}_m(\mathbb{A}_F) \xrightarrow{\text{rec}} \text{Gal}^{ab}(\bar{F}/F)$$

For an affine conic

$$C : ax^2 + by^2 = c$$

described by a class $\chi \in H^1(\text{Gal}(\bar{F}/F), \pm 1)$, can replace this by

$$C(F) \hookrightarrow C(\mathbb{A}_F) \longrightarrow \text{Hom}(H^1(\text{Gal}(\bar{F}/F), \mathbb{Q}/\mathbb{Z}(\chi)), \mathbb{Q}/\mathbb{Z}).$$

Diophantine geometry: remark on non-abelian reciprocity

There is a **non-abelian class field theory** with coefficients in a fairly general variety X over a number field F generalising CFT with coefficients in \mathbb{G}_m .

This consists (with some simplifications) of a filtration

$$X(\mathbb{A}_F) = X(\mathbb{A}_F)_1 \supset X(\mathbb{A}_F)_2 \supset X(\mathbb{A}_F)_3 \supset \dots$$

and a sequence of maps

$$rec_n : X(\mathbb{A}_F)_n \longrightarrow \mathfrak{G}_n(X)$$

to a sequence of groups such that

$$X(\mathbb{A}_F)_{n+1} = rec_n^{-1}(0).$$

Diophantine geometry: remark on non-abelian reciprocity

$$\cdots \ rec_3^{-1}(0) \subset rec_2^{-1}(0) \subset rec_1^{-1}(0) \subset X(\mathbb{A}_F)$$

|| || || ||

$$\cdots \ X(\mathbb{A}_F)_4 \subset X(\mathbb{A}_F)_3 \subset X(\mathbb{A}_F)_2 \subset X(\mathbb{A}_F)_1$$

$$\begin{array}{cccc} & & & \\ & rec_4 \downarrow & rec_3 \downarrow & rec_2 \downarrow & rec_1 \downarrow \\ \cdots & \mathfrak{G}_4(X) & \mathfrak{G}_3(X) & \mathfrak{G}_2(X) & \mathfrak{G}_1(X) \end{array}$$

Diophantine geometry: remark on non-abelian reciprocity

Put

$$X(\mathbb{A}_F)_\infty = \cap_{n=1}^{\infty} X(\mathbb{A}_F)_n.$$

Theorem (Non-abelian reciprocity)

$$X(F) \subset X(\mathbb{A}_F)_\infty.$$

For a fixed p , can define $X(\mathbb{Q}_p)_n := pr_p(X(\mathbb{A}_F)_\infty)$

Conjecture

Suppose X is a smooth projective curve of genus ≥ 2 . Then

$$X(F) = X(\mathbb{Q}_p)_\infty = \cap_n X(\mathbb{Q}_p)_n.$$

IV. Principal bundles in Diophantine geometry: a little history

Principal bundles in Diophantine geometry: a little history

Weil [Weil1] in 1929 constructed an embedding

$$j : X \hookrightarrow J_X,$$

where J_X is an abelian variety of dimension g .

That is, over \mathbb{C} ,

$$J_X(\mathbb{C}) = \mathbb{C}^g / \Lambda = H^0(X(\mathbb{C}), \Omega_{X(\mathbb{C})}^1)^*/H_1(X, \mathbb{Z}).$$

The map j is defined over \mathbb{C} by fixing a basepoint b and

$$j(x)(\alpha) = \int_b^x \alpha \mod H_1(X, \mathbb{Z}),$$

for $\alpha \in H^0(X(\mathbb{C}), \Omega_{X(\mathbb{C})}^1)$.

Principal bundles in Diophantine geometry: a little history

But Weil's point was that J_X is also a projective algebraic variety defined over \mathbb{Q} , and if $b \in X(\mathbb{Q})$, then the map j is also defined over \mathbb{Q} .

The reason is that J_X is a moduli space of line bundles of degree 0 on X and

$$j(x) = \mathcal{O}(x) \otimes \mathcal{O}(-b).$$

The main application is that

$$j : X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q}).$$

Weil also proved that $J(\mathbb{Q})$ is a finitely-generated abelian group, and hoped, without success, that this could be somehow used to study $X(\mathbb{Q})$.

Principal bundles in Diophantine geometry: a little history

In the 1938 paper ‘Généralisation des fonctions abéliennes’, Weil [Weil2] studied

$$Bun_X(GL_n) = GL_n(K(X)) \backslash GL_n(\mathbb{A}_{K(X)}) / \left[\prod_x GL_n(\widehat{\mathcal{O}_x}) \right]$$

as a ‘non-abelian Jacobian’.

Proved a number of foundational theorems, including the fact that vector bundles of degree zero admit flat connections, beginning non-abelian Hodge theory.

Principal bundles in Diophantine geometry: a little history

This paper was very influential in geometry, leading to the paper of Narasimhan and Seshadri [NS]:

$$Bun_X(GL_n)_0^{st} \simeq H^1(X, U(n))^{irr}.$$

This was extended by Donaldson [Donaldson], influencing this work on smooth manifolds and gauge theory, and by Simpson [Simpson] to

$$Higgs(GL_n) \simeq H^1(X, GL_n).$$

Serre on Weil's paper:

'a text presented as analysis, whose significance is essentially algebraic, but whose motivation is arithmetic'

Diophantine principal bundles

Go back to Hodge theory of Jacobian:

$$X(\mathbb{C}) \longrightarrow J_X(\mathbb{C}) \simeq \mathrm{Ext}_{MHS, \mathbb{Z}}^1(\mathbb{Z}, H_1(X(\mathbb{C}), \mathbb{Z})).$$

$$X(\mathbb{Q}) \longrightarrow J_X(\mathbb{Q}) \otimes \mathbb{Z}_p \simeq \mathrm{Ext}_{\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), f}^1(\mathbb{Z}_p, H_1^{et}(\bar{X}, \mathbb{Z}_p)).$$

(Second isomorphism conjectural.)

Also,

$$H_1 = \pi_1^{ab}$$

suggesting the possibility of extending the constructions to non-abelian homotopy and moduli space of non-abelian structures:

- over \mathbb{C} , Hain's higher Albanese varieties [Hain];
- over \mathbb{Q}_p , p -adic period spaces;
- over global fields, Selmer schemes and variants.

Bibliography

-  Balakrishnan, Jennifer; Dan-Cohen, Ishai; Kim, Minhyong; Wewers, Stefan A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. <https://arxiv.org/abs/1209.0640>. To be published in Math. Ann.
-  Coates, John; Kim, Minhyong Selmer varieties for curves with CM Jacobians. Kyoto J. Math. 50 (2010), no. 4, 827–852.
-  Coates, J.; Sujatha, R. Cyclotomic fields and zeta values. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.
-  Donaldson, S. K. An application of gauge theory to four-dimensional topology. J. Differential Geom. 18 (1983), no. 2, 279–315.
-  Grothendieck, Alexander Brief an G. Faltings. London Math. Soc. Lecture Note Ser., 242, Geometric Galois actions, 1, 49–58, Cambridge Univ. Press, Cambridge, 1997.
-  Hain, Richard, M. Higher Albanese manifolds, in Hodge theory

Bibliography

-  Dogra, Netan Unlikely intersections and the Chabauty-Kim method over number fields. arXiv:1903.05032
-  Kim, Minhyong Remark on fundamental groups and effective Diophantine methods for hyperbolic curves. Number theory, analysis and geometry, 355–368, Springer, New York, 2012.
-  Kim, Minhyong Diophantine geometry and non-abelian reciprocity laws I. Elliptic curves, modular forms and Iwasawa theory, 311–334, Springer Proc. Math. Stat., 188, Springer, Cham, 2016.
-  Kim, Minhyong Principal bundles and reciprocity laws in number theory. Algebraic geometry: Salt Lake City 2015, 305–318, Proc. Sympos. Pure Math., 97.2, Amer. Math. Soc., Providence, RI, 2018.
-  Narasimhan, M. S.; Seshadri, C. S. Stable and unitary vector bundles on a compact Riemann surface. Ann. of Math. (2) 82 1965 540–567.

Bibliography

-  Simpson, Carlos T. Higgs bundles and local systems. *Inst. Hautes Études Sci. Publ. Math.* No. 75 (1992), 5–95.
-  Weil, André L'arithmétique sur les courbes algébriques. *Acta Math.* 52 (1929), no. 1, 281–315.
-  Weil, André Généralisation des fonctions abéliennes. *J. Math Pur. Appl.* 17 (1938), no. 9, 47–87.

AWS 2020: COMPUTATIONAL TOOLS FOR QUADRATIC CHABAUTY

JENNIFER BALAKRISHNAN

1. COURSE OUTLINE

Given a smooth projective curve X/\mathbf{Q} , one aim of Kim's nonabelian Chabauty program [Kim09, Kim10a, Kim10b] is to determine $X(\mathbf{Q})$ algorithmically. This course will highlight the computational aspects of the *quadratic Chabauty* method [BD18, BD17, BDM⁺19], and in particular, describe algorithms used to compute the finite set of p -adic points $X(\mathbf{Q}_p)_2$ in certain cases where

$$r < g + \rho - 1,$$

where g is the genus of X , ρ is the Picard number of the Jacobian J , and $r = \text{rk } J(\mathbf{Q})$. This course will be closely linked to Steffen Müller's course on the theoretical aspects of quadratic Chabauty. Here is a provisional outline of the lectures in this course.

Lecture I: The basic tools. Start by carrying out the linear algebra of explicit Chabauty–Coleman for curves over \mathbf{Q} , with Coleman integration as a black box. Describe how the Chabauty–Coleman diagram generalizes and motivate the presence of iterated Coleman integrals. Discuss Coleman integration [Col85, Bes12] and give preliminaries for explicit Coleman integration, starting with the p -adic point-counting algorithm of Kedlaya and Tuitman [Ked01, Ked07, Tui16, Tui17].

Lecture II: The basic tools, continued. Give algorithms for computing Coleman integrals of differentials of the first and second kind on curves [BBK10, BT17]. Describe algorithms to compute Coleman–Gross local p -adic heights [CG89, BB12], and in particular, Coleman integrals of 1-forms of the third kind on curves.

Lecture III: p -adic heights for quadratic Chabauty. Discuss the Nekovář p -adic height [Nek93] and our intended application. Show how universal properties [Kim09, Had11] lead us to computing the Hodge filtration and Frobenius structure. Reduce to linear algebra and solving p -adic differential equations.

Lecture IV: Examples. Apply the computation of the Nekovář height in a collection of examples to determine $X(\mathbf{Q})$. This could include bielliptic genus 2 curves, modular curves of genus 3 with real multiplication, and curves with few rational points. Discuss where the current frontier is and what remains to be done.

2. PROJECTS

Below are some ideas for possible projects:

- (1) *Coleman integration for curves over number fields and a Chabauty–Coleman solver.* The goals of this project would be to give an algorithm to compute Coleman integrals on curves over number fields, implement the algorithm, and use this to give a Chabauty–Coleman solver for curves over number fields that would take as input a genus g curve X defined over a number

Date: September 5, 2019.

field K with $r = \text{rk } J(K) < g$, a prime \mathfrak{p} of good reduction, and r generators of the Mordell–Weil group modulo torsion and output the set $X(K_{\mathfrak{p}})_1$.

Suggested reading: Coleman integration.

- (2) *Quadratic Chabauty on modular curves $X_0(N)^+$.* Galbraith [Gal96, Gal99, Gal02] has constructed models for all modular curves $X_0(N)^+ = X_0(N)/w_N$ of genus ≤ 5 (with the exception of $N = 263$) and has conjectured that he has found all exceptional points on these curves. This project will use quadratic Chabauty to prove as much as possible about Galbraith’s conjecture. Another goal is to investigate whether we can use p -adic Gross-Zagier to carry out quadratic Chabauty for $X_0(N)^+$, starting with the case of such curves of genus 2.

Suggested reading: Modular curves, p -adic heights, p -adic L -functions.

- (3) *Quadratic Chabauty and Kim’s conjecture.* When X/\mathbf{Q} is a genus g curve with $r = \text{rk } J(\mathbf{Q}) = g - 1$, then typically the set of p -adic points $X(\mathbf{Q}_p)_1$ cut out by the Chabauty-Coleman method strictly contains $X(\mathbf{Q})$. In this project, we will first give an algorithm to compute the quadratic Chabauty set $X(\mathbf{Q}_p)_2$ under these hypotheses. Then we will investigate whether the quadratic Chabauty set, which satisfies

$$X(\mathbf{Q}) \subset X(\mathbf{Q}_p)_2 \subset X(\mathbf{Q}_p)_1 \subset X(\mathbf{Q}_p),$$

is equal to $X(\mathbf{Q})$. (See [Bia19] for the case of integral points on punctured elliptic curves.) If $X(\mathbf{Q}) \neq X(\mathbf{Q}_p)_2$, we would like to characterize the points in $X(\mathbf{Q}_p)_2 \setminus X(\mathbf{Q})$. This project could be carried out on a database of genus 2 and 3 curves [The19].

Suggested reading: Chabauty-Coleman method, p -adic heights.

For the computational part of Projects 1 and 3, we will use the computer algebra system **Magma**. For Project 2, **Magma** would be useful, but restricting to the case of hyperelliptic curves would also be very interesting (and likely more tractable, from the point of view of determining Mordell–Weil ranks unconditionally), and in this case, we could use **SageMath**.

REFERENCES

- [BB12] J. S. Balakrishnan and A. Besser. Computing local p -adic height pairings on hyperelliptic curves. *IMRN*, 2012(11):2405–2444, 2012. [↑1](#).
- [BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010. [↑1](#).
- [BD17] Jennifer S Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *arXiv preprint arXiv:1705.00401*, 2017. [↑1](#).
- [BD18] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points I: p -adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. [↑1](#).
- [BDM⁺19] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019. [↑1](#).
- [Bes12] A. Besser. Heidelberg lectures on Coleman integration. In Jakob Stix, editor, *The Arithmetic of Fundamental Groups*, volume 2 of *Contributions in Mathematical and Computational Sciences*, pages 3–52. Springer Berlin Heidelberg, 2012. [↑1](#).
- [Bia19] Francesca Bianchi. Quadratic Chabauty for (bi)elliptic curves and Kim’s conjecture. *arXiv:1904.04622*, 2019. [↑3](#).
- [BT17] Jennifer S. Balakrishnan and Jan Tuitman. Explicit Coleman integration for curves. *Arxiv preprint*, 2017. [↑1](#).
- [CG89] Robert F. Coleman and Benedict H. Gross. p -adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, MA, 1989. [↑1](#).
- [Col85] R. Coleman. Torsion points on curves and p -adic abelian integrals. *Annals of Math.*, 121:111–168, 1985. [↑1](#).
- [Gal96] S. D. Galbraith. Equations for modular curves. *Oxford DPhil thesis*, 1996. [↑2](#).
- [Gal99] Steven D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1999. [↑2](#).

- [Gal02] Steven D. Galbraith. Rational points on $X_0^+(N)$ and quadratic \mathbb{Q} -curves. *J. Théor. Nombres Bordeaux*, 14(1):205–219, 2002. ↑2.
- [Had11] M. Hadian. Motivic fundamental groups and integral points. *Duke Math. J.*, 160(3):503–565, 2011. ↑1.
- [Ked01] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16:323–338, 2001. erratum *ibid.* **18** (2003), 417–418. ↑1.
- [Ked07] K. Kedlaya. p -Adic cohomology: from theory to practice. *Arizona Winter School Notes*, 2007. ↑1.
- [Kim09] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. ↑1.
- [Kim10a] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010. ↑1.
- [Kim10b] M. Kim. p -Adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication. *Ann. of Math.* (2), 172(1):751–759, 2010. ↑1.
- [Nek93] J. Nekovar. On p -adic height pairings. In *Séminaire de Théorie des Nombres, Paris 1990-1991*, pages 127–202. Birkhäuser, 1993. ↑1.
- [The19] The LMFDB Collaboration. The L-functions and Modular Forms Database. <http://www.lmfdb.org>, 2019. [Online; accessed 1 July 2019]. ↑3.
- [Tui16] Jan Tuitman. Counting points on curves using a map to \mathbf{P}^1 . *Math. Comp.*, 85(298):961–981, 2016. ↑1.
- [Tui17] Jan Tuitman. Counting points on curves using a map to \mathbf{P}^1 , II. *Finite Fields Appl.*, 45:301–322, 2017. ↑1.

E-mail address: `jbalal@bu.edu`

COMPUTATIONAL TOOLS FOR QUADRATIC CHABAUTY

JENNIFER S. BALAKRISHNAN AND J. STEFFEN MÜLLER

CONTENTS

1. Introduction	2
1.1. A question about triangles	3
1.2. The Chabauty–Coleman method and explicit Coleman integration	8
1.3. Some p -adic cohomology	11
1.4. More p -adic cohomology	20
1.5. Iterated Coleman integrals	25
1.6. An application (preview)	28
2. p -adic heights on Jacobians of curves	29
2.1. p -adic heights on elliptic curves	29
2.2. p -adic heights on Jacobians of curves	33
2.3. An application to integral points	38
3. Nekovář’s p -adic heights	41
3.1. p -adic Hodge theory	41
3.2. Nekovář’s construction of p -adic heights	42
3.3. Local heights	44
4. Quadratic Chabauty: theory	47
4.1. Chabauty–Kim theory	48
4.2. Quadratic Chabauty	51
4.3. Dimension counts	51
4.4. Constructing a $\mathbb{Q}_p(1)$ -quotient of U_2	52
4.5. Beyond potentially good reduction: the twisting construction	54
4.6. Extending the quadratic Chabauty Lemma	55
5. Computing with quadratic Chabauty	55
5.1. Twisting and mixed extensions	58
5.2. Algorithms for the local height at p	60
5.3. Algorithms for quadratic Chabauty	67
5.4. An example	69
5.5. Future directions	73

Date: February 23, 2020.

Acknowledgements	73
Appendix A. Some nonabelian cohomology	73
A.1. The twisting construction	74
References	75

1. INTRODUCTION

The *quadratic Chabauty* method is the first nonabelian step of Kim’s program for achieving an algorithmic determination of the set $X(\mathbb{Q})$ of rational points on a nice¹ curve X/\mathbb{Q} of genus g of 2 or more. The quadratic Chabauty set $X(\mathbb{Q}_p)_2 \supset X(\mathbb{Q})$ is a finite subset of $X(\mathbb{Q}_p)$ for those curves with good reduction at p and Jacobian J having Mordell–Weil rank r and Néron–Severi rank $\rho(J)$ satisfying the hypothesis

$$r < g + \rho(J) - 1.$$

In these notes², we develop tools for carrying out the quadratic Chabauty method in the case when $r = g$ and $\rho(J) \geq 2$, with a focus on algorithmic and computational³ aspects. The goal of these notes are two-fold: first, to serve as a user’s guide for those interested in getting started with the quadratic Chabauty method, and second, to highlight some interesting problems along the way.

Kim’s nonabelian Chabauty program is a vast generalization of the Chabauty–Coleman method. The latter solely uses *abelian* geometric data: the structure of the Jacobian, as well as p -adic abelian integrals. It applies to curves satisfying the hypothesis $r < g$ and relies on the construction of an annihilating differential, which essentially can be computed using p -adic linear algebra.

Since the classical Chabauty–Coleman method motivates some of our framing of the quadratic Chabauty method, we begin our discussion by giving a survey of the tools used to carry out the former method, where there are still a number of tractable computational challenges. The main construction here is how p -adic (Coleman) integrals can be computed using p -adic cohomology. Then when the Chabauty–Coleman hypothesis is satisfied, one can use the calculation of Coleman integrals to compute a finite set of points $X(\mathbb{Q}_p)_1 \supset X(\mathbb{Q})$.

We also describe how n -fold iterated Coleman integrals can be computed, which in the case of $n = 2$, provides input into computations involving p -adic heights. We then survey a few constructions of p -adic heights in various settings, which leads into the quadratic Chabauty method. We briefly describe how this fits into Kim’s nonabelian Chabauty program, though a more comprehensive treatment of the theory will be covered in Kim’s lecture course. Finally, we combine the algorithms for quadratic Chabauty to carry out an example to determine rational points on the Atkin–Lehner quotient modular curve $X_0(167)^+$, which has genus 2 and rank 2.

Throughout, we illustrate our techniques with examples, and where possible, we include or link to code snippets for carrying out computations in **SageMath** [The20] or **Magma** [BCP97].

¹Throughout, by a *nice* curve, we mean one that is smooth, projective, and geometrically irreducible.

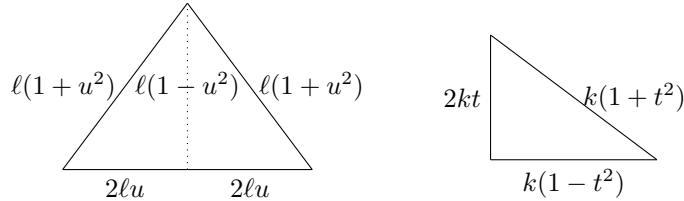
²These are lecture notes for the course “Computational tools for quadratic Chabauty”, taught by JB at the 2020 Arizona Winter School on Nonabelian Chabauty. They were originally planned as a combined set of lecture notes for this course and an additional course, “Quadratic Chabauty”, taught by SM at the 2020 AWS. SM withdrew his participation after realizing that, in contrast to previous editions, the 2020 edition of the school would be supported by the NSA.

³While computations of p -adic objects are usually not exact, one can analyze the precision necessary to produce provably correct results.

1.1. A question about triangles. We start with a question from Euclidean geometry that leads to an interesting Diophantine problem. We say that a *rational triangle* is one all of whose side lengths are rational.

Question. Does there exist a rational right triangle and a rational isosceles triangle that have the same area and the same perimeter?

This would mean that we have a pair of triangles with the following side lengths:



Let us rescale so that we may assume $\ell = 1$. We further suppose that $k, t, u \in \mathbb{Q}$, $0 < t, u < 1$ and $k > 0$. By equating areas and perimeters, we obtain the following system of equations:

$$\begin{aligned} k^2 t (1 - t^2) &= 2u(1 - u^2) \\ k + kt &= 1 + 2u + u^2 \end{aligned}$$

Let $x = 1 + u$. After some algebra, we see that there is $x \in \mathbb{Q} \cap (1, 2)$ such that

$$2xk^2 + (-3x^3 - 2x^2 + 6x - 4)k + x^5 = 0.$$

Then noting that the discriminant of the polynomial in k is a rational square, we have that

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

and simplifying, this gives us a genus 2 curve

$$X : y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16.$$

We would like to compute the set of rational points $X(\mathbb{Q})$ on X . Some useful input now is knowing the Mordell–Weil rank of the Jacobian of X : it turns out that the rank is equal to 1. In general, computing the rank of a Jacobian is a difficult problem, but **Magma** has an implementation of 2-descent on Jacobians of hyperelliptic curves that can be used here:

```
> R<x>:=PolynomialRing(RationalField());
> X:=HyperellipticCurve(x^6+12*x^5-32*x^4+52*x^2-48*x+16);
> J:=Jacobian(X);
> RankBounds(J);
1 1
```

The output of **RankBounds** is a lower bound on rank, followed by an upper bound on rank, which are both equal to 1. Consequently, the *Chabauty–Coleman* bound (more on this in a bit; see Theorem 1.4 if you’d like to skip ahead) gives

$$\#X(\mathbb{Q}) \leq 10.$$

Are there rational points on X ? After searching in a box, we find

$$\{\infty^\pm, (0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3)\} \subseteq X(\mathbb{Q}),$$

and we have found precisely 10 points. So we have determined $X(\mathbb{Q})$, and the rational point $(12/11, 868/11^3)$ gives us a unique pair of triangles.

Theorem 1.1 (Hirakawa–Matsumura [HM19]). *Up to similitude, there exists a unique pair of a rational right triangle and a rational isosceles triangle which have the same perimeter and the same area. The unique pair consists of the right triangle with side (377, 135, 352) and isosceles triangle with sides (366, 366, 132).*

We begin with some context for these results. It was conjectured by Mordell in 1922 that nice curves of genus 2 or more have only finitely many rational points. This was proved by Faltings:

Theorem 1.2 (Faltings [Fal83]). *Let X/\mathbb{Q} be a nice curve of genus ≥ 2 . Then the set $X(\mathbb{Q})$ is finite.*

How do we determine the set $X(\mathbb{Q})$? Faltings' proof is not constructive. There is another proof due to Vojta [Voj91] (also revisited by Bombieri [Bom90]), but it is also not effective. We note that the recent proof of Mordell's conjecture by Lawrence and Venkatesh [LV18] gives another approach to finiteness, see also [BBB⁺19].

One method that allows us to compute the set $X(\mathbb{Q})$ in some cases is due to Coleman [Col85b], who re-interpreted earlier work of Chabauty, who proved Mordell's conjecture in the following special case:

Theorem 1.3 (Chabauty, 1941). *Let X/\mathbb{Q} be a nice curve of genus $g \geq 2$. Suppose the Mordell-Weil group of J has rank $r < g$. Then $X(\mathbb{Q})$ is finite.*

Coleman gave an effective version of Chabauty's theorem:

Theorem 1.4 (Coleman [Col85a]). *Let X/\mathbb{Q} be a nice curve of genus at least 2. Suppose the Mordell-Weil rank of $J(\mathbb{Q})$ is less than g . If $p > 2g$ is a prime of good reduction for X ,*

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2.$$

This result comes from bounding the number of zeros of a p -adic (Coleman) integral. We will say a bit more about this later.

Going back to the triangle problem: recall that we have the genus 2 curve

$$X : y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16.$$

The curve X has good reduction at $p = 5$, and we compute the set of \mathbb{F}_5 -rational points:

$$X(\mathbb{F}_5) = \{\infty^\pm, (0, \pm 1), (1, \pm 1), (2, \pm 2)\},$$

so $\#X(\mathbb{F}_5) = 8$. Thus by Coleman's theorem, we have

$$\#X(\mathbb{Q}) \leq 8 + 2 \cdot 2 - 2 = 10.$$

Since the Chabauty–Coleman method involves p -adic integration of certain differentials, we first set some notation on differentials and then discuss p -adic integration. We assume throughout that p is a prime of good reduction for a nice curve X .

Definition 1.5. Let X be a nice curve over a field k . The set of differentials on X over k is a 1-dimensional $k(X)$ -vector space $\Omega^1(k)$.

Definition 1.6. Let $0 \neq \omega \in \Omega^1(k)$ and $P \in X(k)$. Let $t \in k(X)$ be a uniformizer at P , and use this to write $\omega = \omega(t)dt$. Then $v_P(\omega) := v_P(\omega(t))$ is the valuation of ω at P .

Definition 1.7. If $v_P(\omega) \geq 0$ (or $\omega = 0$), then ω is regular at P and ω is regular if it is regular at all points $P \in X(\bar{k})$. This is also known as a differential of the first kind. A differential of the second kind is a differential that has residue zero at all points $P \in X(\bar{k})$. A differential of the third kind has at most simple poles at all points.

Example 1.8. Let $X: y^2 = f(x)$ be a hyperelliptic curve of genus g over k . Then $H^0(X, \Omega^1)$ has basis

$$\left\{ \frac{dx}{2y}, \frac{x dx}{2y}, \dots, \frac{x^{g-1} dx}{2y} \right\}$$

so every regular differential can be uniquely written as $\frac{p(x)dx}{2y}$ with a polynomial p of degree $\deg(p) \leq g - 1$.

Now we begin with an introduction to Coleman's theory of p -adic line integration.

Theorem 1.9 (Coleman). *Let X/\mathbb{Q}_p be a nice curve with good reduction at p . Then the p -adic integral*

$$\int_P^Q \omega \in \overline{\mathbb{Q}}_p$$

defined for each pair of points $P, Q \in X(\overline{\mathbb{Q}}_p)$ and regular differential $\omega \in H^0(X, \Omega^1)$ satisfies the following properties:

- (1) *The integral is $\overline{\mathbb{Q}}_p$ -linear in ω .*
- (2) *If P, Q reduce to the same point $\bar{P} \in X_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$, then we call the integral a tiny integral. It can be evaluated by writing $\omega = \omega(t)dt$ with t a uniformizer at P reducing to a uniformizer at \bar{P} and ω a power series, then integrating formally and obtaining a power series ℓ such that $d\ell(t) = \omega(t)dt$ and $\ell(0) = 0$ and finally evaluating $\ell(t(Q))$, which converges. This implies*

$$\int_P^P \omega = 0.$$

(3)

$$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^Q \omega.$$

Therefore it makes sense to define $\int_D \omega$ for

$$D = \sum_{j=1}^n ((Q_j) - (P_j)) \in \text{Div}_X^0(\overline{\mathbb{Q}}_p)$$

as

$$\int_D \omega = \sum_{j=1}^n \int_{Q_j}^{P_j} \omega.$$

- (4) *If D is principal, then $\int_D \omega = 0$.*
- (5) *The integral is compatible with the action of $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.*
- (6) *Fix $P_0 \in X(\overline{\mathbb{Q}}_p)$. If $0 \neq \omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$, then the set of points $P \in X(\overline{\mathbb{Q}}_p)$ reducing to a fixed point on $X(\overline{\mathbb{F}}_p)$ such that $\int_{P_0}^P \omega = 0$, is finite.*

Remark 1.10. The integral above is known as the *Coleman integral* [Col82, Col85b]. The statement that the curve has good reduction is not necessary but simplifies the statement of (2). The theory of Coleman integration of forms of the second and third kind was developed by Coleman [Col85b] and Coleman–de Shalit [CdS88], respectively.

Remark 1.11. There are a number of closely related approaches to p -adic integration, by Berkovich [Ber07], Zarhin [Zar96] Colmez [Col98], Besser [Bes02], and Vologodsky [Vol03]. See also the excellent survey of Besser [Bes12].

Corollary 1.12. *Given the hypothesis of the previous theorem, let $b \in X(\mathbb{Q}_p)$, let J be the Jacobian of X , and*

$$\begin{aligned} i : X &\rightarrow J \\ P &\mapsto [P - b] \end{aligned}$$

be the Abel-Jacobi embedding of X into J . Then there is a map

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(X_{\mathbb{Q}_p}, \Omega^1) &\rightarrow \mathbb{Q}_p \\ (Q, \omega) &\mapsto \langle Q, \omega \rangle \end{aligned}$$

that is additive in Q and \mathbb{Q}_p -linear in ω and is given by

$$\langle [D], \omega \rangle = \int_D \omega$$

for $D \in \text{Div}_X^0(\overline{\mathbb{Q}}_p)$. In particular, for $P \in X(\mathbb{Q}_p)$, we have the Abel-Jacobi morphism AJ_b that takes P to the linear functional

$$\langle i(P), \omega \rangle = \int_b^P \omega =: \text{AJ}_b(P).$$

Remark 1.13. If $P \in J(\mathbb{Q}_p)$ has finite order, then $\langle P, \omega \rangle = 0$ for all $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$. To see this, if $nP = 0$, then $\langle P, \omega \rangle = \frac{1}{n} \langle nP, \omega \rangle = 0$. In fact, one can show that the torsion points are the only points with this property. On the other hand, if ω has the property that $\langle P, \omega \rangle = 0$ for all $P \in J(\mathbb{Q}_p)$, then $\omega = 0$.

In the Chabauty–Coleman method, we will make use of a certain subspace of the space of regular 1-forms. Throughout, we will assume that $b \in X(\mathbb{Q})$ and use it to embed X into J :

Definition 1.14. Let $A = \{\omega \in H^0(X, \Omega^1) : \text{for all } P \in J(\mathbb{Q}), \langle P, \omega \rangle = 0\}$ be the subspace of *annihilating differentials*.

The embedding i induces an isomorphism of vector spaces $H^0(J_{\mathbb{Q}_p}, \Omega^1) \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)$ and we likewise have the pairing

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) &\rightarrow \mathbb{Q}_p \\ (Q, \omega_J) &\mapsto \int_0^Q \omega_J, \end{aligned}$$

which induces a homomorphism

$$\log : J(\mathbb{Q}_p) \rightarrow H^0(J_{\mathbb{Q}_p}, \Omega^1)^*.$$

We thus have the following diagram:

$$(1) \quad \begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) \xrightarrow{\log} H^0(J_{\mathbb{Q}_p}, \Omega^1)^* \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \end{array}$$

Remark 1.15. In general, since we are only considering the case of good reduction, we will identify the p -adic abelian integral on the Jacobian with the abelian integral given by p -adic integration on the curve. In the case of bad reduction (as will be discussed in Zureick-Brown’s lecture course), there is a difference in the two integrals, as noted by Stoll [Sto19] and Katz–Rabinoff–Zureick-Brown [KRZB16]. See also the work of Besser–Zerbes [BZ17] for a discussion of Vologodsky integration in the semistable case.

From now on, we will assume basic familiarity with rigid geometry, see for instance [Sch98, FvdP04].

Definition 1.16. Let X^{an} denote the rigid analytic space over \mathbb{Q}_p associated to X/\mathbb{Q}_p . There is a specialization map from X^{an} to the reduction of X modulo p . The fibers of this map are called *residue disks*.

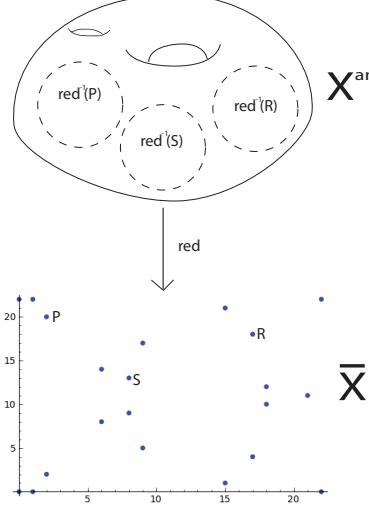


FIGURE 1. Residue disks in X^{an}

Corollary 1.17. Let X/\mathbb{Q} be a nice curve of genus g whose Jacobian has Mordell–Weil rank r less than g . Then $\#X(\mathbb{Q})$ is finite.

Proof. If $X(\mathbb{Q}) = \emptyset$, then the claim is trivially true. Fix a prime p of good reduction for X and fix $b \in X(\mathbb{Q})$ to define $i : X \rightarrow J$. Let A be the subspace of annihilating differentials. By additivity of integration pairing in the first argument, this condition is equivalent to requiring $\langle P_j, \omega \rangle = 0$ for a basis $\{P_j\}_{j=1}^r$ of the free part of $J(\mathbb{Q})$. So it leads to at most r linear constraints and $\dim(A) \geq g - r > 0$. Thus there is some $0 \neq \omega \in A$. Since $i(P) \in J(\mathbb{Q})$ for all $P \in X(\mathbb{Q})$ it follows that $\int_b^P \omega = 0$ for all $P \in X(\mathbb{Q})$. By Theorem 1.9 (6), the number of such P is finite in each residue disk of $X(\mathbb{Q}_p)$. Since the number of residue disks (i.e., $\#X(\mathbb{F}_p)$) is finite, the total number of points in $X(\mathbb{Q})$ is finite as well. \square

Remark 1.18. By *computing rational points via the Chabauty–Coleman method*, we mean that we compute the finite set of p -adic points

$$X(\mathbb{Q}_p)_1 := \{z \in X(\mathbb{Q}_p) : \int_b^z \omega = 0 \text{ for } \omega \in A\}.$$

By construction, this set contains $X(\mathbb{Q})$. One potential difficulty is that $X(\mathbb{Q}_p)_1$ might be strictly larger than the set of known rational points, so more work must be done to provably extract $X(\mathbb{Q})$; see Section 5.3.3 for one approach to address this, known as the *Mordell–Weil sieve*.

We can use results about the number of zeros of p -adic power series (studied via Newton polygons) to refine the bound in the proof above. Combining this with Riemann–Roch gives Coleman’s result, that for X satisfying the hypotheses of Corollary 1.17 and $p > 2g$ a good prime, we have (Theorem 1.4):

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2.$$

Remark 1.19. Here are some related results:

- (1) Stoll [Sto06] showed that one can choose the “best” ω for each residue disk, which improves the bound if $r < g$ and $p > 2r + 2$ is a good prime:

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r.$$

Stoll also showed that one can weaken the assumption that $p > 2r + 2$; if $p > 2$, then

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r + \left\lfloor \frac{2r}{p-2} \right\rfloor.$$

- (2) Katz–Zureick-Brown [KZB13] extended Stoll’s result to the case of bad reduction. If $p > 2g$ and \mathcal{X} is the minimal proper regular model for X over \mathbb{Z}_p , then

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}_{sm}(\mathbb{F}_p) + 2r$$

where $\mathcal{X}_{sm}(\mathbb{F}_p)$ is the set of smooth \mathbb{F}_p -rational points in the special fiber of \mathcal{X} .

As will be discussed in Zureick-Brown’s lecture course, the Chabauty–Coleman method can be used to prove uniform bounds on the number of rational points on a nice curve. The first result along these lines was given by Stoll, for hyperelliptic curves:

Theorem 1.20 (Stoll [Sto19]). *Let X/\mathbb{Q} be a hyperelliptic curve of genus g with Jacobian of Mordell–Weil rank r . If $r \leq g - 3$, then*

$$\#X(\mathbb{Q}) \leq 8rg + 33(g-1) - 1 \quad \text{if } r \geq 1 \quad \text{and} \quad \#X(\mathbb{Q}) \leq 33(g-1) + 1 \quad \text{if } r = 0.$$

This was generalized by Katz–Rabinoff–Zureick-Brown to nice curves:

Theorem 1.21 (Katz–Rabinoff–Zureick-Brown [KRZB16]). *If X/\mathbb{Q} is a nice curve of genus g with $r \leq g - 3$, then*

$$\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28.$$

1.2. The Chabauty–Coleman method and explicit Coleman integration. Here we discuss how to construct an annihilating differential in the Chabauty–Coleman method, using explicit Coleman integration.

Example 1.22. Consider

$$X : y^2 = x^5 - 2x^3 + x + \frac{1}{4},$$

which has LMFDB label 971.a.971.1 [LMF20b]. Here are some facts about this curve:

- Searching for rational points in a box, we find that the set of rational points $X(\mathbb{Q})$ contains $\{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}$.
- The Jacobian is simple, and its Mordell–Weil group has the structure $J(\mathbb{Q}) \simeq \mathbb{Z}$. The point

$$[(-1, -1/2) - (0, 1/2)] \in J(\mathbb{Q})$$

has infinite order, as can be seen by computing Coleman integrals on regular 1-forms (see below).

- The conductor N is 971, which is prime. So X has good reduction at $p = 3$, and we compute that $\#X(\mathbb{F}_3) = 7$. Using Stoll’s refinement of the Chabauty–Coleman bound gives

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_3) + 2 \cdot 1 + \left\lfloor \frac{2 \cdot 1}{3-2} \right\rfloor = 11,$$

so this bound by itself will not prove⁴ that we have all of the \mathbb{Q} -points.

⁴Note that we know that we have all of the \mathbb{Q} -points, but we suspect we do, and we would like to prove this.

Our strategy will be to use $p = 3$ to construct an annihilating differential. A basis of $H^0(X_{\mathbb{Q}_3}, \Omega^1)$ is

$$\left\{ \omega_i = \frac{x^i dx}{2y} \right\}_{i=0,1}.$$

So the annihilating differential η is a \mathbb{Q}_3 -linear combination of ω_0 and ω_1 . We will use the values of

$$\int_{(0,1/2)}^{(-1,-1/2)} \omega_i$$

to compute η .

We can do this in **SageMath** as follows:

```
R.<x> = QQ[]
X = HyperellipticCurve(x^5-2*x^3+x+1/4)
p = 3
K = Qp(p,15)
XK = X.change_ring(K)
XK.coleman_integrals_on_basis(XK(0,1/2),XK(-1,-1/2)) #basis is {x^i*dx/(2y)}, i = 0,...,3
(3 + 3^2 + 3^4 + 3^5 + 2*3^6 + 2*3^7 + 2*3^8 + 3^10 + O(3^11),
2 + 2*3 + 2*3^3 + 3^4 + 3^6 + 2*3^8 + 2*3^9 + O(3^10),
2*3^-1 + 2*3 + 2*3^2 + 3^3 + 3^5 + 3^6 + 3^7 + O(3^9),
2*3^-2 + 3^-1 + 2 + 2*3 + 3^2 + 2*3^3 + 3^4 + 2*3^5 + 2*3^6 + 2*3^7 + O(3^8))
```

We find that

$$\alpha := \int_{(0,1/2)}^{(-1,-1/2)} \omega_0 = 3 + 3^2 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 3^{10} + O(3^{11}),$$

$$\beta := \int_{(0,1/2)}^{(-1,-1/2)} \omega_1 = 2 + 2 \cdot 3 + 2 \cdot 3^3 + 3^4 + 3^6 + 2 \cdot 3^8 + 2 \cdot 3^9 + O(3^{10}).$$

With a slightly different choice of basis⁵, we can also do these computations in **Magma** (using the package [BTb], available on GitHub) as follows:

```
> load "coleman.m";
> data:=coleman_data(y^2-(x^5-2*x^3+x+1/4),3,10);
> P1:= set_point(0,1/2, data);
> P2:= set_point(-1,-1/2,data);
> coleman_integrals_on_basis(P1,P2,data); //8 times the integrals above
(-7609*3 + O(3^10) 13537 + O(3^10) 77056*3^-1 + O(3^10) -6512*3^-2 + O(3^10))
```

So $\int_{(0,1/2)}^{(-1,-1/2)} \beta \omega_0 - \alpha \omega_1 = 0$, and we take

$$\eta = \beta \omega_0 - \alpha \omega_1$$

as our annihilating differential.

In order to use η to compute $X(\mathbb{Q})$, or more precisely the finite set $X(\mathbb{Q}_3)_1$, that by construction, contains $X(\mathbb{Q})$, we next compute the collection of “indefinite” Coleman integrals

$$\left\{ \int_{(0,1/2)}^{P_t} \eta \right\}$$

⁵In this example, the **Magma** basis is the **SageMath** basis rescaled by a factor of 8.

where P_t ranges over all residue disks, and solve for all $z \in X(\mathbb{Q}_3)$ such that $\int_{(0,1/2)}^z \eta = 0$. Note that to compute these indefinite Coleman integrals, we can take P_0 a lift of an \mathbb{F}_3 -point in the same residue disk as P_t . Then

$$\int_{(0,1/2)}^{P_t} \eta = \int_{(0,1/2)}^{P_0} \eta + \int_{P_0}^{P_t} \eta$$

where the first is some 3-adic constant, and the latter is a tiny integral computed using a power series. So to compute α, β and $\int_{(0,1/2)}^{P_0} \eta$, we need to compute Coleman integrals between points not in the same residue disk.

Now we explain how to compute these integrals on the curve, using the action of Frobenius on p -adic cohomology.

Remark 1.23. Before we go on, we should note that there is a standard alternative approach to the one presented below for computing Coleman integrals of regular 1-forms between points not in the same residue disk that goes as follows.

Suppose we want to compute the Coleman integral $\int_P^Q \omega$, where $P, Q \in X(\mathbb{Q}_p)$. Letting J denote the Jacobian of X , we first compute an integer k such that the point $k(P - Q)$ is trivial in $J(\mathbb{F}_p)$: for instance, we could take k to be the order of $J(\mathbb{F}_p)$. Then computing $D := [k(P - Q)]$ as an element in the residue disk at 0 of $J(\mathbb{Q}_p)$, we can rewrite the integral as a sum of tiny integrals over D , and then use $\int_{[P-Q]} \omega = \frac{1}{k} \int_D \omega$.

This has worked well in a number of examples in the literature, though there are a few potential limitations. First, implementations of Jacobian arithmetic over \mathbb{Q}_p are currently restricted to very special curves, such as those that are hyperelliptic. Secondly, while the Chabauty–Coleman method only uses integrals of regular 1-forms, there are other applications for which integrals of forms of the second or third kind are useful. Moreover, since this approach uses properties of the Jacobian, it does not have an obvious generalization to iterated integrals. So from the perspective of the nonabelian Chabauty method, where iterated integration is needed, we present the following approach.

We will integrate over a wide open subspace of X^{an} :

Definition 1.24. A wide open subspace of X^{an} is the complement in X^{an} of the union of a finite collection of disjoint closed disks of radius $\lambda_i < 1$.

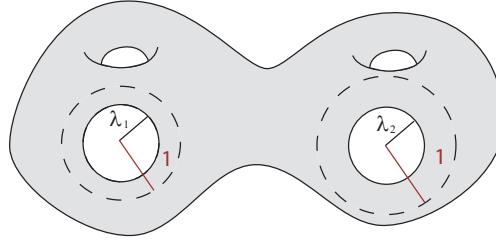


FIGURE 2. A wide open subspace of X^{an}

Here are some further properties of Coleman integrals that we will need:

Theorem 1.25 (Coleman [Col85b]). *Let η and ξ be 1-forms on a wide open subspace V of X^{an} , and $P, Q, R \in V(\overline{\mathbb{Q}}_p)$. Let $a, b \in \overline{\mathbb{Q}}_p$. The definite Coleman integral has the following properties:*

(1) *Linearity:*

$$\int_P^Q (a\eta + b\xi) = a \int_P^Q \eta + b \int_P^Q \xi.$$

(2) *Additivity in endpoints:*

$$\int_P^Q \eta = \int_P^R \eta + \int_R^Q \eta.$$

(3) *Change of variables:* if $V' \subset X'$ is a wide open subspace of the rigid analytic space X' , ω' a 1-form on V' and $\phi : V \rightarrow V'$ a rigid analytic map, then

$$\int_P^Q \phi^* \omega' = \int_{\phi(P)}^{\phi(Q)} \omega'.$$

(4) *Fundamental Theorem of Calculus:*

$$\int_P^Q df = f(Q) - f(P)$$

for f a rigid analytic function on V .

(5) *Galois compatibility:* If $P, Q \in V(\mathbb{Q}_p)$ and ω is defined over \mathbb{Q}_p , then $\int_P^Q \omega \in \mathbb{Q}_p$.

We would first like to integrate $\int_P^Q \omega$ for ω a 1-form of the second kind, where $P, Q \in V(\mathbb{Q}_p)$. We first discuss how to do this in the case when X is a *hyperelliptic* curve and then present a more general construction in Section 1.4. (In our discussion of p -adic heights in Section 2.2, we will also describe how to compute integrals of forms of the third kind.)

The idea is to do the following:

- (1) Take ϕ to be a lift of p -power Frobenius from the special fiber.
- (2) Compute a basis $\{\omega_i\}$ of 1-forms of the second kind.
- (3) Compute $\phi^* \omega_i$ via Kedlaya's zeta function algorithm [Ked01, Ked03] and use properties of Coleman integrals to relate $\int_P^Q \phi^* \omega_i$ to $\int_P^Q \omega_i$ and other terms we can compute.
- (4) Use linear algebra to solve for $\int_P^Q \omega_i$.

To do this, we introduce some p -adic cohomology as in Kedlaya's algorithm. For further details, two standard references for rigid analytic geometry are the books by Fresnel and van der Put [FvdP04] and Bosch, Güntzer, and Remmert [BGR84]. See also [Edi] for a nice exposition by Edixhoven of Kedlaya's algorithm.

1.3. Some p -adic cohomology. In [Ked01], Kedlaya gave an algorithm to compute the zeta function of a hyperelliptic curve over a finite field, using Monsky–Washnitzer cohomology. Here is a brief outline of Kedlaya's algorithm:

- (1) Work in an affine piece of the hyperelliptic curve, given by deleting Weierstrass points.
- (2) Take ϕ to be a lift of p -power Frobenius from the special fiber, sending $x \rightarrow x^p$ and Hensel lifting to find the image of y .
- (3) Compute the action of Frobenius on a basis of de Rham cohomology (of a lift of the curve) and reduce the pole order of each resulting differential using relations in cohomology.

It turns out that Kedlaya's algorithm produces a few other outputs that can be assembled into an algorithm for Coleman integration on hyperelliptic curves, as given by Balakrishnan–Bradshaw–Kedlaya [BBK10]. In this section, we give an overview of Kedlaya's algorithm and the corresponding Coleman integration algorithm.

For simplicity, we will assume that we start with a genus g hyperelliptic curve \tilde{X} defined over \mathbb{Q} , given by $y^2 = \tilde{P}(x)$, where $\tilde{P}(x)$ is a monic polynomial of degree $2g+1$. Let $p \neq 2$ be a prime at which \tilde{X} has good reduction, and consider $\overline{X}/\mathbb{F}_p$, with affine equation $y^2 = P(x)$. Take $X = \overline{X} \setminus \{\infty, y=0\}$.

Let $A = \mathbb{Z}_p[x, y, y^{-1}]/(y^2 - \tilde{P}(x))$. First, we form the weak completion A^\dagger of A , which can be described as follows. Let v_p denote the p -adic valuation on \mathbb{Z}_p , and extend it to polynomials by $v_p(\sum a_i x^i) = \min_i \{v_p(a_i)\}$. The elements of A^\dagger can then be described as the series

$$\sum_{n=-\infty}^{\infty} (S_n(x) + T_n(x)y)y^{2n}$$

where the S_n and T_n are polynomials of degree at most $2g$ such that

$$\liminf_{n \rightarrow \infty} \frac{v_p(S_n)}{n}, \quad \liminf_{n \rightarrow \infty} \frac{v_p(S_{-n})}{n}, \quad \liminf_{n \rightarrow \infty} \frac{v_p(T_n)}{n}, \quad \liminf_{n \rightarrow \infty} \frac{v_p(T_{-n})}{n}$$

are all positive.

Monsky–Washnitzer cohomology is a p -adic cohomology theory which takes smooth affine varieties over fields of characteristic $p > 0$ as input, and outputs finite-dimensional \mathbb{Q}_p -vector spaces. There is a comparison theorem due to the work of Berthelot [Ber97, Prop. 1.10] (comparing Monsky–Washnitzer and rigid cohomology) and Baldassarri–Chiarelotto [BC94] (comparing rigid cohomology with de Rham cohomology), which relates Monsky–Washnitzer cohomology groups with algebraic de Rham cohomology groups:

Theorem 1.26 (Special case of Baldassarri–Chiarelotto and Berthelot). *Let Y be a smooth affine variety over \mathbb{F}_p and \tilde{Y} a smooth affine variety over \mathbb{Q}_p that is a lift of Y . Then the Monsky–Washnitzer cohomology of Y coincides with the algebraic de Rham cohomology of \tilde{Y} :*

$$H_{\text{dR}}^1(\tilde{Y}) = H_{\text{MW}}^1(Y).$$

The Monsky–Washnitzer cohomology groups are equipped with an action of Frobenius, hence Theorem 1.26 tells us that we can compute the action of Frobenius on de Rham cohomology.

Proposition 1.27. *The first de Rham cohomology of A splits into two eigenspaces under the hyperelliptic involution*

$$X \rightarrow X, (x, y) \mapsto (x, -y).$$

The first eigenspace $H^1(A)^+$ is the positive eigenspace generated by

$$\left\{ \frac{x^i dx}{y^2} : i = 0, \dots, 2g \right\},$$

and the second eigenspace $H^1(A)^-$ is the negative eigenspace generated by

$$\left\{ \frac{x^i dx}{y} : i = 0, \dots, 2g-1 \right\},$$

Moreover, passing to A^\dagger does not change the cohomology, and we compute the action of Frobenius on $H^1(A^\dagger)^-$. We lift p -power Frobenius to an endomorphism σ of A^\dagger in the following manner: On polynomials in $\mathbb{Z}_p[x]$, we send

$$(2) \quad \sigma : x \mapsto x^p.$$

Since $y^2 = \tilde{P}(x)$ inside A and A^\dagger , we see that the action of σ on y must satisfy the following:

$$(y^\sigma)^2 = (y^2)^\sigma = (\tilde{P}(x))^\sigma = \tilde{P}(x)^\sigma \left(\frac{y^2}{\tilde{P}(x)} \right)^p = \frac{y^{2p} \tilde{P}(x)^\sigma}{\tilde{P}(x)^p}.$$

We have

$$\sigma : y \mapsto y^p \left(\frac{\tilde{P}(x)^\sigma}{\tilde{P}(x)^p} \right)^{\frac{1}{2}} = y^p \left(1 + \frac{\tilde{P}(x)^\sigma - \tilde{P}(x)^p}{\tilde{P}(x)^p} \right)^{\frac{1}{2}},$$

and by using a Taylor expansion for $(1 + \cdot)^{-\frac{1}{2}}$, we get an identity

$$(3) \quad \frac{1}{y^\sigma} = \frac{1}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{\tilde{P}(x)^\sigma - \tilde{P}(x)^p}{\tilde{P}(x)^p} \right)^j = \frac{1}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{\tilde{P}(x)^\sigma - \tilde{P}(x)^p}{y^{2p}} \right)^j.$$

The reason we write the expansion for $\frac{1}{y^\sigma}$ in this way is to see the p -adic convergence, since $\tilde{P}(x)^\sigma - \tilde{P}(x)^p$ is divisible by p , so as $j \rightarrow \infty$, the summands go to 0.

This expansion will be used below, and perhaps now it is more clear why we removed Weierstrass points from our curve: given our choice of Frobenius lift, we cannot divide by y .

Finally, we extend the p -power Frobenius action to differentials by sending

$$(4) \quad \sigma^* : dx \mapsto d(x^p) = px^{p-1}dx.$$

In order to prove Proposition 1.27, we will need two key reduction lemmas to compute $(\frac{x^i dx}{y})^\sigma$.

Lemma 1.28 (Kedlaya [Ked01, p. 5]). *If $R(x) = \tilde{P}(x)B(X) + \tilde{P}'(x)C(X)$, then*

$$(5) \quad \frac{R(x)dx}{y^s} = \left(B(x) + \frac{2C'(x)}{s-2} \right) \frac{dx}{y^{s-2}}$$

as elements in $H_{MW}^1(X)$.

Also, using $y^2 = \tilde{P}(x)$, we have $d(y^2) = d\tilde{P}(x)$, so $2ydy = \tilde{P}'(x)dx$. This gives us

$$(6) \quad dy = \frac{\tilde{P}'(x)dx}{2y}.$$

This allows us to compute:

$$\begin{aligned} d(x^i y^j) &= ix^{i-1} y^j dx + x^i j y^{j-1} dy \\ &\stackrel{(6)}{=} ix^{i-1} y^j dx + j x^i y^{j-1} \frac{\tilde{P}'(x)dx}{2y} = (2ix^{i-1} y^{j+1} + j x^i \tilde{P}'(x) y^{j-1}) \frac{dx}{2y} \end{aligned}$$

(So the *highest* monomial of $d(x^i y^j)$ is $x^{i-1} y^{j+1}$ if $1 \leq i < 2g+1$ and $x^{2g} y^{j-1}$ if $i = 0$. The *lowest* monomial of $d(x^i y^j)$ is of the form $x^k y^{j-1}$ with $0 \leq k < 2g+1$.) As a special case of this computation, we have

$$\begin{aligned} d(2Q(x)y) &= 2Q(x)dy + 2Q'(x)ydx \\ &\stackrel{(6)}{=} 2Q(x) \frac{\tilde{P}'(x)dx}{2y} + 2Q'(x)ydx \\ &\stackrel{y^2=\tilde{P}(x)}{=} (Q(x)\tilde{P}'(x) + 2Q'(x)\tilde{P}(x)) \frac{dx}{y}, \end{aligned}$$

proving the second reduction lemma:

Lemma 1.29 (Kedlaya [Ked01, p. 5]). *If $Q(x) = x^{m-2g}$, then*

$$(7) \quad d(2Q(x)y) = (Q(x)\tilde{P}'(x) + 2Q'(x)\tilde{P}(x)) \frac{dx}{y} = 0$$

as elements in $H_{MW}^1(X)$.

To compute $(\frac{x^i dx}{y})^\sigma$, we expand using (2), (3), (4) and reduce using the relations (5) and (7). The reduction process is subtracting appropriate linear combinations of $d(x^i y^j)$ and using the relationship $y^2 = \tilde{P}(x)$.

The relation

$$\left(\frac{x^i dx}{y}\right)^\sigma = \frac{1}{y^\sigma} x^{pi} p x^{p-1} dx$$

plus (3) gives an infinite sum

$$(8) \quad \left(\frac{x^i dx}{y}\right)^\sigma = \frac{px^{p+1}}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{\tilde{P}(x)^\sigma - \tilde{P}(x)^p}{y^{2p}}\right)^j dx.$$

To implement the expansion and reduction on a computer, we have to take a truncation of this infinite sum, and thus we need to know how many terms we need to take to get a provably correct result (more on this in a minute). Suppose we have computed this precision and the result in (8) is

$$(9) \quad \sum_{j=-L_1}^{L_2} \frac{R_j(x) dx}{y^{2j+1}}.$$

Here is how we use the reduction relations: we eliminate the $j = L_2$ term, then $j = L_2 - 1$ term. Iterate this procedure until no terms with $j > 0$ remain. Repeat the same thing for $j = -L_1, -(L_1 - 1), \dots$ terms. At the end of this reduction algorithm, we will be left with

$$\left(\frac{x^i dx}{y}\right)^\sigma = dh_i + \sum_{j=0}^{2g-1} M_{ji} \frac{x^j dx}{y},$$

and as $dh_i \sim 0$ in cohomology, this gives us the matrix of Frobenius M .

Precision is lost when we divide by p in the reduction algorithm. We need to measure the loss of precision at each step to know how many provably correct digits we have. Let $R(x) \in \mathbb{Z}_p[x]$ be a polynomial of degree at most $2g$ and $m \geq 0$.

By (5), the reduction of

$$\omega := R(x) \frac{dx}{y^{2m+1}}$$

is $\omega = B(x) \frac{dx}{y} + df$ for some $B(x) \in \mathbb{Q}_p[x]$ with degree at most $2g - 1$ and $f = \sum_{k=-1}^{m-1} \frac{F_k(x)}{y^{2k+1}}$ with each F_k having degree at most $2g$. The first precision result is:

Lemma 1.30 ([Ked01, Lemma 2], [Edi, §4.3.4]). *In the above setting⁶, we have*

$$p^{\lfloor \text{Log}_p(2m+1) \rfloor} B(x) \in \mathbb{Z}_p[x].$$

By (7), the reduction of

$$\omega := \frac{R(x)y^{2m} dx}{y}$$

is $\omega = B(x) \frac{dx}{y} + df$ for some $B(x) \in \mathbb{Q}_p[x]$ with degree at most $2g - 1$, and

$$f = Cy^{2m+1} + \sum_{k=0}^{m-1} F_k(x) y^{2k+1}$$

⁶In this chapter, Log_p will denote the base p logarithm, to disambiguate from \log_p in subsequent chapters, which will denote the p -adic logarithm.

with $C \in \mathbb{Q}_p$ and each F_k having degree at most $2g$.

Lemma 1.31 ([Ked03]). *In the above setting, we have*

$$p^{\lfloor \text{Log}_p((2g+1)(2m+1)) \rfloor} B(x) \in \mathbb{Z}_p[x].$$

Putting Lemmas 1.30 and 1.31 together, one gets the following:

Proposition 1.32 ([Cha16, p. 34]). *To get N correct digits in the matrix of Frobenius M , we start with precision*

$$N_1 = N + \max\{\lfloor \text{Log}_p(2N_2 - 3) \rfloor, \lfloor \text{Log}_p(2g + 1) \rfloor\} + 1 + \lfloor \text{Log}_p(2g - 1) \rfloor,$$

in which N_2 is the smallest integer such that

$$N_2 - \max\{\lfloor \text{Log}_p(2N_2 + 1) \rfloor, \lfloor \text{Log}_p(2g + 1) \rfloor\} \geq N.$$

In particular, in (8), we take the truncation

$$\left(\frac{x^i dx}{y}\right)^\sigma = \frac{px^{pi+p-1}}{y^p} \sum_{j=0}^{N_2-1} \binom{-\frac{1}{2}}{j} \left(\frac{\tilde{P}(x)^\sigma - \tilde{P}(x)^p}{y^{2p}}\right)^j dx.$$

Algorithm 1.33 (Kedlaya's algorithm).

Input:

- The basis of differentials $\{\omega_i = x^i dx/y\}_{i=0}^{2g-1}$ of $H_{\text{dR}}^1(X_{\mathbb{Q}_p})$ for a genus g hyperelliptic curve X given by a monic odd degree model, with good reduction at p .
- The desired precision N .

Output: The $2g \times 2g$ matrix M of a p -power lift of Frobenius ϕ , as well as functions $h_i \in A^\dagger$ such that $\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j$ to precision $O(p^N)$

- (1) Compute the working precision N_1 as in Proposition 1.32, so that all computations will be done mod p^{N_1} .
- (2) For each i , compute $F_i := \phi^*(\omega_i)$ and group the resulting terms as $(\sum p^{k+1} c_{i,k,j} y^j) dx/y$, where the $c_{i,k,j} \in \mathbb{Z}_p[x]$ have degree less than or equal to $2g + 1$.
- (3) Compute a list of differentials $d(x^i y^j)$, where $0 \leq i < 2g + 1$ and $j \equiv 1 \pmod{2}$.
- (4) If F_i has a term $(x^i y^j) dx/y$ with $j < 0$, consider the term $(c_{i,k,j} y^j) dx/y$ where j is minimal. Take the unique linear combination of the $d(x^k y^{1+j})$ such that when this linear combination is subtracted off of F_i and re-initialize this as F_i . Do this until F_i no longer has terms of the form $(x^m y^j) dx/y$ with $j < 0$.
- (5) If F_i has terms with $j \geq 0$, let $(x^m y^j) dx/y$ be the term with the highest monomial of F_i . Let $(x^k y^l) dx/y$ be the term such that $d(x^k y^l)$ has highest term $(x^m y^j) dx/y$ and subtract off the appropriate multiple of $d(x^k y^l)$ such that the resulting sum no longer has terms of the form $(x^m y^j) dx/y$ with $j \geq 0$. Re-initialize this as F_i and repeat this process until the resulting F_i is of the form $(M_{0i} + M_{1i} x + \cdots + M_{2g-1i} x^{2g-1}) dx/y$.
- (6) For each i , return the expression

$$\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j.$$

Remark 1.34. Analyzing p -adic precision is a delicate task. We illustrate this in one example found by Chan [Cha16] below, where the previously published bounds contained a small inaccuracy. For the remainder of these notes, we do not say much more about p -adic precision analysis of the relevant

constructions and instead give relevant pointers to the literature. We encourage the reader to keep the issue of p -adic precision in mind as they work through the algorithms.

Example 1.35 ([Cha16, Remark 13]). Consider the elliptic curve over \mathbb{Q} defined by

$$y^2 = \tilde{P}(x) = x^3 + x + 1.$$

This curve has good reduction at the prime $p = 5$. We wish to obtain $N = 2$ correct digits of expansion. Proposition 1.32 tells us that taking $N_2 = N_1 = 3$ suffices. Consider the two differentials $\frac{dx}{y}, \frac{xdx}{y}$. We expand (8) and use the equation $y^2 = \tilde{P}(x)$ as needed to reduce the degree in x in the numerators to produce the following:

$$\begin{aligned} \left(\frac{dx}{y}\right)^{\sigma} &= \left(\frac{25x+50}{y^{15}} + \frac{75x^2+100x+25}{y^{13}} + \frac{50x^2+50x+100}{y^{11}} + \frac{75x+50}{y^9} + \frac{50x^2+50x}{y^7} \right. \\ &\quad \left. + \frac{70x^2+70x+25}{y^5} + \frac{5x}{y^3} \right) dx \pmod{5^3}, \\ \left(\frac{xdx}{y}\right)^{\sigma} &= \left(\frac{100x^2+100x+75}{y^{15}} + \frac{25x^2+50x+75}{y^{13}} + \frac{50x^2+100x+100}{y^{11}} + \frac{25x^2+75x+75}{y^9} \right. \\ &\quad \left. + \frac{75x^2+100}{y^7} + \frac{85x^2+90+50}{y^5} + \frac{15x^2+30x+85}{y^3} + \frac{5x^3+65x+65}{y} \right) dx \pmod{5^3}. \end{aligned}$$

Let F_k denote the polynomial in x in the numerator in each of the summands: i.e., writing them as $\frac{F_k(x)dx}{y^{2k+1}}$ modulo 5^3 . Compute the sequence S_k for $k = 7, 6, \dots, 0$ inductively by first setting $S_7 = F_7$, and afterwards, given S_{k+1} , find polynomials B_{k+1}, C_{k+1} such that $S_{k+1} = B_{k+1}\tilde{P} + C_{k+1}\tilde{P}'$, and then set $S_k(x) = F_k(x) + B_{k+1}(x) + \frac{2C'_{k+1}(x)}{2k+1}$. Carrying this out, one finds

$$\begin{aligned} \left(\frac{dx}{y}\right)^{\sigma} &= 15x \frac{dx}{y} \pmod{5^2} \\ \left(\frac{xdx}{y}\right)^{\sigma} &= (22x+18) \frac{dx}{y} \pmod{5^2} \end{aligned}$$

This gives us the matrix of the 5-power Frobenius

$$\begin{pmatrix} 0 & 18 \\ 15 & 22 \end{pmatrix} \pmod{5^2},$$

with $N = 2$ correct digits of expansion. Note that taking $N_1 = 3$ is necessary as well, as taking $N_1 = 2$ instead gives the matrix

$$\begin{pmatrix} 15 & 18 \\ 0 & 22 \end{pmatrix} \pmod{5^2}.$$

Now here is the application to Coleman integration, as carried out by Balakrishnan–Bradshaw–Kedlaya [BBK10]. Below we let ϕ denote the lift of p -power Frobenius described earlier.

Algorithm 1.36 (Coleman integration on a hyperelliptic curve [BBK10]).

Input:

- A prime $p > 2$ of good reduction for a hyperelliptic curve X
- Points $P, Q \in X(\mathbb{Q}_p)$ not contained in a Weierstrass residue disk
- A 1-form ω of the second kind

Output: The Coleman integral $\int_P^Q \omega$.

- (1) Since ω is of the second kind, we may write it as a linear combination of a basis $\{\omega_i\}_{i=0}^{2g-1}$ for $H_{dR}^1(X)$ together with an exact form. Use Kedlaya's algorithm to write $\omega = dh + \sum_{i=0}^{2g-1} a_i \omega_i$, which allows us to specialize to the case of Coleman integrals of basis differentials.
- (2) Use Kedlaya's algorithm to write, for each basis differential ω_i , the reduced form

$$\phi^* \omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji} \omega_j.$$

- (3) Using properties of the Coleman integral, we have

$$(10) \quad \begin{pmatrix} \vdots \\ \int_P^Q \omega_j \\ \vdots \end{pmatrix} = (M^t - I)^{-1} \begin{pmatrix} \vdots \\ h_i(P) - h_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i \\ \vdots \end{pmatrix}.$$

- (4) Compute $\int_P^Q \omega = h(Q) - h(P) + \sum_{i=0}^{2g-1} a_i \int_P^Q \omega_i$.

Remark 1.37. We derive (3) above using the following:

$$\begin{aligned} \int_{\phi(P)}^{\phi(Q)} \omega_i &= \int_P^Q \phi^* \omega_i \\ (\text{by Kedlaya}) &= \int_P^Q dh_i + \sum_{j=0}^{2g-1} M_{ji} \omega_j \\ &= \int_P^Q dh_i + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j \\ &= h_i(Q) - h_i(P) + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j. \end{aligned}$$

By the additivity of the Coleman integral on endpoints, we get

$$\int_P^{\phi(P)} \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_i + \int_{\phi(Q)}^Q \omega_i = \int_P^{\phi(P)} \omega_i + \int_{\phi(Q)}^Q \omega_i + h_i(Q) - h_i(P) + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j.$$

The left hand side of the equality becomes $\int_P^Q \omega_i$. For the right hand side, P and $\phi(P)$ are in the same residue disk, making $\int_P^{\phi(P)} \omega_i$ a tiny integral and therefore computable via its power series expansion. The same is true for the pair $\phi(Q)$ and Q . The h_i are given to us explicitly from Kedlaya's algorithm, and we can evaluate them on Q and P . Notice that $M^t - 1$ is invertible since, by the Weil conjectures, the eigenvalues of M have norm $\sqrt{p} \neq 1$. Therefore we can compute the left hand side by solving the linear equation.

Remark 1.38. For Weierstrass residue disks, the lift of Frobenius is not defined over the entirety of the disc, but due to overconvergence it is defined near the boundary of the residue disk. So if W is a Weierstrass point and we would like to compute $\int_W^P \omega_i$, we choose a point S close to the boundary of the Weierstrass disk of W and decompose the integral as

$$\int_W^P \omega_i = \int_W^S \omega_i + \int_S^P \omega_i.$$

On the right hand side, the first term is a tiny integral while the second term can be computed using the above method. However, this is computationally expensive, as we have to work over a totally ramified extension of \mathbb{Q}_p to compute the integral.

Remark 1.39. For precision estimates in Algorithm 1.36, see [BBK10, §4.1]. Roughly speaking, there is some loss of precision from truncations of power series giving the necessary tiny integrals, as well as from the valuation of the determinant of the matrix $M^t - 1$.

Remark 1.40. In the case of p -adic integration for a *bad* prime p , Katz and Kaya [KK20] recently gave an algorithm to compute p -adic abelian integrals on hyperelliptic curves. They do this by covering a hyperelliptic curve with bad reduction at p by annuli and basic wide open sets, and then reduce the computation of Berkovich–Coleman integrals to the known algorithms for integration of a 1-form of the second or third kind on a hyperelliptic curve with good reduction [BBK10, BB12] and to integration in annuli.

Remark 1.41. For a genus g hyperelliptic curve over \mathbb{F}_{p^n} , Kedlaya’s algorithm computes the matrix of p -power Frobenius mod p^N in time $\tilde{O}(pN^2g^2n)$, where $\tilde{O}(X)$ denotes $O(X(\log X)^k)$ for some $k \geq 0$. Harvey [Har07] showed that one could interpret the reductions in cohomology in terms of linear recurrences to reduce the dependence on p in the runtime of the algorithm to \sqrt{p} . This was later generalized by Minzlaff [Min10] to superelliptic curves. Best showed that similar ideas can be used to improve the runtime of Coleman integration algorithms, first in the case of hyperelliptic curves over \mathbb{Q}_p [Bes19] and superelliptic curves over unramified extensions of \mathbb{Q}_p [Bes20].

Now we return to the Chabauty–Coleman method for a nice curve X/\mathbb{Q} .

Example 1.42. Recall the set-up of Example 1.22, with the genus 2 curve

$$X : y^2 = x^5 - 2x^3 + x + \frac{1}{4},$$

with known rational points

$$X(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}.$$

We computed an annihilating differential

$$\eta = \beta\omega_0 - \alpha\omega_1,$$

where

$$\begin{aligned} \alpha &:= \int_{(0,1/2)}^{(-1,-1/2)} \omega_0 = 3 + 3^2 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 3^{10} + O(3^{11}), \\ \beta &:= \int_{(0,1/2)}^{(-1,-1/2)} \omega_1 = 2 + 2 \cdot 3 + 2 \cdot 3^3 + 3^4 + 3^6 + 2 \cdot 3^8 + 2 \cdot 3^9 + O(3^{10}), \end{aligned}$$

and these values of α and β were produced using Algorithm 1.36.

Now we would like to determine the set

$$X(\mathbb{Q}_3)_1 := \{z \in X(\mathbb{Q}_3) : \int_{(0,1/2)}^z \eta = 0\} \supset X(\mathbb{Q}).$$

We begin by enumerating the points in $X(\mathbb{F}_3)$:

$$X(\mathbb{F}_3) = \{\infty, (0, \pm 1), (1, \pm 1), (2, \pm 1)\},$$

which indexes the residue disks. Now we would like to compute the power series expansions of the collection of “indefinite” Coleman integrals $\left\{ \int_{(0,1/2)}^{P_t} \eta \right\}$, where P_t ranges over all residue disks, and solve for all $z \in X(\mathbb{Q}_3)$ such that $\int_{(0,1/2)}^z \eta = 0$. Note that to compute these indefinite Coleman integrals, we can take P_0 a lift of an \mathbb{F}_3 -point in the same residue disk as P_t . Then

$$(11) \quad \int_{(0,1/2)}^{P_t} \eta = \int_{(0,1/2)}^{P_0} \eta + \int_{P_0}^{P_t} \eta,$$

where the first integral on the right-hand side of (11) is some 3-adic constant, and the second is a tiny integral computed using a local coordinate at P_0 . However, since each residue disk contains one rational point, we may take P_0 to be the rational point in the residue disk. This sets the constant of integration to 0 in each disk, by construction of the annihilating differential. Thus the computation is now purely local. Moreover, using the hyperelliptic involution, we need only to consider the residue disk of P_0 and not the disk of $i(P_0)$ as well.

So we carry out the computation in the residue disks of ∞ , $(0,1/2)$, $(1,1/2)$, and $(-1,1/2)$. For instance, in the residue disk of $(1,1/2)$, a local coordinate is given by

$$\begin{aligned} x(t) &= 1 + t + O(t^{20}) \\ y(t) &= \frac{1}{2} + 4t^2 + 8t^3 - 11t^4 - 63t^5 + 24t^6 + 680t^7 + 695t^8 - 7210t^9 - 19881t^{10} + 64544t^{11} + 374802t^{12} - 301946t^{13} \\ &\quad - 5872722t^{14} - 5265422t^{15} + 78467963t^{16} + 210631116t^{17} - 840861878t^{18} - 4667976084t^{19} + O(t^{20}) \end{aligned}$$

and the power series for $\int_{(0,1/2)}^{P_t} \eta = \int_{P_0}^{P_t} \eta$ is given by

$$\begin{aligned} &\left(2 + 3 + 2 \cdot 3^2 + 3^3 + 2 \cdot 3^5 + 3^6 + 2 \cdot 3^8 + 3^9 + O(3^{10}) \right) t + \left(3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^6 + 3^7 + 3^8 + 3^9 + 2 \cdot 3^{10} + O(3^{12}) \right) t^2 + \\ &\left(2 \cdot 3 + 3^2 + 3^5 + 3^7 + 3^8 + 3^{10} + O(3^{11}) \right) t^3 + \left(3^3 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 3^{12} + O(3^{13}) \right) t^4 + \\ &\left(2 \cdot 3^4 + 2 \cdot 3^7 + 3^8 + 3^9 + 2 \cdot 3^{11} + 2 \cdot 3^{12} + 2 \cdot 3^{13} + O(3^{14}) \right) t^5 + \left(3^4 + 2 \cdot 3^5 + 3^6 + 3^7 + 2 \cdot 3^8 + 3^9 + 3^{11} + 3^{12} + O(3^{14}) \right) t^6 + \\ &\left(2 \cdot 3^6 + 2 \cdot 3^7 + 3^8 + 3^{10} + 2 \cdot 3^{11} + 3^{12} + 2 \cdot 3^{14} + O(3^{16}) \right) t^7 + \left(2 \cdot 3^8 + 2 \cdot 3^9 + 3^{11} + 3^{12} + 2 \cdot 3^{14} + 2 \cdot 3^{15} + 2 \cdot 3^{16} + O(3^{18}) \right) t^8 + \\ &\left(2 \cdot 3^6 + 2 \cdot 3^9 + 2 \cdot 3^{10} + 3^{12} + 2 \cdot 3^{14} + 2 \cdot 3^{15} + O(3^{16}) \right) t^9 + \left(2 \cdot 3^9 + 3^{10} + 2 \cdot 3^{11} + 3^{13} + 3^{16} + 3^{17} + O(3^{19}) \right) t^{10} + \dots, \end{aligned}$$

which just has a simple zero at $t = 0$, corresponding to $(1,1/2)$.

Repeating this for each residue disk, we find that each residue disk has a simple zero at the rational point and no others, which gives that

$$X(\mathbb{Q}_3)_1 = X(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\},$$

and proves that

$$X(\mathbb{Q}) = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}.$$

Here is **SageMath** code to carry out this computation:

```
R.<x> = QQ[]
X = HyperellipticCurve(x^5-2*x^3+x+1/4)
p = 3
K = Qp(p,15) #some amount of precision loss
XK = X.change_ring(K)
a,b,_,_ = XK.coleman_integrals_on_basis(XK(0,1/2),XK(-1,-1/2))
for P in [X(0,1,0), X(0,1/2), X(-1,1/2), X(1,1/2)]:
    x,y = X.local_coord(P)
    t = x.parent().gen()
    S = K[[t]]
    dx = x.derivative()
```

```

omega0 = dx/(2*y)
omega1 = x*omega0
try:
    I = (b*S(omega0)-a*S(omega1)).integral()(p*t)
except TypeError:
    I = (b*S(omega0.power_series())-a*S(omega1.power_series())).integral()(p*t)
    I = I.power_series()
coeffval = min(c.valuation() for c in I.list())
I = I/p^coeffval
r = (I).truncate(20).roots()
[rt for rt in r if (rt[0]).valuation() > -1]

```

We note that **Magma** has an implementation of the Chabauty–Coleman method for genus 2 curves of ranks 0 and 1 (with an additional Mordell–Weil sieve step):

```

> R<x> := PolynomialRing(Rationals());
> X := HyperellipticCurve(x^5-2*x^3+x+1/4);
> C := IntegralModel(X);
> RationalPoints(C:Bound:=1000);
{@ (1 : 0 : 0), (-1 : -1 : 1), (-1 : 1 : 1), (0 : -1 : 1), (0 : 1 : 1), (1 : -1
: 1), (1 : 1 : 1) @}
> J := Jacobian(C);
> P := J!(C![0,1] - C![-1,-1]); //a point of infinite order
> Chabauty(P);
{ (1 : 1 : 1), (0 : -1 : 1), (0 : 1 : 1), (1 : 0 : 0), (-1 : 1 : 1), (1 : -1 :
1), (-1 : -1 : 1) }
{ 11, 19, 41, 43, 83, 179, 211 }
[ 2, 7, 23, 3, 13, 3 ]

```

1.4. More p -adic cohomology. We saw how Kedlaya’s zeta function algorithm played a crucial role in computing Coleman integrals on hyperelliptic curves. It would certainly be useful to compute Coleman integrals on curves beyond those that are hyperelliptic. And indeed, in the years since Kedlaya’s algorithm, a number of related zeta function algorithms were given: for superelliptic curves by Gaudry–Gürel [GG01], hyperelliptic curves given by an even degree model by Harrison [Har12], hyperelliptic curves in characteristic 2 by Denef–Vercauteren [DV06b], C_{ab} curves by Denef–Vercauteren [DV06a], and nondegenerate curves by Castryck–Denef–Vercauteren [CDV06]. However, the more general of these algorithms were not obviously practical and were not implemented.

More recently, Tuitman [Tui16, Tui17] gave an efficient algorithm to compute the action of Frobenius on rigid cohomology on smooth curves, by using a plane model with a map to \mathbb{P}^1 . We give a survey of Tuitman’s algorithm and show how it can be turned into an algorithm to compute Coleman integrals on plane curves.

First, we set up Tuitman’s algorithm from the point of view of explicit Coleman integration, as done by Balakrishnan–Tuitman [BTa]. Let X be a nice curve over \mathbb{Q} of genus g , birational to

$$Q(x, y) = y^{d_x} + Q_{d_x-1}y^{d_x-1} + \cdots + Q_0 = 0,$$

such that $Q(x, y)$ is irreducible and $Q_i(x) \in \mathbb{Z}[x]$ for $i = 0, \dots, d_x - 1$. Here is a rough outline of Tuitman’s algorithm:

- (1) Consider the map: $x : X \rightarrow \mathbb{P}^1$ and remove the ramification locus $r(x)$ of x . (This is the analogue of removing the Weierstrass points in Kedlaya's algorithm.)
- (2) Choose a lift of Frobenius sending $x \mapsto x^p$ and compute the image of y via Hensel lifting.
- (3) Compute the action of Frobenius on differentials and reduce pole orders using relations in cohomology via Lauder's fibration algorithm.

Then for a basis $\{\omega_i\}_{i=0}^{2g-1}$ of $H_{\text{rig}}^1(X \otimes \mathbb{Q}_p)$, Tuitman's algorithm computes

$$\phi^* \omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji} \omega_j,$$

and, as before, this algorithm for computing the action of Frobenius on cohomology can be used to give an algorithm for Coleman integration.

We let $\Delta(x) \in \mathbb{Z}[x]$ be the discriminant of Q with respect to y , and let $r(x) = \Delta / \gcd(\Delta, d\Delta/dx)$. Note that $r(x)$ is squarefree and divides $\Delta(x)$.

Set

$$\begin{aligned} S &= \mathbb{Z}_p\langle x, 1/r \rangle, & S^\dagger &= \mathbb{Z}_p\langle x, 1/r \rangle^\dagger, \\ R &= \mathbb{Z}_p\langle x, 1/r, y \rangle/(Q), & R^\dagger &= \mathbb{Z}_p\langle x, 1/r, y \rangle^\dagger/(Q), \end{aligned}$$

where $\langle \cdot \rangle^\dagger$ denotes the ring of overconvergent functions given by weak completion of the corresponding polynomial ring.

Definition 1.43. Let $W^0 \in \text{GL}_{d_x}(\mathbb{Q}[x, 1/r])$ and $W^\infty \in \text{GL}_{d_x}(\mathbb{Q}[x, 1/x, 1/r])$ denote matrices such that, if we denote

$$b_j^0 = \sum_{i=0}^{d_x-1} W_{i+1, j+1}^0 y^i \quad \text{and} \quad b_j^\infty = \sum_{i=0}^{d_x-1} W_{i+1, j+1}^\infty y^i$$

for all $0 \leq j \leq d_x - 1$, then

- (1) $[b_0^0, \dots, b_{d_x-1}^0]$ is an integral basis for $\mathbb{Q}(X)$ over $\mathbb{Q}[x]$,
- (2) $[b_0^\infty, \dots, b_{d_x-1}^\infty]$ is an integral basis for $\mathbb{Q}(X)$ over $\mathbb{Q}[1/x]$,

where $\mathbb{Q}(X)$ denotes the function field of X . Moreover, let $W \in \text{GL}_{d_x}(\mathbb{Q}[x, 1/x])$ denote the change of basis matrix $W = (W^0)^{-1}W^\infty$.

Example 1.44. Let X/\mathbb{Q} be an odd degree monic hyperelliptic curve of genus g given by the plane model

$$Q(x, y) = y^2 - f(x) = 0.$$

We have that

$$r(x) = f(x)$$

and:

$$W^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad W^\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1/x^{g+1} \end{pmatrix}.$$

This means that $b^0 = [1, y]$ and $b^\infty = [1, y/x^{g+1}]$ are integral bases for the function field of X over $\mathbb{Q}[x]$ and $\mathbb{Q}[1/x]$, respectively.

Definition 1.45. We say that the triple (Q, W^0, W^∞) has good reduction at a prime number p if the conditions below (taken from [Tui17, Assumption 1]) are satisfied.

Assumption 1 ([Tui17, Assumption 1]).

- (1) The discriminant of $r(x)$ is contained in \mathbb{Z}_p^\times .

- (2) If we let $\mathbb{F}_p(x, y)$ be the field of fractions of $\mathbb{F}_p[x, y]/(Q)$, then:
 - (a) The reduction modulo p of $[b_0^0, \dots, b_{d_x-1}^0]$ is an integral basis for $\mathbb{F}_p(x, y)$ over $\mathbb{F}_p[x]$.
 - (b) The reduction modulo p of $[b_0^\infty, \dots, b_{d_x-1}^\infty]$ is an integral basis for $\mathbb{F}_p(x, y)$ over $\mathbb{F}_p[1/x]$.
- (3) $W^0 \in \mathrm{GL}_{d_x}(\mathbb{Z}_p[x, 1/r])$ and $W^\infty \in \mathrm{GL}_{d_x}(\mathbb{Z}_p[1/x, 1/r])$.
- (4) Denote:

$$\begin{aligned}\mathcal{R}^0 &= \mathbb{Z}_p[x]b_0^0 + \dots + \mathbb{Z}_p[x]b_{d_x-1}^0, \\ \mathcal{R}^\infty &= \mathbb{Z}_p[1/x]b_0^\infty + \dots + \mathbb{Z}_p[1/x]b_{d_x-1}^\infty.\end{aligned}$$

Then the discriminants of the finite \mathbb{Z}_p -algebras $\mathcal{R}^0/(r(x))$ and $\mathcal{R}^\infty/(1/x)$ are contained in \mathbb{Z}_p^\times .

Definition 1.46. We say that a point of X^{an} is *very infinite* if its x -coordinate is ∞ and *very bad* if it is either very infinite or its x -coordinate is a zero of $r(x)$.

Definition 1.47. We say that a residue disk (as well as any point inside it) is *infinite* or *bad* if it contains a very infinite or a very bad point, respectively. A point or residue disk is called *finite* if it is not infinite and *good* if it is not bad.

We let U denote the complement of the very bad points in X^{an} .

Definition 1.48. Let $\{\omega_i\}_{i=0, \dots, 2g-1}$ be p -adically integral 1-forms on U such that

- (1) $\omega_0, \dots, \omega_{g-1}$ form a basis for $H^0(X_{\mathbb{Q}_p}, \Omega^1)$,
- (2) $\omega_0, \dots, \omega_{2g-1}$ form a basis for $H_{\mathrm{rig}}^1(X \otimes \mathbb{Q}_p)$,
- (3) $\mathrm{ord}_P(\omega_i) \geq -1$ for all i at all finite very bad points P ,
- (4) $\mathrm{ord}_P(\omega_i) \geq -1 + (\mathrm{ord}_0(W) + 1)e_P$ for all i at all very infinite points P .

In [Tui16, Tui17], it is explained how 1-forms satisfying properties (2)-(4) can be computed. Briefly, one computes a basis for $H_{\mathrm{rig}}^1(U)$ and uses the kernel of a residue map to extract those 1-forms of the second kind, to produce a basis for $H_{\mathrm{rig}}^1(X \otimes \mathbb{Q}_p)$. The algorithm can be easily adapted so that (1) is satisfied as well, which is the convention we take.

Definition 1.49. The p -th power Frobenius ϕ acts on $H_{\mathrm{rig}}^1(X \otimes \mathbb{Q}_p)$, so there exist a matrix $M \in M_{2g \times 2g}(\mathbb{Q}_p)$ and functions $h_0, \dots, h_{2g-1} \in R^\dagger \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ji} \omega_j$$

for $i = 0, \dots, 2g-1$.

After we compute the action of Frobenius on a 1-form, we need to reduce the pole order using relations in cohomology. Tuitman's algorithm uses Lauder's fibration algorithm, which solves for a cohomologous differential of lower pole order using a linear system. Tuitman applies it first to points not lying over infinity:

Proposition 1.50. Let r' denote dr/dx for points not over infinity. For all $\ell \in \mathbb{N}$ and every $w \in \mathbb{Q}_p[x]^{\oplus d_x}$, there exist vectors $u, v \in \mathbb{Q}_p[x]^{\oplus d_x}$ such that $\deg(v) < \deg(r)$ and

$$\frac{\sum_{i=0}^{d_x-1} w_i b_i^0}{r^\ell} \frac{dx}{r} = \left(d \frac{\sum_{i=0}^{d_x-1} v_i b_i^0}{r^\ell} \right) + \frac{\sum_{i=0}^{d_x-1} u_i b_i^0}{r^{\ell-1}} \frac{dx}{r}$$

Proof. Since r is separable, r' is invertible in $\mathbb{Q}_p[x]/r$. We check that there is a unique solution v to the $d_x \times d_x$ linear system

$$(M/r' - \ell I) v \equiv w/r' \pmod{r}$$

over $\mathbb{Q}_p[r]/(r)$: take

$$u = \frac{w - (M - \ell r' I)v}{r} - \frac{dv}{dx}.$$

□

For reducing pole orders at points over infinity, we have the following proposition:

Proposition 1.51. *For every vector $w \in \mathbb{Q}_p[x, 1/x]^{\oplus d_x}$ with $\text{ord}_\infty(w) \leq -\deg r$, there exist $u, v \in \mathbb{Q}_p[x, 1/x]^{\oplus d_x}$ with $\text{ord}_\infty(u) > \text{ord}_\infty(w)$ such that*

$$\left(\sum_{i=0}^{d_x-1} w_i b_i^\infty \right) \frac{dx}{r} = d \left(\sum_{i=0}^{d_x-1} v_i b_i^\infty \right) + \left(\sum_{i=0}^{d_x-1} u_i b_i^\infty \right) \frac{dx}{r}.$$

Here is Tuitman's algorithm for computing the matrix M and the functions h_0, \dots, h_{2g-1} :

Algorithm 1.52 (Tuitman's algorithm [Tui16, Tui17]).

Input:

- A prime $p > 2$ of good reduction (in the sense of Definition 1.45) for a nice curve X/\mathbb{Q}
- A basis $\{\omega_i\}$ of $H_{\text{rig}}^1(X \otimes \mathbb{Q}_p)$

Output: The matrix $M \in M_{2g \times 2g}(\mathbb{Q}_p)$ and overconvergent functions $h_i \in R^\dagger \otimes \mathbb{Q}_p$ such that $\phi^* \omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji} \omega_j$.

- (1) Compute the Frobenius lift: set $\phi(x) = x^p$ and determine the elements $\phi(1/r) \in S^\dagger$ and $\phi(y) \in R^\dagger$ by Hensel lifting.
- (2) Finite pole order reduction: For $i = 0, \dots, 2g-1$, find $h_{i,0} \in R^\dagger \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + G_i \left(\frac{dx}{r(x)} \right),$$

where $G_i \in R \otimes \mathbb{Q}_p$ only has poles at very infinite points.

- (3) Infinite pole order reduction. For $i = 0, \dots, 2g-1$, find $h_{i,\infty} \in R \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + dh_{i,\infty} + H_i \left(\frac{dx}{r(x)} \right),$$

where $H_i \in R \otimes \mathbb{Q}_p$ still only has poles at very infinite points P and satisfies

$$\text{ord}_P(H_i) \geq (\text{ord}_0(W) - \deg(r) + 2)e_P$$

at all these points.

- (4) Final reduction: For $i = 0, \dots, 2g-1$, find $h_{i,end} \in R \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + dh_{i,\infty} + dh_{i,end} + \sum_{j=0}^{2g-1} M_{ji} \omega_j,$$

where $M \in M_{2g \times 2g}(\mathbb{Q}_p)$ is the matrix of ϕ^* on $H_{\text{rig}}^1(U \otimes \mathbb{Q}_p)$ with respect to the basis $\{\omega_i\}_{i=0}^{2g-1}$.

The matrix M and the functions

$$h_i := h_{i,0} + h_{i,\infty} + h_{i,end}$$

are exactly what we need from [Tui16, Tui17] to compute Coleman integrals, giving the necessary input into Algorithm 1.53.

Algorithm 1.53 (Coleman integration on a plane curve [BTa]).

Input:

- A prime $p > 2$ of good reduction (in the sense of Definition 1.45) for a nice curve X/\mathbb{Q}
- Points $P, Q \in X(\mathbb{Q}_p)$ not contained in very bad residue disks
- A 1-form ω of the second kind

Output: The Coleman integral $\int_P^Q \omega$.

- (1) Since ω is of the second kind, we may write it as a linear combination of a basis $\{\omega_i\}_{i=0}^{2g-1}$ for $H_{\text{rig}}^1(X \otimes \mathbb{Q}_p)$ together with an exact form. Use Tuitman's algorithm to write $\omega = dh + \sum_{i=0}^{2g-1} a_i \omega_i$, which allows us to specialize to the case of Coleman integrals of basis differentials.
- (2) Compute the action of Frobenius on $H_{\text{rig}}^1(X \otimes \mathbb{Q}_p)$ using Algorithm 1.52 and store M and h_0, \dots, h_{2g-1} .
- (3) Compute the integrals $\int_P^{\phi(P)} \omega_i$ and $\int_{\phi(Q)}^Q \omega_i$ for $i = 0, \dots, 2g - 1$ using local coordinates and tiny integrals.
- (4) Compute $h_i(P) - h_i(Q)$ for $i = 0, \dots, 2g - 1$ and use the system of equations

$$\sum_{j=0}^{2g-1} (M^t - I)_{ij} \left(\int_P^Q \omega_j \right) = h_i(P) - h_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i$$

to solve for all $\int_P^Q \omega_i$.

Remark 1.54. As in the case of integrating from a Weierstrass point on a hyperelliptic curve, to integrate from a very bad point B on a plane curve, split up the integral

$$\int_B^Q \omega_i = \int_B^{B'} \omega_i + \int_{B'}^Q \omega_i$$

for B' a point near the boundary of the residue disk of B , then apply Algorithm 1.53 to compute $\int_{B'}^Q \omega_i$ and compute $\int_B^{B'} \omega_i$ using a tiny integral.

Remark 1.55. For precision estimates in Algorithm 1.53, see [BTa, §4].

Example 1.56. We show how the algorithm above can be used to show that a Jacobian of a non-hyperelliptic genus 55 curve has positive rank (for more details, including timing data, see [BTa, §6.4]). We consider the genus 55 curve X with plane model given by $Q(x, y) = 0$ below:

$$\begin{aligned} Q(x, y) = & x^{11}y - x^7y^5 - x^6y^6 - x^4y^8 + xy^{11} + y^{12} + x^{11} - x^{10}y + x^8y^3 - x^6y^5 + x^5y^6 + x^3y^8 - x^2y^9 - xy^{10} + \\ & y^{11} + x^{10} + x^9y - x^8y^2 + x^7y^3 + x^6y^4 + x^5y^5 - x^4y^6 + xy^9 + y^{10} - x^9 + x^8y + x^7y^2 + x^6y^3 + x^5y^4 + \\ & x^4y^5 + x^3y^6 - x^2y^7 + y^9 + x^8 - x^7y + x^6y^2 - x^5y^3 + xy^7 + y^8 + x^7 + x^6y + x^5y^2 - x^2y^5 - xy^6 + \\ & y^7 - x^6 - x^4y^2 - x^2y^4 + xy^5 - x^5 + x^3y^2 - x^2y^3 + y^5 - x^4 + x^3y + x^2y^2 + xy^3 + y^4 - x^2y - xy^2 + \\ & y^3 - x^2 - xy + x + y. \end{aligned}$$

Let $p = 7$ and consider $P_1 = (0, 0)$ and $P_2 = (1, 0)$, which are each good points on X . We compute the Coleman integrals $\left\{ \int_{P_1}^{P_2} \omega_i \right\}_{i=1}^{110}$ for the basis $\{\omega_i\}$ of $H_{\text{rig}}^1(X \otimes \mathbb{Q}_p)$ constructed as in Definition 1.48 with $N = 5$ as our precision. We find that

$$\int_{P_1}^{P_2} \omega_1 = 5 \cdot 7 + O(7^2),$$

and thus the Jacobian of X has positive rank.

The **Magma** code for this example is available at `./examples/g55.m` in [BTb].

Project 1.57 (Coleman integration for curves over number fields). Give an algorithm to compute Coleman integrals on curves over number fields and implement the algorithm. To start, see the Github repository of Balakrishnan–Tuitman [BTb] for plane curves defined over \mathbb{Q} . Before implementing, it would be good to think through the current scope of curves and number fields that are practical.

Project 1.58 (A Chabauty–Coleman solver). Use the project above as well as estimates on precision of p -adic power series to give a Chabauty–Coleman solver for curves over number fields that would take as input a genus g curve X defined over a number field K with $r = \text{rk } J(K) < g$, a prime \mathfrak{p} of good reduction, and r generators of the Mordell–Weil group modulo torsion and output the set $X(K_{\mathfrak{p}})_1$. To start, see the Github repositories of Balakrishnan–Tuitman [BTb] and Hashimoto–Morrison [HM].

1.5. Iterated Coleman integrals. Let X/\mathbb{Q} be a nice curve of genus g with a plane model and let p be a prime of good reduction. In [Col82], Coleman described a construction of iterated p -adic integrals on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ with applications to Beilinson’s conjecture. This was extended by Coleman–de Shalit [CdS88] to any curve and by Besser [Bes02] to higher-dimensional varieties. (For the classical theory of iterated integrals, see the work of Chen [Che71].)

By an *iterated Coleman integral* we mean an iterated path integral

$$(12) \quad \int_P^Q \eta_n \dots \eta_1 = \int_0^1 \int_0^{t_1} \dots \int_0^{t_{n-1}} f_n(t_n) \dots f_1(t_1) dt_n \dots dt_1.$$

We will henceforth use notation on the left hand side of (12) to describe iterated integrals, where the implicit integrations are with respect to a dummy variable: e.g.,

$$\int_P^Q \eta_2 \eta_1 := \int_P^Q \eta_2(R) \int_P^R \eta_1 = \int_P^Q \eta_2(R) I(R),$$

where $I(R) = \int_P^R \eta_1$.

The main idea is to apply an algorithm for computing the action of Frobenius on p -adic cohomology (e.g., Kedlaya or Tuitman) to produce the relationship

$$\phi^* \omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji} \omega_j,$$

observe that the eigenvalues of $M^{\otimes n}$, are not 1, and reduce the computation of an n -fold iterated integral to a computation of an $(n - 1)$ -fold iterated integral. For instance, in writing down a linear system for computing single Coleman integrals, we used the fundamental theorem of calculus to produce the constants

$$\int_P^Q dh_i = h_i(Q) - h_i(P),$$

and now we will apply this idea inductively. As before, iterated integrals between points in the same residue disk can be computed using a local coordinate at one point and (iteratively) integrating power series.

More formally, here is how we compute a tiny iterated integral:

Algorithm 1.59 (Tiny iterated integral on a plane curve X).

Input:

- A prime $p > 2$ of good reduction (in the sense of Definition 1.45) for a plane curve X/\mathbb{Q}
- Points $P, Q \in X(\mathbb{Q}_p)$ in same residue disk.

Output: The tiny iterated integral $\int_P^Q \eta_1 \dots \eta_n$

- (1) Compute a local coordinate $(x(t), y(t))$ at P .
- (2) For each k , write $\eta_k(x, y)$ as $\eta_k(t)dt$.
- (3) Let $I_{n+1} = 1$. Compute for $k = n, n-1, \dots, 2$

$$I_k = \int_P^{R_{k-1}} \eta_k I_{k+1} = \int_P^{t(R_{k-1})} \eta_k(t) I_{k+1} dt$$

where $t(R_{k-1})$ is parametrizing points in the residue disk of P .

$$(4) \int_P^Q \eta_1 \dots \eta_n = \int_P^{t(Q)} \eta_1(t) I_2(t) dt.$$

To compute more general iterated Coleman integrals, we will use the following properties.

Proposition 1.60. *Let $\omega_{i_1}, \dots, \omega_{i_n}$ be forms of the second kind, holomorphic at $P, Q \in X(\mathbb{Q}_p)$.*

- (1) $\int_P^P \omega_{i_1} \dots \omega_{i_n} = 0$
- (2) $\sum_{\text{all permutations } \sigma} \int_P^Q \omega_{\sigma(i_1)} \dots \omega_{\sigma(i_n)} = \prod_{j=1}^n \int_P^Q \omega_{i_j}$
- (3) $\int_P^Q \omega_{i_1} \dots \omega_{i_n} = (-1)^n \int_Q^P \omega_{i_n} \dots \omega_{i_1}$

As a corollary, we have

$$\text{Corollary 1.61. } \int_P^Q \underbrace{\omega_i \dots \omega_i}_n = \frac{1}{n!} \left(\int_P^Q \omega_i \right)^n$$

The following lemma gives the analogue of additivity in endpoints:

Lemma 1.62. *Let $P, P', Q \in X(\mathbb{Q}_p)$. Then*

$$\int_P^Q \omega_{i_1} \dots \omega_{i_n} = \sum_{j=0}^n \int_{P'}^Q \omega_{i_1} \dots \omega_{i_j} \int_P^{P'} \omega_{i_{j+1}} \dots \omega_{i_n}$$

Now for ease of exposition, we will focus our attention on the case of $n = 2$, the double Coleman integrals [Bal13, Bal15].

Applying Lemma 1.62 twice, we may link double integrals between different residue disks:

$$\int_P^Q \omega_i \omega_k = \int_P^{P'} \omega_i \omega_k + \int_{P'}^{Q'} \omega_i \omega_k + \int_{Q'}^Q \omega_i \omega_k + \int_P^{P'} \omega_k \int_{P'}^Q \omega_i + \int_{P'}^{Q'} \omega_k \int_{Q'}^Q \omega_i.$$

We can directly compute double integrals using a linear system. Indeed, using Lemma 1.62, we take $\phi(P)$ and $\phi(Q)$ to be the points in the disks of P and Q , respectively, which gives

$$(13) \quad \int_P^Q \omega_i \omega_k = \int_P^{\phi(P)} \omega_i \omega_k + \int_{\phi(P)}^{\phi(Q)} \omega_i \omega_k + \int_{\phi(Q)}^Q \omega_i \omega_k + \int_P^{\phi(P)} \omega_k \int_{\phi(P)}^Q \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_k \int_{\phi(Q)}^Q \omega_i.$$

Then we expand the following

$$(14) \quad \begin{aligned} \int_{\phi(P)}^{\phi(Q)} \omega_i \omega_k &= \int_P^Q \phi^*(\omega_i \omega_k) = \int_P^Q \phi^*(\omega_i) \phi^*(\omega_k) \\ &= \int_P^Q (df_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j)(df_k + \sum_{j=0}^{2g-1} M_{kj}^t \omega_j) \\ &= c_{ik} + \int_P^Q \left(\sum_{j=0}^{2g-1} M_{ij}^t \omega_j \right) \left(\sum_{j=0}^{2g-1} M_{kj}^t \omega_j \right), \end{aligned}$$

where

$$\begin{aligned} c_{ik} &= \int_P^Q df_i(R)(f_k(R)) - f_k(P)(f_i(Q) - f_i(P)) + \int_P^Q \sum_{j=0}^{2g-1} M_{ij}^t \omega_j(R)(f_k(R) - f_k(P)) \\ &\quad + f_i(Q) \int_P^Q \sum_{j=0}^{2g-1} M_{kj}^t \omega_j - \int_P^Q f_i(R) \left(\sum_{j=0}^{2g-1} M_{kj}^t \omega_j(R) \right). \end{aligned}$$

Putting together (13) and (14), we get

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i \omega_k \\ \vdots \end{pmatrix} = (I_{4g^2 \times 4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^P \omega_i \omega_k - \left(\int_P^Q \omega_i \right) \left(\int_{\phi(P)}^P \omega_k \right) \\ - \left(\int_Q^{\phi(Q)} \omega_i \right) \left(\int_{\phi(P)}^{\phi(Q)} \omega_k \right) + \int_{\phi(Q)}^Q \omega_i \omega_k \\ \vdots \end{pmatrix}.$$

Algorithm 1.63 (Double Coleman integrals [Bal13, Bal15]).

Input:

- A prime $p > 2$ of good reduction (in the sense of Definition 1.45) for a plane curve X/\mathbb{Q}
- Points $P, Q \in X(\mathbb{Q}_p)$ in the region of overconvergence for the lift of p -power Frobenius

Output: The double integrals $\left(\int_P^Q \omega_i \omega_j \right)_{i,j=0}^{2g-1}$.

- (1) Use Algorithm 1.53 to compute the single integrals $\int_P^Q \omega_i$, $\int_{\phi(P)}^{\phi(Q)} \omega_i$ for all i .
- (2) Use Algorithm 1.59 to compute $\int_{\phi(P)}^P \omega_i \omega_k$, $\int_{\phi(Q)}^Q \omega_i \omega_k$ for all i, k
- (3) Compute the constants c_{ik} for all i, k using single integrals.
- (4) Recover the double integrals using the linear system

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i \omega_k \\ \vdots \end{pmatrix} = (I_{4g^2 \times 4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^P \omega_i \omega_k - \left(\int_P^Q \omega_i \right) \left(\int_{\phi(P)}^P \omega_k \right) \\ - \left(\int_Q^{\phi(Q)} \omega_i \right) \left(\int_{\phi(P)}^{\phi(Q)} \omega_k \right) + \int_{\phi(Q)}^Q \omega_i \omega_k \\ \vdots \end{pmatrix}.$$

Remark 1.64. In [Bal13, Bal15], Algorithm 1.63 was described and implemented for hyperelliptic curves, as it used Kedlaya's algorithm (and Harrison's generalization) for the Frobenius step. With Tuitman's algorithm in place of Kedlaya's, one can run the algorithm for (a plane model of) a nice curve.

Example 1.65. Let X/\mathbb{Q} be the genus 2 curve

$$y^2 = x^5 - 2x^4 + 2x^3 - x + 1$$

which is [LMF20a] and has good reduction at $p = 5$.

Using Algorithm 1.63, we compute 5-adic double Coleman integrals between the points $P = (0, 1)$ and $Q = (1, 1)$, where $\omega_i = \frac{x^i}{2y}dx$:

$$\begin{pmatrix} \int_P^Q \omega_0 \omega_0 \\ \int_P^Q \omega_0 \omega_1 \\ \int_P^Q \omega_0 \omega_2 \\ \int_P^Q \omega_0 \omega_3 \\ \int_P^Q \omega_1 \omega_0 \\ \int_P^Q \omega_1 \omega_1 \\ \int_P^Q \omega_1 \omega_2 \\ \int_P^Q \omega_1 \omega_3 \\ \int_P^Q \omega_2 \omega_0 \\ \int_P^Q \omega_2 \omega_1 \\ \int_P^Q \omega_2 \omega_2 \\ \int_P^Q \omega_2 \omega_3 \\ \int_P^Q \omega_3 \omega_0 \\ \int_P^Q \omega_3 \omega_1 \\ \int_P^Q \omega_3 \omega_2 \\ \int_P^Q \omega_3 \omega_3 \end{pmatrix} = \begin{pmatrix} 3 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + 4 \cdot 5^5 + 5^6 + O(5^8) \\ 3 \cdot 5^2 + 3 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 5^6 + 3 \cdot 5^7 + O(5^8) \\ 2 \cdot 5 + 4 \cdot 5^2 + 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + O(5^7) \\ 4 \cdot 5 + 5^2 + 4 \cdot 5^3 + 5^4 + 3 \cdot 5^5 + 2 \cdot 5^6 + O(5^7) \\ 5^3 + 3 \cdot 5^4 + 2 \cdot 5^5 + 4 \cdot 5^6 + 5^7 + O(5^8) \\ 2 \cdot 5^2 + 5^3 + 4 \cdot 5^4 + 5^6 + O(5^8) \\ 2 \cdot 5^2 + 4 \cdot 5^3 + 5^4 + 3 \cdot 5^5 + 5^6 + O(5^7) \\ 1 + 4 \cdot 5 + 2 \cdot 5^2 + 5^3 + 5^4 + 4 \cdot 5^5 + 3 \cdot 5^6 + O(5^7) \\ 4 \cdot 5^3 + 3 \cdot 5^4 + 3 \cdot 5^5 + 3 \cdot 5^6 + O(5^7) \\ 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 5^5 + O(5^7) \\ 2 + 4 \cdot 5 + 4 \cdot 5^2 + 5^3 + 2 \cdot 5^4 + 4 \cdot 5^5 + O(5^6) \\ 3 + 2 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + O(5^6) \\ 4 \cdot 5 + 5^2 + 3 \cdot 5^3 + 4 \cdot 5^4 + 3 \cdot 5^5 + 3 \cdot 5^6 + O(5^7) \\ 4 + 4 \cdot 5 + 5^2 + 4 \cdot 5^3 + 3 \cdot 5^5 + 4 \cdot 5^6 + O(5^7) \\ 3 + 4 \cdot 5 + 4 \cdot 5^2 + 2 \cdot 5^5 + O(5^6) \\ 2 + 3 \cdot 5 + 4 \cdot 5^2 + 5^4 + 4 \cdot 5^5 + O(5^6) \end{pmatrix}.$$

Using SageMath code available on GitHub [Bal], here is how to generate the values of the double integrals above:

```
R.<x> = QQ[]
X = HyperellipticCurve(x^5-2*x^4+2*x^3-x+1)
K = Qp(5,8)
XK = X.change_ring(K)
P = XK(0,1)
Q = XK(1,1)
XK.double_integrals_on_basis(P,Q)
```

Project 1.66. There is a certain amount of redundancy that allows one to express double (or higher iterated) integrals in terms of single integrals. For instance, looking at double integrals in the case of $g = 1$, we have that $\int_P^Q \omega_i \omega_i = \frac{1}{2} \left(\int_P^Q \omega_i \right)^2$ for $i = 0, 1$ and $\int_P^Q \omega_0 \omega_1 + \int_P^Q \omega_1 \omega_0 = \int_P^Q \omega_0 \int_P^Q \omega_1$. Can these relations be used to give a more efficient algorithm to compute double (or higher iterated) integrals?

1.6. An application (preview). Let \mathcal{E}/\mathbb{Z} be the minimal regular model of an elliptic curve. Let $\mathcal{X} = \mathcal{E} \setminus \mathcal{O}$. Let $\omega_0 = \frac{dx}{2y+a_1x+a_3}$, $\omega_1 = x\omega_0$ in Weierstrass coordinates.

Let b be a tangential basepoint at the point at infinity or an integral 2-torsion point. (For more about tangential basepoints, see Deligne [Del89] or Besser [Bes12, §1.5.4]. Roughly, the issue is that ω_1 has a pole at the point at infinity, so to make sense of an integral from the point at infinity, we must normalize with respect to a choice of tangent vector, which essentially means that we are fixing a direction at b .) Let p be a prime of good reduction. Suppose \mathcal{E} has analytic rank 1 and Tamagawa product 1. Consider

$$\log(z) = \int_b^z \omega_0, \quad D_2(z) = \int_b^z \omega_0 \omega_1.$$

One can think of $\log(z)$ as the Coleman integral extending \log on the formal group of \mathcal{E}/\mathbb{Z}_p . The function D_2 is labeled as such to suggest a dilogarithm.

Theorem 1.67 ([Kim10, BKK11]). *Suppose P is a point of infinite order in $\mathcal{E}(\mathbb{Z})$. Then $\mathcal{X}(\mathbb{Z}) \subseteq \mathcal{E}(\mathbb{Z})$ is in the zero set of*

$$f(z) = (\log(P))^2 D_2(z) - (\log(z))^2 D_2(P),$$

or in other words, $\frac{D_2(z)}{(\log(z))^2}$ is constant on integral points.

We will return to this result and discuss how it is related to p -adic height pairings in the following section.

2. p -ADIC HEIGHTS ON JACOBIANS OF CURVES

From a computational point of view, the main idea of quadratic Chabauty is to replace the *linear* relations that make it possible to cut out rational points among p -adic points in the method of Chabauty–Coleman by *bilinear* relations. This can be achieved using the theory of p -adic heights, developed in various degrees of generality by Bernardi [Ber81], Néron [Nér76], Perrin-Riou [PR83], Schneider [Sch82], Mazur–Tate [MT83], Zarhin [Zar90], Iovita–Werner [IW03], Coleman–Gross [CG89], and Nekovář [Nek93].

Most of these constructions are quite similar to constructions of the real valued (or Néron–Tate) height pairing. Recall that this is a symmetric bilinear pairing $A(K) \times A(K) \rightarrow \mathbb{R}$, where A is an abelian variety over a global field K , such that the associated quadratic form $\hat{h}: A(K) \rightarrow \mathbb{R}$ satisfies the Northcott property: for all real numbers B the set of points $P \in A(K)$ such that $\hat{h}(P) < B$ is finite. The latter property has no analogue in the p -adic world, but the bilinearity carries over.

2.1. p -adic heights on elliptic curves. We begin with a discussion of p -adic heights on elliptic curves defined over the rationals, following the work of Mazur–Stein–Tate [MST06]. In this context already, we can see a hint of some objects that will show up in explicit quadratic Chabauty.

Let E/\mathbb{Q} be an elliptic curve, given by a Weierstrass equation with integral coefficients, and let \mathcal{O} be the point at infinity. Let $p \geq 5$ be a prime of good ordinary reduction for E . Let $P \in E(\mathbb{Q})$ be a nonzero point. Write

$$P = (x(P), y(P)) = \left(\frac{a(P)}{d(P)^2}, \frac{b(P)}{d(P)^3} \right),$$

where

$$a(P), b(P), d(P) \in \mathbb{Z}, \quad d(P) \geq 1, \quad \gcd(a(P), d(P)) = 1 = \gcd(b(P), d(P)).$$

We call $d(P)$ the *denominator* of P . Suppose that P satisfies two conditions:

- (i) P reduces to \mathcal{O} in $E(\mathbb{F}_p)$;
- (ii) P reduces to a nonsingular point of $E(\mathbb{F}_\ell)$ for all bad primes ℓ .

Fix a branch $\log_p: \mathbb{Q}_p^* \rightarrow \mathbb{Q}_p$ of the p -adic logarithm.

Definition 2.1. The *cyclotomic p -adic height* on such a point $P \in E(\mathbb{Q})$ is

$$h(P) = \frac{1}{p} \log_p \left(\frac{\sigma(P)}{d(P)} \right) \in \mathbb{Q}_p,$$

where $\sigma(P)$ is the p -adic sigma function associated to E/\mathbb{Z}_p .

Remark 2.2. More generally, p -adic heights depend on a choice of idèle class character, see Remark 2.11. Over \mathbb{Q} , up to scalars, this is uniquely determined and is the *cyclotomic* character.

Mazur and Tate gave 11 different characterizations of the p -adic sigma function [MT91]. We will describe one characterization, which is particularly useful for computations.

Let $x(t) = t^{-2} + \dots \in \mathbb{Z}_p((t))$ be x in the formal group of E/\mathbb{Z}_p ; then $y(t) = t^{-3} + \dots \in \mathbb{Z}_p((t))$.

Theorem 2.3 (Mazur–Tate [MT91]). *There is exactly one odd⁷*

$$\sigma(t) = t + \dots \in t\mathbb{Z}[[t]].$$

and constant $c \in \mathbb{Z}_p$ that together satisfy the p -adic differential equation:

$$x(t) + c = -\frac{d}{\omega} \left(\frac{1}{\sigma} \frac{d\sigma}{\omega} \right),$$

where ω is the invariant differential associated to the chosen Weierstrass model for E

$$\omega = \frac{dx}{2y + a_1x + a_3}, \quad \text{and } c = \frac{a_1^2 + 4a_2 - \mathbf{E}_2(E, \omega)}{12}.$$

We will return to $\mathbf{E}_2(E, \omega)$ in a bit.

Lemma 2.4. *The height function h extends uniquely to the full Mordell–Weil group $E(\mathbb{Q})$ so that $h(nP) = n^2 h(P)$ for all $n \in \mathbb{Z}$ and $P \in E(\mathbb{Q})$. For $P, Q \in E(\mathbb{Q})$ setting*

$$(P, Q) = h(P) + h(Q) - h(P + Q),$$

we get a symmetric bilinear pairing on $E(\mathbb{Q})$.

To compute $h(Q)$ for arbitrary $Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, let $n_1 = \#E(\mathbb{F}_p)$ and $n_2 = \text{lcm}(\{c_v\})$, where the c_v are the Tamagawa numbers. Let $n = \text{lcm}(n_1, n_2)$. Then $P := nQ$ satisfies (i) and (ii) needed earlier, so we may compute $h(P) = h(nQ)$, and then

$$h(Q) = \frac{1}{n^2} h(nQ) = \frac{1}{n^2} h(P).$$

One reason why the p -adic height is interesting is that, in analogy with canonical height, one can define the p -adic regulator Reg_p of E/\mathbb{Q} as the determinant of the matrix of pairings on $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. Then the p -adic regulator fits into a p -adic Birch and Swinnerton-Dyer conjecture. The simplest instance of this is as follows:

Conjecture 2.5 (Mazur–Tate–Teitelbaum [MTT86]). *Suppose E has good ordinary reduction at p . Let $\mathcal{L}_p(E, T)$ be the p -adic L -function attached to E/\mathbb{Q} . Then we have*

(1)

$$\text{ord}_{T=0} \mathcal{L}_p(E, T) = \text{rk } E(\mathbb{Q})$$

⁷By odd, we mean that $\sigma(I(t)) = -\sigma(t)$ where $I(t) = -t - a_1t^2 + \dots$ is the formal inverse law.

- (2) The leading coefficient $\mathcal{L}_p^*(E, 0)$ of the expansion of the p -adic L -function at $T = 0$ satisfies the following:

$$\mathcal{L}_p^*(E, 0) = \frac{\epsilon_p \prod_v c_v |\text{III}(E/\mathbb{Q})| \text{Reg}_p}{(\#E(\mathbb{Q})_{\text{tors}})^2}$$

where $\epsilon_p = (1 - \alpha^{-1})^2$, and α is the unit root of $x^2 - a_p x + p = 0$.

Remark 2.6. For numerical methods for the computation of the quantities appearing in the conjecture and applications, see the work of Stein–Wuthrich [SW13].

Remark 2.7. For a precision analysis of computation of p -adic heights on elliptic curves, see the work of Harvey [Har08, Theorem 3].

Example 2.8. Both **SageMath** and **Magma** have implementations of p -adic heights on elliptic curves over \mathbb{Q} for good ordinary primes $p \geq 5$ (with **SageMath** more generally handling semistable reduction). Beware that the normalizations⁸ may be slightly different! In **SageMath**, the normalization⁹ is chosen for the p -adic Birch–Swinnerton-Dyer conjecture to hold as stated in [MTT86], so differs from [MST06] by a factor of $2p$:

```
sage: E = EllipticCurve([1,1])
sage: p = 5
sage: h = E.padic_height(p,8)
sage: P = E(0,1)
sage: for i in range(1,4):
....:     1/i^2*h(i*P)
....:
2*5 + 4*5^3 + 4*5^4 + 5^6 + 5^7 + 0(5^8)
2*5 + 4*5^3 + 4*5^4 + 5^6 + 5^7 + 0(5^8)
2*5 + 4*5^3 + 4*5^4 + 5^6 + 5^7 + 0(5^8)
```

Magma’s normalization¹⁰ is that of [Har08] and is $2p$ (or $-2p$ in some cases) times that in other papers. In this example, it differs from **SageMath** by a sign:

```
> E:=EllipticCurve([1,1]);
> P:=E![0,1];
> pAdicHeight(P,5);
1480998027523*5 + 0(5^20)
```

Using the Northcott property, it is easy to see that the canonical height of a point $P \in E(\mathbb{Q})$ vanishes if and only if P is torsion. Similarly, we have

Conjecture 2.9 (Schneider [Sch82]). *The cyclotomic p -adic height pairing is nondegenerate. Equivalently, Reg_p is nonzero.*

For elliptic curves with complex multiplication, Bertrand [Ber75] proved using p -adic transcendence theory that the p -adic height of a non-torsion point is nonzero, which proves Schneider’s conjecture if the curve has rank 1, but this is still all we know.

⁸This is something to be aware of regarding the literature on heights as well.

⁹http://doc.sagemath.org/html/en/reference/curves/sage/schemes/elliptic_curves/ell_rational_field.html

¹⁰<https://magma.maths.usyd.edu.au/magma/handbook/text/1485#16955>

Remark 2.10. It is also of interest to study the p -adic height in families of elliptic curves, as initiated by Wuthrich [Wut04], who used this to derive interesting results in view of Schneider's conjecture. Recently, Bianchi [Bia19b] gave an algorithm using p -adic cohomology to compute p -adic heights in families of elliptic curves.

To complete our construction of the p -adic height, we now discuss how to compute the special value $\mathbf{E}_2(E, \omega)$. Katz [Kat73, App. 2] gives an interpretation to $\mathbf{E}_2(E, \omega)$ as the “direction” of the unit root eigenspace W of Frobenius acting on Monsky–Washnitzer cohomology for E . Fix an affine model for E/\mathbb{Z}_p of the form $y^2 = f(x)$ and let ϕ^* be the usual lift of p -power Frobenius from the residue field acting with respect to the basis of $H_{\text{MW}}^1(E')^-$ given by $\left\{ \frac{dx}{y}, \frac{x dx}{y} \right\}$.

Let

$$(\phi^*)^n \left(x \frac{dx}{y} \right) = a_n \frac{dx}{y} + b_n \frac{x dx}{y}.$$

Then we have

$$\mathbf{E}_2(E, \omega) \equiv \frac{-12a_n}{b_n} \pmod{p^n}.$$

What does this have to do with integral points on E ? Here is a rough idea. We fix an affine minimal model for E/\mathbb{Z}_p of the form $y^2 = f(x)$ and recall the p -adic differential equation satisfied by the p -adic sigma function:

$$x + c = -\frac{d}{\omega} \left(\frac{1}{\sigma} \frac{d\sigma}{\omega} \right),$$

in the formal group of E/\mathbb{Z}_p . Rewriting, we have

$$\omega(x + c) = -d \left(\frac{1}{\sigma} \frac{d\sigma}{\omega} \right),$$

and letting $\omega_0 := \omega$ and $\omega_1 := x\omega$, this implies that

$$\begin{aligned} \int (\omega_1 + c\omega_0) &= -\frac{d\sigma}{\sigma\omega_0}, \\ \omega_0 \int (\omega_1 + c\omega_0) &= -\frac{d\sigma}{\sigma} = -d \log \sigma \\ \int (\omega_0\omega_1 + c\omega_0\omega_0) &= -\log \sigma. \end{aligned}$$

Since

$$\int \omega_0\omega_1 = D_2$$

and

$$c \int \omega_0\omega_0 = \frac{c}{2} \left(\int \omega_0 \right)^2 = \frac{c}{2} (\log)^2,$$

it follows that

$$(15) \quad D_2 + \frac{c}{2} (\log)^2 = -\log \sigma.$$

Now suppose we may interpret the left hand side of (15) as a Coleman function. Note that the right hand side of (15) is essentially the global p -adic height without a denominator contribution. Then in the case of a rank 1 elliptic curve, if we are able to impose hypotheses (say we restrict to considering integral points and curves with Tamagawa product 1) under which the denominator does not contribute,

we have that the right hand side is further equal to $\alpha(\log)^2$ for some computable constant α . Thus we have that

$$\frac{D_2}{(\log)^2}$$

is constant, which would give Theorem 1.67. Of course, one needs to be more careful at various points of this sketch, but this is essentially our first approach toward a fragment of the quadratic Chabauty method (for integral points on rank 1 elliptic curves), as given by Balakrishnan–Besser [BB15]. To say more, we introduce p -adic heights on Jacobians of curves.

2.2. p -adic heights on Jacobians of curves. Let X/\mathbb{Q} be a nice curve with genus $g \geq 1$, and p be a prime of good reduction for X . As above, we fix a branch $\log_p : \mathbb{Q}_p^* \rightarrow \mathbb{Q}_p$. We also fix the following data:

- (a) an idèle class character $\chi : \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^* \rightarrow \mathbb{Q}_p$ (see Remark 2.11 below),
- (b) a splitting s of the Hodge filtration on $H_{\text{dR}}^1(X/\mathbb{Q}_p)$ such that $\ker(s)$ is isotropic with respect to the cup product pairing.

Remark 2.11. Here we mention briefly the role of idèle class characters. More generally, suppose X is a nice curve defined over a number field K . An *idèle class character*

$$\chi = \sum_v \chi_v : \mathbb{A}_K^*/K^* \rightarrow \mathbb{Q}_p$$

is a continuous homomorphism that decomposes as a sum of local characters χ_v . Below are some properties:

- For any prime $\mathfrak{q} \nmid p$ we have $\chi_{\mathfrak{q}}(\mathcal{O}_{K_{\mathfrak{q}}}^*) = 0$ because of continuity. So if $\pi_{\mathfrak{q}}$ is a uniformizer in $K_{\mathfrak{q}}$, then $\chi_{\mathfrak{q}}$ is completely determined by $\chi_{\mathfrak{q}}(\pi_{\mathfrak{q}})$.
- For any $\mathfrak{p} \mid p$, there is a \mathbb{Q}_p -linear map $t_{\mathfrak{p}}^{\chi}$ such that we can decompose

$$(16) \quad \begin{array}{ccc} \mathcal{O}_{\mathfrak{p}}^* & \xrightarrow{\chi_{\mathfrak{p}}} & \mathbb{Q}_p, \\ & \searrow \log_{\mathfrak{p}} \quad \nearrow t_{\mathfrak{p}}^{\chi} & \\ & K_{\mathfrak{p}} & \end{array}$$

because $\chi_{\mathfrak{p}}$ takes values in the torsion-free group $(\mathbb{Q}_p, +)$.

If a continuous idèle class character χ is ramified at \mathfrak{p} , that is, if the local character $\chi_{\mathfrak{p}}$ does not vanish on $\mathcal{O}_{\mathfrak{p}}^*$, then we can extend $\log_{\mathfrak{p}}$ to

$$\log_{\mathfrak{p}} : K_{\mathfrak{p}}^* \rightarrow K_{\mathfrak{p}}$$

in such a way that the diagram (16) remains commutative.

Remark 2.12. A splitting of the Hodge filtration on $H_{\text{dR}}^1(X/\mathbb{Q}_p)$ corresponds to fixing a subspace $W := \ker(s)$ of $H_{\text{dR}}^1(X/\mathbb{Q}_p)$ complementary to the space of holomorphic forms $H^0(X_{\mathbb{Q}_p}, \Omega^1)$, i.e.

$$H_{\text{dR}}^1(X/\mathbb{Q}_p) = H^0(X_{\mathbb{Q}_p}, \Omega^1) \oplus W.$$

The isotropy condition on W is necessary in order to obtain a symmetric height pairing below.

In this subsection, we will construct a height pairing h on the Jacobian J of X . Everything can be generalized to number fields K , making choices as above.

Definition 2.13. (Coleman–Gross [CG89]) The (cyclotomic) p -adic height pairing is a symmetric bi-additive pairing

$$\mathrm{Div}^0(X) \times \mathrm{Div}^0(X) \rightarrow \mathbb{Q}_p, (D_1, D_2) \mapsto h(D_1, D_2),$$

for $D_1, D_2 \in \mathrm{Div}^0(X)$ with disjoint support, such that the following holds:

(i) We have

$$\begin{aligned} h(D_1, D_2) &= \sum_{\text{finite primes } v} h_v(D_1, D_2) \\ &= h_p(D_1, D_2) + \sum_{\ell \neq p} h_\ell(D_1, D_2) \\ &= \int_{D_2} \omega_{D_1} + \sum_{\ell \neq p} m_\ell \log_p \ell, \end{aligned}$$

where the integral is a Coleman integral, the sum is finite and $m_v \in \mathbb{Q}$ is an intersection multiplicity.

(ii) For $\beta \in \mathbb{Q}(X)^*$, we have

$$h(D, \mathrm{div}(\beta)) = 0.$$

By (ii), h defines a symmetric bilinear pairing $J(\mathbb{Q}) \times J(\mathbb{Q}) \rightarrow \mathbb{Q}_p$.

This construction of the p -adic height is similar to the Arakelov-theoretic description of the canonical height due to Faltings and Hrilić.

2.2.1. Local heights at p . We will now provide more detail on the local height pairings h_v , beginning with the case $v = p$, as described by Coleman–Gross [CG89] and computed by Balakrishnan–Besser in the case of hyperelliptic curves [BB12, BB19].

We first discuss the construction of the differential ω_{D_1} in (i). Let $\{\omega_0, \dots, \omega_{2g-1}\}$ be a basis for $H_{\mathrm{dR}}^1(X)$ with $\{\omega_0, \dots, \omega_{g-1}\} \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$. Fix a lift ϕ of Frobenius.

Let $T(\mathbb{Q}_p)$ be the group of differentials of the third kind on X . In this section, we take this to mean something stronger than in the previous section: that they have at most simple poles and *integer* residues.

We have a residue divisor homomorphism

$$\mathrm{Res} : T(\mathbb{Q}_p) \rightarrow \mathrm{Div}^0(X), \omega \mapsto \mathrm{Res}(\omega) = \sum_P (\mathrm{Res}_P \omega) P,$$

which induces a short exact sequence

$$(17) \quad 0 \rightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1) \rightarrow T(\mathbb{Q}_p) \xrightarrow{\mathrm{Res}} \mathrm{Div}^0(X) \rightarrow 0.$$

The differential ω_{D_1} will be a differential of the third kind with $\mathrm{Res}(\omega_{D_1}) = D_1$. Here is an example:

Example 2.14. Suppose that X is a hyperelliptic curve with affine model $y^2 = f(x)$, and D_1 is the divisor $(P) - (Q)$ with non-Weierstrass points $P, Q \in X(\mathbb{Q})$. We want to write down a differential ω having simple poles with residues $+1$ at P and -1 at Q respectively, and no other poles. For example,

$$(18) \quad \omega = \frac{dx}{2y} \left(\frac{y + y(P)}{x - x(P)} - \frac{y + y(Q)}{x - x(Q)} \right)$$

has residue divisor equal to D_1 , as desired. However, adding any holomorphic differential η to ω , and taking the residue divisor map of $\eta + \omega$ will again give us D_1 , as we can see by (17). So we must make some choice, which we do below.

We can fix a normalized differential with a given residue divisor using the complementary subspace W mentioned above. For this, let $T_l(\mathbb{Q}_p)$ denote the group of logarithmic differentials $\frac{df}{f}$ with $f \in \mathbb{Q}_p(X)^*$. Since

$$T_l(\mathbb{Q}_p) \cap H^0(X_{\mathbb{Q}_p}, \Omega^1) = 0$$

and $\text{Res} \frac{df}{f} = \text{div } f$, from the short exact sequence (17) we get a new short exact sequence

$$0 \rightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1) \rightarrow T(\mathbb{Q}_p)/T_l(\mathbb{Q}_p) \rightarrow J(\mathbb{Q}_p) \rightarrow 0.$$

Proposition 2.15. *There is a canonical homomorphism*

$$\Psi : T(\mathbb{Q}_p)/T_l(\mathbb{Q}_p) \rightarrow H_{\text{dR}}^1(X)$$

with the following properties:

- (1) Ψ is the identity on differentials of the first kind;
- (2) Ψ sends third kind differentials to second kind modulo exact differentials.

Proof. See [CG89, §2]. □

Definition 2.16. Let $D \in \text{Div}^0(X)$. Then we define ω_D to be the unique differential of the third kind with $\text{Res}(\omega_D) = D$ and $\Psi(\omega_D) \in W$.

In fact, Ψ can be extended to general meromorphic (and even rigid analytic) forms. Having fixed our normalized differential ω_D , we can now define:

Definition 2.17. The local height at p of $D_1, D_2 \in \text{Div}^0(X)$ with disjoint support is

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}$$

As in Section 2.1, we can take W to be the unit root subspace if p is ordinary. It can be computed as follows:

Proposition 2.18. *If ϕ is a lift of Frobenius, then $\{(\phi^*)^n \omega_g, \dots, (\phi^*)^n \omega_{2g-1}\}$ is a basis for the unit root subspace modulo p^n .*

For the following algorithm, recall that $H_{\text{dR}}^1(X/\mathbb{Q}_p)$ is equipped with the cup product: a canonical, alternating, non-degenerate bilinear form, which we compute using Serre's formula:

$$\begin{aligned} H_{\text{dR}}^1(X/\mathbb{Q}_p) \times H_{\text{dR}}^1(X/\mathbb{Q}_p) &\rightarrow \mathbb{Q}_p \\ ([\mu_1], [\mu_2]) &\mapsto [\mu_1 \cup \mu_2] = \sum_{Q \in X(\mathbb{C}_p)} \text{Res}_Q \left(\mu_2 \int \mu_1 \right). \end{aligned}$$

Remark 2.19. Note that since μ_2 is of the second kind, it has residue zero everywhere, and so the result above does not depend on a choice of constant of integration for $\int \mu_1$.

Algorithm 2.20 (Coleman integral of differentials of the third kind [BB12]).

Input:

- A differential ω with $\text{Res}(\omega) = (P) - (Q)$ such that $P, Q \in X(\mathbb{Q}_p)$ are non-Weierstrass points.
- Points $R, S \in X(\mathbb{Q}_p)$ such that R, S do not lie in residue disk of P, Q .

Output: The integral $\int_S^R \omega$.

- (1) Compute $\Psi(\omega) \in H_{\text{dR}}^1(X)$: suppose $\Psi(\omega) = \sum_{i=0}^{2g-1} b_i[\omega_i]$. Then by taking the cup products $\Psi(\omega) \cup [\omega_j]$ for all j , one can solve for the coefficients b_i by computing residues. Let $\alpha := \phi^*\omega - p\omega$. Use Frobenius equivariance to get

$$\Psi(\alpha) = \phi^*\Psi(\omega) - p\Psi(\omega).$$

- (2) Let β be a 1-form with $\text{Res}(\beta) = (R) - (S)$. Compute $\Psi(\beta)$.
(3) Compute $\Psi(\alpha) \cup \Psi(\beta)$. (This is easy, since both are elements in $H_{\text{dR}}^1(X)$ that we have computed.)
(4) Compute $\int_{\phi(S)}^S \omega$ and $\int_R^{\phi(R)} \omega$. (These are tiny integrals.)
(5) Compute $\sum_{A \in X(\mathbb{C}_p)} \text{Res}_A (\alpha \int \beta)$. (This is more involved since there are more poles that are not defined over \mathbb{Q}_p .)
(6) Finally, we get

$$\int_S^R \omega = \frac{1}{1-p} (\Psi(\alpha) \cup \Psi(\beta) + \sum_{A \in X(\mathbb{C}_p)} \text{Res}_A \left(\alpha \int \beta \right) - \int_{\phi(S)}^S \omega - \int_R^{\phi(R)} \omega).$$

Remark 2.21. We introduce this auxiliary differential α in Step (1) above, because α is almost of the second kind, meaning that the sum of residues of α in each annulus in 0.

Algorithm 2.22 (The local height at p of the global p -adic height, $h_p(D_1, D_2)$ [BB12]).

- (1) Let ω be a differential in $T(\mathbb{Q}_p)$ with $\text{Res}(\omega) = D_1$.
(2) Compute $\Psi(\omega) = \sum_{i=0}^{2g-1} a_i \omega_i \in H_{\text{dR}}^1(X)$. Then $\Psi(\omega) - \sum_{i=0}^{g-1} a_i \omega_i \in W$. Let

$$\omega_{D_1} = \omega - \sum_{i=0}^{g-1} a_i \omega_i.$$

- (3) Compute using Algorithm 2.20

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}.$$

Remark 2.23. For the precision needed in Algorithm 2.22, see [BB12, §6.2].

Example 2.24 ([BBM17, Example 9.2]). Consider the genus 3 curve

$$X : y^2 = (x^3 + x + 1)(x^4 + 2x^3 - 3x^2 + 4x + 4).$$

This is a new modular curve C_{496}^J studied by Baker–González–Jiménez–González–Poonen [BGJGP05]. For this curve, $J(\mathbb{Q}) \simeq \mathbb{Z}^3 \oplus \mathbb{Z}/2$. Let $P = (-1, 2), Q = (0, 2), R = (-2, 12), S = (3, 62)$ and let w denote the hyperelliptic involution.

We take $p = 7$ and use Algorithm 2.22 to compute the local height $h_7(D_2, D_3)$ where $D_2 = (S) - (w(Q))$ and $D_3 = (w(S)) - (R)$. Let ω be the differential (18) constructed in Example 2.14 using residue divisor D_2 . Using Algorithm 2.20, we find

$$\int_{D_3} \omega = 7 + 4 \cdot 7^2 + 6 \cdot 7^3 + 7^4 + 3 \cdot 7^5 + 3 \cdot 7^6 + 3 \cdot 7^7 + O(7^{10}).$$

Let $\eta := \sum_{i=0}^2 a_i \omega_i$ where $\Psi(\omega) = \sum_{i=0}^5 a_i \omega_i$. We calculate that

$$\begin{aligned} \eta &= (4 + 5 \cdot 7 + 2 \cdot 7^2 + 2 \cdot 7^3 + 5 \cdot 7^4 + 5 \cdot 7^5 + 2 \cdot 7^8 + 7^9 + O(7^{10}))\omega_0 + \\ &\quad (1 + 4 \cdot 7 + 6 \cdot 7^2 + 7^3 + 6 \cdot 7^4 + 5 \cdot 7^6 + 5 \cdot 7^7 + 3 \cdot 7^8 + 7^9 + O(7^{10}))\omega_1 + \\ &\quad (5 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 7^4 + 4 \cdot 7^6 + 2 \cdot 7^7 + 3 \cdot 7^8 + 5 \cdot 7^9 + O(7^{10}))\omega_2, \end{aligned}$$

and using Algorithm 1.36, we find

$$\begin{aligned}\int_{D_3} \omega_0 &= 2 \cdot 7 + 4 \cdot 7^2 + 7^3 + 6 \cdot 7^4 + 7^5 + 5 \cdot 7^6 + 7^7 + 5 \cdot 7^8 + 4 \cdot 7^9 + O(7^{10}) \\ \int_{D_3} \omega_1 &= 4 \cdot 7 + 4 \cdot 7^2 + 3 \cdot 7^3 + 2 \cdot 7^4 + 6 \cdot 7^5 + 4 \cdot 7^6 + 2 \cdot 7^7 + 5 \cdot 7^8 + O(7^{10}) \\ \int_{D_3} \omega_2 &= 7^2 + 3 \cdot 7^3 + 3 \cdot 7^4 + 3 \cdot 7^5 + 5 \cdot 7^6 + 3 \cdot 7^7 + 7^8 + 4 \cdot 7^9 + O(7^{10}),\end{aligned}$$

so we have

$$\int_{D_3} \eta = 5 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + 4 \cdot 7^4 + 6 \cdot 7^5 + 7^6 + 7^7 + 6 \cdot 7^8 + 4 \cdot 7^9 + O(7^{10}).$$

Putting this together, we have

$$h_7(D_2, D_3) = \int_{D_3} \omega - \int_{D_3} \eta = 3 \cdot 7 + 3 \cdot 7^3 + 4 \cdot 7^4 + 3 \cdot 7^5 + 7^6 + 2 \cdot 7^7 + 7^8 + 4 \cdot 7^9 + O(7^{10}).$$

Likewise we may compute $h_7(D_3, D_2) = \int_{D_2} \omega_{D_3}$ and numerically verify that $h_7(D_2, D_3) = h_7(D_3, D_2)$.

Using SageMath code available on GitHub [Bal], here is how to compute the above values:

```
R.<x> = QQ[]
X = HyperellipticCurve((x^3+x+1)*(x^4 +2*x^3-3*x^2+4*x+4))
p = 7
K = Qp(p,10)
XK = X.change_ring(K)
S = XK(3,62)
iS = XK(3,-62)
iQ = XK(0,-2)
R = XK(-2,12)
XK.height([(1,S),(-1,iQ)],[(-1,iS),(1,R)])
XK.height([(1,iS),(-1,R)],[(-1,S),(-1,iQ)])
```

Remark 2.25. Forthcoming work of Gajović will give an extension of Algorithm 2.22 to more general nice curves, based on Tuitman's algorithm. The main issue is the computation of the normalized differential ω_D .

Remark 2.26. The construction of Coleman–Gross local heights can be extended to curves with bad reduction, replacing Coleman integration with Vologodsky integration; see for instance [Bes17]. Kaya is currently working on an extension of Algorithm 2.22 to hyperelliptic curves with semistable reduction.

Since the global p -adic height respects linear equivalence, it can be extended to pairs of divisors with common support. The local height pairings can also be extended in a non-canonical way. We first discuss this for the pairing at p . This uses the following idea of Gross [Gro86]. At each point x in the common support of our divisors, choose a basis $t := t_x$ of the tangent space. Let $z := z_x$ be a uniformizing parameter at x with $\partial_t z = 1$. Any rational function f on $X_{\mathbb{Q}_p}$ then has a well-defined value at x ,

$$f[x] = \frac{f}{z^m}(x),$$

where m is the order of f at x . This depends only on t , but not on z .

For an odd degree hyperelliptic curve, we will let ω_i be $\frac{x^i dx}{2y}$ and we let $\bar{\omega}_i$ denote the dual of ω_i with respect to the cup product pairing.

Proposition 2.27 ([BB15]). *Let X/\mathbb{Q} be a hyperelliptic curve given by a monic odd degree model. Then there is a natural choice of tangent vectors such that the local height $h_p(P - \infty, P - \infty)$ can be written as a double integral*

$$h_p(P - \infty, P - \infty) = -2 \sum_{i=0}^{g-1} \int_b^P \omega_i \bar{\omega}_i,$$

where b is a tangential base point at ∞ .

The proof uses p -adic Arakelov theory, as developed by Besser [Bes05]. In this theory, the local height is given by a p -adic Green function. One shows equality in the proposition by first computing the curvature of this p -adic Green function, then proving that the two values are the same up to a constant which one can then show to be 0.

As a consequence, we have that

$$\theta(z) := h_p((z) - (\infty), (z) - (\infty))$$

extends to a locally analytic function on $X(\bar{\mathbb{Q}}_p) \setminus \{\infty\}$, where we fix the choice of tangent vectors as in Proposition 2.27.

2.3. An application to integral points. For certain curves, we can use p -adic heights to study integral points.

Theorem 2.28 (Quadratic Chabauty for integral points on hyperelliptic curves [BBM16, Theorem 3.1]). *Let $f(x) \in \mathbb{Z}[x]$ be a monic separable polynomial of degree $2g+1 \geq 3$. Let $\mathcal{U} = \text{Spec}(\mathbb{Z}[x, y]/(y^2 - f(x)))$ and let X be the normalization of the projective closure of the generic fiber of \mathcal{U} . Let J be the Jacobian of X and assume that $\text{rk } J(\mathbb{Q}) = g$. Choose a prime p of good reduction and suppose that $\log: J(\mathbb{Q}) \otimes \mathbb{Q}_p \rightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ is an isomorphism¹¹. Then there exist explicitly computable constants $\alpha_{ij} \in \mathbb{Q}_p$ such that the function*

$$\rho(z) = \theta(z) - \sum_{0 \leq i \leq j \leq g-1} \alpha_{ij} \int_{\infty}^z \omega_i \int_{\infty}^z \omega_j$$

takes values in an explicitly computable finite set $S \subset \mathbb{Q}_p$ for all z in $\mathcal{U}(\mathbb{Z}[\frac{1}{p}])$.

Proof. The key idea is that the global height $h((P) - (\infty), (P) - (\infty))$ can be decomposed in two ways:

- (i) Because of the assumption on \log , and since the global height h is a symmetric bilinear pairing we can find $\alpha_{ij} \in \mathbb{Q}_p$ such that for all $P \in X(\mathbb{Q})$ we have

$$h((P) - (\infty), (P) - (\infty)) = \sum \alpha_{ij} \int_{\infty}^P \omega_i \int_{\infty}^P \omega_j,$$

and this extends to a locally analytic function on $X(\bar{\mathbb{Q}}_p)$ away from the residue disk at infinity.

- (ii) We have

$$h((P) - (\infty), (P) - (\infty)) = \theta(P) + \sum_{\ell \neq p} h_{\ell}(P - \infty, P - \infty).$$

¹¹If this fails, we can simply use Chabauty–Coleman to compute the rational points.

Hence we deduce

$$\rho(P) = \sum_{\ell \neq p} h_\ell(P - \infty, P - \infty)$$

for all $P \in X(\mathbb{Q})$. The proof of the theorem now follows from

Proposition 2.29 ([BBM16, Proposition 3.3]). *Let $\ell \neq p$ be prime. There is a proper regular model \mathcal{X} of $X \otimes \mathbb{Q}_\ell$ over \mathbb{Z}_ℓ such that if $z \in X(\mathbb{Q}_\ell)$ is integral then $h_\ell((z) - (\infty), (z) - (\infty))$ depends solely on the component of the special fiber \mathcal{X}_ℓ that the section in $\mathcal{X}(\mathbb{Z}_\ell)$ corresponding to z intersects, and is explicitly computable. If the sections corresponding to z and ∞ intersect the same component, then the local height is 0.*

We will not prove this here, but see Section 2.3.1 below. \square

As a special case of Theorem 2.28, we have the following extension of Theorem 1.67.

Corollary 2.30. *Let f, p, \mathcal{U} and X satisfy the conditions of Theorem 2.28. Suppose that there exists a regular model \mathcal{X}/\mathbb{Z} of X such that, for every bad prime ℓ , all \mathbb{Q}_ℓ -rational points on X reduce to the same irreducible component of the special fiber of $\mathcal{X} \times \mathbb{Z}_\ell$. Then there exists explicitly computable constants $\alpha_{ij} \in \mathbb{Q}_p$ such that the function*

$$\rho(z) = \theta(z) - \sum_{0 \leq i \leq j \leq g-1} \alpha_{ij} \int_{\infty}^z \omega_i \int_{\infty}^z \omega_j$$

vanishes on $\mathcal{U}(\mathbb{Z}[\frac{1}{p}])$.

We can use Theorem 2.28 to compute the integral points on a curve X satisfying the conditions in practice. We give some more computational details here; for more, see [BBM17]. For an extension to number fields, see [BBBM19]. For $P \in J(\mathbb{Q}_p)$ and $i \in \{0, \dots, g-1\}$, we set $f_i(P) := \int_0^P \omega_i$; then f_0, \dots, f_{g-1} restrict to linearly independent functionals on $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ by assumption.

Algorithm 2.31 (The set of integral points on a curve X/\mathbb{Q} satisfying the assumptions of Theorem 2.28).

- (1) Let $D_1, \dots, D_g \in \text{Div}^0(X)$ be representatives of a basis for $J(\mathbb{Q}) \otimes \mathbb{Q}$. Then compute the global height pairings $h(D_i, D_j)$. A basis for the space of bilinear forms on $J(\mathbb{Q}) \otimes \mathbb{Q}$ is given by $1/2(f_k f_\ell + f_\ell f_k)$ so compute $1/2(f_k(D_i) f_\ell(D_j) + f_\ell(D_i) f_k(D_j))$ and do linear algebra to compute $\alpha_{k\ell}$:

$$h(D_i, D_j) = \sum_{k, \ell < g-1} \alpha_{k\ell} (1/2(f_k(D_i) f_\ell(D_j) + f_\ell(D_i) f_k(D_j))).$$

- (2) In order to compute $\{\bar{\omega}_i\}$ for $0 \leq i \leq g-1$ such that $[\bar{\omega}_i] \cup [\omega_j] = \delta_{ij}$ we proceed as follows:
 - (i) Compute a splitting of $H_{\text{dR}}^1(X_{\mathbb{Q}_p}) = H^0(X_{\mathbb{Q}_p}, \Omega^1) \oplus W$, isotropic with respect to the cup product. For instance, when p is ordinary we can take W to be the unit root eigenspace of Frobenius. In this case, modulo p^n , we have a basis for W is given by $\{(\phi^*)^n \omega_g, \dots, (\phi^*)^n \omega_{2g-1}\}$.
 - (ii) For $j = 0, \dots, g-1$, let $\widetilde{\omega}_j$ be a projection on W along $H^0(X_{\mathbb{Q}_p}, \Omega^1)$, i.e., $\widetilde{\omega}_j = \omega_j - \sum_{i=0}^{g-1} a_i \omega_i$ for some $a_i \in \mathbb{Q}_p$.
 - (iii) Use the cup product matrix to compute

$$\bar{\omega}_j = \sum_{i=g}^{2g-1} b_{ji} \widetilde{\omega}_i$$

- for $j = 0$ to $g - 1$.
- (3) Expand $\theta(z) := -2 \sum_{i=0}^{g-1} \int \omega_i \bar{\omega}_i$ into a power series in each residue disk D not containing ∞ , compute a \mathbb{Z}_p -point $P \in D$, the value $\theta(P)$, and a local coordinate z_P at P . Then

$$\theta(z) = -2 \sum_{i=0}^{g-1} \int_b^{g-1} \omega_i \bar{\omega}_i = -2 \left(\sum_{i=0}^{g-1} \int_b^P \omega_i \bar{\omega}_i + \sum_{i=0}^{g-1} \int_P^{z_P} \omega_i \bar{\omega}_i + \sum_{i=0}^{g-1} \int_P^P \omega_i \int_b^P \bar{\omega}_i \right)$$

which is equal to

$$\theta(P) - 2 \left(\sum_{i=0}^{g-1} \int_P^{z_P} \omega_i \bar{\omega}_i + \sum_{i=0}^{g-1} \int_P^{z_P} \omega_i \int_b^P \bar{\omega}_i \right),$$

where b is a tangential basepoint at infinity.

- (4) Use intersection theory to compute the finite set S_ℓ of possible values of $h_\ell((z) - (\infty), (z) - (\infty))$ for bad primes ℓ and integral $X(\mathbb{Q}_\ell)$. Obtain a finite set $S \subset \mathbb{Q}_p$ such that $\sum_{\ell \neq p} h_\ell(P - \infty, P - \infty) \in S$ for $P \in \mathcal{U}(\mathbb{Z}[\frac{1}{p}])$.
- (5) Now proceed similar to the classical Chabauty–Coleman method: We can expand ρ in each disk, set it equal to each value in S , solve for all $z \in \mathcal{U}(\mathbb{Z}_p)$ such that $\rho(z) \in S$. Take the collection of all such points, we will call that solution set \mathcal{Z} .
- (6) If \mathcal{Z} is strictly larger than the known points in $\mathcal{U}(\mathbb{Z})$, we can run the Mordell–Weil sieve [BS10] (see also Section 5.3.3), possibly after re-running steps (1)–(4) on a collection of good primes p .

2.3.1. Local heights away from p . We say a few more words about the local heights at $\ell \neq p$. Given divisors $D_1, D_2 \in \text{Div}^0(X)$ with disjoint support, we can express $h_\ell(D_1, D_2)$ as an intersection multiplicity

$$h_\ell(D_1, D_2) = (\mathcal{D}_1 \cdot \mathcal{D}_2) \chi_\ell(\ell),$$

where $\chi_\ell(\ell) = \log_p(\ell)$, see the beginning of the present subsection. Here \mathcal{D}_i is an extension of D_i to a regular model \mathcal{X} of $X_{\mathbb{Q}_\ell}$ such that \mathcal{D}_i has trivial intersection with all vertical divisors. For instance, we can pick a regular model that dominates the Zariski closure of X . We can extend the local height pairing to divisors with common support via tangent vectors as above. Then we find that for $z \in X(\mathbb{Q}_\ell)$, $h_\ell(z - \infty, z - \infty)$ decomposes into

- terms which only depend on the irreducible component of the special \mathcal{X}_ℓ that the section $z_{\mathcal{X}} \in \mathcal{X}(\mathbb{Z}_\ell)$ corresponding to z intersects,
- the intersection multiplicity between $z_{\mathcal{X}}$ and $\infty_{\mathcal{X}}$.

The latter term vanishes if z is integral. In general, it is determined by the denominator of $x(P)$, which is why it's not obvious how to go beyond integral points using this construction.

Example 2.32. In the case of elliptic curves, we have the Mazur–Stein–Tate p -adic height

$$h(P) = \frac{1}{p} \log_p(\sigma(P)) - \frac{1}{p} \log_p(D(P))$$

on a certain finite index subgroup of the Mordell–Weil group, as well as the Coleman–Gross p -adic height

$$h(P - \infty) = h_p(P - \infty) + \sum_{v \neq p} (P - \infty).$$

Extending appropriately, we have $\frac{1}{p} \log(\sigma(P)) = h_p(P - \infty)$ and $-\frac{1}{p} \log_p(D(P)) = \sum_{v \neq p} (P - \infty)$.

To compute local heights h_ℓ for $\ell \neq p$, we need to compute regular models (implemented in **Magma** by Donnelly, see also recent work of Dokchitser [Dok18]) and Gröbner bases of ideals of divisors. For more details, see [Hol12, Mü14, VBHM20].

Example 2.33 ([BBM17, Example 9.2]). Let $X : y^2 = (x^3 + x + 1)(x^4 + 2x^3 - 3x^2 + 4x + 4)$ be the new modular curve C_{496}^J discussed in Example 2.24. Recall that the Mordell–Weil group of the Jacobian is

$$J(\mathbb{Q}) \simeq \mathbb{Z}^3 \oplus \mathbb{Z}/2.$$

Let $P = (-1, 2), Q = (0, 2), R = (-2, 12), S = (3, 62)$. We want to show that up to the hyperelliptic involution w , these are the only integral points. Generators for $J(\mathbb{Q}) \otimes \mathbb{Q}$ are given by $\{P_1 = [P - \infty], P_2 = [S - w(Q)], P_3 = [w(S) - R]\}$. Then the set S in Theorem 2.28 is

$$S = \{a \log_p 2 + b \log_p 31 : a \in \{0, 15/4, 7/4\}, b \in \{0, 1/2\}\}.$$

We can carry out quadratic Chabauty for $p = 7, 17$, and 37 and apply the Mordell–Weil sieve (see Section 5.3.3) to conclude the desired result.

3. NEKOVÁŘ’S p -ADIC HEIGHTS

The quadratic Chabauty method uses p -adic heights to cut out rational points on certain nice curves X/\mathbb{Q} using bilinear relations. We showed in Section 2.3 that the construction of Coleman and Gross leads to an algorithm to compute the integral points on certain hyperelliptic curves, and we mentioned why this approach does not extend easily to rational points.

As explained below in Section 4, we will in fact cut out a subset $X(\mathbb{Q}_p)_U \supseteq X(\mathbb{Q})$ of $X(\mathbb{Q}_p)$, depending on a certain non-abelian unipotent quotient U of the \mathbb{Q}_p -étale fundamental group of $X_{\overline{\mathbb{Q}}}$. The set $X(\mathbb{Q}_p)_U$ is defined using a non-abelian generalization of Chabauty’s method due to Kim, which we briefly summarize in Section 4.1. Kim’s philosophy suggests that our construction should not use the geometry of the Jacobian, but rather a “motivic” version (but see Remark 5.5 below). In this section, we recall such a motivic construction of p -adic heights, due to Nekovář [Nek93].

3.1. p -adic Hodge theory. We begin by briefly recalling some notions from p -adic Hodge theory. A good reference for most of what we need in this section is [Bel09], but [Nek93, §1] recalls the relevant background in a concise way. See [Ber04, And03, BC09] for other accounts of p -adic Hodge theory. In Section 4.1 we will also use results from Olsson’s non-abelian p -adic Hodge theory [Ols11].

Fix a prime p . For any prime v , let G_v denote the absolute Galois group of \mathbb{Q}_v . Let V be a p -adic Galois representation, by which we mean a finite dimensional \mathbb{Q}_p -vector space with a continuous action of G_p . Fontaine defined p -adic period rings $B_{\text{cris}} \subset B_{\text{dR}}$ and functors $D_{\text{cris}}, D_{\text{dR}}$:

$$D_{\text{cris}}(V) = (B_{\text{cris}} \otimes_{\mathbb{Q}_p} V)^{G_p}, \quad D_{\text{dR}}(V) = (B_{\text{dR}} \otimes_{\mathbb{Q}_p} V)^{G_p}.$$

We always have

$$\dim_{\mathbb{Q}_p} D_{\text{cris}}(V) \leq \dim_{\mathbb{Q}_p}(V).$$

If equality holds, then we say that V is *crystalline*. Similarly, V is called *de Rham* if

$$\dim_{\mathbb{Q}_p} D_{\text{dR}}(V) = \dim_{\mathbb{Q}_p}(V).$$

If V is crystalline, then it is also de Rham. Note that V is crystalline if it is unramified; in fact the p -adic notion *unramified* is too strong to be useful; the “right” p -adic analogue of the ℓ -adic notion *unramified* turns out to be *crystalline*.

An element $\xi \in H^1(G_p, V)$ corresponds to an isomorphism class of extension of \mathbb{Q}_p by V

$$0 \rightarrow V \rightarrow E \rightarrow \mathbb{Q}_p \rightarrow 0;$$

here ξ is the image of the neutral element of $H^0(G_p, \mathbb{Q}_p)$ under the connecting homomorphism $H^0(G_p, \mathbb{Q}_p) \rightarrow H^1(G_p, V)$. We call ξ *crystalline*, provided that the Galois representation E is.

Definition 3.1. The *local Bloch–Kato Selmer group* $H_f^1(G_p, V)$ be the set of crystalline classes in $H^1(G_p, V)$. The (global) *Bloch–Kato Selmer group* $H_f^1(G_{\mathbb{Q}}, V)$ is the group of $\xi \in H^1(G_{\mathbb{Q}}, V)$ whose image $\text{loc}_v(V) \in H^1(G_v, V)$ is crystalline for $v = p$ and unramified for all $v \neq p$.

Example 3.2. Suppose that K is a finite extension of \mathbb{Q}_p . Then Kummer theory gives an isomorphism

$$\kappa: \widehat{K^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} H^1(G_K, \mathbb{Q}_p(1)),$$

where $\widehat{K^*} = \varprojlim K^* \otimes \mathbb{Z}/p^n \mathbb{Z}$ is the p -adic completion. According to [Bel09, Proposition 2.9], this isomorphism identifies $\mathcal{O}_K^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ with $H_f^1(G_p, \mathbb{Q}_p(1))$.

Example 3.3. Let K be a number field. Then, by [Bel09, Proposition 2.12] we have

$$H_f^1(G_K, \mathbb{Q}_p(1)) \simeq \mathcal{O}_K^* \otimes_{\mathbb{Z}} \mathbb{Q}_p.$$

Remark 3.4. More generally, when G is a topological group and V, W are finite-dimensional continuous \mathbb{Q}_p -representations of G , we can identify $H^1(G, V^* \otimes W)$ with the group $\text{Ext}^1(V, W)$, and we can define and identify $H_f^1(G, V^* \otimes W)$ and $\text{Ext}_f^1(V, W)$, where the former contains crystalline torsors and the latter crystalline extensions.

Nekovář’s approach is inspired by a motivic construction due to Scholl [Sch94] of archimedean local height pairings arising in Beilinson’s extension of canonical heights to Chow groups based on mixed Hodge structures.

3.2. Nekovář’s construction of p -adic heights. Fix a prime p and a finite set of primes T_0 . Let $T := T_0 \cup \{p\}$. For “good”¹² p -adic Galois representations V , Nekovář constructs a bilinear p -adic height pairing on Bloch–Kato Selmer groups

$$h: H_f^1(G_{\mathbb{Q}}, V) \times H_f^1(G_{\mathbb{Q}}, V^*(1)) \rightarrow \mathbb{Q}_p.$$

This global p -adic height depends only on

- (a) the choice of an idèle class character $\chi: \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \rightarrow \mathbb{Q}_p^{\times}$,
- (b) a splitting s of the Hodge filtration on $V_{\text{dR}} := D_{\text{cris}}(V)$.

For everything that follows, we let X/\mathbb{Q} denote a nice curve of genus $g \geq 2$ such that X has good reduction at p and such that T_0 contains the set of primes of bad reduction for X . We set $V = H^1_{\text{ét}}(X_{\overline{\mathbb{Q}}})^*$. This V is “good” in the sense of Nekovář; in particular V is crystalline and $V_{\text{dR}} = H^1_{\text{dR}}(X_{\mathbb{Q}_p})^*$ by a theorem of Faltings [Fal89]. Note that the choices (a) and (b) are exactly the choices required in the construction of Coleman and Gross.

In [Nek93, Section 2], Nekovář presents a global construction of the height pairing h . We will not discuss it here, but rather focus on a construction of local heights h_v , so that we have

$$h = h_p + \sum_{v \neq p} h_v.$$

See [Nek93, §4] for more details. See also [BDM⁺19, §3], [BD18a, §4.2] for similar treatments, and a reformulation in terms of non-abelian cohomology. A generalization of Nekovář’s construction is discussed in [BD18b].

¹²The conditions for being “good” are spelled out in [Nek93, 2.1.2]. In particular, we want V to be crystalline at p and unramified outside T .

Recall that, starting with two points in $J(\mathbb{Q})$, the local Coleman–Gross heights are defined by first choosing divisors of degree 0 representing these points. The local heights then depend on these choices, whereas the global height does not. In our present setting, the idea is to interpret classes $e_1 \in H_f^1(G_{\mathbb{Q}}, V)$ and $e_2 \in H_f^1(G_{\mathbb{Q}}, V^*(1))$ as extensions

$$\begin{aligned} 0 &\rightarrow V \rightarrow E_1 \rightarrow \mathbb{Q}_p \rightarrow 0 \\ 0 &\rightarrow \mathbb{Q}_p(1) \rightarrow E_2 \rightarrow V \rightarrow 0, \end{aligned}$$

where we identify $H_f^1(G_{\mathbb{Q}}, V)$ with crystalline extensions of V by \mathbb{Q}_p with a continuous $G_{\mathbb{Q}}$ -action. Nekovář shows [Nek93, Proposition 4.4] that one can lift these extensions to form a *mixed extension* E of E_1 and E_2 , i.e. a p -adic $G_{\mathbb{Q}}$ -representation with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$, sitting in a commutative diagram

$$(19) \quad \begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & E_2 & \longrightarrow & V \longrightarrow 0 \\ & & \downarrow = & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & E & \longrightarrow & E_1 \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & \mathbb{Q}_p & \xrightarrow{=} & \mathbb{Q}_p & & \\ & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & . \end{array}$$

and having a weight filtration by $G_{\mathbb{Q}}$ -subrepresentations

$$0 = W_{-3}E \subseteq W_{-2}E \subseteq W_{-1}E \subseteq W_0E = E,$$

so that $W_{-1}E \simeq E_2$ and $W_0E/W_{-2}E \simeq E_1$. In other words, the mixed extension E has a block matrix representation

$$\begin{pmatrix} 1 & 0 & 0 \\ * & \rho_V & 0 \\ * & * & \chi_p \end{pmatrix}$$

where the representation ρ_V corresponds to V and χ_p is the p -adic cyclotomic character.

Given any mixed extension E of $G_{\mathbb{Q}}$ -representations with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$, we can define projections

$$(20) \quad \pi_1(E) := [W_0E/W_{-2}E] \in H^1(G_{\mathbb{Q}}, V), \quad \pi_2(E) := [W_{-1}E] \in H^1(G_{\mathbb{Q}}, V^*(1)).$$

For a mixed extension E of E_1 and E_2 as above, we then have $\pi_i(E) = e_i$.

For every prime v , we can define local mixed extension of G_v -representations with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$ in an analogous way. We say a global mixed extension E is *crystalline* if $\text{loc}_p(E)$ is crystalline. If E is crystalline, the projections $\pi_i(E)$ are crystalline as well.

Nekovář defines a local height h_v on mixed extension of G_v -representations with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$. We will assume it is of the form $\text{loc}_v(E)$ for a global mixed extension E . The local height is not well-defined on $H_f^1(G_{\mathbb{Q}}, V) \times H_f^1(G_{\mathbb{Q}}, V^*(1))$, it depends on the chosen mixed extension (in fact

on its equivalence class). Such mixed extensions can be added via the Baer sum; the local heights are then bi-additive in the sense of [BD18a, Definition 4.4]. By [Nek93, Theorem 4.11],

$$(21) \quad h(e_1, e_2) = \sum_v h_v(\text{loc}_v(E))$$

is independent of the choice of E and defines a bilinear pairing

$$h: H_f^1(G_{\mathbb{Q}}, V) \times H_f^1(G_{\mathbb{Q}}, V^*(1)) \rightarrow \mathbb{Q}_p.$$

By Poincaré duality, we have $V \simeq V^*(1)$, so we in fact get a bilinear pairing

$$h: H_f^1(G_{\mathbb{Q}}, V) \times H_f^1(G_{\mathbb{Q}}, V) \rightarrow \mathbb{Q}_p.$$

Remark 3.5. If $\ker(s)$ is isotropic with respect to the dual of the cup product, then this pairing is symmetric by [Nek93, Theorem 4.11 (4)].

Remark 3.6. One can associate a mixed extension as above to a pair of divisors $D_1, D_2 \in \text{Div}^0(X)$ with disjoint support via an étale Abel–Jacobi map, see [Nek93, Section 5]. Besser [Bes04] shows that for our choice of V , the local Coleman–Gross and Nekovář heights (with respect to these choices) are equivalent.

3.3. Local heights. The construction of the local heights h_v is not particularly intuitive. The rough idea is to construct a class $c \in H^1(G_v, \mathbb{Q}_p(1))$ (crystalline when $v = p$) from a local mixed extension E_v . One can then use the Kummer isomorphism

$$\kappa_v: \widehat{\mathbb{Q}_v^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} H^1(G_v, \mathbb{Q}_p(1))$$

to define a p -adic number

$$(22) \quad h_v(E_v) := \chi_v(c) \in \mathbb{Q}_p,$$

where χ_v is the map

$$(23) \quad \chi_v: H^1(G_v, \mathbb{Q}_p(1)) \rightarrow \widehat{\mathbb{Q}_v^*} \otimes \mathbb{Q}_p \rightarrow \mathbb{Q}_p$$

induced by the local component $\chi_v: \mathbb{Q}_v^* \rightarrow \mathbb{Q}_p$ of our chosen idèle class character and by κ_v^{-1} . Our exposition follows [BDM⁺19, §3] closely.

3.3.1. Local heights away from p . First consider a prime $\ell \neq p$. Our main focus will be on algorithms for h_p , so we will only discuss this case briefly. Note that $\chi_{\ell}(\mathbb{Z}_{\ell}^*) = 0$ because of continuity, hence the second map in (23) factors through the valuation $\text{ord}_{\ell}: \mathbb{Q}_{\ell}^* \rightarrow \mathbb{Z}$ for $v = \ell$.

It is explained in [BDM⁺19, §3.2] that we have $H^1(G_{\ell}, V) = H^1(G_{\ell}, V^*(1)) = 0$, essentially since (by the weight-monodromy conjecture for curves) $H^0(G_{\ell}, V) = H^0(G_{\ell}, V^*(1))^* = 0$. Hence, if E_{ℓ} is a mixed extension of G_{ℓ} -representations with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$, then, from the local version of the diagram (19), we obtain a splitting $E_{\ell} \simeq V \oplus N$, where N is an extension

$$0 \rightarrow \mathbb{Q}_p(1) \rightarrow N \rightarrow \mathbb{Q}_p \rightarrow 0,$$

so the class $c := [N]$ lies in $H^1(G_{\ell}, \mathbb{Q}_p(1))$, and we define $h_{\ell}(E_{\ell})$ as in (22). See [Nek93, §4.6] and [BDM⁺19, §3.2]. If E_{ℓ} is unramified, then $h_{\ell}(E_{\ell}) = 0$, so the sum in (21) is finite. More generally, a simple argument shows:

Remark 3.7. Suppose that E_{ℓ} is potentially unramified. Then $h_{\ell}(E_{\ell})$ is trivial by [BDM⁺19, Lemma 3.2]. This implies that the local heights at ℓ of interest to us are trivial when X has potentially good reduction at ℓ .

3.3.2. Local heights at p . We now describe the main object we will need to compute in order to apply quadratic Chabauty for rational points: the local height $h_p(E_p)$, where E_p is a crystalline mixed extension E_p of G_p -extensions with graded pieces \mathbb{Q}_p , V and $\mathbb{Q}_p(1)$. The construction is in terms of p -adic Hodge theory. More precisely, the local height $h_p(E_p)$ is defined in terms of $D_{\text{cris}}(E_p)$, which turns out to be a mixed extension of filtered ϕ -module, defined below. For the mixed extensions of interest to us, we will show later that we can construct $D_{\text{cris}}(E_p)$ explicitly, by solving differential equations and applying linear algebra.

The definition of $h_p(E_p)$ is similar to the construction of local heights away from p , but the construction of the class $c \in H^1_f(G_p, \mathbb{Q}_p(1))$ is more involved, because we do not have $H^1(G_p, V) = H^1(G_p, V^*(1)) = 0$. We will end this section by making the construction rather explicit, in terms of splittings of filtered ϕ -modules.

Definition 3.8. A filtered ϕ -module (over \mathbb{Q}_p) is a finite dimensional \mathbb{Q}_p -vector space W , equipped with an exhaustive and separated decreasing filtration Fil^i and an automorphism ϕ . Recall

- exhaustive means $W = \cup_i \text{Fil}^i$,
- separated means $\cap_i \text{Fil}^i = 0$,
- decreasing means $\text{Fil}^{i+1} \subseteq \text{Fil}^i$.

Example 3.9. Here are some examples of filtered ϕ -modules:

- (1) \mathbb{Q}_p with $\text{Fil}^0 = \mathbb{Q}_p$, $\text{Fil}^n = 0$ for all $n > 0$, and $\phi = \text{id}$.
- (2) $\mathbb{Q}_p(1) = D_{\text{cris}}(\mathbb{Q}_p(1))$ with $\text{Fil}^{-1} = \mathbb{Q}_p$, $\text{Fil}^n = 0$ for all $n > -1$, and $\phi = 1/p$.
- (3) By Faltings' comparison theorem [Fal89], we have $H^1_{\text{dR}}(X_{\mathbb{Q}_p}) = D_{\text{cris}}(H^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p))$ and $H^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ is crystalline. Frobenius ϕ on crystalline cohomology and the Hodge filtration endow $H^1_{\text{dR}}(X_{\mathbb{Q}_p})$ with the structure of a filtered ϕ -module.
- (4) $V_{\text{dR}} := H^1_{\text{dR}}(X_{\mathbb{Q}_p})^* = D_{\text{cris}}(V)$ with the dual filtration and action.
- (5) The direct sum of \mathbb{Q}_p , V and $\mathbb{Q}_p(1)$ has the structure of a filtered ϕ -module as well.

In general, we think of the filtration as a Hodge filtration and of the automorphism as a Frobenius action coming from comparison theorems.

Remark 3.10. To be precise, all filtered ϕ -modules below are *admissible* (i.e. they come from p -adic Galois representations), but we drop the adjective for simplicity.

The following construction will be used several times, so we state it as a

Lemma 3.11. *For any filtered ϕ -module W for which*

$$W^{\phi=1} = 0$$

we have an isomorphism

$$\text{Ext}_{\text{Fil}, \phi}^1(\mathbb{Q}_p, W) \simeq W / \text{Fil}^0.$$

Proof. Given an extension of \mathbb{Q}_p by W in the category of filtered ϕ -modules

$$0 \rightarrow W \rightarrow E \rightarrow \mathbb{Q}_p \rightarrow 0$$

choose a splitting $s^\phi: \mathbb{Q}_p \rightarrow E$ which is ϕ -equivariant. Furthermore, choose a splitting $s^{\text{Fil}}: \mathbb{Q}_p \rightarrow E$ which respects the filtration. Then, since $W^{\phi=1} = 0$, s^ϕ is unique, while s^{Fil} is only determined up to an element of $\text{Fil}^0 W$, so

$$s^\phi - s^{\text{Fil}} + \text{Fil}^0 W \in W / \text{Fil}^0 W$$

is independent of choices.

The inverse of this map is the Bloch–Kato exponential. See [Nek93, Theorem 1.15] and [BK90, §3.8]. \square

The condition $W^{\phi=1} = 0$ will be satisfied by most filtered ϕ -modules we encounter. For instance, it holds trivially for $W = \mathbb{Q}_p(1)$, and the Weil conjectures imply that it holds for $W = V_{\text{dR}}$.

The filtered ϕ -module $\mathbb{Q}_p \oplus V \oplus \mathbb{Q}_p(1)$ has a weight filtration, just like the mixed extensions of Galois representations we encountered above. We call such objects *mixed extensions of filtered ϕ -modules with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$* .

Now let E_p be a crystalline mixed extension of G_p -representations with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$. Then $E_{\text{dR}} := D_{\text{cris}}(E_p)$ is a mixed extension of filtered ϕ -modules with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$. In analogy with the case of Galois-representations, we can define crystalline extensions

$$E_1 := E_{\text{dR}} / \mathbb{Q}_p(1)$$

and

$$E_2 := \ker(E_{\text{dR}} \rightarrow \mathbb{Q}_p).$$

of filtered ϕ -modules:

$$\begin{aligned} 0 \rightarrow V_{\text{dR}} &\rightarrow E_1 \rightarrow \mathbb{Q}_p \rightarrow 0 \\ 0 \rightarrow \mathbb{Q}_p(1) &\rightarrow E_2 \rightarrow V_{\text{dR}} \rightarrow 0, \end{aligned}$$

fitting into a commutative diagram (19) of filtered ϕ -modules.

By Lemma 3.11, we have

$$\text{Ext}_{\text{Fil},\phi}^1(\mathbb{Q}_p, E_2) \simeq E_2 / \text{Fil}^0.$$

Hence we can map the extension E_{dR} of \mathbb{Q}_p by E_2 into $V_{\text{dR}} / \text{Fil}^0$ via the exact sequence

$$(24) \quad 0 \rightarrow \mathbb{Q}_p(1) \rightarrow E_2 / \text{Fil}^0 \rightarrow V_{\text{dR}} / \text{Fil}^0 \rightarrow 0,$$

and the image of E_{dR} is $[E_1]$.

Let $\gamma: V_{\text{dR}} \rightarrow E_2$ be the unique Frobenius equivariant splitting of

$$0 \rightarrow \mathbb{Q}_p(1) \rightarrow E_2 \rightarrow V_{\text{dR}} \rightarrow 0.$$

We define

$$\delta: V_{\text{dR}} / \text{Fil}^0 \xrightarrow{s} V_{\text{dR}} \xrightarrow{\gamma} E_2 \rightarrow E_2 / \text{Fil}^0.$$

Then $[E_{\text{dR}}]$ and $\delta([E_1])$ have the same image in $V_{\text{dR}} / \text{Fil}^0$; hence $[E_{\text{dR}}] - \delta([E_1]) \in \mathbb{Q}_p(1)$ by (24). Recall that our goal was to construct a class in $H_f^1(G_p, \mathbb{Q}_p(1))$. But since

$$\mathbb{Q}_p(1) \simeq \text{Ext}_{\text{Fil},\phi}^1(\mathbb{Q}_p, \mathbb{Q}_p(1)) \simeq H_f^1(G_p, \mathbb{Q}_p(1))$$

by Lemma 3.11, we can think of this difference as a class

$$c := [E_{\text{dR}}] - \delta([E_1]) \in H_f^1(G_p, \mathbb{Q}_p(1)).$$

As above, we define the height of E_p by

$$(25) \quad h_p(E_p) := \chi_p(c).$$

In order to apply quadratic Chabauty in practice, it will be crucial to compute (25). To this end, we now give a more explicit version, based on splittings of E_{dR} . Namely, suppose that we are given a vector space splitting

$$s_0: \mathbb{Q}_p \oplus V_{\text{dR}} \oplus \mathbb{Q}_p(1) \xrightarrow{\sim} E_{\text{dR}}.$$

We choose two further splittings

$$s^\phi: \mathbb{Q}_p \oplus V_{\text{dR}} \oplus \mathbb{Q}_p(1) \xrightarrow{\sim} E_{\text{dR}}$$

$$s^{\text{Fil}}: \mathbb{Q}_p \oplus V_{\text{dR}} \oplus \mathbb{Q}_p(1) \xrightarrow{\sim} E_{\text{dR}},$$

where s^ϕ is Frobenius-equivariant and s^{Fil} respects the filtrations. As in the proof of Lemma 3.11, we have that s^ϕ is unique and s^{Fil} is not.

Now choose bases for $\mathbb{Q}_p, V_{\text{dR}}, \mathbb{Q}_p(1)$ such that with respect to these bases we have

$$s_0^{-1} \circ s^\phi = \begin{pmatrix} 1 & 0 & 0 \\ \alpha_\phi & 1 & 0 \\ \gamma_\phi & \beta_\phi^T & 1 \end{pmatrix}$$

$$s_0^{-1} \circ s^{\text{Fil}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\text{Fil}} & \beta_{\text{Fil}}^T & 1 \end{pmatrix}$$

(the point is to make the “ α_{Fil} -term” in $s_0^{-1} \circ s^{\text{Fil}}$ zero).

Finally, the splitting s of the Hodge filtration defines idempotents

$$s_1, s_2: V_{\text{dR}} \rightarrow V_{\text{dR}}$$

projecting onto

$$s(V_{\text{dR}}/\text{Fil}^0) \text{ and } \text{Fil}^0$$

components, respectively. A computation shows

Proposition 3.12. *We have*

$$h_p(E_p) = \chi_p(\gamma_\phi - \gamma_{\text{Fil}} - \beta_\phi^T s_1(\alpha_\phi) - \beta_{\text{Fil}}^T s_2(\alpha_\phi)).$$

4. QUADRATIC CHABAUTY: THEORY

In this section we discuss the theoretical justification for the quadratic Chabauty method. Since we focus on computational methods in this course and the foundations of non-abelian Chabauty, of which quadratic Chabauty is a special case, are covered in Kim’s lectures, we will be brief. Kim’s approach relies on choosing a unipotent quotient U of the \mathbb{Q}_p -étale fundamental group of a curve and defining a subset of p -adic points containing the rational points using local conditions. The hope is that this set can be proved to be finite and can be computed explicitly.

Our main situation of interest is when the Chabauty condition is not satisfied, but the curve satisfies the quadratic Chabauty condition (29). In particular, this condition holds when the Mordell-Weil rank is equal to the genus and the Picard number is greater than 1, a situation frequently encountered for modular curves, as shown by Siksek [Sik17]. In this case, we can construct a non-abelian quotient U such that the corresponding set of p -adic points is finite and, we can indeed compute it. In the present section, we show finiteness.

4.1. Chabauty–Kim theory. Let X be a nice curve over \mathbb{Q} of genus $g > 1$, and let J be its Jacobian. Assume $X(\mathbb{Q}) \neq \emptyset$ and fix $b \in X(\mathbb{Q})$. We fix a prime p of good reduction, we let T_0 denote the set of bad primes for X , and we set $T := T_0 \cup \{p\}$.

We begin by reformulating classical Chabauty in terms of p -adic Hodge theory, see also [Cor19] and Zureick-Brown’s lectures. As in the previous section, we let $V := H_{\text{ét}}^1(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^*$, and $V_{\text{dR}} := H_{\text{dR}}^1(X_{\mathbb{Q}_p})^*$, viewed as a filtered vector space with the dual filtration to the Hodge filtration, so that there is an isomorphism $V_{\text{dR}}/\text{Fil}^0 \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$. Let G_T be the maximal quotient of $G_{\mathbb{Q}}$ unramified outside T . The étale formulation of classical Chabauty can be summarized in the following commutative diagram:

$$(26) \quad \begin{array}{ccccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & & \\ \downarrow & & \downarrow & \searrow \text{AJ}_b & \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \\ \downarrow & & \downarrow & & \downarrow \simeq \\ H_f^1(G_T, V) & \longrightarrow & H_f^1(G_p, V) & \xrightarrow{\simeq} & H_1^{\text{dR}}(X_{\mathbb{Q}_p})/F^0 \end{array}$$

We give a very brief summary of Kim’s generalization, referring to [Kim09] and Kim’s lectures for more details. Choose a Galois-stable unipotent quotient U of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, the unipotent \mathbb{Q}_p -étale fundamental group of $X_{\overline{\mathbb{Q}}}$ with base point b . The latter is the \mathbb{Q}_p -pro-unipotent completion of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})$. We also want U to be motivic, in the sense that it also has a de Rham realization. In fact we will assume that U is a quotient of the maximal n -unipotent (i.e. having unipotency index $\leq n$) quotient of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, which we denote by U_n .

There is a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & \prod_{v \in T} X(\mathbb{Q}_v) \\ j_U \downarrow & & \downarrow \prod j_{U,v} \\ H^1(G_T, U) & \xrightarrow{\prod \text{loc}_v} & \prod_{v \in T} H^1(G_v, U). \end{array}$$

where j_U and $j_{U,v}$ denote the global, respectively local, unipotent Kummer maps defined in [Kim05, Kim09]. It is a highly nontrivial result due to Kim [Kim05, Kim09] that the nonabelian pointed continuous cohomology sets $H^1(G_T, U)$ and $H^1(G_v, U)$ are affine algebraic varieties over \mathbb{Q}_p . Kim also shows that the localization maps are variety morphisms and that the crystalline torsors have the structure of (the \mathbb{Q}_p -points on) a subvariety.

In analogy with the classical theory of Selmer groups, we can cut down $H^1(G_T, U)$ by local conditions to find a pointed set containing the images of the rational points, which we hope to be able to compute.

Definition 4.1 ([BD18a, Definition 2.2]). We define the *Selmer variety* $\text{Sel}(U)$ to be the reduced scheme associated to the subscheme of $H^1(G_T, U)$ containing those classes c such that

- $\text{loc}_p(c)$ is crystalline,
- $\text{loc}_{\ell}(c) \in j_{U,\ell}(X(\mathbb{Q}_{\ell}))$ for all $\ell \neq p$,
- the projection of c to $H^1(G_T, V)$ comes from an element of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$.

See Kim [Kim09] for a proof that $H_f^1(G_p, U)$ is a subvariety of $H_f^1(G_p, U)$; it also follows from loc. cit. and [KT08] that $\text{Sel}(U)$ is a subvariety of $H^1(G_T, U)$ (see [Kim12]) for an explanation why the conditions above might not produce a reduced scheme). The relation between our (slightly non-standard) definition

of the Selmer variety and other definitions in the literature is discussed in [BD18a, Remark 2.3]. Our version has the convenient feature that our results will not depend on finiteness of the p -primary part of the Shafarevich-Tate group of J .

Since $j_{U,p}(X(\mathbb{Q}_p)) \subset H_f^1(G_p, U)$ by Olsson's comparison theorem [Ols11, Theorem 1.4] in non-abelian p -adic Hodge theory, we obtain another commutative diagram

$$(27) \quad \begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ j_U \downarrow & & \downarrow j_{U,p} \\ \text{Sel}(U) & \xrightarrow{\text{loc}_p} & H_f^1(G_p, U). \end{array}$$

Remark 4.2. Note that under our definitions, $\text{Sel}(U)$ need not be contained in $H_f^1(G_T, U)$, because $j_{U,\ell}(z)$ need not be unramified for all $\ell \neq p$ and $z \in X(\mathbb{Q}_\ell)$. In contrast to Bloch–Kato's foundational paper [BK90] and much of the subsequent literature, many papers in non-abelian Chabauty do not require unramified away from p in their definition of the global H_f^1 . Following [BD18b], we will try to avoid confusion by writing $H_{f,S}^1(G_T, U)$ to mean those classes that are crystalline at p and unramified at all primes ℓ that are not in S , where we will always choose S to be a subset of T_0 . In this notation, we have $H_{f,\emptyset}^1(G_T, U) = H_f^1(G_T, U)$ and $\text{Sel}(U) \subset H_{f,T_0}^1(G_T, U)$ (but see Remark 4.4 below).

Although the image of $j_{U,\ell}$ can be unramified, we have the following result about its image.

Theorem 4.3 (Kim–Tamagawa [KT08]). *Suppose that $\ell \neq p$. Then the image $j_{U,\ell}(X(\mathbb{Q}_\ell))$ is finite. For a prime ℓ of good reduction for X , the image is trivial.*

This crucial result will enable us to control certain local heights away from p in a manner somewhat similar to Proposition 2.29. In fact we will use the following generalization of the second statement.

Remark 4.4 ([BD18a, Lemma 5.4]). If X has potentially good reduction at ℓ , then $j_{U,\ell}(X(\mathbb{Q}_\ell))$ is trivial. Hence

$$\text{Sel}(U) \subset H_{f,T'_0}^1(G_T, U),$$

where T'_0 is the set of bad primes of X where X has potentially good reduction.

We define

$$X(\mathbb{Q}_p)_U := j_p^{-1}(\text{loc}_p \text{Sel}(U)) \subset X(\mathbb{Q}_p).$$

By commutativity of the diagram (27), we have that $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_U$. Since U is a quotient of the maximal n -step unipotent quotient U_n of the \mathbb{Q}_p -étale fundamental group of $X_{\overline{\mathbb{Q}}}$ with base point b , we obtain

$$(28) \quad X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_n := X(\mathbb{Q}_p)_{U_n} \subset X(\mathbb{Q}_p)_U.$$

Of course this is only useful for the purpose of computing rational points if $X(\mathbb{Q}_p)_U$ is finite and can be computed in practice. Kim conjectured that the first condition is eventually satisfied:

Conjecture 4.5 (Kim [Kim09]). *For $n \gg 0$, $X(\mathbb{Q}_p)_n$ is finite.*

There is very strong evidence for this conjecture, as shown in [Kim09, Section 3]. It is implied by a special case of the conjecture of Bloch–Kato (and other standard conjectures on motives).

For computational purposes this is sufficient, once we can compute $X(\mathbb{Q}_p)_n$ as in Conjecture 4.5. The reasons is that the Mordell–Weil sieve, discussed in Section 5.3.3 can often be used to show that given p -adic points do not come from a rational point. However, one of the most exciting potential applications

of Kim's ideas would be an effective version of the Mordell conjecture. But while heuristics imply that the Mordell-Weil sieve should always work eventually [Poo06], it is not effective. The following stronger conjecture circumvents this issue.

Conjecture 4.6 (Kim [BDCKW18]). *For $n \gg 0$, $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$.*

The n in Conjecture 4.6 may not be the n of Conjecture 4.5. They can differ already for the Chabauty–Coleman case $n = 1$. See recent work of Bianchi [Bia19a] along these lines in the case of punctured elliptic curves.

Project 4.7 (Quadratic Chabauty and Kim's conjecture). When X/\mathbb{Q} is a genus g curve with $r = \text{rk } J(\mathbb{Q}) = g - 1$, then typically the set of p -adic points $X(\mathbb{Q}_p)_1$ cut out by the Chabauty–Coleman method strictly contains $X(\mathbb{Q})$. In this project, we will first give an algorithm to compute the quadratic Chabauty set $X(\mathbb{Q}_p)_2$ under these hypotheses. Then we will investigate whether the quadratic Chabauty set, which satisfies

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_2 \subset X(\mathbb{Q}_p)_1 \subset X(\mathbb{Q}_p),$$

is equal to $X(\mathbb{Q})$. (See [Bia19a] for the case of integral points on punctured elliptic curves.) If $X(\mathbb{Q}) \neq X(\mathbb{Q}_p)_2$, we would like to characterize the points in $X(\mathbb{Q}_p)_2 \setminus X(\mathbb{Q})$. This project could be carried out on a database of genus 2 and 3 curves [The19].

Generalizing the étale formulation of classical Chabauty, Kim's approach is to show finiteness of $X(\mathbb{Q}_p)_U$ using p -adic Hodge theory. He obtains the following amendment of diagram (27):

$$\begin{array}{ccccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & & \\ j_U \downarrow & & j_{U,p} \downarrow & & j_U^{\text{dR}} \searrow \\ \text{Sel}(U) & \xrightarrow{\text{loc}_{U,p}} & H_f^1(G_p, U) & \xrightarrow{\simeq} & U^{\text{dR}}/\text{Fil}^0 \end{array}$$

We refer to [Kim09] and Kim's lectures for the definitions of $U^{\text{dR}} := D_{\text{cris}}(U)$ (a quotient of Deligne's de Rham fundamental group $\pi_1^{\text{dR}}(X_{\mathbb{Q}_p}, b)$), the isomorphism $H_f^1(G_p, U) \rightarrow U^{\text{dR}}/\text{Fil}^0$ (coming from Olsson's comparison theorem [Ols11, Theorem 1.4]), and the locally analytic maps j_U^{dR} (these are iterated Coleman integrals).

Note that this diagram specializes to Diagram (26) for $U = V$.

The analogue of the analytic properties of AJ_b (specifically that if there exists a nonzero functional we can construct that vanishes on $\overline{J(\mathbb{Q})}$ with Zariski dense image, given by a convergent p -adic power series then there are finitely many zeros on each residue disk of $X(\mathbb{Q}_p)$) is as follows:

Theorem 4.8 (Kim [Kim09]). *The map j_U^{dR} has Zariski dense image and is given by convergent p -adic power series on every residue disk.*

The analogue of the Chabauty–Coleman hypothesis of $r < g$ is the non-density of $\text{loc}_{U,p}$.

Theorem 4.9 (Kim [Kim09]). *Suppose $\text{loc}_{U,p}$ is non-dominant. Then $X(\mathbb{Q}_p)_U$ is finite.*

All known finiteness results come from bounding the dimension of $\text{Sel}(U)$. For instance, Coates and Kim used Iwasawa theory to obtain dimension bounds in the following setting:

Theorem 4.10 (Coates–Kim [CK10]). *Let X/\mathbb{Q} be a nice curve of genus $g \geq 2$ and suppose that J is isogenous over $\overline{\mathbb{Q}}$ to a product $\prod A_i$ of abelian varieties, with A_i having CM by a number field K_i of degree $2 \dim A_i$. Then $X(\mathbb{Q}_p)_n$ is finite for $n \gg 0$.*

Example 4.11. Theorem 4.10 shows eventual finiteness in many nontrivial settings. For instance, Ellenberg and Hast use it to prove finiteness of rational points on solvable covers of \mathbb{P}^1 over \mathbb{Q} , see [EH17].

4.2. Quadratic Chabauty. Suppose that the set $X(\mathbb{Q}_p)_1$ cut out by classical Chabauty–Coleman is infinite. The goal of the quadratic Chabauty method is to

- (a) show that $X(\mathbb{Q}_p)_2$ is finite
- (b) construct explicit functions on $X(\mathbb{Q}_p)$ cutting out (a finite set containing) $X(\mathbb{Q}_p)_2$.

In this section, we tackle (a), using Theorem 4.9. We will focus on (b) in Section 5.

Let $\rho(J)$ denote the *Picard number* of J , that is, the rank of $\text{NS}(J)$, the Néron–Severi group of J (as a variety over \mathbb{Q}). In this section, we will prove the following fundamental result.

Theorem 4.12 ([BD18a, Lemma 3.2]). *Suppose that*

$$(29) \quad \text{rk}(J(\mathbb{Q})) < g + \rho(J) - 1.$$

Then $X(\mathbb{Q}_p)_2$ is finite.

We call (29) the *quadratic Chabauty condition*. The rough idea of the proof is to show that, assuming (29), there exists a Galois-stable quotient U of U_2 such that $\dim \text{Sel}(U) < \dim H_f^1(G_p, U)$. The result then follows from (28) and Theorem 4.9.

In fact, we will first prove a simpler, but important special case.

Proposition 4.13. *Suppose that X has potentially good reduction everywhere. If $\text{rk}(J(\mathbb{Q})) = g$ and $\rho(J) > 1$, then $X(\mathbb{Q}_p)_2$ is finite.*

For instance, this suffices to prove finiteness of $X(\mathbb{Q}_p)_2$ for the split (or non-split) Cartan modular curve at level 13 [BDM⁺19].

4.3. Dimension counts. From now on, suppose that U is a Galois-stable quotient of U_2 which sits in a Galois-equivariant short exact sequence

$$(30) \quad 1 \rightarrow [U, U] \rightarrow U \rightarrow V \rightarrow 1,$$

where $V = H_{\text{ét}}^1(\bar{X}, \mathbb{Q}_p)$. We want to choose U so that $X(\mathbb{Q}_p)_U$ is finite. Of course we cannot take $U = V$, since that would only recover Chabauty’s result. The idea is to choose U only “slightly non-abelian”. In order to do so, we first compute $\dim H_f^1(G_p, U)$ and bound $\dim \text{Sel}(U)$ in terms of data depending only on $[U, U]$; this will then suggest find a quotient U such that $[U, U] \simeq \mathbb{Q}_p(1)$ (or a direct sum thereof).

We start with the local computation.

Lemma 4.14. *We have*

$$\dim H_f^1(G_p, U) = \dim H_f^1(G_p, [U, U]) + g.$$

Proof. Note that all representations in (30) are de Rham. Hence, we obtain a short exact sequence

$$(31) \quad 1 \rightarrow D_{\text{dR}}([U, U])/F^0 \rightarrow D_{\text{dR}}(U)/F^0 \rightarrow D_{\text{dR}}(V)/F^0 \rightarrow 1.$$

Now we have an isomorphism of schemes (algebraic by [Kim05, Section 1])

$$H_f^1(G_p, W) \simeq D_{\text{dR}}(W)/F^0$$

for $W \in \{[U, U], V, U\}$ (since $\phi = 1$ on these; compare Lemma 3.11) and therefore we deduce

$$(32) \quad \dim H_f^1(G_p, U) = \dim H_f^1(G_p, [U, U]) + \dim H_f^1(G_p, V)$$

from (31). But $H_f^1(G_p, V) \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)$, so the result follows. \square

We now turn to the dimension of $\text{Sel}(U)$. We have that $H^0(G_T, W) = 0$, for all terms in (30), so the corresponding six-term exact sequence of non-abelian Galois cohomology (see Proposition A.2) induces an exact sequence

$$H^1(G_T, [U, U]) \rightarrow H^1(G_T, U) \rightarrow H^1(G_T, V).$$

It is shown in [Kim05] that this is an exact sequence of pointed varieties, inducing another exact sequence

$$(33) \quad H_f^1(G_T, [U, U]) \rightarrow H_f^1(G_T, U) \rightarrow H_f^1(G_T, V)$$

of pointed varieties (note that this is in general weaker than the local version leading to (32)).

For now let's assume that X has potentially good reduction everywhere. This implies that a class $c \in \text{Sel}(U)$ satisfies $\text{loc}_\ell(c) = 0$ (and, in particular, is unramified) for all $\ell \neq p$; hence

$$(34) \quad \text{Sel}(U) \subset H_{f,\emptyset}^1(G_T, U) = H_f^1(G_T, U).$$

This is where we use the third requirement in Definition 4.1: we may now conclude

$$(35) \quad \dim \text{Sel}(U) \leq \text{rk}(J(\mathbb{Q})) + \dim H_f^1(G_T, [U, U])$$

from (33) and (34) without any finiteness assumptions on the Shafarevich-Tate group.

To prove non-density of the localization map, we want $H_{f,\emptyset}^1(G_T, U)$ (or $H_{f,T_0'}^1(G_T, U)$ if we don't have potentially good reduction) to be small, and $H_f^1(G_p, U)$ to be large. Hence it is natural to look for quotients U such that $[U, U] \simeq \mathbb{Q}_p(1)$, since in this case Example 3.2, Example 3.3, Lemma 4.14 and (35) imply:

Lemma 4.15. *Suppose that X has potentially good reduction everywhere. If $\text{rk}(J(\mathbb{Q})) \leq g$ and $[U, U] \simeq \mathbb{Q}_p(1)$, then $X(\mathbb{Q}_p)_U$ is finite.*

We will generalize Lemma 4.15 below. For now, let us note:

Corollary 4.16. *Suppose that X has potentially good reduction everywhere and that $\text{rk}(J(\mathbb{Q})) \leq g$. If there exists a Galois stable quotient U of U_2 such that $[U, U] \simeq \mathbb{Q}_p(1)$, then $X(\mathbb{Q}_p)_2$ is finite.*

4.4. Constructing a $\mathbb{Q}_p(1)$ -quotient of U_2 . We will now show that a quotient of U_2 as in Corollary 4.16 exists when the Picard number of J is strictly greater than 1.

Lemma 4.17. *Suppose that $\rho(J) > 1$. Then there exists a Galois-stable quotient U of U_2 surjecting onto V such that $[U, U] = \mathbb{Q}_p(1)$.*

Combining Corollary 4.16 and Lemma 4.17, we deduce Proposition 4.13.

All known methods to construct such a quotient U use a geometric approach. We will follow [BDM⁺19] in phrasing the construction in terms of a correspondence $Z \subset X \times X$. See [Smi05, Chapter 3] for background on correspondences and [Mil80, Chapter VI.9] for background on cycle classes. Applying the Künneth projector to the cycle class in $H^2(\bar{X} \times \bar{X})$ of Z , we obtain

$$\xi_Z \in H^1(\bar{X}, \mathbb{Q}_p) \otimes H^1(\bar{X}, \mathbb{Q}_p)(1) \simeq \text{End } H^1(\bar{X}, \mathbb{Q}_p).$$

Definition 4.18. A nontrivial correspondence $Z \subset X \times X$ is nice if

- (i) there are $c_1, c_2 \in \text{Pic}(X)$ such that the pushforward of the class $[Z] \in \text{Pic}(X \times X)$ under the canonical involution $(x, y) \mapsto (y, x)$ is $[Z] + \pi_1^* c_1 + \pi_2^* c_2$ where π_1, π_2 are the canonical projections,
- (ii) the class ξ_Z , viewed as an endomorphism of $H^1(\bar{X}, \mathbb{Q}_p)$, has trace zero.

Note that a correspondence satisfying (i) induces an endomorphism of J fixed by the Rosati involution, i.e. a nontrivial element of $\text{NS}(J)$. This proves the first part of the following result. The second part follows from (ii), since the trace factors through the cup product.

Lemma 4.19 ([BDM⁺19, Lemma 2.4]). *Suppose J is absolutely simple, and let $Z \subset (X \times X)$ be a correspondence satisfying (i) above. Then ξ_Z lies in the subspace*

$$\bigwedge^2 H^1(\bar{X}, \mathbb{Q}_p)(1) \subseteq H^1(\bar{X}, \mathbb{Q}_p) \otimes H^1(\bar{X}, \mathbb{Q}_p)(1).$$

Moreover Z is nice if and only if the image of ξ_Z in $H^2(\bar{X}, \mathbb{Q}_p)(1)$ under the cup product is zero.

Composing the cycle class map with the Künneth projector, we therefore get a morphism

$$(36) \quad c_Z: \mathbb{Q}_p(-1) \rightarrow \ker \left(\bigwedge^2 H^1(\bar{X}, \mathbb{Q}_p) \xrightarrow{\cup} H^2(\bar{X}, \mathbb{Q}_p) \right)$$

for every nice correspondence Z .

Proof of Lemma 4.17. Let $U[2] := \ker(U_2 \rightarrow U_1 = V)$, so that we have an exact sequence

$$1 \rightarrow U[2] \rightarrow U_2 \rightarrow V \rightarrow 1.$$

A Galois-stable quotient of U_2 surjecting onto V is therefore of the form U_2/W , where W is a Galois-stable subrepresentation of $U[2]$. So if we have a Galois-equivariant morphism $\gamma: U[2] \rightarrow \mathbb{Q}_p(1)$, then we can form a suitable quotient $U := U_2/\ker \gamma$ of U_2 via pushout:

$$\begin{array}{ccccccc} 1 & \longrightarrow & U[2] & \longrightarrow & U_2 & \longrightarrow & V \longrightarrow 1 \\ & & \downarrow \gamma & & \downarrow & & \downarrow = \\ 1 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & U & \longrightarrow & V \longrightarrow 1 \end{array}$$

To describe the representation $U[2]$, note that there is an anti-symmetric pairing

$$V \times V = U_1 \times U_1 \rightarrow U[2]$$

induced by the commutator map. It is surjective with kernel equal to the image of $H_{\text{ét}}^2(\bar{X}, \mathbb{Q}_p)$ inside $\wedge^2 V$ under the dual of the cup product $\cup^*: \wedge^2 H^1(\bar{X}, \mathbb{Q}_p) \rightarrow H_{\text{ét}}^2(\bar{X}, \mathbb{Q}_p)^*$, so the Galois representation $U[2]$ can be described via an exact sequence

$$1 \rightarrow H_{\text{ét}}^2(\bar{X}, \mathbb{Q}_p) \xrightarrow{\cup^*} \wedge^2 V \rightarrow U[2] \rightarrow 1.$$

Hence we want a morphism

$$\gamma: \text{Coker}(\cup^*: H_{\text{ét}}^2(\bar{X}, \mathbb{Q}_p) \rightarrow \wedge^2 V) \rightarrow \mathbb{Q}_p(1).$$

By Lemma 4.19, if Z is a nice correspondence, then we can take $\gamma := c(Z)^*(1)$, where c_Z^* is the dual of the map in (36). Then $U := U_2/\ker c(Z)^*(1)$ has the desired properties. Lemma 4.19 also implies that the subspace of $\text{Pic}(X \times X) \otimes \mathbb{Q}$ consisting of 0 and the classes of nice correspondences has dimension $\rho(J) - 1$, completing the proof. \square

In the following, we will denote the quotient $U_2/\ker c(Z)^*(1)$ associated to a nice correspondence Z by U_Z .

Remark 4.20. By the above, we can think of U as coming from a nontrivial cycle $Z \in \ker(\widetilde{\text{AJ}}^*)$, where

$$\widetilde{\text{AJ}}^*: \text{NS}(J) \rightarrow \text{NS}(X \times X) \rightarrow \text{NS}(X)$$

is as in [DF19, Section 2].

Remark 4.21. Another construction of U_Z is described in [BBB⁺19, §4.2]. It closely resembles the approach of Edixhoven–Lido [EL19]. Roughly speaking, we start with a cycle $Z \in \ker \widetilde{AJ}^*$ as above, lift it to a line bundle L_Z on J whose restriction to X is trivial and we let U_Z denote the \mathbb{Q}_p -étale fundamental group of the \mathbb{G}_m -torsor L_Z^* . This yields the same U_Z as the one in the proof above, and probably (after taking a multiple and extending to the Néron model) the same \mathbb{G}_m -torsor \mathcal{L}_Z as in Edixhoven–Lido. Betts [Bet] constructs local p -adic heights on $\mathcal{L}_Z(\mathbb{Q}_p)$, factoring through $H_f^1(G_p, U_Z)$; his results could be used as an alternative way to our approach for computing local p -adic heights on $H_f^1(G_p, U_Z)$ discussed below.

4.5. Beyond potentially good reduction: the twisting construction. To finish the proof of Theorem 4.12, we need to generalize Lemma 4.15 by

- allowing $[U, U] \simeq \mathbb{Q}_p(1)^{\oplus n}$, where $0 < n < \rho(J)$, rather than requiring $[U, U] \simeq \mathbb{Q}_p(1)$;
- removing the condition that X has potentially good reduction everywhere.

The first of these is trivial, since we have

$$\dim H_f^1(G_p, \mathbb{Q}_p(1)^{\oplus n}) = n$$

by Example 3.2 and

$$\dim H_f^1(G_T, \mathbb{Q}_p(1)^{\oplus n}) = 0$$

by Example 3.3. Moreover, the proof of Lemma 4.17 can be amended easily to show that we can always construct a suitable quotient $[U, U] \simeq \mathbb{Q}_p(1)^{\oplus \rho(J)-1}$. Hence the proof of Theorem 4.12 is complete once we show the following result:

Lemma 4.22. *Let U be a Galois-stable quotient of U_2 which sits in a Galois-equivariant short exact sequence (30). Then we have*

$$(37) \quad \dim \text{Sel}(U) \leq \text{rk}(J(\mathbb{Q})) + \dim H_f^1(G_T, [U, U]).$$

Proof. Note that (37) is a generalization of (35). Recall that to prove (35), we used that $\text{Sel}(U) \subset H_f^1(G_T, U)$, which might not hold in general, see Remark 4.2. To remedy this, suppose that $\alpha = (\alpha_\ell)_\ell \in \prod_{\ell \in T_0} j_\ell(X(\mathbb{Q}_\ell))$ is a set of *local conditions* such that $\alpha_\ell \in j_\ell(X(\mathbb{Q}_\ell))$ is ramified for some ℓ . Let $\text{Sel}(U)_\alpha$ denote the preimage of α under $\prod_{\ell \in T_0} \text{loc}_\ell$ and let $\beta \in \text{Sel}(U)_\alpha$. The idea is to use the twisting construction in non-abelian cohomology (see Appendix A) to show that $\text{Sel}(U)_\alpha$ is isomorphic to a subvariety $H_f^1(G_T, U^{(\beta)})'$ of $H_f^1(G_T, U^{(\beta)})$. There is an analogue of the exact sequence (33) for $U^{(\beta)}$, leading to an upper bound

$$(38) \quad \dim H_f^1(G_T, U^{(\beta)})' \leq \dim H_f^1(G_T, U^{(\beta)}) \leq \dim H_f^1(G_T, V) + \dim H_f^1(G_T, [U, U])$$

and hence

$$\dim \text{Sel}(U)_\alpha \leq \text{rk}(J(\mathbb{Q})) + \dim H_f^1(G_T, [U, U]).$$

Since $\text{Sel}(U)$ is the disjoint union of finitely many $\text{Sel}(U)_\alpha$ by Theorem 4.3, this proves the lemma.

We give a bit more detail. Letting U act on itself by conjugation, we form the twist $U^{(\beta)}$ of U by the U -torsor β . Let

$$f: H^1(G_T, U) \rightarrow H^1(G_T, U^{(\beta)})$$

denote the bijection from Proposition A.3, sending β to the trivial class. Then f maps crystalline classes to crystalline classes and preimages of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ to preimages of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$, see the proof of [BD18a, Lemma 2.6]. We define $H_f^1(G_T, U^{(\beta)})'$ to be the reduced subscheme of $H_f^1(G_T, U^{(\beta)})$ representing classes c such that

- $\text{loc}_p(c)$ is crystalline

- $\text{loc}_\ell(c) = 0$ for all $\ell \neq p$
- the projection of c to $H^1(G_T, V)$ comes from an element of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$

(compare with Definition 4.1). By the first two items, we have $H_f^1(G_T, U^{(\beta)})' \subset H_f^1(G_T, U^{(\beta)})$, and the discussion above shows that $f(\text{Sel}(U)_\alpha) \subset H_f^1(G_T, U^{(\beta)})'$.¹³

Now consider the twists $[U, U]^{(\beta)}$ and $V^{(\beta)}$, where, as above, U acts by conjugation. Since this action is unipotent, the two twisting morphisms are Galois-equivariant group isomorphisms. Hence the twisting construction turns (33) into a Galois-equivariant exact sequence

$$1 \rightarrow [U, U] \rightarrow U^{(\beta)} \rightarrow V \rightarrow 1,$$

resulting, via Kim's arguments in [Kim05] as in the discussion following Lemma 4.14, in an exact sequence of pointed varieties

$$H^1(G_T, [U, U]) \rightarrow H^1(G_T, U^{(\beta)}) \rightarrow H^1(G_T, V)$$

and, via [Kim09], in another exact sequence of pointed varieties

$$(39) \quad H_f^1(G_T, [U, U]) \rightarrow H_f^1(G_T, U^{(\beta)}) \rightarrow H_f^1(G_T, V).$$

In the above, we are using by Remark A.4 the twisting morphism f is an isomorphism of schemes, since $H^1(G_T, W)$ and $H^1(G_T, W^{(\beta)})$ are affine schemes for $W \in \{[U, U], U, V\}$ by [Kim09]. Finally, (38) follows from (39) just like (35). \square

4.6. Extending the quadratic Chabauty Lemma. Theorem 4.12 has been extended in several ways. First, there is an obvious extension to curves over imaginary quadratic fields, and in fact [BD18a, Lemma 3.2] already includes this case. One needs to restrict to such fields because of the crucial use of Example 3.3.

In [DF19], Dogra and Le Fourn extend Theorem 4.12 for Jacobians admitting an isogeny $J \rightarrow A \times B$ defined over \mathbb{Q} such that $\text{Hom}(A, B) = 0$ and satisfying a condition similar to the quadratic Chabauty condition, but phrased in terms of A and B . See [DF19, Proposition 1.6] for the precise statement. They use this result to show that $X(\mathbb{Q}_p)_2$ is finite for the nonsplit Cartan modular curve at prime level $N \neq p$, whenever this curve has genus at least 2 and at least one rational point.

In [BD18b], Balakrishnan and Dogra weaken the rank condition by replacing $\rho(J)$ by $\rho(J) + \text{rk}(\text{NS}(J_{\bar{\mathbb{Q}}})^{c=-1})$, where c denotes complex conjugation. In this setting, one needs to allow more general $[U, U]$. This essentially exhausts the Artin-Tate part of $[U_2, U_2]$, so new ideas are needed to prove finiteness of $X(\mathbb{Q}_p)_2$ for more general curves.

We expect that $X(\mathbb{Q}_p)_2$ is finite for $\text{rk}(J(\mathbb{Q})) < g^2$, independently of $\text{NS}(J_{\bar{\mathbb{Q}}})$. In fact Balakrishnan–Dogra show in [BD18b, Lemma 2.6] that this would follow from a special case of the Bloch–Kato conjecture [BK90, Conjecture 5.3(i)], applied to $X \times X$. In the proof, they work directly with U_2 , rather than a quotient.

5. COMPUTING WITH QUADRATIC CHABAUTY

Let X/\mathbb{Q} be a nice curve of genus $g \geq 2$. In the previous section, we showed that when X satisfies the quadratic Chabauty condition (29), then there is a Galois-stable quotient $U = U_Z$ of U_2 , depending on a nice correspondence Z , such that $X(\mathbb{Q}_p)_U$ is finite (and hence $X(\mathbb{Q}_p)_2$ is finite as well). We now discuss how to compute $X(\mathbb{Q}_p)_U$ in practice.

¹³It can be shown that f is indeed an isomorphism, but we don't need this in our argument.

Recall the situation discussed in Section 2.3, in particular Corollary¹⁴ 2.30: When X is hyperelliptic and satisfies some additional conditions, then we use the Coleman–Gross construction of the p -adic height pairing

$$h(P - \infty, P - \infty) = h_p(P - \infty, P - \infty) + \sum_{\ell \neq p} h_\ell(P - \infty, P - \infty)$$

for $P \in X(\mathbb{Q})$. We showed that

- (i) the function $P \mapsto h_p(P - \infty, P - \infty)$ extends to a locally analytic function $\theta: X(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$;
- (ii) $h_\ell(z - \infty, z - \infty) = 0$ for integral¹⁵ points $z \in X(\mathbb{Q}_\ell)$;
- (iii) h is a symmetric bilinear pairing on $J(\mathbb{Q}) \otimes \mathbb{Q}_p$, and hence can be written as a linear combination of a basis of such pairings.

More precisely, the local height h_p had an interpretation as a sum of double Coleman integrals, which can be thought of as a solution to a p -adic differential equation. Since we assumed in Corollary 2.30 that \log restricts to an isomorphism $J(\mathbb{Q}) \otimes \mathbb{Q}_p \rightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$, we can construct a basis in (iii) via products of single integrals. These are restrictions of locally analytic functions, so we get a function $\rho: X(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ from (i) and (iii) with finitely many zeros which vanishes on integral points $P \in X(\mathbb{Q})$ (ii).

Remark 5.1. The presence of double Coleman integrals suggest that we have found some part of $X(\mathbb{Z}_p)_2$, the “quadratic” or depth 2 part of Kim’s nonabelian Chabauty, since $X(\mathbb{Q}_p)_n$ or $X(\mathbb{Z}_p)_n$ are cut out by n -fold iterated integrals [Kim09, BDCKW18].

The difficulty in extending this construction to *rational points* is that we do not have a good way to control $\sum_{\ell \neq p} h_\ell(P - \infty, P - \infty)$ (or a similar local height in the non-hyperelliptic case) for general $P \in X(\mathbb{Q})$. This is where we use Chabauty–Kim: Recall that for $\ell \neq p$, the image $j_{U,\ell}(X(\mathbb{Q}_\ell))$ inside $H^1(G_\ell, U)$ is finite by Theorem 4.3, and is trivial if X has potentially good reduction at ℓ by Remark 4.4. Therefore we want (local and global) p -adic heights which factor through Kim’s unipotent Kummer maps $j_{U,v}$. It turns out that Nekovář’s construction of p -adic heights discussed in Section 3, based on p -adic Hodge theory, makes this possible, via the twisting construction in non-abelian cohomology.

Recall that for a prime v the local Nekovář-height h_v is defined on mixed extensions of p -adic G_v -representations with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$. We will see below that we can take a torsor $P \in H^1(G_v, U)$ and produce such a mixed extension $\tau_v(P)$ (depending on Z). In fact, the same construction produces a global mixed extension $\tau(P)$ for $P \in H^1(G_T, U)$. We deduce that the function

$$(40) \quad \text{Sel}(U) \rightarrow \mathbb{Q}_p; \quad P \mapsto h_\ell(\tau_\ell(\text{loc}_\ell(P)))$$

has finite image, and if X has potentially good reduction at ℓ , then the image of the map (40) is trivial.

To ease notation, we write

$$A(x) := \tau(j_{U,p}(x))$$

for $x \in X(\mathbb{Q}_v)$. This assigns a mixed extension of G_v -representations with graded pieces \mathbb{Q}_p, V and $\mathbb{Q}_p(1)$ to a \mathbb{Q}_p -rational point on X .

We now use this to give an analogue of Theorem 2.28 in the simplest situation covered by Theorem 4.12, namely

- (i) $r = g > 1$,
- (ii) $\log: J(\mathbb{Q}) \otimes \mathbb{Q}_p \rightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ is an isomorphism¹⁶, and

¹⁴More generally, see Theorem 2.28.

¹⁵See Proposition 2.29 for a more general statement.

¹⁶If this fails, we can simply use Chabauty–Coleman to compute the rational points.

(iii) $\rho(J) > 1$.

Under these assumptions,

$$H_f^1(G_{\mathbb{Q}}, V) \xrightarrow{\text{loc}_p} H_f^1(G_p, V) \xrightarrow{\log} H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$$

is an isomorphism, so by Poincaré duality we may view the global height h as a bilinear pairing

$$h: H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \times H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \rightarrow \mathbb{Q}_p.$$

By abuse of notation, we may replace the target of the projection maps π_1, π_2 introduced in (20) by $H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$.

As in Section 3.2, we fix

- (a) an idèle class character $\chi: \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^* \rightarrow \mathbb{Q}_p$,
- (b) a splitting s of the Hodge filtration on V_{dR} such that $\ker(s)$ is isotropic with respect to the dual of the cup product pairing.

Recall from Remark 3.5 that the isotropicity condition implies that h is symmetric. The following result sums up the theoretical foundation for our approach to computing rational points via p -adic heights:

Theorem 5.2 (Quadratic Chabauty for rational points [BD18a, Proposition 5.5]). *Let X/\mathbb{Q} be a nice curve, let J be the Jacobian of X , assume that $\text{rk } J(\mathbb{Q}) = g > 1$, and that $\rho(J) > 1$. Choose a prime p of good reduction for X such that $\log: J(\mathbb{Q}) \otimes \mathbb{Q}_p \rightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ is an isomorphism. Choose a nice correspondence Z on X and let $U = U_Z$. Finally, fix a basis ψ_1, \dots, ψ_N of $(H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbb{Q}_p}, \Omega^1)^*)^*$.*

Then there exist computable constants $\alpha_i \in \mathbb{Q}_p$ such that the function $X(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ defined by

$$\rho(x) := h_p(A(x)) - \sum_{i=1}^N \alpha_i \psi_i \circ (\pi_1, \pi_2)(A(x))$$

has finitely many zeros and takes values in a finite set $S \subset \mathbb{Q}_p$ on $X(\mathbb{Q}_p)_U$.

If X has everywhere potentially good reduction, then this holds for $S = \{0\}$.

Proof. By the above, $\rho(X(\mathbb{Q}_p)_U)$ is contained in the finite subset of \mathbb{Q}_p coming from the possible values of the functions in (40). To show that ρ only has finitely many zeros, we use that by [BD18b, Lemma 3.7],

$$(\pi_*, h_p \circ \tau_p) : H_f^1(G_p, U) \longrightarrow H_f^1(G_p, V) \times \mathbb{Q}_p$$

is an isomorphism of schemes. Because $j_{U,p}$ has Zariski dense image [Kim09], the result follows. \square

To fill in the gaps in the discussion above, we will construct τ (and τ_p) in the next subsection. This will be done by first constructing a mixed extension A_Z as a quotient of the universal enveloping algebra of the Lie algebra of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, following the construction of U itself. Then we define τ via the twisting construction in non-abelian cohomology.

In Section 5.2, we discuss how to compute $\pi_1(A(x)), \pi_2(A(x))$ and $h_p(A(x))$ for $x \in X(\mathbb{Q}_p)$. Further computational issues are addressed in Section 5.3; there, we also give an algorithmic version of Theorem 5.2 (Algorithm 5.27), and we describe how the set S can be computed and how the coefficients α_i can be derived for a suitable basis $\{\psi_i\}$. In particular, this will show:

Corollary 5.3. *In the situation of Theorem 5.2, the function ρ and the set S are explicitly computable.*

Finally, we give a worked example, determining rational points on the modular curve $X_0(167)/w_{67}$ in Section 5.4, and we discuss some possible future directions in Section 5.5.

Remark 5.4. In Theorem 5.2, the dependence on Z is hidden by our notation. In fact, both the mixed extensions $A(x)$ (and thus the function ρ) and the set S depend on Z . Due to our crucial use of local heights, ρ depends on the choices of χ and s , and S depends on χ .

Remark 5.5. In [BD18a, Section 6], Balakrishnan and Dogra show that for $z \in X(\mathbb{Q}_v)$, the mixed extension $A(x)$ can be expressed geometrically, as the mixed extension associated to the divisors $z - b$ and $D_Z(b, z)$ on X of degree 0 as in [Nek93, Section 5]. They use this to compute the rational points on a bielliptic genus 2 curve over \mathbb{Q} and the $\mathbb{Q}(i)$ -rational points on the bielliptic genus 2 curve $X_0(37)$, answering a question of Daniels and Lozano-Robledo. Here

$$D_Z(b, z) = \Delta^*(Z) - i_{1,b}^*(Z) - i_{2,z}^*(Z),$$

where $i_{1,b}(x) = (x, b) \in X \times X$, $i_{2,z}(x) = (z, x)$ and $\Delta: X \rightarrow X \times X$ is the diagonal embedding. One needs that Z does not intersect $(\Delta - X \times x_1 - x_2 \times X)$ for any pair $(x_1, x_2) \in X \times X$. In particular, this approach requires that we have explicit equations for Z as a divisor on $X \times X$. When X is a bielliptic curve of genus 2, then Z is a sum of sections, and the heights can be computed on the corresponding elliptic curves.

In work in progress of Besser, Müller, and Srinivasan, a version of Theorem 5.2 is proved by applying the construction of Coleman–Gross and p -adic Arakelov theory [Bes05] directly to the divisors $z - P$ and $D_Z(b, P)$ without relying on fundamental groups or p -adic Hodge theory. This also leads to an alternative way to compute the function ρ and the set S .

Remark 5.6. What if we have two nice correspondences Z, Z' ? Under our assumptions, the corresponding sets $X(\mathbb{Q}_p)_{U_Z}$ and $X(\mathbb{Q}_p)_{U_{Z'}}$ are the same if and only if Z and Z' are dependent¹⁷, see [BD18a, Remark 5.7].

Remark 5.7. In the remainder of these notes, we discuss how Theorem 5.2 can be turned into a method for *computing* the rational points for a given curve X . However, it is also possible to *bound* $\#X(\mathbb{Q})$ for curves X satisfying our assumptions; see [BD19a]. See also [DF19] for an extension.

5.1. Twisting and mixed extensions. In this section, we first construct a mixed extension A_Z of Galois representations with graded pieces \mathbb{Q}_p , V and $\mathbb{Q}_p(1)$, depending on a nice correspondence Z on X , which we fix. The idea is to mimic the construction of U_Z , but on the Lie algebra side. For more details, see [BD18a, Section 5], and see [BD18b, Sections 3,4] for a generalization.

Recall that U_Z is a unipotent quotient of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}$, the unipotent \mathbb{Q}_p -étale fundamental group of $X_{\overline{\mathbb{Q}}}$. We first define

$$\mathbb{Z}_p[[\pi_1^{\text{ét},(p)}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}]] := \varprojlim \mathbb{Z}_p[\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)]/N$$

where the limit is over all group algebras of finite quotients of p -power order [Qui69, Appendix A].

Letting I denote the augmentation ideal of $\mathbb{Q}_p \otimes \mathbb{Z}_p[[\pi_1^{\text{ét},(p)}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}]]$, we define the algebra

$$A_n := A_n(b) := \mathbb{Q}_p \otimes \mathbb{Z}_p[[\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}]]/I^{n+1}.$$

Then A_n is a quotient of the enveloping algebra of U_n ; in fact the limit of the A_n is (isomorphic to) the pro-universal enveloping algebra of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}$, see [CK10, §2]. Moreover, there is an action of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}$ on A_n which factors through U_n .

For $n = 1, 2$, we can describe A_n as follows:

$$1 \rightarrow V \rightarrow A_1 \rightarrow \mathbb{Q}_p \rightarrow 1,$$

¹⁷as elements of the space of nice correspondences (together with 0); i.e. as elements of $\ker(\text{NS}(J) \rightarrow \text{NS}(X))$

and, similar to the situation¹⁸ considered in Section 4.4, there is an exact sequence

$$(41) \quad 1 \rightarrow \text{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}) \rightarrow A_2 \rightarrow A_1 \rightarrow 1,$$

coming from the isomorphism $I^2/I^3 \cong \text{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2})$. Following the argument in Lemma 4.17, we can define a quotient of A_2 using Z as follows.

Definition 5.8. The representation $A_Z := A_Z(b)$ is the pushout of A_2 by

$$\text{cl}_Z^* : \text{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}) \rightarrow \mathbb{Q}_p(1).$$

Note that U_Z acts faithfully on A_Z on the left; the action is unipotent with respect to the I -adic filtration. In fact we have:

Lemma 5.9. *The I -adic filtration gives A_Z the structure of a crystalline mixed extension of G_T -representations with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$.*

To show that A_Z is crystalline, one first proves that A_2 is crystalline using [Ols11, Theorem 1.4].

Recall that we want to construct a mixed extension with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$ from a given torsor $P \in \text{Sel}(U_Z)$. Via the action of U_Z on A_Z , this can now be achieved by twisting A_Z (see Appendix A).

Definition 5.10. For $P \in H^1(G_T, U)$ we define

$$\tau(P) := P \times_{U_Z} A_Z.$$

When $x \in X(\mathbb{Q})$ and P is the path torsor $P(b, x) := \pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b, x)$, then we define $A(x) := \tau(P)$.

The most important features of the twisting map τ are summarized in the following lemma. Since we want to focus on computational methods, we refer to [BD18a, §5.1] and [BD18b, §3.3] for proofs of these assertions.

Lemma 5.11. *Let $P \in H^1(G_T, U)$. Then we have the following:*

- (i) $\tau(P)$ is a mixed extension of G_T -representations with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$.
- (ii) The map τ is injective.
- (iii) If P is crystalline at p , then $\tau(P)$ is crystalline at p as well.
- (iv) We have $\pi_1(\tau(P)) = P \times_{U_Z} A_1$ and $\pi_2(\tau(P)) = P \times_{U_Z} IA_Z$.

Remark 5.12. Similarly, we can construct a mixed extension $\tau_v(P)$ of G_v -representations from a local torsor $P \in H^1(G_v, U)$, with the special case $A(x)$ for $x \in X(\mathbb{Q}_v)$. The analogue of Lemma 5.11 remains valid for τ_v .

For our algorithm, we need to describe $\pi_i(A(x))$ explicitly for $i = 1, 2$ and $x \in X(\mathbb{Q})$. See [BD18a, § 5.2] and [BD18b, Lemma 3.5] for more details. We find that on $H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$, we have

$$\pi_1(A(x)) = \log([x - b])$$

(similar to Section 2.3), but $\pi_2(A(x))$ is more difficult to describe, since it depends on Z . In $\text{Ext}^1(V, \mathbb{Q}_p(1))$ we have

$$[P(b, x) \times_{U_Z} IA_Z] = E_Z(\pi_1(A(x))) + [IA_Z],$$

¹⁸Note that $\text{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}) \cong \text{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} \wedge^2 V) \oplus \text{Sym}^2 V$; in Section 4.4 there was no $\text{Sym}^2 V$ summand.

where E_Z is the endomorphism of $H_f^1(G_T, V)$ induced by Z . So let $c_Z \in H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ be the constant functional corresponding to $[IA_Z]$. This is a p -adic logarithm of the Chow-Heegner point associated to Z , see [BDM⁺19, Remarks 3.11 and 5.6] and [DRS12]. Then, in $H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$, we find

$$(42) \quad \pi_2(A(x)) = E_Z(\log([x - b])) + c_Z,$$

where, by abuse of notation, E_Z denotes the endomorphism of $H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ induced by Z .

In practice, we can read off $\pi_i(A(x))$ directly from our explicit description of $A(x)$, see (48) below.

5.2. Algorithms for the local height at p . To compute $X(\mathbb{Q}_p)_U$, we need to compute $h_p(A(x))$, so we need to choose a nice correspondence Z and write the locally analytic function

$$\begin{aligned} \theta: X(\mathbb{Q}_p) &\rightarrow \mathbb{Q}_p \\ x &\mapsto h_p(A(x)) \end{aligned}$$

as a power series on every residue disk of $X(\mathbb{Q}_p)$. In this section, we follow [BDM⁺19] closely.

By Proposition 3.12 we have the formula

$$(43) \quad h_p(A(x)) = \chi_p(\gamma_\phi - \gamma_{\text{Fil}} - \beta_\phi^T \cdot s_1(\alpha_\phi) - \beta_{\text{Fil}}^T s_2(\alpha_\phi)),$$

for the local height of the mixed extension $A(x)$. The quantities on the right hand side only depend on the filtered ϕ -module $D_{\text{cris}}(A(x))$, so it suffices to compute an explicit description of this. In particular, we do not need to construct the representation $A(x)$ at all.

We will utilize the de Rham realization of A_Z : this is a filtered connection \mathcal{A}_Z with Frobenius structure (more precisely, a unipotent isocrystal), and Olsson's comparison theorem [Ols11, Theorem 1.4] then implies the following isomorphism of filtered ϕ -modules:

Lemma 5.13 ([BDM⁺19, Lemma 5.4]). *We have*

$$x^* \mathcal{A}_Z = D_{\text{cris}}(A(x)), \quad \text{for all } x \in X(\mathbb{Q}_p).$$

Hence it suffices to construct the Hodge filtration and Frobenius structure of \mathcal{A}_Z . We will construct the filtered connection \mathcal{A}_Z as a quotient of a universal connection $\mathcal{A}_2^{\text{dR}}$ via push-out, similar to the construction of U_Z and A_Z . The universal properties of $\mathcal{A}_2^{\text{dR}}$ then allow us to determine the Hodge filtration and Frobenius structure of \mathcal{A}_Z uniquely. The Hodge filtration is determined by the Hodge filtration on its graded pieces, as well as its global nature: that starting with an affine piece Y , it extends nicely to X , by work of Hadian. The Frobenius structure is determined by its action on the unit vector [BDM⁺19, Lemma 5.2], which is essentially an initial condition for our p -adic differential equation that we can extend via parallel transport.

Definition 5.14. A filtered connection (V, ∇) is a connection on X together with an exhaustive, descending filtration

$$\dots \supseteq \text{Fil}^i V \supseteq \text{Fil}^{i+1} V \supseteq \dots$$

satisfying Griffiths transversality

$$\nabla(\text{Fil}^i V) \subseteq \text{Fil}^{i-1} V \otimes \Omega^1.$$

We use the Tannakian formalism, see [Del90, DM82]. Let $\mathcal{C}^{\text{dR}}(X)$ be the category of unipotent vector bundles¹⁹ with connection on X . The fiber functor b^* at the base point $b \in X(\mathbb{Q})$ gives $\mathcal{C}^{\text{dR}}(X)$ the structure of a neutral Tannakian category. Its fundamental group $\pi_1^{\text{dR}}(X, b)$ is pro-unipotent (it is the direct limit of its n -step unipotent quotients $U_n^{\text{dR}}(b)$), so we obtain a unipotent Tannakian category.

¹⁹In general, one would also require flatness, but this is automatic for curves.

For $n \neq 1$, we define

$$A_n^{\text{dR}}(b) := A(\mathcal{C}^{\text{dR}}(X, b^*)) / I^{n+1},$$

where $A(\mathcal{C}^{\text{dR}}(X, b^*))$ is the pro-universal enveloping algebra with augmentation ideal I . For $x \in X(\mathbb{Q}_p)$, we have associated path torsors

$$A_n^{\text{dR}}(b, x) := A_n^{\text{dR}}(b) \times_{\pi_1^{\text{dR}}(X, b)} \pi_1^{\text{dR}}(X; b, x).$$

The theory of universal objects in unipotent Tannakian categories (see [BDM⁺19, Appendix A.1] and [BD18b, Appendix A]) shows that there is a universal n -step unipotent object (see [BDM⁺19, Definition A.2, Lemma A.3])

$$\mathcal{A}_n^{\text{dR}} := \mathcal{A}_n^{\text{dR}}(b)$$

associated to the $\pi_1^{\text{dR}}(X, b)$ -representation $A_n^{\text{dR}}(b)$. In other words, if \mathcal{V} is an n -step unipotent connection on X and $v \in b^*\mathcal{V}$, then there is a unique morphism of connections $f: \mathcal{A}_n^{\text{dR}} \rightarrow \mathcal{V}$ such that $b^*(f)(e_n) = v$ (e_n being the unit element). As discussed in [Kim09], $\mathcal{A}_n^{\text{dR}}$ carries a Hodge filtration Fil^\bullet satisfying the following universal property.

Theorem 5.15 (Hadian [Had11]). *For all $n > 0$ the Hodge filtration Fil^\bullet on $\mathcal{A}_n^{\text{dR}}(b)$ is the unique filtration such that*

- (1) *Fil $^\bullet$ makes $(\mathcal{A}_n^{\text{dR}}(b), \nabla)$ into a filtered connection.*
- (2) *The natural maps induce a sequence of filtered connections:*

$$V_{\text{dR}}^{\otimes n} \otimes \mathcal{O}_X \rightarrow \mathcal{A}_n^{\text{dR}}(b) \rightarrow \mathcal{A}_{n-1}^{\text{dR}}(b) \rightarrow 0.$$

- (3) *The identity element of $\mathcal{A}_n^{\text{dR}}(b)$ lies in $\text{Fil}^0 \mathcal{A}_n^{\text{dR}}(b)$.*

In analogy with (41), we obtain an exact sequence of filtered vector bundles

$$0 \rightarrow \text{coker}(H_{\text{dR}}^2(X)^* \xrightarrow{\cup^*} V_{\text{dR}}^{\otimes 2}) \otimes \mathcal{O}(X) \rightarrow \mathcal{A}_2^{\text{dR}} \rightarrow \mathcal{A}_1^{\text{dR}} \rightarrow 0.$$

Recall the discussion of nice correspondences in Section 4.4; the statements there have natural de Rham analogues. We will denote the Tate class in $H_{\text{dR}}^1(X/\mathbb{Q}) \otimes H_{\text{dR}}^1(X/\mathbb{Q})$ induced by a nice correspondence Z (and its matrix representation with respect to the basis $\{\omega_i\}$) also by Z ; in analogy with (36), Z induces a map

$$(44) \quad \text{coker}(H_{\text{dR}}^2(X)^* \xrightarrow{\cup^*} V_{\text{dR}}^{\otimes 2}) \rightarrow \mathbb{Q}_p(1).$$

As before, we can now form a quotient by push-out, noting that it carries the structure of a filtered connection.

Definition 5.16. The filtered connection $\mathcal{A}_Z := \mathcal{A}_Z(b)$ is the pushout of $\mathcal{A}_2^{\text{dR}}$ by the map (44).

Remark 5.17. The important part of Theorem 5.15 is the *uniqueness*. Below, the sub-bundle Fil^0 of the quotient \mathcal{A}_Z of $\mathcal{A}_2^{\text{dR}}$ is determined in an explicit trivialization on Y , by writing down a general form for a basis, solving for the coefficients using the fact that it extends uniquely to X and satisfies the three conditions.

Remark 5.18. In our setting, Griffiths transversality is actually an empty condition, since $\text{Fil}^1 \mathcal{A}_Z = 0$ and $\text{Fil}^{-1} \mathcal{A}_Z = \mathcal{A}_Z$.

5.2.1. *Computing the Hodge filtration.* The Hodge filtration on \mathcal{A}_Z is determined by the Hodge filtration on its graded pieces, via the universal property in Hadian's theorem.

We first determine it on an affine open $Y \subseteq X$. This is easier than working directly on X , since unipotent vector bundles on Y are trivial. Let $b \in Y(\mathbb{Q})$ and suppose

$$\#(X \setminus Y)(\overline{\mathbb{Q}}) = d$$

and let L/\mathbb{Q} be a finite extension over which all points of $D = X \setminus Y$ are defined.

Choose differentials $\omega_0, \dots, \omega_{2g+d-2} \in H^0(Y_{\overline{\mathbb{Q}}}, \Omega^1)$ such that

- (1) The differentials $\omega_0, \dots, \omega_{2g-1}$ are of the second kind on X and form a symplectic basis of $H^1_{dR}(X_{\mathbb{Q}})$ with respect to the cup product pairing.
- (2) The differentials

$$\omega_{2g}, \dots, \omega_{2g+d-2}$$

are of the third kind on X , by which we mean that all poles are simple; in this section, we do not require integer residues.

The connection $\mathcal{A}_n^{dR}(X)|_Y$ can be obtained as a quotient of a connection $\mathcal{A}_n^{dR}(Y)$ having similar universal properties, but on Y . More precisely $\mathcal{A}_n^{dR}(X)|_Y$ is the maximal quotient of $\mathcal{A}_n^{dR}(Y)$ which extends to a holomorphic connection on X . The connection $\mathcal{A}_n^{dR}(Y)$ can be computed explicitly via a universal property due to Kim (see [BDM⁺19, Section 4.2]). It follows from this and from [BDM⁺19, Remark 4.9] that we may choose a trivialization

$$s_0(b, \cdot) : (\mathbb{Q} \oplus V_{dR} \oplus \mathbb{Q}(1)) \otimes \mathcal{O}_Y \xrightarrow{\sim} \mathcal{A}_Z|_Y$$

such that the connection ∇ on \mathcal{A}_Z via this trivialization is given by

$$s_0^{-1} \nabla s_0 = d + \Lambda,$$

where

$$\Lambda = - \begin{pmatrix} 0 & 0 & 0 \\ \vec{\omega} & 0 & 0 \\ \eta & \vec{\omega}^T Z & 0 \end{pmatrix}$$

for some η of the third kind on X , and where

$$\vec{\omega} = \{\omega_0, \dots, \omega_{2g-1}\}.$$

This is to be understood with respect to a basis

$$\{1, T_0, \dots, T_{2g-1}, S\}$$

of the 2-step unipotent filtration, where T_0, \dots, T_{2g+d-2} is the basis of $V_{dR}(Y) = H^1_{dR}(Y)^*$ dual to $\omega_0, \dots, \omega_{2g+d-2}$.

Lemma 5.19 ([BDM⁺19, Lemma 4.10]). *The differential η in Λ is the unique differential satisfying the following two conditions:*

- (1) η is in the span of

$$\{\omega_{2g}, \dots, \omega_{2g+d-2}\}.$$

- (2) The connection ∇ extends to a holomorphic connection on the whole of X .

The proof uses a unipotent gauge transformation C_x at all $x \in D = X \setminus Y$, which we now introduce. In a formal neighborhood of a point $x \in X \setminus Y$ with local coordinate t_x , we can find a trivialization of \mathcal{A}_Z

$$s_x : ((\mathbb{Q} \oplus V_{dR} \oplus \mathbb{Q}(1)) \otimes L[[t_x]], d) \xrightarrow{\sim} (\mathcal{A}_Z|_{L[[t_x]]}, \nabla)$$

since \mathcal{A}_Z is unipotent and any unipotent connection on a formal disk is trivial and we define

$$C_x = s_x^{-1} s_0 = \begin{pmatrix} 1 & 0 & 0 \\ \Omega_x & 1 & 0 \\ g_x & \Omega_x^T Z & 1 \end{pmatrix},$$

where

$$d\Omega_x = -\vec{\omega} \quad dg_x = \Omega_x^T Z d\Omega_x - \eta.$$

We now describe the Hodge filtration on \mathcal{A}_Z with respect to s_0 , i.e. we give an explicit isomorphism

$$(45) \quad s^{\text{Fil}}: ((\mathbb{Q} \oplus V_{\text{dR}} \oplus \mathbb{Q}(1)) \otimes \mathcal{O}_Y) \xrightarrow{\sim} \mathcal{A}_Z$$

that respects the Hodge filtration on both sides.

It suffices to describe $\text{Fil}^0 \mathcal{A}_Z$; define

$$\gamma_{\text{Fil}} \in \mathcal{O}_Y, \quad b_{\text{Fil}} = (b_g, \dots, b_{2g-1})^T \in \mathbb{Q}^g$$

by the requirement that

$$\gamma_{\text{Fil}}(b) = 0$$

and for all $x \in D$:

$$g_x + \gamma_{\text{Fil}} - b_{\text{Fil}}^T N^T \Omega_x - \Omega_x^T Z N N^T \Omega_x \in L[[t_x]]$$

where

$$N = (0_g, 1_g)^T \in M_{2g \times g}(\mathbb{Q}).$$

Theorem 5.20 ([BDM⁺19, Theorem 4.11]). *We can choose s^{Fil} in (45) such that the restriction of $s_0^{-1} s^{\text{Fil}}$ to $(\mathbb{Q} \oplus \text{Fil}^0 V_{\text{dR}}) \otimes \mathcal{O}_Y$ is given by the $(2g+2) \times (g+1)$ matrix*

$$\begin{pmatrix} 1 & 0 \\ 0 & N \\ \gamma_{\text{Fil}} & b_{\text{Fil}}^T \end{pmatrix}.$$

From this result, we obtain the following algorithm for computing γ_{Fil} and b_{Fil} , as desired for (43).

Algorithm 5.21 (The Hodge filtration on \mathcal{A}_Z).

- (1) Compute local coordinates t_x at each $x \in D$.
- (2) For each $x \in D$ compute Laurent series expansions of the elements in $\vec{\omega}$ at x to large enough precision, which is at least mod $t_x^{d_x}$, where d_x is the order of the largest pole occurring.
- (3) Compute the vector Ω_x , defined by

$$d\Omega_x = -\vec{\omega}_x.$$

- (4) Solve for η as the unique linear combination of $\omega_{2g}, \dots, \omega_{2g+d-2}$ such that $d\Omega_x^T Z \Omega_x - \eta$ has residue zero at all $x \in D$.
- (5) Solve the system of equations for g_x such that $dg_x = \Omega_x^T Z d\Omega_x - \eta$.
- (6) Compute the vector of constants $b_{\text{Fil}} = (b_g, \dots, b_{2g-1}) \in \mathbb{Q}^g$ and the function γ_{Fil} characterized by $\gamma_{\text{Fil}}(b) = 0$ and

$$g_x + \gamma_{\text{Fil}} - b_{\text{Fil}}^T N^T \Omega_x - \Omega_x^T Z N N^T \Omega_x \in L[[t_x]],$$

where $N = (0_g, 1_g)^T \in M_{2g \times g}(\mathbb{Q})$. Set $\beta_{\text{Fil}} = (0, \dots, 0, b_g, \dots, b_{2g-1})^T$.

Remark 5.22. If X is hyperelliptic, then we have that $\eta = 0$ and $\beta_{\text{Fil}} = (0, \dots, 0)^T$ by [BD18b, Lemma 6.5].

5.2.2. Computing the Frobenius structure. The importance of the filtered connection discussed above is that we can base change \mathcal{A}_Z to \mathbb{Q}_p . This base change has a Frobenius structure and we get an isomorphism of filtered ϕ -modules

$$x^* \mathcal{A}_Z = D_{\text{cris}}(A(x))$$

for all $x \in X(\mathbb{Q}_p)$. We will describe the Frobenius structure on the isocrystal $\mathcal{A}_Z^{\text{rig}}(\bar{b})$.

For now, we will focus on the affine story. For details on the rigid structure, see the appendix of [BDM⁺19]. Let A be an affinoid algebra over K , a complete discrete valuation field of characteristic 0, and let A^\dagger be its weak completion. Let $\bar{A} = A^\dagger/\pi$ where π is a uniformizer of R , the ring of integers of K .

The main idea behind isocrystals and their relation to iterated Coleman integrals is that the integrals can be seen as solutions to certain p -adic differential equations. For instance, the iterated Coleman integral

$$\int \omega_n \dots \omega_1$$

is the y_n -coordinate of a solution to the following system of p -adic differential equations:

$$dy_0 = 0, dy_1 = \omega_1 y_0, \dots, dy_n = \omega_n y_{n-1},$$

or equivalently,

$$d\vec{y} = \Omega \vec{y}, \text{ where } \Omega := \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ \omega_1 & 0 & \cdots & 0 & 0 \\ 0 & \omega_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \omega_n & 0 \end{pmatrix},$$

with $y_0 = 1$. This is a unipotent differential equation.

Definition 5.23. A unipotent isocrystal on \bar{A} is an A^\dagger -module M together with an (integrable) connection

$$\nabla : M \rightarrow M \otimes_{A^\dagger} \Omega^1(\otimes K)$$

that is an iterated extension of trivial connections, where the trivial connection is $\mathbb{1} = (A^\dagger, d)$.

A morphism of unipotent isocrystals is a map of A^\dagger -modules that is horizontal (i.e. commutes with connection).

There is an analogous category of unipotent isocrystals via rigid triples (see [BDM⁺19, Appendix A]). Let $\mathcal{C}^{\text{rig}}(X_{\mathbb{F}_p})$ be the category of (rigid) unipotent isocrystals on the special fiber of X . This has an action of Frobenius on path torsors $\pi_1^{\text{rig}}(X_{\mathbb{F}_p}, \bar{b}, \bar{x})$ of π_1^{rig} , and hence on the n -step unipotent quotients:

$$\phi_n : A_n(\bar{b}, \bar{x}) \rightarrow A_n(\bar{b}, \bar{x}).$$

There is a Frobenius structure on $\mathcal{A}_n^{\text{rig}}(\bar{b})$, the universal n -step object. The Frobenius structure is an isomorphism

$$\Phi_n : \phi^* \mathcal{A}_n^{\text{rig}}(\bar{b}) \xrightarrow{\sim} \mathcal{A}_n^{\text{rig}}(\bar{b})$$

of overconvergent unipotent isocrystals, where ϕ is a lift of Frobenius from the special fiber.

There is a corresponding de Rham realization pullback Frobenius on $X_{\mathbb{F}_p}$, which gives a Frobenius action on $\pi_1^{\text{dR}}(X_{\mathbb{Q}_p}, b, x)$ and a Frobenius operator on the n -step unipotent quotients

$$\phi_n(b, x) : A_n^{\text{dR}}(b, x) \rightarrow A_n^{\text{dR}}(b, x).$$

Theorem 5.24 (Chiarelletto-Le Strum [CLS99]). *There is an equivalence of categories*

$$\mathcal{C}^{\text{dR}}(X_{\mathbb{Q}_p}) \xrightarrow{\sim} \mathcal{C}^{\text{rig}}(X_{\mathbb{F}_p})$$

given by the analytification functor $(\cdot)^{\text{an}}$.

For any $x \in X(\mathbb{Q}_p)$ with reduction \bar{x} , we have a canonical isomorphism of fiber functors

$$i_x : \bar{x}^* \circ (\cdot)^{\text{an}} \equiv x^*$$

such that if $x, y \in X(\mathbb{Q}_p)$ belong to the same residue disk, the canonical isomorphism $i_x \circ i_y^{-1}$ is given by parallel transport $T_{x,y}$ along the connection.

Let b_0 and x_0 be Teichmüller representatives of b and x , respectively. We relate the Frobenius operator $\phi_n(\cdot)$ to the isocrystal $\mathcal{A}_n^{\text{rig}}(\bar{b})$ by defining

$$\phi_n(b, x) = \tau_{b,x} \circ \phi_n(b_0, x_0) \circ \tau_{b,x}^{-1}$$

where $\tau_{b,x}$ is the canonical isomorphism from Theorem 5.24, given by

$$\begin{aligned} \tau_{b,x} : \text{Hom}(b_0^*, x_0^*) &\xrightarrow{\sim} \text{Hom}(b^*, x^*) \\ g &\mapsto T_{x,x_0} \circ g \circ T_{b_0,b}. \end{aligned}$$

We can describe $\tau_{b,x}$ on $A_n^{\text{dR}}(b, x)$ via formal integration on residue disks. Since $A_n^{\text{dR}}(b, x)$ is a quotient of $A_n^{\text{dR}}(Y)(b, x)$, it suffices to describe the parallel transport here.

Recall that we've fixed s_0 where

$$s_0(b, x) : \bigoplus_{i=0}^n V_{\text{dR}}(Y)^{\otimes i} \xrightarrow{\sim} A_n^{\text{dR}}(b, x).$$

For any $x_1, x_2 \in X(\mathbb{Q}_p)$ that lie in the same residue disk, we define $I(x_1, x_2) \in \bigoplus_{i=0}^n V_{\text{dR}}(Y)^{\otimes i}$ as

$$I(x_1, x_2) = 1 + \sum_w \int_{x_1}^{x_2} w(\omega_0, \dots, \omega_{2g+d-2})$$

where the sum is over all words w in $\{T_0, \dots, T_{2g+d-2}\}$ of length at most n , making substitution of T_i with ω_i . Here, the integrals are given by formally integrating power series.

This gives $\tau_{b,x}$, when considered on $A_n^{\text{dR}}(Y)$ via s_0 as

$$\begin{aligned} \tau_{b,x} : \bigoplus_{i=0}^n V_{\text{dR}}(Y)^{\otimes i} &\xrightarrow{\sim} \bigoplus_{i=0}^n V_{\text{dR}}(Y)^{\otimes i} \\ (46) \qquad \qquad \qquad v &\mapsto I(x_0, x)vI(b, b_0). \end{aligned}$$

By Besser's theory of Coleman integration on unipotent connections [Bes02], we have that for any points $b, b_0, x, x_0 \in Y(\mathbb{Q}_p)$, the map (46) describes the unique Frobenius-equivariant isomorphism $A_n^{\text{dR}}(b_0, x_0) \xrightarrow{\sim} A_n^{\text{dR}}(b, x)$ if $I(\cdot, \cdot)$ is interpreted using Coleman integration.

By taking quotients of the various \mathcal{A}_Z^* by our nice correspondence Z , we get Frobenius operators

$$\phi_Z(b, x) : A_Z^{\text{dR}}(b, x) \rightarrow A_Z^{\text{dR}}(b, x)$$

and a quotient $\mathcal{A}_Z^{\text{rig}}(\bar{b})$ of the universal 2-step object.

Moreover, Theorem 5.24 gives us an isomorphism

$$\Phi_Z : \phi_Z^* \mathcal{A}_Z^{\text{rig}}(\bar{b}) \xrightarrow{\sim} \mathcal{A}_Z^{\text{rig}}(\bar{b}).$$

We have the following equations:

$$\begin{aligned}\phi_Z(b_0, x_0) &= x_0^* \Phi_Z \\ \phi_Z(b, x) &= \tau_{b,x} \circ \phi_Z(b_0, x_0) \circ \tau_{b,x}^{-1}\end{aligned}$$

which is how we compute $\phi_Z(b, x)$.

The connections on $\phi^* \mathcal{A}_Z^{\text{dR}}(b) |_Y$ are described with respect to s_0 and are equal to $d + \Lambda$ (as before) and $d + \Lambda_\phi$ where

$$\Lambda_\phi := - \begin{pmatrix} 0 & 0 & 0 \\ \phi^* \vec{\omega} & 0 & 0 \\ \phi^* \eta & \phi^* \vec{\omega}^T Z & 0 \end{pmatrix}.$$

So to make the Frobenius structure explicit, we need to compute G (which is equal to Φ_Z^{-1} , the inverse of the Frobenius structure) such that $\Lambda_\phi G + dG = G\Lambda$.

Proposition 5.25. *We can take G as follows:*

$$G = \begin{pmatrix} 1 & 0 & 0 \\ \vec{f} & F & 0 \\ h & \vec{g}^T & p \end{pmatrix},$$

where we have

$$\begin{aligned}\phi^* \vec{\omega} &= F \vec{\omega} + d\vec{f} \quad (\text{with } \vec{f}(b_0) = 0) \\ d\vec{g}^T &= d\vec{f}^T Z F \\ dh &= \vec{\omega}^T Z \vec{f} + d\vec{f}^T Z \vec{f} - \vec{g} \omega + \phi^* \eta - \eta \quad (\text{with } h(b_0) = 0).\end{aligned}$$

Algorithm 5.26 (The Frobenius structure on \mathcal{A}_Z).

- (1) Use Tuitman's algorithm (Algorithm 1.52) to compute the matrix²⁰ of Frobenius F and the overconvergent function f such that $\phi^* \vec{\omega} = F \vec{\omega} + d\vec{f}$.
- (2) Compute the matrix $L = I(x, x_0)^+ I(b_0, b)^-$, where we define for any pair $x_1, x_2 \in X(\mathbb{Q}_p)$ the following parallel transport matrices:

$$I^\pm(x_1, x_2) = \begin{pmatrix} 1 & 0 & 0 \\ \int_{x_1}^{x_2} \vec{\omega} & 1 & 0 \\ \int_{x_1}^{x_2} \eta + \int_{x_1}^{x_2} \vec{\omega} + Z \vec{\omega} & \pm \int_{x_1}^{x_2} \vec{\omega}^T Z & 1 \end{pmatrix}.$$

- (3) Solve the p -adic differential equation of Proposition 5.25, then compute

$$M(b_0, x_0) = \begin{pmatrix} 1 & 0 & 0 \\ (I - F)^{-1} \vec{f} & 1 & 0 \\ \frac{1}{1-p} (g^T (I - F)^{-1} \vec{f} + h) & g^T (F - p)^{-1} & 1 \end{pmatrix} (x_0)$$

(using the same notation as in Proposition 5.25).

- (4) Compute the matrix

$$\begin{aligned}s_0^{-1}(b, x) \circ s^\phi(b, x) &= L \cdot M(b_0, x_0) \\ &= \begin{pmatrix} 1 & 0 & 0 \\ \vec{\alpha}_\phi(b, x) & 1 & 0 \\ \gamma(b, x) & \vec{\beta}_\phi(b, x) & 1 \end{pmatrix}.\end{aligned}$$

²⁰In Section 1, this was denoted by M , but we rename it here to F to avoid the clash in notation; likewise f was previously denoted as h .

To summarize, we have described algorithms to compute matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\text{Fil}}(b, x) & \beta_{\text{Fil}}^T(b) & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ \alpha_\phi(b, x) & 1 & 0 \\ \gamma_\phi(b, x) & \beta_\phi^T(b, x) & 1 \end{pmatrix},$$

and the entries are exactly the ingredients for our formula (43) for the local height $h_p(A(x))$.

5.3. Algorithms for quadratic Chabauty. Theorem 5.2 suggests the following method for computing $X(\mathbb{Q}_p)_U$, where $U = U_Z$ is associated to a nice correspondence Z as above.

Algorithm 5.27 (Quadratic Chabauty for rational points).

- (1) Write the function $x \mapsto h_p(A(x))$ as a convergent power series on every residue disk in $X(\mathbb{Q}_p)$.
- (2) Compute the finite set S of possible values of ρ .
- (3) Compute the constants α_i .
- (4) Write the function $x \mapsto \psi_i \circ (\pi_1, \pi_2)(A(x))$ as a convergent power series on every residue disk in $X(\mathbb{Q}_p)$ and solve for its zero set $X(\mathbb{Q}_p)_U$.
- (5) Show that $X(\mathbb{Q}_p)_U \setminus X(\mathbb{Q})_{\text{known}} = \emptyset$.

We have already discussed the first step of Algorithm 5.27. In this section we describe algorithms for the other steps.

Note that we might have to repeat this for several affine patches Y covering X (but see Section 5.4 for a worked example, where we get away with only one affine patch Y). Moreover, we cannot use the algorithm directly for a residue disk D in which Tuitman's lift of Frobenius is not defined. If there are no small rational points in such a disk, then we can try to show that there are none at all using the Mordell-Weil sieve, see Section 5.3.3. Otherwise, we can pick an affine patch such that Frobenius is defined in this disk or we can use a trick described in [BDM⁺19, §5.5], essentially reducing the computation of $h_p(A(x))$ for $x \in D(\mathbb{Q}_p)$ to the computation of Coleman integrals $\int_b^P \omega_i$, where $P \in D(\mathbb{Q})$.

If $\rho(J) > 2$, then we can run the algorithm above for several independent nice correspondences, and we expect that this suffices to prove $X(\mathbb{Q})_{\text{known}} = X(\mathbb{Q})$ (provided this is indeed the case, of course).

Remark 5.28. As suggested by the notation, the set of points cut out by the condition $\rho(x) \in S$ in Theorem 5.2 does not depend on the choices of s or χ (note that we are working over \mathbb{Q} , so χ is well-defined up to a scalar multiple). See [BDM⁺19, Remark 3.12].

5.3.1. Local heights away from p . Let $\ell \neq p$ be prime. We already know that by Theorem 4.3 the function

$$(47) \quad \text{Sel}(U) \rightarrow \mathbb{Q}_p; \quad P \mapsto h_\ell(\tau_\ell(\text{loc}_\ell(P)))$$

takes values in a finite set S_ℓ , and that S_ℓ is trivial when X has potentially good reduction at ℓ . For our intended application, we need to be able to compute S_ℓ . This problem was solved recently by Betts and Dogra.

Lemma 5.29 (Betts–Dogra [BD19b]).

- (1) The functions $j_{U,\ell}$ and (47) are constant on preimages of components of a regular semistable model of X/\mathbb{Q}_ℓ .
- (2) The function (47) and the set S_ℓ can be computed explicitly [BD19b, §12.1].

Betts and Dogra express (47) in terms of harmonic analysis on the reduction graph of X at ℓ in the sense of Zhang [Zha93]. To make this explicit, it is necessary to compute the endomorphism induced by Z on the reduction graph. For interesting examples, such as nice correspondences on modular curves derived from Hecke correspondences, this is often known. An algorithmic version of Lemma 5.29 will appear in [BDM⁺].

The lemma implies, in particular, that S_ℓ is often trivial, even when X does not have potentially good reduction at ℓ . For instance, if $X: y^2 = f(x)$ is hyperelliptic, $\ell > 2$ and the discriminant $\Delta(X)$ satisfies $\text{ord}_\ell(\Delta(X)) = 1$, then this holds.

We give a slightly more elaborate example. This was used in [BBB⁺19, Section 6]; a proof will appear in [BDM⁺].

Example 5.30. Let $N > 2$ be prime and let w_N be the Atkin–Lehner involution on $X_0(N)$. Then the curve $X_0(N)^+ = X_0(N)/w_N$ has good reduction away from N . At N , there is a regular semistable model (over an extension) whose special fiber is a projective line intersecting itself $g(X_0(N)^+)$ times. Therefore the local heights at N are all trivial on $\text{Sel}(U)$, although $X_0(N)^+$ does not have potentially good reduction at N .

5.3.2. Fitting the height pairing. The third step of Algorithm 5.27 consists of writing the height pairing in terms of a given basis $\{\psi_i\}$ of the space $(H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbb{Q}_p}, \Omega^1)^*)^*$ of bilinear pairings on $H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$. This is similar to the computation of an annihilating differential in the classical method of Chabauty–Coleman. In order to do so, we need to pick a basis $\{\psi_i\}$ and we need to evaluate ψ_i and the height pairing on sufficiently many elements to determine it. Since the height pairing is symmetric by construction, we can restrict to symmetric bilinear pairings.

One source of elements of $H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ comes from representations $A(x)$ for rational points $x \in X(\mathbb{Q})$. The advantage is that we already know how to compute $h(A(x))$ for these. So if we have sufficiently many $x \in X(\mathbb{Q})$ so that we can generate $H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ using the elements

$$\pi_1(A(x)) \otimes \pi_2(A(x)) = \log([x - b]) \otimes (E_Z(\log([x - b])) + c_Z),$$

(see (42) and the discussion preceding it) then we can compute the coefficients of h in terms of the dual basis $\{\psi_i\}$. Computationally, we can read off $\pi_i(A(x))$ from our explicit description of the Hodge filtration and Frobenius structure on $A(x)$. Namely, for $x \in Y(\mathbb{Q})$, we have

$$(48) \quad \pi_1(A(x)) \otimes \pi_2(A(x)) = \alpha_\phi(b, x)^\top \cdot \begin{pmatrix} I_g \\ 0_g \end{pmatrix} \otimes \beta_\phi^\top(b, x) - \beta_{\text{Fil}}^\top(b) \cdot \begin{pmatrix} 0_g \\ I_g \end{pmatrix}.$$

The required number of rational points can be decreased by working with $\text{End}_0(J)$ -equivariant heights. If the splitting s of the Hodge filtration on V_{dR} commutes with the endomorphisms on J , then h is $\text{End}_0(J)$ -equivariant. Hence we determine h in terms of a basis of

$$(H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes_{\text{End}_0(J) \otimes \mathbb{Q}_p} H^0(X_{\mathbb{Q}_p}, \Omega^1)^*)^*.$$

We still need (at least) $g + 1$ rational points on X .

Example 5.31. Let $X = X_{S_4}(13)$ be the modular curve associated to the pullback of $S_4 \subset \text{PGL}_2(\mathbb{F}_{13})$ to $\text{GL}_2(\mathbb{F}_{13})$, as studied by Banwait–Cremona [BC14]. Then $g = r = \rho(J) = 3$, and there are 4 obvious rational points on X . In [BDM⁺] we apply the method just discussed and a nice correspondence constructed from the action of the Hecke operator T_{23} on $H^1_{\text{dR}}(X_{\mathbb{Q}_{23}})$ to determine the equivariant 23-adic height pairing using

$$\log([x - b]) \otimes E_Z(\log([x - b])) + c_Z$$

for the known rational points $x \in X(\mathbb{Q})$. Applying Algorithm 5.27, we prove that indeed $\#X(\mathbb{Q}) = 4$.

Remark 5.32. If p is ordinary and s is the unit root splitting, then the height is equivariant.

However, even if we use equivariant heights, it is often the case that we do not have enough rational points on X for this approach. Instead, we can use the fact that the construction of Coleman–Gross and Nekovář result in the same height, see Remark 3.6. We can then determine the height pairing in terms of a basis of bilinear pairings on $J(\mathbb{Q}) \otimes \mathbb{Q}_p \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ given by products of single integrals as in Section 2.3. In other words, we use the approach already employed in the first step of Algorithm 2.31, computing the heights of pairs of divisors on X of degree 0 with disjoint support via the Coleman–Gross construction as discussed there. This approach is currently restricted to hyperelliptic curves having an odd degree model at p .

5.3.3. The Mordell–Weil sieve. We briefly review the Mordell–Weil sieve. The original idea is due to Scharaschkin [Sch99], see [BS10] for an implementation-oriented account. Let $M > 1$ be an integer, let S be a finite set of primes of good reduction for X and consider the commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q})/MJ(\mathbb{Q}) \\ \downarrow & & \downarrow \alpha_S \\ \prod_{v \in S} X(\mathbb{F}_v) & \xrightarrow{\beta_S} & \prod_{v \in S} J(\mathbb{F}_v)/MJ(\mathbb{F}_v). \end{array}$$

Commutativity gives us a way to exclude the existence of rational points satisfying certain local conditions, by choosing the set S and the integer M carefully. When $X(\mathbb{Q})$ is empty, heuristics due to Poonen [Poo06] predict that there should always be a choice of S and M so that the images of α_S and β_S do not intersect.

We can use the Mordell–Weil sieve to show that for a fixed prime p , a given residue class in $X(\mathbb{Q}_p)$ does not contain a rational point. For this application we choose $M = M' \cdot p$ for some auxiliary integer M' and we choose S to be a set containing the prime divisors q of pM' , and additional primes ℓ so that $\gcd(\#J(\mathbb{F}_\ell), \#J(\mathbb{F}_q))$ is large for some of these q .

In our setting, we can also apply this method as follows: Suppose we have a point $P \in X(\mathbb{Q}_p)_U$, computed to finite precision p^N , and we want to show that it does not come from a rational point. Assume that it does, so there are integers a_1, \dots, a_g such that

$$[P - b] = a_1 P_1 + \dots + a_g P_g,$$

where P_1, \dots, P_g generate $J(\mathbb{Q}) \otimes \mathbb{Q}$. We can compute (for instance using linearity of single Coleman integrals), $(\tilde{a}_1, \dots, \tilde{a}_g) \in \mathbb{Z}/p^N\mathbb{Z}$ so that $a_i \equiv \tilde{a}_i \pmod{p^N}$ for all $i \in \{1, \dots, g\}$. We can then use the Mordell–Weil sieve to show that the corresponding coset of $p^N J(\mathbb{Q})$ does not contain the image of a rational point on X . We can also apply quadratic Chabauty with several primes p or choose $M = p^n M'$, where M' is a small auxiliary integers as above. For more details on the combination of quadratic Chabauty and the Mordell–Weil sieve see [BBM17] and [BBB⁺19, §6.7].

5.4. An example. Let N be a positive integer and consider the Atkin–Lehner involution w_N . Then the quotient

$$X_0(N)^+ := X_0(N)/w_N$$

is a nice curve whose non-cuspidal points classify unordered pairs $\{E_1, E_2\}$ of elliptic curves admitting an N -isogeny between them.

In this section we illustrate the quadratic Chabauty method by computing the rational points on $X := X_0(167)^+$. It was shown by Galbraith [Gal96] that X has genus 2 and that

$$y^2 = x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$$

is a model for X . There are four small rational points on X , namely the two points at infinity and $(1, \pm 1)$. For reasons explained below, we prefer a model without rational points at infinity, so we instead use the model

$$(49) \quad X: y^2 = -3x^6 + 2x^5 - 3x^4 - 2x^3 + 2x^2 - 4x + 1$$

with small rational points $(0, \pm 1)$ and $(-1, \pm 1)$. The Jacobian $J = J_0(167)^+$ of X is geometrically irreducible. It has real multiplication, so the Picard number is 2. Using **Magma**, we compute that the rank of $J(\mathbb{Q})$ is also 2. We can do this in two different ways:

- via a 2-descent on J ;
- by computing that analytic rank of the unique (up to conjugation) newform of level 167 and weight 2 invariant under w_{167} is equal to 1; we may conclude $\text{rk}(J(\mathbb{Q})) = 2$ by the work of Gross–Zagier and Kolyvagin–Logachev.

We fix the prime $p = 7$ of good ordinary reduction. Then the logarithm gives an isomorphism $J(\mathbb{Q}) \otimes \mathbb{Q}_7 \rightarrow H^0(X_{\mathbb{Q}_7}, \Omega_1)^*$. According to Theorem 5.2, all requirements for quadratic Chabauty are satisfied, and we may follow Algorithm 5.27 to compute a finite set of 7-adic points containing $X(\mathbb{Q})$.

5.4.1. Step (1): Expand $h_7(A(x))$. The most involved step is the computation (and expansion) of the local height $h_7(A(x))$ for a nice correspondence Z via the explicit formula (43). See [BBB⁺19, Section 6] for a more detailed description of the analogous computation for $X_0(67)^+$. We fix the unit root splitting s of the Hodge filtration and the standard idèle class character χ having $\chi_7 = \log_7$, the Iwasawa branch of the 7-adic log.

We first find a symplectic basis of $H_{\text{dR}}^1(X/\mathbb{Q}_7)$, given by

$$\omega_0 = -\frac{dx}{y}, \quad \omega_1 = (-1-x)\frac{dx}{y}, \quad \omega_2 = \frac{1}{6}x^2(1-x+2x^2)\frac{dx}{y}, \quad \omega_3 = \frac{1}{18}(-1-x^2+4x^3)\frac{dx}{y},$$

constructed so that the cup product is the standard symplectic form with respect to $(\omega_0, \dots, \omega_3)$. Our subsequent computations will be in terms of this basis. Via Tuitman’s algorithm (Algorithm 1.52), we determine the matrix Φ_7 of Frobenius on $H_{\text{dR}}^1(X/\mathbb{Q}_7)$. Eichler–Shimura ²¹ then allows us to compute the matrix representing the Hecke operator on $H_{\text{dR}}^1(X/\mathbb{Q}_7)$:

$$T_7 = \Phi_7^{\mathbf{T}} + 7 \cdot (\Phi_7^{\mathbf{T}})^{-1} = \begin{pmatrix} -1 & 1/2 & 0 & -1/12 \\ 1/2 & -3/2 & 1/12 & 0 \\ 0 & 0 & -1 & 1/2 \\ 0 & 0 & 1/2 & -3/2 \end{pmatrix}.$$

From this we obtain the following matrix representing the endomorphism on $H_{\text{dR}}^1(X/\mathbb{Q}_7)$ corresponding to a nice correspondence

$$Z = (\text{Tr}(T_7) \cdot I_4 - 4T_7)C^{-1} = \begin{pmatrix} 0 & -1/3 & -1 & -2 \\ 1/3 & 0 & -2 & 1 \\ 1 & 2 & 0 & 0 \\ 2 & -1 & 0 & 0 \end{pmatrix},$$

where C is the matrix of the cup product on our basis $\{\omega_i\}$.

²¹There are of course other methods for the computation of Hecke operators, but we have to compute Φ_7 anyway, so we might as well use it.

The next step is the computation of the Hodge filtration (see Section 5.2.1). We use the base point $b = (-1, -1)$ and the affine patch Y cut out by our defining equation (49), so we only need a single differential ω_4 of the third kind, having a pole of order 1 at the two points at infinity. Since X is hyperelliptic, we have that η and β_{Fil} are trivial by Remark 5.22. Applying Algorithm 5.21, we find $\gamma_{\text{Fil}} = 2x + 2$.

We compute the Frobenius structure based on the matrix Φ_7 as discussed in 5.2.2. Equation (43) then allows us to expand the function $x \mapsto h_7(A(x))$ into a 7-adic power series on those residue disks of $X(\mathbb{Q}_7)$ where our lift of Frobenius is defined.

5.4.2. Step (2): Find the possible values of ρ . This step requires us to find the possible values of $h_\ell(A(x))$ for $\ell \neq 7$ and $x \in X(\mathbb{Q}_\ell)$. Fortunately these are all trivial by Example 5.30.

5.4.3. Step (3): Determine the height pairing as a bilinear pairing. Since $X(\mathbb{Q})$ consists of two pairs of points swapped by the hyperelliptic involution, we do not have enough rational points on X to determine the height pairing as a bilinear pairing using only 7-adic heights of the form $h(A(x))$ for $x \in X(\mathbb{Q})$, even taking $\text{End}_0(J)$ -equivariance into account. Instead we determine the height pairing between points in $J(\mathbb{Q})$ via the Coleman–Gross construction.

A basis of $J(\mathbb{Q})$ is given by the points with Mumford representation $P = (x^2 - x + 1, x - 1)$ and $Q = (x^2, -2x + 1)$; this can be computed using the methods²² of [Sto02, MS16].

For our computations, we use the following representatives

$$\begin{aligned} D_1 &= D_0 - \text{div}_0(x - 4), & D'_1 &= \text{div}_0(x - 6) - D'_0 \\ D_2 &= 2(0, 1) - \text{div}_0(x - 6), & D'_2 &= \text{div}_0(x - 4) - 2(0, -1), \end{aligned}$$

where D_0 (resp. D'_0) is the divisor cut out by $x^2 + x + 1$ and $y - (x - 1)$ (resp. $y - (1 - x)$). Then we can compute the local height pairings $h_v(D_1, D_2)$ and $h_v(D_i, D'_i)$ for $i = 1, 2$, noting that their base changes to $X(\mathbb{Q}_7)$ split as sums of \mathbb{Q}_7 -rational points.

The model (49) is regular outside 2. While the curve X has good reduction at 2, the model (49) does not (the reduction modulo 2 is not reduced), but a regular model can be found easily. Using **Magma**, we find

$$\begin{aligned} \sum_{\ell \neq p} h_\ell(D_1, D'_1) &= 2\log 2 - \log 13 - \log 31, \\ \sum_{\ell \neq p} h_\ell(D_1, D_2) &= 2\log 2 - \log 31, \\ \sum_{\ell \neq p} h_\ell(D_2, D'_2) &= -4\log 2 - 2\log 3. \end{aligned}$$

In order to compute the local height pairings at 7, we move the unique Weierstrass point in $X(\mathbb{Q}_7)$ to infinity and work with the corresponding odd degree model of X over \mathbb{Q}_7 as required by our current **Sage**-implementation. Algorithm 2.22 gives

$$\begin{aligned} h_7(D_1, D'_1) &= 3 \cdot 7 + 6 \cdot 7^2 + 7^4 + 6 \cdot 7^5 + 5 \cdot 7^6 + 3 \cdot 7^7 + 3 \cdot 7^8 + 2 \cdot 7^9 + O(7^{10}) \\ h_7(D_1, D_2) &= 4 \cdot 7 + 6 \cdot 7^2 + 4 \cdot 7^3 + 5 \cdot 7^4 + 5 \cdot 7^5 + 7^6 + 5 \cdot 7^7 + 2 \cdot 7^8 + 3 \cdot 7^9 + O(7^{10}) \\ h_7(D_2, D'_2) &= 2 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + 5 \cdot 7^4 + 5 \cdot 7^5 + 4 \cdot 7^6 + 4 \cdot 7^7 + 7^8 + 5 \cdot 7^9 + O(7^{10}). \end{aligned}$$

²²Strictly speaking, a basis of a finite index subgroup is enough, as long as we can show that a given prime does not divide the index.

As described in step (1) of Algorithm 2.31, we can now express the height h in terms of products of single integrals with coefficients

$$\begin{aligned}\alpha_{00} &= 5 \cdot 7^{-1} + 4 + 4 \cdot 7 + 4 \cdot 7^2 + 2 \cdot 7^4 + 2 \cdot 7^5 + 7^6 + 2 \cdot 7^7 + 3 \cdot 7^9 + O(7^{10}) \\ \alpha_{01} &= 5 \cdot 7^{-1} + 5 + 6 \cdot 7 + 2 \cdot 7^2 + 4 \cdot 7^3 + 6 \cdot 7^4 + 4 \cdot 7^5 + 4 \cdot 7^6 + 5 \cdot 7^7 + 2 \cdot 7^8 + 6 \cdot 7^9 + O(7^{10}) \\ \alpha_{11} &= 6 \cdot 7^{-1} + 1 + 7 + 3 \cdot 7^2 + 5 \cdot 7^3 + 5 \cdot 7^4 + 6 \cdot 7^5 + 5 \cdot 7^6 + 2 \cdot 7^7 + 2 \cdot 7^8 + 3 \cdot 7^9 + O(7^{10}).\end{aligned}$$

Hence we obtain our desired function

$$\rho: X(\mathbb{Q}_7) \rightarrow \mathbb{Q}_7$$

as in Theorem 5.2. We find that it indeed vanishes on the four known rational points; we also see that it has the additional zeros

$$\begin{aligned}&(2 \cdot 7 + 6 \cdot 7^2 + 7^3 + 7^4 + 2 \cdot 7^5 + O(7^6), \pm(1 + 3 \cdot 7 + 4 \cdot 7^2 + 3 \cdot 7^3 + 5 \cdot 7^4 + 4 \cdot 7^5 + O(7^6))) \\ &(6 + 6 \cdot 7 + 2 \cdot 7^2 + 3 \cdot 7^3 + 3 \cdot 7^4 + 7^5 + O(7^6), \pm(6 + 6 \cdot 7 + 2 \cdot 7^2 + 4 \cdot 7^3 + 2 \cdot 7^4 + 2 \cdot 7^5 + O(7^6))) \\ &(5 + 2 \cdot 7 + 4 \cdot 7^2 + 6 \cdot 7^3 + 7^5 + O(7^6), \pm(4 + 2 \cdot 7 + 6 \cdot 7^2 + 7^3 + 2 \cdot 7^4 + 2 \cdot 7^5 + O(7^6))) \\ &(5 + 4 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + 3 \cdot 7^4 + 7^5 + O(7^6), \pm(4 + 5 \cdot 7 + 2 \cdot 7^2 + 4 \cdot 7^3 + 2 \cdot 7^5 + O(7^6))).\end{aligned}$$

This means that we have computed $X(\mathbb{Q}_7)_U \cap Y(\mathbb{Q}_7) \setminus D_{\text{bad}}$, where D_{bad} is the residue disk of the unique Weierstrass point $(1, 0) \in X(\mathbb{F}_7)$ (where our Frobenius lift is not defined). Since the Picard number is 2, we cannot show that these do not come from a rational point using an additional nice correspondence, see Remark 5.6. Instead we apply the Mordell-Weil sieve with the auxiliary integer 95 and the primes $v \in \{3, 5, 19, 31\}$, noting that

$$\#J(\mathbb{F}_3) = 19, \quad \#J(\mathbb{F}_5) = 7^2, \quad \#J(\mathbb{F}_{19}) = 2^2 \cdot 5 \cdot 19, \quad \#J(\mathbb{F}_{31}) = 2^2 \cdot 11 \cdot 19.$$

So now we have shown that $X_0(167)^+$ consists only of the four known rational points – almost. We still have to deal with the disks at infinity and the disk D_{bad} . But since we do not expect any rational points in these disks, we can use the Mordell-Weil sieve to prove this. Since $J(\mathbb{F}_7) \cong \mathbb{Z}/109\mathbb{Z}$, we need primes v such that $109 \mid \#J(\mathbb{F}_v)$, which does not happen too often and makes the computation quite involved²³. But using the auxiliary integer 60, we finally succeed in proving that none of these disks contain a rational point. Comparing with [Gal96, Table 7], we obtain the following:

Theorem 5.33. *There are exactly four rational points on $X_0(167)^+$, and they are all cusps or CM-points.*

For $N = 67, 73, 103$ the rational points on $X_0(N)^+$ were computed in [BBB⁺19]; these all have genus 2. In [BDM⁺] we compute the rational points for all other prime values of N such that $X_0(N)^+$ has genus 2 or 3. See [BGX19] for recent results on the rational points on $X_0(N)^+$ for several composite squarefree values of N such that $X_0(N)^+$ has genus 2, based on a combination of elliptic curve Chabauty with covering techniques.

Project 5.34 (Quadratic Chabauty on modular curves $X_0(N)^+$). Galbraith [Gal96, Gal99, Gal02] has constructed models for all modular curves $X_0(N)^+ = X_0(N)/w_N$ of genus ≤ 5 (with the exception of $N = 263$) and has conjectured that he has found all exceptional points on these curves. This project will use quadratic Chabauty to prove as much as possible about Galbraith’s conjecture. Another goal is to investigate whether we can use p -adic Gross-Zagier to carry out quadratic Chabauty for $X_0(N)^+$, starting with the case of such curves of genus 2.

²³We end up using 5-digit primes.

5.5. Future directions. So far, all curves whose rational points have been computed using quadratic Chabauty are either bielliptic of genus 2 ([BD18a, BD18b, EL19]) or modular [BDM⁺19, BBB⁺19, BDM⁺]. For instance, in joint work [BDM⁺19] with Dogra, Tuitman and Vonk we use quadratic Chabauty to compute the rational points on the non-split Cartan modular curve $X_{\text{ns}}^+(13)$ (or the split Cartan curve of the same level, which is isomorphic to it).

It would be interesting to extend the practical scope of the method. As a first step, one could consider (modular) curves satisfying $r = g$ whose Jacobians have complex multiplication. Possible examples include twisted Fermat curves $ax^m + by^m + cz^m$ or van Wamelen's list of genus 2 curves whose Jacobians have CM and are simple [vW99].

Also note that [BD18a] contains a general recipe for quadratic Chabauty when the quadratic Chabauty condition is satisfied, but $r > g$. This has not been used in practice yet. More generally, the Bloch–Kato conjecture predicts that quadratic Chabauty should be applicable when $r < g^2$, without any assumptions on ρ (see [BD18b]), and it would be very interesting to make this explicit.

Acknowledgements. We are very grateful to Francesca Bianchi, Stephanie Chan, Netan Dogra, and Enis Kaya for detailed feedback on an earlier draft of these notes. Additionally, special thanks are due to the participants of the Boston University fall 2019 course MA 841: Oana Adascalitei, Alex Best, María Inés de Frutos Fernández, Stevan Gajović, Sachi Hashimoto, Aashraya Jha, Wanlin Li, Ricky Magner, Angus McAndrew, John Sim, Yifan Wu, and Susan Ye. JB was partially supported by NSF grant DMS-1702196, the Clare Boothe Luce Professorship (Henry Luce Foundation), Simons Foundation grant #550023, and a Sloan Research Fellowship. SM was supported by an NWO VIDI grant.

APPENDIX A. SOME NONABELIAN COHOMOLOGY

We collect some results on nonabelian cohomology, closely following Serre [Ser02, §I.5].

Let G be a profinite group. Consider the category of G -sets: an object E in this category is a discrete topological space on which G acts continuously, and a morphism between G -sets E_1 and E_2 is a map $f : E_1 \rightarrow E_2$ that commutes with the action of G . If $s \in G$ and $x \in E$, the image of x under s will be denoted by sx . A G -group A is a group in the category of G -sets. This means that A is a G -set, with a group structure that is invariant under G , so that ${}^s(xy) = {}^sx {}^sy$. (Note that when A is commutative, one gets a G -module.)

If E is a G -set, we let

$$H^0(G, E) = E^G,$$

the set of elements of E fixed by G . If E is a G -group, $H^0(G, E)$ is a group. If A is a G -group, a 1-cocycle of G in A is a map $s \mapsto a_s$ of G to A that is continuous and such that $a_{st} = a_s {}^s a_t$ for $s, t \in G$. We denote the set of these cycles as $Z^1(G, A)$. Two cocycles a and a' are cohomologous if there exists $b \in A$ such that $a'_s = b^{-1} a_s {}^s b$. This is an equivalence relation \sim in $Z^1(G, A)$, and the quotient set is denoted as

$$H^1(G, A) = Z^1(G, A) / \sim.$$

We now give another useful interpretation of $H^1(G, A)$ for a G -group A . We say that A acts on the left on a G -set E if it acts on E in the usual way and if ${}^s(a \cdot x) = {}^s a \cdot {}^s x$ for $a \in A, x \in E$. An action on the right is defined analogously. A G -equivariant (left²⁴) A -torsor is a non-empty G -set P , on which A acts on the left, so that for each pair $x, y \in P$, there exists a unique $a \in A$ such that $y = a \cdot x$. We have the following:

²⁴Right A -torsors are defined analogously.

Proposition A.1 ([Ser02, Prop. 33]). *Let A be a G -group. There is a bijection between the equivalence classes of G -equivariant A -torsors and the set $H^1(G, A)$.*

Note that while $H^0(G, A)$ is a group, $H^1(G, A)$ is merely a *pointed set* when G is non-abelian: it has no group structure, but a distinguished element, given by the class of the unit cocycle. Moreover, the association $A \mapsto H^i(G, A)$ is functorial for $i = 0, 1$. We can talk about exact sequences of pointed sets (where the image of a map is the inverse image of the neutral element). For instance, we get the following important result:

Proposition A.2 (Six-term exact sequence in non-abelian cohomology [Ser02, Prop. 38]). *Let*

$$1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$$

be a short exact sequence of G -groups. The following sequence of pointed sets:

$$1 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C) \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C)$$

is exact.

However, some desirable features are lacking: for instance, injectivity does not follow from having a trivial kernel. More generally, we would like to determine fibers of maps between pointed sets $H^1(G, A) \rightarrow H^1(G, B)$. Serre's twisting construction, motivated by the theory of fiber bundles, and described below, makes it possible to turn fibers into kernels.

There are analogous constructions when G and A are topological groups, and G acts continuously on A . Considering continuous cocycles and continuous G -equivariant A -torsors yields the continuous cohomology set $H^1(G, A)$, and the results of [Ser02, §I.5.3] remain valid. Henceforth, we shall assume that we are in this setting, and we shall mostly omit the word “continuous”.

A.1. The twisting construction. Let G be a topological group, let A be a topological group with a continuous G -action, and let P be a continuous G -equivariant A -torsor. Let F be a G -set on which A acts on the right. We form the twist of F by P as follows: consider the equivalence relation that identifies an element (f, p) with $(a \cdot p, fa^{-1})$, for $a \in A$. This relation is compatible with the action of G , and the quotient $F \times_A P$ is a G -set. An element of $F \times_A P$ can be written as $f \cdot p$ for $p \in P, f \in F$, and one has $f(ap) = (fa)p$. Note that for all $p \in P$, the map $f \mapsto f \cdot p$ is a bijection of F onto $F \times_A P$. For this reason, one says that $F \times_A P$ is obtained from F by twisting it using P . This construction gives P the structure of a G -equivariant $F \times_A P$ -torsor. We write $A^{(P)} := A \times_A P$, where A acts on itself by conjugation. This construction is easily seen to be functorial in A .

Proposition A.3 ([Ser02, Prop. 35]). *Let P be a G -equivariant A -torsor. Then there is a bijection $H^1(G, A) \rightarrow H^1(G, A^{(P)})$, mapping the class of P in $H^1(G, A)$ to the neutral element of $H^1(G, A^{(P)})$.*

So if we have a map $H^1(G, A) \rightarrow H^1(G, B)$ of pointed sets, coming from a G -group homomorphism $A \rightarrow B$, and we want to determine the fiber above the image of some G -equivariant A -torsor P , then we can do this using the induced diagram

$$\begin{array}{ccc} H^1(G, A) & \longrightarrow & H^1(G, A^{(P)}) \\ \downarrow & & \downarrow \\ H^1(G, B) & \longrightarrow & H^1(G, B^{(P \times_A B)}) \end{array}$$

which commutes due to functoriality of the twisting construction [Ser02, §5.4]. This approach is used in [Ser02, §I.5.5] to determine information about images and fibers of the maps in the six-term exact sequence in Proposition A.2.

Remark A.4. We record some additional useful properties of the twisting construction:

- (1) Alternatively, the twisting construction can also be described in terms of cocycles, see [Ser02, §I.5.3] and [Bet, §4.0.1].
- (2) If $H^1(G, A)$ and $H^1(G, A^{(P)})$ are representable by schemes, then the twisting bijection in Proposition A.3 is an isomorphism of schemes.
- (3) If v is a prime and U/\mathbb{Q}_v is the representation of the absolute Galois group G_p of \mathbb{Q}_p on a finitely generated pro-unipotent group in the sense of [Bet, Section 4], then we can describe $H^1(G_p, U(Q_v))$ via finite-dimensional G_p -equivariant quotients: Writing $U = \varprojlim U_n$ as an inverse limit of such quotients, we have a natural bijection

$$H^1(G_p, U(\mathbb{Q}_v)) = \varprojlim H^1(G_p, U_n(\mathbb{Q}_v)).$$

In particular, this includes pro-unipotent fundamental groups, such as the ones considered by Kim.

REFERENCES

- [And03] Yves André. Period mappings and differential equations. *From \mathbf{C} to \mathbf{C}_p , MSJ Memoirs*, 12, 2003. ↑3.1.
- [Bal] J.S. Balakrishnan. Sage code. <https://github.com/jbalakrishnan/AWS>. ↑1.65, 2.24.
- [Bal13] J.S. Balakrishnan. Iterated Coleman integration for hyperelliptic curves. In E. W. Howe and K. S. Kedlaya, editors, *ANTS-X: Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Series*, pages 41–61. Mathematical Sciences Publishers, 2013. ↑1.5, 1.63, 1.64.
- [Bal15] J.S. Balakrishnan. Coleman integration for even-degree models of hyperelliptic curves. *LMS J. Comput. Math.*, 18(1):258–265, 2015. ↑1.5, 1.63, 1.64.
- [BB12] J.S. Balakrishnan and A. Besser. Computing local p -adic height pairings on hyperelliptic curves. *IMRN*, 2012(11):2405–2444, 2012. ↑1.40, 2.2.1, 2.20, 2.22, 2.23.
- [BB15] Jennifer S. Balakrishnan and Amnon Besser. Coleman–Gross height pairings and the p -adic sigma function. *Journal für die reine und angewandte Mathematik (Crelle’s Journal)*, 2015(698):89–104, 2015. ↑2.1, 2.27.
- [BB19] J.S. Balakrishnan and A. Besser. Errata for “Computing local p -adic height pairings on hyperelliptic curves”. http://math.bu.edu/people/jbala/cg_heights_errata.pdf, 2019. ↑2.2.1.
- [BBB+19] Jennifer S. Balakrishnan, Alex J. Best, Francesca Bianchi, Brian Lawrence, J. Steffen Müller, Nicholas Triantafillou, and Jan Vonk. Two recent p -adic approaches towards the (effective) Mordell conjecture. <https://arxiv.org/abs/1910.12755>, 2019. ↑1.1, 4.21, 5.3.1, 5.3.3, 5.4.1, 5.4.3, 5.5.
- [BBBM19] Jennifer S. Balakrishnan, Francesca Bianchi, Amnon Besser, and J. Steffen Müller. Explicit quadratic Chabauty over number fields. <https://arxiv.org/abs/1910.04653>, 2019. ↑2.3.
- [BBK10] J.S. Balakrishnan, R. W. Bradshaw, and K. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010. ↑1.3, 1.3, 1.36, 1.39, 1.40.
- [BBM16] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Quadratic Chabauty: p -adic heights and integral points on hyperelliptic curves. *Journal für die reine und angewandte Mathematik (Crelle’s Journal)*, 2016(720):51–79, 2016. ↑2.28, 2.29.
- [BBM17] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Math. Comp.*, 86:1403–1434, 2017. ↑2.24, 2.3, 2.33, 5.3.3.
- [BC94] Francesco Baldassarri and Bruno Chiarellotto. Algebraic versus rigid cohomology with logarithmic coefficients. In *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, volume 15 of *Perspect. Math.*, pages 11–50. Academic Press, San Diego, CA, 1994. ↑1.3.
- [BC09] O. Brinon and B. Conrad. CMI summer school notes on p -adic Hodge theory. 2009. ↑3.1.
- [BC14] Barinder S. Banwait and John E. Cremona. Tetrahedral elliptic curves and the local-global principle for isogenies. *Algebra Number Theory*, 8(5):1201–1229, 2014. ↑5.31.
- [BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24(3-4):235–265, 1997. ↑1.
- [BD18a] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points I: p -adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. ↑3.2, 3.2, 4.1, 4.4, 4.12, 4.5, 4.6, 5.2, 5.5, 5.6, 5.1, 5.1, 5.5.

- [BD18b] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *IMRN, to appear*, 2018. <https://arxiv.org/abs/1705.00401>. ↑3.2, 4.2, 4.6, 5, 5.1, 5.1, 5.1, 5.2, 5.22, 5.5.
- [BD19a] Jennifer S. Balakrishnan and Netan Dogra. An effective Chabauty-Kim theorem. *Compos. Math.*, 155(6):1057–1075, 2019. ↑5.7.
- [BD19b] L. Alexander Betts and Netan Dogra. Ramification of étale path torsors and harmonic analysis on graphs, Sep 2019. <https://arxiv.org/abs/1909.05734>. ↑5.29, 2.
- [BDCKW18] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. *Math. Ann.*, 372(1-2):369–428, 2018. ↑4.6, 5.1.
- [BDM⁺] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Quadratic Chabauty for modular curves: Algorithms and examples. in progress. ↑5.3.1, 5.31, 5.4.3, 5.5.
- [BDM⁺19] J.S. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3), 2019. ↑3.2, 3.3, 3.3.1, 3.7, 4.2, 4.4, 4.19, 5.1, 5.2, 5.13, 5.2, 5.2, 5.2.1, 5.19, 5.20, 5.2.2, 5.2.2, 5.3, 5.28, 5.5.
- [Bel09] J. Bellaïche. CMI summer school notes on an introduction to the conjecture of Bloch-Kato. 2009. ↑3.1, 3.2, 3.3.
- [Ber75] Daniel Bertrand. Valeurs algébriques de fonctions méromorphes. In *Séminaire Delange-Pisot-Poitou, 15e année (1973/74), Théorie des nombres, Fasc. 1, Exp. No. 21*, page 6. 1975. ↑2.1.
- [Ber81] Dominique Bernardi. Hauteur p -adique sur les courbes elliptiques. In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 1–14. Birkhäuser, Boston, Mass., 1981. ↑2.
- [Ber97] Pierre Berthelot. Finitude et pureté cohomologique en cohomologie rigide. *Invent. Math.*, 128(2):329–377, 1997. With an appendix in English by Aise Johan de Jong. ↑1.3.
- [Ber04] Laurent Berger. An introduction to the theory of p -adic representations. *Geometric aspects of Dwork theory*, 1:255–292, 2004. ↑3.1.
- [Ber07] Vladimir G. Berkovich. *Integration of one-forms on p -adic analytic spaces*, volume 162 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2007. ↑1.11.
- [Bes02] Amnon Besser. Coleman integration using the Tannakian formalism. *Math. Ann.*, 322(1):19–48, 2002. ↑1.11, 1.5, 5.2.2.
- [Bes04] Amnon Besser. The p -adic height pairings of Coleman-Gross and of Nekovář. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 13–25. Amer. Math. Soc., Providence, RI, 2004. ↑3.6.
- [Bes05] Amnon Besser. p -adic Arakelov theory. *J. Number Theory*, 111(2):318–371, 2005. ↑2.2.1, 5.5.
- [Bes12] Amnon Besser. Heidelberg lectures on Coleman integration. In J. Stix, editor, *The arithmetic of fundamental groups—PIA 2010*, volume 2 of *Contrib. Math. Comput. Sci.*, pages 3–52. Springer, Heidelberg, 2012. ↑1.11, 1.6.
- [Bes17] Amnon Besser. p -adic heights and Vologodsky integration. <https://arxiv.org/abs/1711.06957>, 2017. ↑2.26.
- [Bes19] Alex J. Best. Explicit Coleman integration in larger characteristic. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 85–102. Math. Sci. Publ., Berkeley, CA, 2019. ↑1.41.
- [Bes20] Alex J. Best. Square root time Coleman integration on superelliptic curves. <https://alexjbest.github.io/papers/coleman-superelliptic.pdf>, 2020. ↑1.41.
- [Bet] L. Alexander Betts. The motivic anabelian geometry of local heights on abelian varieties. <https://arxiv.org/abs/1706.04850>. ↑4.21, 1, 3.
- [BGJGP05] Matthew H Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. Finiteness results for modular curves of genus at least 2. *American Journal of Mathematics*, 127(6):1325–1387, 2005. ↑2.24.
- [BGR84] S. Bosch, U. Güntzer, and R. Remmert. *Non-Archimedean analysis*, volume 261 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1984. A systematic approach to rigid analytic geometry. ↑1.2.
- [BGX19] Francesc Bars, Josep González, and Xavier Xarles. Hyperelliptic parametrizations of \mathbb{Q} -curves. 2019. <https://arxiv.org/abs/1910.10545>. ↑5.4.3.
- [Bia19a] Francesca Bianchi. Quadratic Chabauty for (bi)elliptic curves and Kim’s conjecture. arXiv:1904.04622, 2019. ↑4.1, 4.7.
- [Bia19b] Francesca Bianchi. Topics in the theory of p -adic heights on elliptic curves. *Oxford DPhil thesis*, 2019. ↑2.10.

- [BK90] Spencer Bloch and Kazuya Kato. L -functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990. [†3.3.2, 4.2, 4.6](#).
- [BKK11] Jennifer S. Balakrishnan, Kiran S. kedlaya, and Minhyong Kim. Appendix and erratum to “Massey products for elliptic curves of rank 1”. *J. Amer. Math. Soc.*, 24(1):281–291, 2011. [↑1.67](#).
- [Bom90] Enrico Bombieri. The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 17(4):615–640, 1990. [↑1.1](#).
- [BS10] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010. [↑6, 5.3.3](#).
- [BTa] Jennifer S. Balakrishnan and Jan Tuitman. Explicit Coleman integration for curves. <https://arxiv.org/abs/1710.01673>. [↑1.4, 1.53, 1.55, 1.56](#).
- [BTb] J. S. Balakrishnan and J. Tuitman. Magma code. <https://github.com/jtuitman/Coleman>. [↑1.22, 1.56, 1.57, 1.58](#).
- [BZ17] Amnon Besser and Sarah Livia Zerbes. Vologodsky integration on curves with semi-stable reduction, 2017. <https://arxiv.org/abs/1711.06950>. [↑1.15](#).
- [CdS88] Robert Coleman and Ehud de Shalit. p -adic regulators on curves and special values of p -adic L -functions. *Invent. Math.*, 93(2):239–266, 1988. [↑1.10, 1.5](#).
- [CDV06] W. Castryck, J. Denef, and F. Vercauteren. Computing zeta functions of nondegenerate curves. *IMRP Int. Math. Res. Pap.*, pages Art. ID 72017, 57, 2006. [↑1.4](#).
- [CG89] Robert F. Coleman and Benedict H. Gross. p -adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, MA, 1989. [↑2, 2.13, 2.2.1, 2.2.1](#).
- [Cha16] S. Chan. Topics in the theory of zeta functions of curves. *Oxford MMath thesis*, 2016. https://www.ucl.ac.uk/~ucahytc/chan_dissertation.pdf. [↑1.32, 1.34, 1.35](#).
- [Che71] Kuo-tsai Chen. Algebras of iterated path integrals and fundamental groups. *Trans. Amer. Math. Soc.*, 156:359–379, 1971. [↑1.5](#).
- [CK10] John Coates and Minhyong Kim. Selmer varieties for curves with CM Jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010. [↑4.10, 5.1](#).
- [CLS99] Bruno Chiarellotto and Bernard Le Stum. F -isocristaux unipotents. *Compositio Math.*, 116(1):81–110, 1999. [↑5.24](#).
- [Col82] R. F. Coleman. Dilogarithms, regulators and p -adic L -functions. *Invent. Math.*, 69(2):171–208, 1982. [↑1.10, 1.5](#).
- [Col85a] Robert F. Coleman. Effective Chabauty. *Duke Mathematical Journal*, 52(3):765–770, 1985. [↑1.4](#).
- [Col85b] Robert F. Coleman. Torsion points on curves and p -adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985. [↑1.1, 1.10, 1.25](#).
- [Col98] Pierre Colmez. Intégration sur les variétés p -adiques. *Astérisque*, (248):viii+155, 1998. [↑1.11](#).
- [Cor19] David Corwin. From Chabauty’s method to Kim’s non-abelian Chabauty’s method. 2019. <https://math.berkeley.edu/~dcorwin/files/ChabautytoKim.pdf>. [↑4.1](#).
- [Del89] P. Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over \mathbb{Q} (Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 79–297. Springer, New York, 1989. [↑1.6](#).
- [Del90] P. Deligne. Catégories tannakiennes. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 111–195. Birkhäuser Boston, Boston, MA, 1990. [↑5.2](#).
- [DF19] Netan Dogra and Samuel Le Fourn. Quadratic Chabauty for modular curves and modular forms of rank one, June 2019. <https://arxiv.org/abs/1906.08751v3>. [↑4.20, 4.6, 5.7](#).
- [DM82] P. Deligne and J. S. Milne. *Tannakian Categories*, pages 101–228. Springer Berlin Heidelberg, Berlin, Heidelberg, 1982. [↑5.2](#).
- [Dok18] T. Dokchitser. Models of curves over DVRs. 2018. <https://arxiv.org/abs/1807.00025>. [↑2.3.1](#).
- [DRS12] H. Darmon, V. Rotger, and I. Sols. Iterated integrals, diagonal cycles, and rational points on elliptic curves. *Publ. Math. de Besançon*, 2:19–46, 2012. [↑5.1](#).
- [DV06a] Jan Denef and Frederik Vercauteren. Counting points on C_{ab} curves using Monsky-Washnitzer cohomology. *Finite Fields Appl.*, 12(1):78–102, 2006. [↑1.4](#).
- [DV06b] Jan Denef and Frederik Vercauteren. An extension of Kedlaya’s algorithm to hyperelliptic curves in characteristic 2. *J. Cryptology*, 19(1):1–25, 2006. [↑1.4](#).

- [Edi] B. Edixhoven. Point counting after Kedlaya, EIDMA-Stieltjes graduate course, Leiden, September 22–26, 2003. http://www.math.leidenuniv.nl/~edix/oww/mathofcrypt/carls_edixhoven/kedlaya.pdf. ↑1.2, 1.30.
- [EH17] Jordan S. Ellenberg and Daniel Rayor Hast. Rational points on solvable curves over \mathbb{Q} via non-abelian chabauty. *ArXiv preprint*, 2017. ↑4.11.
- [EL19] Bas Edixhoven and Guido Lido. Geometric quadratic Chaubauty, Oct 2019. <https://arxiv.org/abs/1910.10752>. ↑4.21, 5.5.
- [Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. ↑1.2.
- [Fal89] Gerd Faltings. Crystalline cohomology and p -adic Galois-representations. In *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, pages 25–80. Johns Hopkins Univ. Press, Baltimore, MD, 1989. ↑3.2, 3.
- [FvdP04] Jean Fresnel and Marius van der Put. *Rigid analytic geometry and its applications*, volume 218 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 2004. ↑1.1, 1.2.
- [Gal96] S. D. Galbraith. Equations for modular curves. *Oxford DPhil thesis*, 1996. ↑5.4, 5.4.3, 5.34.
- [Gal99] Steven D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1999. ↑5.34.
- [Gal02] Steven D. Galbraith. Rational points on $X_0^+(N)$ and quadratic \mathbb{Q} -curves. *J. Théor. Nombres Bordeaux*, 14(1):205–219, 2002. ↑5.34.
- [GG01] Pierrick Gaudry and Nicolas Gürel. An extension of Kedlaya’s point-counting algorithm to superelliptic curves. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001. ↑1.4.
- [Gro86] Benedict H Gross. Local heights on curves. In *Arithmetic geometry*, pages 327–339. Springer, 1986. ↑2.2.1.
- [Had11] M. Hadian. Motivic fundamental groups and integral points. *Duke Math. J.*, 160(3):503–565, 2011. ↑5.15.
- [Har07] D. Harvey. Kedlaya’s algorithm in larger characteristic. *Int Math Res Notices*, 2007(rnm095):rnm095–29, 2007. ↑1.41.
- [Har08] D. Harvey. Efficient computation of p -adic heights. *LMS J. Comput. Math.*, 11:40–59, 2008. ↑2.7, 2.8.
- [Har12] M. C. Harrison. An extension of Kedlaya’s algorithm for hyperelliptic curves. *J. Symb. Comp.*, 47(1):89 – 101, 2012. ↑1.4.
- [HM] S. Hashimoto and T. Morrison. Magma code. <https://github.com/travismo/Coleman>. ↑1.58.
- [HM19] Yoshinosuke Hirakawa and Hideki Matsumura. A unique pair of triangles. *Journal of Number Theory*, 194:297–302, 2019. ↑1.1.
- [Hol12] David Holmes. Computing Néron-Tate heights of points on hyperelliptic Jacobians. *J. Number Theory*, 132(6):1295–1305, 2012. ↑2.3.1.
- [IW03] Adrian Iovita and Annette Werner. p -adic height pairings on abelian varieties with semistable ordinary reduction. *J. Reine Angew. Math.*, 564:181–203, 2003. ↑2.
- [Kat73] N. Katz. p -Adic properties of modular schemes and modular forms. In P. Deligne and W. Kuyk, editors, *Modular forms in one variable III*, volume 350 of *LNM*, pages 69–190. Springer-Verlag, 1973. ↑2.1.
- [Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001. ↑3, 1.3, 1.28, 1.29, 1.30.
- [Ked03] Kiran S. Kedlaya. Errata for: “Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology” [J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338; mr1877805]. volume 18, pages 417–418. 2003. Dedicated to Professor K. S. Padmanabhan. ↑3, 1.31.
- [Kim05] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel. *Inventiones mathematicae*, 161(3):629–656, 2005. ↑4.1, 4.3, 4.3, 4.5.
- [Kim09] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. ↑4.1, 4.1, 4.5, 4.1, 4.1, 4.8, 4.9, 4.5, 4.5, 5.1, 5, 5.2.
- [Kim10] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010. ↑1.67.
- [Kim12] Minhyong Kim. Tangential localization for Selmer varieties. *Duke Math. J.*, 161(2):173–199, 2012. ↑4.1.
- [KK20] Eric Katz and Enis Kaya. p -adic integration on bad reduction hyperelliptic curves. preprint, 2020. ↑1.40.
- [KRZB16] Eric Katz, Joseph Rabinoff, and David Zureick-Brown. Uniform bounds for the number of rational points on curves of small Mordell–Weil rank. *Duke Mathematical Journal*, 165(16):3189–3240, 2016. ↑1.15, 1.21.
- [KT08] M. Kim and A. Tamagawa. The l -component of the unipotent Albanese map. *Math. Ann.*, 340(1):223–235, 2008. ↑4.1, 4.3.
- [KZB13] Eric Katz and David Zureick-Brown. The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions. *Compos. Math.*, 149(11):1818–1838, 2013. ↑2.

- [LMF20a] The LMFDB Collaboration. The L-functions and modular forms database, home page of the genus 2 curve 8832.a.17664.1. <https://www.lmfdb.org/Genus2Curve/Q/8832/a/17664/1>, 2020. [Online; accessed 7 February 2020]. $\uparrow 1.65$.
- [LMF20b] The LMFDB Collaboration. The L-functions and modular forms database, home page of the genus 2 curve 971.a.971.1. <https://www.lmfdb.org/Genus2Curve/Q/971/a/971/1>, 2020. [Online; accessed 30 January 2020]. $\uparrow 1.22$.
- [LV18] B. Lawrence and A. Venkatesh. Diophantine problems and p -adic period mappings. 2018. <https://arxiv.org/abs/1807.02721>. $\uparrow 1.1$.
- [Mil80] J. Milne. *\acute{E} tale cohomology*. Princeton University Press, 1980. $\uparrow 4.4$.
- [Min10] Moritz Minzlaff. Computing zeta functions of superelliptic curves in larger characteristic. *Mathematics in Computer Science*, 3(2):209–224, 2010. $\uparrow 1.41$.
- [MS16] Jan Steffen M \ddot{u} ller and Michael Stoll. Canonical heights on genus-2 Jacobians. *Algebra Number Theory*, 10(10):2153–2234, 2016. $\uparrow 5.4.3$.
- [MST06] Barry Mazur, William Stein, and John Tate. Computation of p -adic heights and log convergence. *Doc. Math.*, pages 577–614, 2006. $\uparrow 2.1$, 2.8 .
- [MT83] B. Mazur and J. Tate. Canonical height pairings via biextensions. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 195–237. Birkhäuser Boston, Boston, MA, 1983. $\uparrow 2$.
- [MT91] Barry Mazur and John Tate. The p -adic sigma function. *Duke Mathematical Journal*, 62(3):663–688, 1991. $\uparrow 2.1$, 2.3 .
- [MTT86] B. Mazur, J. Tate, and J. Teitelbaum. On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986. $\uparrow 2.5$, 2.8 .
- [Mül14] J. Steffen M \ddot{u} ller. Computing canonical heights using arithmetic intersection theory. *Mathematics of Computation*, 83(285):311–336, 2014. $\uparrow 2.3.1$.
- [Nek93] J. Nekovář. On p -adic height pairings. In *Séminaire de Théorie des Nombres, Paris 1990-1991*, pages 127–202. Birkhäuser, 1993. $\uparrow 2$, 3 , 3.1 , 3.2 , 12 , 3.2 , 3.5 , 3.6 , $3.3.1$, $3.3.2$, 5.5 .
- [Nér76] André Néron. Hauteurs et fonctions thêta. *Rend. Sem. Mat. Fis. Milano*, 46:111–135 (1978), 1976. $\uparrow 2$.
- [Ols11] M. Olsson. Towards non-abelian p -adic Hodge theory in the good reduction case. *Memoirs of the AMS*, (990), 2011. $\uparrow 3.1$, 4.1 , 4.1 , 5.1 , 5.2 .
- [Poo06] Bjorn Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experiment. Math.*, 15(4):415–420, 2006. $\uparrow 4.1$, $5.3.3$.
- [PR83] Bernadette Perrin-Riou. Descente infinie et hauteur p -adique sur les courbes elliptiques à multiplication complexe. *Invent. Math.*, 70(3):369–398, 1982/83. $\uparrow 2$.
- [Qui69] Daniel Quillen. Rational homotopy theory. *Ann. of Math. (2)*, 90:205–295, 1969. $\uparrow 5.1$.
- [Sch82] Peter Schneider. p -adic height pairings. I. *Invent. Math.*, 69(3):401–409, 1982. $\uparrow 2$, 2.9 .
- [Sch94] A. J. Scholl. Height pairings and special values of L -functions. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 571–598. Amer. Math. Soc., Providence, RI, 1994. $\uparrow 3.1$.
- [Sch98] Peter Schneider. Basic notions of rigid analytic geometry. In *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, volume 254 of *London Math. Soc. Lecture Note Ser.*, pages 369–378. Cambridge Univ. Press, Cambridge, 1998. $\uparrow 1.1$.
- [Sch99] Victor Scharaschkin. *Local-global problems and the Brauer-Manin obstruction*. ProQuest LLC, Ann Arbor, MI, 1999. Thesis (Ph.D.)–University of Michigan. $\uparrow 5.3.3$.
- [Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, English edition, 2002. $\uparrow \text{A}$, A.1 , A.2 , A , A.3 , A.1 , 1 .
- [Sik17] S. Siksek. Quadratic Chabauty for modular curves. *preprint*, 2017. $\uparrow 4$.
- [Smi05] B. Smith. *Explicit endomorphisms and correspondences*. PhD thesis, University of Sydney, 2005. $\uparrow 4.4$.
- [Sto02] Michael Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002. $\uparrow 5.4.3$.
- [Sto06] Michael Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142(5):1201–1214, 2006. $\uparrow 1$.
- [Sto19] Michael Stoll. Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank. *J. Eur. Math. Soc. (JEMS)*, 21(3):923–956, 2019. $\uparrow 1.15$, 1.20 .
- [SW13] William Stein and Christian Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Mathematics of Computation*, 82(283):1757–1792, 2013. $\uparrow 2.6$.
- [The19] The LMFDB Collaboration. The L-functions and Modular Forms Database. <http://www.lmfdb.org>, 2019. [Online; accessed 1 July 2019]. $\uparrow 4.7$.

- [The20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. <https://www.sagemath.org>. $\uparrow 1$.
- [Tui16] Jan Tuitman. Counting points on curves using a map to \mathbf{P}^1 . *Math. Comp.*, 85(298):961–981, 2016. $\uparrow 1.4, 1.4, 1.52, 1.4$.
- [Tui17] Jan Tuitman. Counting points on curves using a map to \mathbf{P}^1 , II. *Finite Fields Appl.*, 45:301–322, 2017. $\uparrow 1.4, 1.45, 1, 1.4, 1.52, 1.4$.
- [VBHM20] Raymond Van Bommel, David Holmes, and J. Steffen Müller. Explicit arithmetic intersection theory and computation of Néron-Tate heights. *Mathematics of Computation*, 89(321):395–410, 2020. $\uparrow 2.3.1$.
- [Voj91] Paul Vojta. Siegel’s theorem in the compact case. *Ann. of Math. (2)*, 133(3):509–548, 1991. $\uparrow 1.1$.
- [Vol03] Vadim Vologodsky. Hodge structure on the fundamental group and its application to p -adic integration. *Mosc. Math. J.*, 3(1):205–247, 260, 2003. $\uparrow 1.11$.
- [vW99] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999. $\uparrow 5.5$.
- [Wut04] Christian Wuthrich. On p -adic heights in families of elliptic curves. *J. London Math. Soc. (2)*, 70(1):23–40, 2004. $\uparrow 2.10$.
- [Zar90] Yuri G. Zarhin. p -adic heights on abelian varieties. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 317–341. Birkhäuser Boston, Boston, MA, 1990. $\uparrow 2$.
- [Zar96] Yu. G. Zarhin. p -adic abelian integrals and commutative Lie groups. volume 81, pages 2744–2750. 1996. Algebraic geometry, 4. $\uparrow 1.11$.
- [Zha93] Shouwu Zhang. Admissible pairing on a curve. *Invent. Math.*, 112(1):171–193, 1993. $\uparrow 5.3.1$.

J. S. BALAKRISHNAN, DEPARTMENT OF MATHEMATICS AND STATISTICS, BOSTON UNIVERSITY, 111 CUMMINGTON MALL, BOSTON, MA 02215, USA

Email address: jbala@bu.edu

J. S. MÜLLER, BERNOULLI INSTITUTE, UNIVERSITY OF GRONINGEN, NIJENBORGH 9, 9747 AG GRONINGEN, THE NETHERLANDS

Email address: steffen.muller@rug.nl

AWS 2020: Geometric quadratic Chabauty

Bas Edixhoven

1 Course outline

The quadratic Chabauty method was developed by Balakrishnan and Dogra and extended in [BDMTV], for finding all rational points on a curve C of genus at least two, provided that $r < g + \rho - 1$. Here, r is the rank of $J(\mathbb{Q})$, with J the jacobian of C , g is the genus of C , and ρ is the Picard number (over \mathbb{Q}) of J .

The course has two aims. To describe the quadratic Chabauty method in terms of algebraic geometry only: models over the integers of line bundles on J . And to give an algorithm that can verify, in each given instance where $r < g + \rho - 1$, that the list of known rational points is complete. The course does not aim at effective or uniform finiteness results for *classes of curves*.

The course will follow the preprint [E-L], providing more background where or when needed. The number $g + \rho - 1$ is the dimension of a product T of $\rho - 1$ principal \mathbb{G}_m -bundles on J . As in the classical (linear) Chabauty method, we are intersecting, for p a prime number, but now in $T(\mathbb{Q}_p)$ in stead of in $J(\mathbb{Q}_p)$, the closure of $T(\mathbb{Z})$, which has dimension $\leq r$, with $C(\mathbb{Q}_p)$.

2 Projects and required background

1. Translation between the fundamental group approach and the geometric approach to quadratic Chabauty.

The aim is to understand how to pass from the geometric description to the one in [BDMTV]. In particular: how do p -heights come in? The freshness of this question and the presence of practitioners of both sides make the Arizona Winter School an ideal opportunity for this. The starting point is the fundamental group of $T(\mathbb{C})$ (see [B-E, §4]), and then p -adic local systems on $T_{\mathbb{Q}}$.

Required background. Basic knowledge of the algebraic geometry in [E-L], mainly over \mathbb{C} and over \mathbb{Q} . Some height theory (Arakelov and p -adic). Some working knowledge of Galois cohomology, etale cohomology, and algebraic de Rham cohomology. References: [Po], [H-S], and [H].

2. Comparing computations with participants to Jennifer Balakrishnan's project 2: modular curves $X_0(n)^+$.

The aim here is to apply the geometric quadratic Chabauty method to the curves $X_0(n)^+$ mentioned in Jennifer Balakrishnan's project, and then to compare the whole process with the participants of that project.

We hope that this comparison gives some insight in running times on both sides, actually even for linear Chabauty (as treated in David Zureick-Brown lectures): Coleman integrals on $C(\mathbb{Q}_p)$ versus computations in $J(\mathbb{Z}/p^2\mathbb{Z})$.

Here one can build on Guido Lido's code in cocalc, to be found with [E-L].

Required background: Section 8 of [E-L].

3. Generalise the geometric quadratic Chabauty method from \mathbb{Q} to number fields, and compare with [BBBM].

The idea is to use Weil restriction, to reduce to geometry over \mathbb{Q} .

Required background: Section 2 of [E-L].

References

- [BBBM] Jennifer S. Balakrishnan, Amnon Besser, Francesca Bianchi, Steffen Müller. *Explicit quadratic Chabauty over number fields.*
<https://arxiv.org/pdf/1910.04653v1.pdf>
- [BDMTV] Jennifer Balakrishnan, Netan Dogra, Steffen Müller, Jan Tuitman, Jan Vonk. *Explicit Chabauty-Kim for the split Cartan modular curve of level 13.* Ann. of Math. (2) 189 (2019), no. 3, 885–944.
<https://annals.math.princeton.edu/2019/189-3/p06>
- [B-E] Daniel Bertrand and Bas Edixhoven, *Pink’s conjecture on unlikely intersections and families of semi-abelian varieties.*
<https://arxiv.org/abs/1904.01788>
- [E-L] Bas Edixhoven and Guido Lido. *Geometric quadratic Chabauty.*
<https://arxiv.org/abs/1910.10752>
- [H-S] Marc Hindry and Joseph Silverman. *Diophantine geometry. An introduction.* Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000.
- [H] Johan Huisman. *Heights on abelian varieties.* Chapter 5 in “Diophantine approximation and abelian varieties. Introductory lectures.” Papers from the conference held in Soesterberg, April 12–16, 1992. Edited by Bas Edixhoven and Jan-Hendrik Evertse. Lecture Notes in Mathematics, 1566. Springer-Verlag, Berlin, 1993.
http://pub.math.leidenuniv.nl/~edixhovensj/publications/1993/Edixhoven-Evertse_Soesterberg_1992.pdf
- [Po] Bjorn Poonen. *Rational points on varieties.* Graduate Studies in Mathematics, 186. American Mathematical Society, Providence, RI, 2017.
<http://www-math.mit.edu/~poonen/papers/Qpoints.pdf>

AWS 2020: Geometric quadratic Chabauty

Bas Edixhoven

1 Course description

The quadratic Chabauty method was developed by Kim, Balakrishnan, Besser, Dogra and Müller, and extended in [BDMTV], for finding all rational points on a curve C of genus at least two, provided that $r < g + \rho - 1$. Here, r is the rank of $J(\mathbb{Q})$, with J the jacobian of C , g is the genus of C , and ρ is the Picard number (over \mathbb{Q}) of J .

The course has two aims. To describe the quadratic Chabauty method in terms of algebraic geometry only: models over the integers of line bundles on J . And to give an algorithm that can verify, in each given instance where $r < g + \rho - 1$, that the list of known rational points is complete. The course does not aim at effective or uniform finiteness results for *classes of curves*.

The course will follow the preprint [E-L], providing more background where or when needed. The number $g + \rho - 1$ is the dimension of a product T of $\rho - 1$ principal \mathbb{G}_m -bundles on J . As in the classical (linear) Chabauty method, we are intersecting, for p a prime number, but now in $T(\mathbb{Q}_p)$ in stead of in $J(\mathbb{Q}_p)$, the closure of $T(\mathbb{Z})$, which has dimension $\leq r$, with $C(\mathbb{Q}_p)$.

Planning of the lectures

The following planning is preliminary, and will be adapted as the course goes on. One idea is to carry the example in Section 8 along through all the lectures.

1. Section 2.
2. Sections 3 and 4.
3. Section 5.
4. Sections 6 and 7 (not in detail).
5. ?

2 Projects and required background

2.1 Translation from the geometric approach to the fundamental group theoretical approach

The aim of this project is to relate the fundamental group approach to quadratic Chabauty as in [BDMTV] to the geometric method in [E-L]. It is claimed that experts more or less know how to do this. It is also true that the authors of the articles just mentioned do *not* know the details, but are really interested in them.

Our starting point is the geometric approach as in [E-L], and, more precisely, the diagram (2.12) on page 5 (see there for details):

$$\begin{array}{ccc} T & \longrightarrow & P^{\times, \rho-1} \\ \downarrow & \nearrow \tilde{j}_b & \downarrow \\ U & \xrightarrow{j_b} & J \xrightarrow{(\text{id}, m \cdot \text{otr}_{c_i} \circ f_i)_i} J \times (J^{\vee 0})^{\rho-1}. \end{array}$$

In [M-B], Theorem 5.4, Moret-Bailly shows how P is naturally equipped with metrics on its fibres over $J(\mathbb{C}) \times J^\vee(\mathbb{C})$, and that for (x, y) in $(J \times J^{\vee 0})(\mathbb{Z})$, the Arakelov degree of $(x, y)^*P$ is the Néron-Tate height of (x, y) .

Now T is the product of $\rho - 1$ principal \mathbb{G}_m -bundles T_i on J . Their associated line bundles \mathcal{L}_i are pullbacks of P and so have natural metrics over $J(\mathbb{C})$. The pullbacks of the \mathcal{L}_i to U are trivial (uniquely up to signs) and the norms of the trivialising sections are constant as functions on $U(\mathbb{C})$, because they are harmonic. These constants $c_{U,i}$ can be read off from (7.8) and (7.2) in [E-L]. For any u in $U(\mathbb{Z})$, the heights of $j_b(u)$ with respect to \mathcal{L}_i are equal to $-\log(c_{U,i})$. Note that the heights on $J(\mathbb{Q})$ attached to the \mathcal{L}_i are not necessarily positive because the \mathcal{L}_i are not ample on $J_\mathbb{Q}$ (they are trivial on $C_\mathbb{Q}$). These heights are \mathbb{R} -valued polynomial functions of degree at most 2 on $J(\mathbb{Q})$, the coefficients of which (with respect to a \mathbb{Z} -basis of $J(\mathbb{Q})$ modulo torsion) are given by the corresponding values of the Néron-Tate height pairing. The knowledge of the heights of the $j_b(u)$ with respect to the \mathcal{L}_i could be very useful information for finding out which elements of $J(\mathbb{Q})$ are in $C(\mathbb{Q})$, but the non-definiteness of the quadratic polynomials and the complexity of their coefficients make it harder. Nevertheless, looking further into this may be an interesting project, especially for modular curves, where ρ is equal to g , and where there are strong results on the Birch and Swinnerton-Dyer conjecture for the isogeny factors of the jacobian where the analytic rank of the L -function is at most 1.

So, following Chabauty, one tries a p -adic approach. Here this means considering, for some chosen prime p , p -adic valued heights and Arakelov theory. This is done in [M-T] for abelian varieties, using biextensions, and in [C-G] for jacobians. The idea is that the product formula must be preserved and that the analytic functions at the archimedean places are replaced by p -adic analytic functions at the p -adic places. For example, the \mathbb{R} -valued adele norm on the ideles of \mathbb{Q} , $x \mapsto \|x\| = \prod_v |x_v|_v$, is trivial on \mathbb{Q}^\times . For $x \in \mathbb{R}^\times$ we have $|x|_\infty = x \cdot \text{sign}(x)$. The factor x can be moved, for $x \in \mathbb{Q}^\times$, to any p -adic place of our choice. So, for a prime p , we obtain the \mathbb{Q}_p^\times -valued adele norm $x \mapsto (x_p \cdot |x_p|_p) \cdot \text{sign}(x_\infty) \cdot \prod_{v \notin \{p, \infty\}} |x_v|_v$, also trivial on \mathbb{Q}^\times . Up to a sign, it corresponds via class field theory for \mathbb{Q} to the p -adic cyclotomic character. The main point is that at all places other than p and ∞ , nothing has changed.

We are now already very close to § 1.4 of [BDMTV], and it should not be very hard to get a precise translation.

For the subsequent interpretation in [BDMTV] of everything in terms of fundamental groups, we note that the embedding $\tilde{j}_b: C_\mathbb{Q} \rightarrow T_\mathbb{Q}$ induces a morphism of fundamental groups. The complex uniformisation of $P^\times(\mathbb{C})$ (see [B-E, §4]) gives the structure of $\pi_1(P^\times(\mathbb{C}))$; it is a non-abelian extension of $\pi_1(J(\mathbb{C}) \times J(\mathbb{C}))$ by \mathbb{Z} . So, apparently, one has to study p -adic local systems on $T_\mathbb{Q}$.

Required background.

Basic knowledge of the algebraic geometry in [E-L], mainly over \mathbb{C} and over \mathbb{Q} . Some Arakelov height theory (see [M-B], [H-S], and [H]) and p -adic height theory ([M-T] and [C-G])).

For the passage from p -adic heights to fundamental groups, some working knowledge of Galois cohomology and etale cohomology (see [Po]), algebraic de Rham cohomology (see https://en.wikipedia.org/wiki/Khler_differential), knowledge in abelian and non-abelian p -adic Hodge theory (see the references in [BDMTV]).

2.2 Comparing computations with participants to Jennifer Balakrishnan's project 2: modular curves $X_0(n)^+$.

The aim here is to apply the geometric quadratic Chabauty method to the curves $X_0(n)^+$ mentioned in Jennifer Balakrishnan's project, and then to compare the whole process with the participants of that project.

We hope that this comparison gives some insight in running times on both sides, actually even for linear Chabauty (as treated in David Zureick-Brown's lectures): Coleman integrals on $C(\mathbb{Q}_p)$ versus computations in $J(\mathbb{Z}/p^2\mathbb{Z})$.

Here one can build on Guido Lido's example (Section 8 in [E-L]) and his code in cocalc, to be found with [E-L]. It may be that at the time of the School the example $X_0(73)^+$ will be available.

Required background

Section 8 (and therefore most of the other sections as well) of [E-L]. Some knowledge of modular curves, see [D-S].

2.3 Generalisation of the geometric quadratic Chabauty method to number fields

This generalisation has already been carried out for bielliptic curves of genus 2 in [BBBM]. It is interesting to see, at first theoretically, how the methods of [E-L] can be generalised to number fields. The first idea is to use Weil restriction, to reduce to geometry over \mathbb{Q} .

Required background

Section 2 of [E-L].

References

- [BBBM] Jennifer S. Balakrishnan, Amnon Besser, Francesca Bianchi, Steffen Müller. *Explicit quadratic Chabauty over number fields*.
<https://arxiv.org/pdf/1910.04653v1.pdf>
- [BDMTV] Jennifer Balakrishnan, Netan Dogra, Steffen Müller, Jan Tuitman, Jan Vonk. *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*. Ann. of Math. (2) 189 (2019), no. 3, 885–944.
<https://annals.math.princeton.edu/2019/189-3/p06>
- [B-E] Daniel Bertrand and Bas Edixhoven. *Pink's conjecture on unlikely intersections and families of semi-abelian varieties*.
<https://arxiv.org/abs/1904.01788>
- [C-G] Robert Coleman and Dick Gross. *p -adic heights on curves*. Algebraic number theory, 73–81, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989.
<https://projecteuclid.org/euclid.aspm/1529259066>
- [D-S] Fred Diamond and Jerry Shurman. *A first course in modular forms*. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005.

- [E-L] Bas Edixhoven and Guido Lido. *Geometric quadratic Chabauty*.
<https://arxiv.org/abs/1910.10752>
- [H-S] Marc Hindry and Joseph Silverman. *Diophantine geometry. An introduction*. Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000.
- [H] Johan Huisman. *Heights on abelian varieties*. Chapter 5 in “Diophantine approximation and abelian varieties. Introductory lectures.” Papers from the conference held in Soesterberg, April 12–16, 1992. Edited by Bas Edixhoven and Jan-Hendrik Evertse. Lecture Notes in Mathematics, 1566. Springer-Verlag, Berlin, 1993.
http://pub.math.leidenuniv.nl/~edixhovensj/publications/1993/Edixhoven-Evertse_Soesterberg_1992.pdf
- [M-T] Barry Mazur and John Tate. *Canonical height pairings via biextensions*. Arithmetic and geometry, Vol. I, 195–237, Progr. Math., 35, Birkhäuser Boston, Boston, MA, 1983.
<http://pub.math.leidenuniv.nl/~edixhovensj/teaching/2019-2020/AWS/Mazur-Tate.pdf>
- [M-B] Laurent Moret-Bailly. *Métriques permises*. Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). Astérisque No. 127 (1985), 29–87.
http://www.numdam.org/article/AST_1985__127__29_0.pdf
- [Po] Bjorn Poonen. *Rational points on varieties*. Graduate Studies in Mathematics, 186. American Mathematical Society, Providence, RI, 2017.
<http://www-math.mit.edu/~poonen/papers/Qpoints.pdf>

Geometric quadratic Chabauty

Bas Edixhoven & Guido Lido

edix@math.leidenuniv.nl guidomaria.lido@gmail.com Math. Inst., Universiteit Leiden

February 13, 2020

Abstract

Determining all rational points on a curve of genus at least 2 can be difficult. Chabauty's method (1941) is to intersect, for a prime number p , in the p -adic Lie group of p -adic points of the jacobian, the closure of the Mordell-Weil group with the p -adic points of the curve. If the Mordell-Weil rank is less than the genus then this method has never failed.

Minhyong Kim's non-abelian Chabauty programme aims to remove the condition on the rank. The simplest case, called quadratic Chabauty, was developed by Balakrishnan, Dogra, Müller, Tuitman and Vonk, and applied in a tour de force to the so-called cursed curve (rank and genus both 3).

This article aims to make the quadratic Chabauty method *small* and *geometric* again, by describing it in terms of only 'simple algebraic geometry' (line bundles over the jacobian and models over the integers).

Keywords: rational points, curves, Chabauty, non-abelian, quadratic, geometric.

2010 Mathematical Subject Classification: 14G05, 11G30.

Contents

1	Introduction	2
2	Algebraic geometry	3
3	From algebraic geometry to formal geometry	6
4	Integral points, closure and finiteness	6
5	Parametrisation of integral points, and power series	10
5.1	Logarithm and exponential	10
5.2	Parametrisation by power series	12
5.3	The p -adic closure	14
6	Explicit description of the Poincaré torsor	14
6.1	Norms	14
6.2	Norms along finite relative Cartier divisors	15

6.3	Explicit description of the Poincaré torsor of a smooth curve	16
6.4	Explicit isomorphism for norms along equivalent divisors	18
6.5	Symmetry of the Norm for divisors on smooth curves	20
6.6	Explicit residue disks and partial group laws	22
6.7	Extension of the Poincaré biextension over Néron models	25
6.8	Explicit description of the extended Poincaré bundle	25
6.9	Integral points of the extended Poincaré torsor	28
7	Description of the map from the curve to the torsor	29
8	An example with genus 2, rank 2, and 14 points	31
8.1	The torsor on the jacobian	32
8.2	Some integral points on the biextension	33
8.3	Some residue disks of the biextension	34
8.4	Geometry mod p of integral points	35
8.5	The rational points with a specific image mod 5.	38
8.6	Determination of all rational points	38
Author contributions	39	
Acknowledgements	39	
References	39	

1 Introduction

Determining all rational points on a curve of genus $g \geq 2$ can be a difficult problem. Chabauty's method (1941) is to intersect, for a prime number p , in the p -adic Lie group of p -adic points of the jacobian, the closure of the Mordell-Weil group with the p -adic points of the curve. If the Mordell-Weil rank r satisfies $r < g$ then this method has never failed.

Minhyong Kim's non-abelian Chabauty programme aims to remove the condition that $r < g$. The 'non-abelian' refers to fundamental groups; the fundamental group of the jacobian of a curve is the abelianised fundamental group of the curve. The most striking result in this direction is the so-called quadratic Chabauty method, applied in [2], a technical tour de force, to the so-called cursed curve ($r = g = 3$). For more details we recommend the introduction of [2].

This article aims to make the quadratic Chabauty method *small* and *geometric* again, by describing it in terms of only 'simple algebraic geometry' (line bundles over the jacobian and models over the integers). Section 2 describes the geometric method in less than 3 pages, sections 3–5 give the necessary theory, sections 6–7 give descriptions that are suitable for computer calculations, and section 8 treats an example with $r = g = 2$ and 14 rational points. Theorem 4.12 gives a criterion for a given list of rational points to be complete, in terms of

points with values in $\mathbb{Z}/p^2\mathbb{Z}$. We expect that this approach will make it possible to treat many more curves.

The biextensions in our approach correspond well with the name ‘quadratic’, and this quadratic nature also manifests itself in the equations over \mathbb{F}_p in Theorem 4.12. The fundamental group playing a role here is a subgroup of a higher dimensional Heisenberg group, where the commutator pairing is the intersection pairing of the fundamental group of the curve (see [3], Section 4). The passage from our approach to that of [2] is given by p -adic local systems on our geometric objects. Because of the technicalities involved we do not go into this (less is more).

2 Algebraic geometry

Let C be a scheme over \mathbb{Z} , proper, flat, regular, with $C_{\mathbb{Q}}$ of dimension one and geometrically connected. Let n be in $\mathbb{Z}_{\geq 1}$ such that the restriction of C to $\mathbb{Z}[1/n]$ is smooth. Let g be the genus of $C_{\mathbb{Q}}$. We assume that $g \geq 2$ and that we have a rational point $b \in C(\mathbb{Q})$; it extends uniquely to a $b \in C(\mathbb{Z})$. We let J be the Néron model over \mathbb{Z} of the jacobian $\text{Pic}_{C_{\mathbb{Q}}/\mathbb{Q}}^0$. We denote by J^{\vee} the Néron model over \mathbb{Z} of the dual $J_{\mathbb{Q}}^{\vee}$ of $J_{\mathbb{Q}}$, and $\lambda: J \rightarrow J^{\vee}$ the isomorphism extending the canonical principal polarisation of $J_{\mathbb{Q}}$. We let $P_{\mathbb{Q}}$ be the Poincaré *line bundle* on $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, trivialised on the union of $\{0\} \times J_{\mathbb{Q}}^{\vee}$ and $J_{\mathbb{Q}} \times \{0\}$. Then the Poincaré *torsor* is the \mathbb{G}_m -torsor on $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$ defined as

$$(2.1) \quad P_{\mathbb{Q}}^{\times} = \mathbf{Isom}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}}(\mathcal{O}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}}, P_{\mathbb{Q}}).$$

For every scheme S over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, $P_{\mathbb{Q}}^{\times}(S)$ is the set of isomorphisms from \mathcal{O}_S to $(P_{\mathbb{Q}})_S$, with a free and transitive action of $\mathcal{O}_S(S)^{\times}$. Locally on S for the Zariski topology, $(P_{\mathbb{Q}}^{\times})_S$ is trivial, and $P_{\mathbb{Q}}^{\times}$ is represented by a scheme over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$.

The theorem of the cube gives $P_{\mathbb{Q}}^{\times}$ the structure of a *biextension* of $J_{\mathbb{Q}}$ and $J_{\mathbb{Q}}^{\vee}$ by \mathbb{G}_m , a notion for the details of which we recommend Section I.2.5 of [9], Grothendieck’s Exposés VII and VIII [11], and references therein. This means the following. For S a \mathbb{Q} -scheme, x_1 and x_2 in $J_{\mathbb{Q}}(S)$, and y in $J_{\mathbb{Q}}^{\vee}(S)$, the theorem of the cube gives a canonical isomorphism of \mathcal{O}_S -modules

$$(2.2) \quad (x_1, y)^* P_{\mathbb{Q}} \otimes_{\mathcal{O}_S} (x_2, y)^* P_{\mathbb{Q}} = (x_1 + x_2, y)^* P_{\mathbb{Q}}.$$

This induces a morphism of schemes

$$(2.3) \quad (x_1, y)^* P_{\mathbb{Q}}^{\times} \times_S (x_2, y)^* P_{\mathbb{Q}}^{\times} \longrightarrow (x_1 + x_2, y)^* P_{\mathbb{Q}}^{\times}.$$

as follows. For any S -scheme T , and z_1 in $((x_1, y)^* P_{\mathbb{Q}}^{\times})(T)$ and z_2 in $((x_2, y)^* P_{\mathbb{Q}}^{\times})(T)$, we view z_1 and z_2 as nowhere vanishing sections of the invertible \mathcal{O}_T -modules $(x_1, y)^* P_{\mathbb{Q}}$ and $(x_2, y)^* P_{\mathbb{Q}}$. The tensor product of these two then gives an element of $((x_1 + x_2, y)^* P_{\mathbb{Q}}^{\times})(T)$. This gives $P_{\mathbb{Q}}^{\times} \rightarrow J_{\mathbb{Q}}^{\vee}$ the structure of a commutative group scheme, which is an extension of $J_{\mathbb{Q}}$ by \mathbb{G}_m ,

over the base $J_{\mathbb{Q}}^{\vee}$. We denote this group law, and the one on $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, as

$$(2.4) \quad \begin{array}{ccc} (z_1, z_2) & \longmapsto & z_1 +_1 z_2 \\ \downarrow & & \downarrow \\ ((x_1, y), (x_2, y)) & \longmapsto & (x_1, y) +_1 (x_2, y) = (x_1 + x_2, y). \end{array}$$

In the same way, $P_{\mathbb{Q}}^{\times} \rightarrow J_{\mathbb{Q}}$ has a group law $+_2$ that makes it an extension of $J_{\mathbb{Q}}^{\vee}$ by \mathbb{G}_{m} over the base $J_{\mathbb{Q}}$. In this way, $P_{\mathbb{Q}}^{\times}$ is both the universal extension of $J_{\mathbb{Q}}$ by \mathbb{G}_{m} as the universal extension of $J_{\mathbb{Q}}^{\vee}$ by \mathbb{G}_{m} . The final ingredient of the notion of biextension is that the two partial group laws are compatible in the following sense. For any \mathbb{Q} -scheme S , for x_1 and x_2 in $J_{\mathbb{Q}}(S)$, y_1 and y_2 in $J_{\mathbb{Q}}^{\vee}(S)$, and, for all i and j in $\{1, 2\}$, $z_{i,j}$ in $((x_i, y_j)^* P_{\mathbb{Q}}^{\times})(S)$, we have

$$(2.5) \quad \begin{array}{ccc} (z_{1,1} +_1 z_{2,1}) +_2 (z_{1,2} +_1 z_{2,2}) & = & (z_{1,1} +_2 z_{1,2}) +_1 (z_{2,1} +_2 z_{2,2}) \\ \downarrow & & \downarrow \\ (x_1 + x_2, y_1) +_2 (x_1 + x_2, y_2) & = & (x_1, y_1 + y_2) +_1 (x_2, y_1 + y_2) \end{array}$$

with the equality in the upper line taking place in $((x_1 + x_2, y_1 + y_2)^* P_{\mathbb{Q}}^{\times})(S)$.

Now we extend the geometry above over \mathbb{Z} . We denote by J^0 the fibrewise connected component of 0 in J , which is an open subgroup scheme of J , and by Φ the quotient J/J^0 , which is an étale (not necessarily separated) group scheme over \mathbb{Z} , with finite fibres, supported on $\mathbb{Z}/n\mathbb{Z}$. Similarly, we let $J^{\vee 0}$ be the fibrewise connected component of J^{\vee} . Theorem 7.1, in Exposé VIII of [11] gives that $P_{\mathbb{Q}}^{\times}$ extends uniquely to a \mathbb{G}_{m} -biextension

$$(2.6) \quad P^{\times} \longrightarrow J \times J^{\vee 0}$$

(Grothendieck's pairing on component groups is the obstruction to the existence of such an extension). Note that in this case the existence and the uniqueness follow directly from the requirement of extending the rigidification on $J_{\mathbb{Q}} \times \{0\}$. For details see Section 6.7.

Our base point $b \in C(\mathbb{Z})$ gives an embedding $j_b: C_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$, which sends, functorially in \mathbb{Q} -schemes S , an element $c \in C_{\mathbb{Q}}(S)$ to the class of the invertible \mathcal{O}_{C_S} -module $\mathcal{O}_{C_S}(c - b)$. Then j_b extends uniquely to a morphism

$$(2.7) \quad j_b: C^{\text{sm}} \longrightarrow J$$

where C^{sm} is the open subscheme of C consisting of points at which C is smooth over \mathbb{Z} . Note that $C_{\mathbb{Q}}(\mathbb{Q}) = C(\mathbb{Z}) = C^{\text{sm}}(\mathbb{Z})$.

Our next step is to lift j_b , at least on certain opens of C^{sm} , to a morphism to a $\mathbb{G}_{\text{m}}^{\rho-1}$ -torsor over J , where ρ is the rank of the free \mathbb{Z} -module $\text{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\vee})^+$, the \mathbb{Z} -module of self-dual morphisms from $J_{\mathbb{Q}}$ to $J_{\mathbb{Q}}^{\vee}$. This torsor will be the product of pullbacks of P^{\times} via morphisms

$$(2.8) \quad (\text{id}, m \cdot \circ \text{tr}_c \circ f): J \rightarrow J \times J^{\vee 0},$$

with $f: J \rightarrow J^{\vee}$ a morphism of group schemes, $c \in J^{\vee}(\mathbb{Z})$, tr_c the translation by c , m the least common multiple of the exponents of all $\Phi(\overline{\mathbb{F}}_p)$ with p ranging over all primes, and $m \cdot$ the multiplication by m map on J^{\vee} . For such a map $m \cdot \circ \text{tr}_c \circ f$, $j_b: C_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ can be lifted to

$(\text{id}, m \cdot \circ \text{tr}_c \circ f)^* P_{\mathbb{Q}}^\times$ if and only if $j_b^*(\text{id}, m \cdot \circ \text{tr}_c \circ f)^* P_{\mathbb{Q}}^\times$ is trivial. The degree of this \mathbb{G}_m -torsor on $C_{\mathbb{Q}}$ is minus the trace of $\lambda^{-1} \circ m \cdot \circ (f + f^\vee)$ acting on $H_1(J(\mathbb{C}), \mathbb{Z})$. For example, for $f = \lambda$ the degree is $-4mg$. Note that $j_b: C_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ induces

$$(2.9) \quad j_b^* = -\lambda^{-1}: J_{\mathbb{Q}}^\vee \rightarrow J_{\mathbb{Q}},$$

(see [8], Propositions 2.7.9 and 2.7.10). This implies that for f such that this degree is zero, there is a unique c such that $j_b^*(\text{id}, \text{tr}_c \circ f)^* P_{\mathbb{Q}}^\times$ is trivial on $C_{\mathbb{Q}}$, and hence also its m th power $j_b^*(\text{id}, m \cdot \circ \text{tr}_c \circ f)^* P_{\mathbb{Q}}^\times$.

The map

$$(2.10) \quad \text{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^\vee) \longrightarrow \text{Pic}(J_{\mathbb{Q}}) \longrightarrow \text{NS}_{J_{\mathbb{Q}}/\mathbb{Q}}(\mathbb{Q}) = \text{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^\vee)^+$$

sending f to the class of $(\text{id}, f)^* P_{\mathbb{Q}}$ sends f to $f + f^\vee$, hence its kernel is $\text{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^\vee)^-$, the group of antisymmetric morphisms. But actually, for f antisymmetric, its image in $\text{Pic}(J_{\mathbb{Q}})$ is already zero (see for example [3] and the references therein). Hence the image of $\text{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^\vee)$ in $\text{Pic}(J_{\mathbb{Q}})$ is free of rank ρ , and its subgroup of classes with degree zero on $C_{\mathbb{Q}}$ is free of rank $\rho-1$. Let $f_1, \dots, f_{\rho-1}$ be elements of $\text{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^\vee)$ whose images in $\text{Pic}(J_{\mathbb{Q}})$ form a basis of this subgroup, and let $c_1, \dots, c_{\rho-1}$ be the corresponding elements of $J^\vee(\mathbb{Z})$.

By construction, for each i , the morphism $j_b: C_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ lifts to $(\text{id}, m \cdot \circ \text{tr}_{c_i} \circ f_i)^* P_{\mathbb{Q}}^\times$, unique up to \mathbb{Q}^\times . Now we spread this out over \mathbb{Z} , to open subschemes U of C^{sm} obtained by removing, for each q dividing n , all but one irreducible components of $C_{\mathbb{F}_q}^{\text{sm}}$, with the remaining irreducible component geometrically irreducible. For such a U , the morphism $\text{Pic}(U) \rightarrow \text{Pic}(C_{\mathbb{Q}})$ is an isomorphism, and $\mathcal{O}_C(U) = \mathbb{Z}$, thus, for each i , there is a lift

$$(2.11) \quad \begin{array}{ccc} & & (\text{id}, m \cdot \circ \text{tr}_{c_i} \circ f_i)^* P^\times \\ U & \xrightarrow{j_b} & J \\ \downarrow & \nearrow \tilde{j}_b & \downarrow \\ & & \end{array}$$

unique up to $\mathbb{Z}^\times = \{1, -1\}$.

At this point we can explain the strategy of our approach to the quadratic Chabauty method. Let T be the $\mathbb{G}_m^{\rho-1}$ -torsor on J obtained by taking the product of all $(\text{id}, m \cdot \circ \text{tr}_{c_i} \circ f_i)^* P^\times$:

$$(2.12) \quad \begin{array}{ccc} U & \xrightarrow{j_b} & J \\ \downarrow & \nearrow \tilde{j}_b & \downarrow \\ T & \longrightarrow & P^{\times, \rho-1} \\ & \xrightarrow{(\text{id}, m \cdot \circ \text{tr}_{c_i} \circ f_i)_i} & J \times (J^{\vee 0})^{\rho-1}. \end{array}$$

Then each $c \in C_{\mathbb{Q}}(\mathbb{Q}) = C^{\text{sm}}(\mathbb{Z})$ lies in one of the finitely many $U(\mathbb{Z})$'s. For each U , we have a lift $\tilde{j}_b: U \rightarrow T$, and, for each prime number p , $\tilde{j}_b(U(\mathbb{Z}))$ is contained in the intersection, in $T(\mathbb{Z}_p)$, of $\tilde{j}_b(U(\mathbb{Z}_p))$ and the closure $\overline{T(\mathbb{Z})}$ of $T(\mathbb{Z})$ in $T(\mathbb{Z}_p)$ with the p -adic topology. Of course, one expects this closure to be of dimension at most $r := \text{rank}(J(\mathbb{Q}))$, and therefore one expects this method to be successful if $r < g + \rho - 1$, the dimension of $T(\mathbb{Z}_p)$. The next two sections make this strategy precise, giving first the necessary p -adic formal and analytic geometry, and then the description of $\overline{T(\mathbb{Z})}$ as a finite disjoint union of images of \mathbb{Z}_p^r under maps constructed from the biextension structure.

3 From algebraic geometry to formal geometry

Let p be a prime number. Given X a smooth scheme of relative dimension d over \mathbb{Z}_p and $x \in X(\mathbb{F}_p)$ let us describe the set $X(\mathbb{Z}_p)_x$ of elements of $X(\mathbb{Z}_p)$ whose image in $X(\mathbb{F}_p)$ is x . The smoothness implies that the maximal ideal of $\mathcal{O}_{X,x}$ is generated by p together with d other elements t_1, \dots, t_d . In this case we call p, t_1, \dots, t_d *parameters at* x ; if moreover $x_l \in X(\mathbb{Z}_p)_x$ is a lift of x such that $t_1(x_l) = \dots = t_d(x_l) = 0$ then we say that the t_i 's are *parameters at* x_l . The t_i can be evaluated on all the points in $X(\mathbb{Z}_p)_x$, inducing a bijection $t := (t_1, \dots, t_d): X(\mathbb{Z}_p)_x \rightarrow (p\mathbb{Z}_p)^d$. We get a bijection

$$(3.1) \quad \tilde{t} := (\tilde{t}_1, \dots, \tilde{t}_d) = \left(\frac{t_1}{p}, \dots, \frac{t_d}{p} \right): X(\mathbb{Z}_p)_x \xrightarrow{\sim} \mathbb{Z}_p^d.$$

This bijection can be geometrically interpreted as follows. Let $\pi: \tilde{X}_x \rightarrow X$ denote the blow up of X in x . By shrinking X , X is affine and the t_i are regular on X , and $t: X \rightarrow \mathbb{A}_{\mathbb{Z}_p}^d$ is étale. Therefore $\pi: \tilde{X}_x \rightarrow X$ is the pull back of the blow up of $\mathbb{A}_{\mathbb{Z}_p}^d$ at the origin over \mathbb{F}_p . The affine open part \tilde{X}_x^p of \tilde{X}_x where p generates the image of the ideal m_x of x is the pullback of the corresponding open part of the blow up of $\mathbb{A}_{\mathbb{Z}_p}^d$, which is the multiplication by p morphism $\mathbb{A}_{\mathbb{Z}_p}^d \rightarrow \mathbb{A}_{\mathbb{Z}_p}^d$ that corresponds to $\mathbb{Z}_p[t_1, \dots, t_d] \rightarrow \mathbb{Z}_p[\tilde{t}_1, \dots, \tilde{t}_d]$ with $t_i \mapsto p\tilde{t}_i$. It follows that the p -adic completion $\mathcal{O}(\tilde{X}_x^p)^{\wedge p}$ of $\mathcal{O}(\tilde{X}_x^p)$ is the p -adic completion $\mathbb{Z}_p\langle\tilde{t}_1, \dots, \tilde{t}_d\rangle$ of $\mathbb{Z}_p[\tilde{t}_1, \dots, \tilde{t}_d]$. Explicitly, we have

$$(3.2) \quad \mathbb{Z}_p\langle\tilde{t}_1, \dots, \tilde{t}_d\rangle = \left\{ \sum_{I \in \mathbb{N}^d} a_I \tilde{t}^I \in \mathbb{Z}_p[[\tilde{t}_1, \dots, \tilde{t}_d]] : \forall n \geq 0, \text{ } \forall^{\text{almost}} I, v_p(a_I) \geq n \right\}.$$

With these definitions, we have

$$(3.3) \quad \begin{aligned} X(\mathbb{Z}_p)_x &= \tilde{X}_x^p(\mathbb{Z}_p) = \text{Hom}(\mathbb{Z}_p\langle\tilde{t}_1, \dots, \tilde{t}_d\rangle, \mathbb{Z}_p) = \mathbb{A}^d(\mathbb{Z}_p), \\ (\tilde{X}_x^p)_{\mathbb{F}_p} &= \text{Spec}(\mathbb{F}_p[\tilde{t}_1, \dots, \tilde{t}_d]). \end{aligned}$$

The affine space $(\tilde{X}_x^p)_{\mathbb{F}_p}$ is canonically a torsor under the tangent space of $X_{\mathbb{F}_p}$ at x .

This construction is functorial. Let Y be a smooth \mathbb{Z}_p -scheme, $f: X \rightarrow Y$ a morphism over \mathbb{Z}_p , and $y := f(x) \in Y(\mathbb{F}_p)$. Then the ideal in $\mathcal{O}_{\tilde{X}_x^p}$ generated by the image of $m_{f(x)}$ is generated by p . That gives us a morphism $\tilde{X}_x^p \rightarrow \tilde{Y}_{f(x)}^p$, and then a morphism from $\mathcal{O}(\tilde{Y}_{f(x)}^p)^{\wedge p}$ to $\mathcal{O}(\tilde{X}_x^p)^{\wedge p}$. Reduction mod p then gives a morphism $(\tilde{X}_x^p)_{\mathbb{F}_p} \rightarrow (\tilde{Y}_{f(x)}^p)_{\mathbb{F}_p}$, the tangent map of f at x , up to a translation.

If this tangent map is injective, and d_x and d_y denote the dimensions of $X_{\mathbb{F}_p}$ at x and of $Y_{\mathbb{F}_p}$ at y , then there are t_1, \dots, t_{d_x} in $\mathcal{O}_{Y,y}$ such that p, t_1, \dots, t_{d_y} are parameters at y , and such that $t_{d_x+1}, \dots, t_{d_y}$ generate the kernel of $\mathcal{O}_{Y,y} \rightarrow \mathcal{O}_{X,x}$. Then the images in $\mathcal{O}_{X,x}$ of p, t_1, \dots, t_{d_x} are parameters at x , and $\mathcal{O}(\tilde{Y}_{f(x)}^p)^{\wedge p} \rightarrow \mathcal{O}(\tilde{X}_x^p)^{\wedge p}$ is $\mathbb{Z}_p\langle\tilde{t}_1, \dots, \tilde{t}_{d_y}\rangle \rightarrow \mathbb{Z}_p\langle\tilde{t}_1, \dots, \tilde{t}_{d_x}\rangle$, with kernel generated by $\tilde{t}_{d_x+1}, \dots, \tilde{t}_{d_y}$.

4 Integral points, closure and finiteness

Let us now return to our original problem. The notation $U, J, T, j_b, \tilde{j}_b, r, \rho$ etc., is as at the end of Section 2. We assume moreover that p does not divide n (n as in the start of Section 2)

and that $p > 2$ (for $p = 2$ everything that follows can probably be adapted by working with residue polydiscs modulo 4).

Let u be in $U(\mathbb{F}_p)$, and $t := \tilde{j}_b(u)$. We want a description of the closure $\overline{T(\mathbb{Z})}_t$ of $T(\mathbb{Z})_t$ in $T(\mathbb{Z}_p)_t$. Using the biextension structure of P^\times , we will produce, for each element of $J(\mathbb{Z})_{j_b(u)}$, an element of $T(\mathbb{Z})$ over it. Not all of these points are in $T(\mathbb{Z})_t$, but we will then produce a subset of $T(\mathbb{Z})_t$ whose closure is $\overline{T(\mathbb{Z})}_t$.

If $T(\mathbb{Z})_t$ is empty then $\overline{T(\mathbb{Z})}_t$ is empty, too. So we assume that we have an element $\tilde{t} \in T(\mathbb{Z})_t$ and we define $x_{\tilde{t}} \in J(\mathbb{Z})$ to be the projection of \tilde{t} . Let $f = (f_1, \dots, f_{\rho-1}) : J \rightarrow J^{\vee, \rho-1}$, let $c = (c_1, \dots, c_{\rho-1}) \in J^{\vee, \rho-1}(\mathbb{Z})$. We denote by $P^{\times, \rho-1}$ the product over $J \times (J^{\vee 0})^{\rho-1}$ of the $\rho-1$ \mathbb{G}_m -torsors obtained by pullback of P^\times via the projections to $J \times J^{\vee 0}$; it is a biextension of J and $(J^{\vee 0})^{\rho-1}$ by $\mathbb{G}_m^{\rho-1}$, and $T = (\text{id}, m \cdot \circ \text{tr}_c \circ f)^* P^{\times, \rho-1}$. We choose a basis x_1, \dots, x_r of the free \mathbb{Z} -module $J(\mathbb{Z})_0$, the kernel of $J(\mathbb{Z}) \rightarrow J(\mathbb{F}_p)$. For each $i, j \in \{1, \dots, r\}$ we choose $P_{i,j}$, $R_{i,\tilde{t}}$, and $S_{\tilde{t},j}$ in $P^{\times, \rho-1}(\mathbb{Z})$ whose images in $(J \times (J^{\vee 0})^{\rho-1})(\mathbb{Z})$ are $(x_i, f(mx_j))$, $(x_i, (m \cdot \circ \text{tr}_c \circ f)(x_{\tilde{t}}))$ and $(x_{\tilde{t}}, f(mx_j))$:

$$(4.1) \quad \begin{array}{ccccccc} P_{i,j} & & R_{i,\tilde{t}} & & S_{\tilde{t},j} & & P^{\times, \rho-1} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ (x_i, f(mx_j)) & & (x_i, (m \cdot \circ \text{tr}_c \circ f)(x_{\tilde{t}})) & & (x_{\tilde{t}}, f(mx_j)) & & J \times (J^{\vee 0})^{\rho-1}. \end{array}$$

For each such choice there are $2^{\rho-1}$ possibilities.

For each $n \in \mathbb{Z}^r$ we use the biextension structure on $P^{\times, \rho-1} \rightarrow J \times (J^{\vee 0})^{\rho-1}$ to define the following points in $P^{\times, \rho-1}(\mathbb{Z})$, with specified images in $(J \times (J^{\vee 0})^{\rho-1})(\mathbb{Z})$:

$$(4.2) \quad \begin{array}{ccc} A_{\tilde{t}}(n) = \sum_{j=1}^r n_j \cdot_2 S_{\tilde{t},j} & & B_{\tilde{t}}(n) = \sum_{i=1}^r n_i \cdot_1 R_{i,\tilde{t}} \\ \downarrow & & \downarrow \\ \left(x_{\tilde{t}}, \sum_{i=1}^r n_i f(mx_i) \right) & & \left(\sum_{i=1}^r n_i x_i, (m \cdot \circ \text{tr}_c \circ f)(x_{\tilde{t}}) \right) \end{array}$$

$$(4.3) \quad \begin{array}{c} C(n) = \sum_{i=1}^r n_i \cdot_1 \left(\sum_{j=1}^r n_j \cdot_2 P_{i,j} \right) \\ \downarrow \\ \left(\sum_{i=1}^r n_i x_i, \sum_{i=1}^r n_i f(mx_i) \right) \end{array}$$

where \sum_1 and \cdot_1 denote iterations of the first partial group law $+_1$ as in (2.4), and analogously for the second group law. We define, for all $n \in \mathbb{Z}^r$,

$$(4.4) \quad D_{\tilde{t}}(n) := (C(n) +_2 B_{\tilde{t}}(n)) +_1 (A_{\tilde{t}}(n) +_2 \tilde{t}) \in P^{\times, \rho-1}(\mathbb{Z}),$$

which is mapped to

$$(4.5) \quad \left(x_{\tilde{t}} + \sum_{i=1}^r n_i x_i, (m \cdot \circ \text{tr}_c \circ f) \left(x_{\tilde{t}} + \sum_{i=1}^r n_i x_i \right) \right) \in (J \times (J^{\vee 0})^{\rho-1})(\mathbb{Z}).$$

Hence $D_{\tilde{t}}(n)$ is in $T(\mathbb{Z})$, and its image in $J(\mathbb{F}_p)$ is $j_b(u)$. We do not know its image in $T(\mathbb{F}_p)$.

We claim that for n in $(p-1)\mathbb{Z}^r$, $D_{\tilde{t}}(n)$ is in $T(\mathbb{Z})_t$. Let n' be in \mathbb{Z}^r and let $n = (p-1)n'$. Then, in the trivial $\mathbb{F}_p^{\times, \rho-1}$ -torsor $P^{\times, \rho-1}(j_b(u), 0)$, on which $+_2$ is the group law, we have:

$$(4.6) \quad A_{\tilde{t}}(n) = (p-1) \cdot_2 A_{\tilde{t}}(n') = 1 \quad \text{in } \mathbb{F}_p^{\times, \rho-1}.$$

Similarly, in $P^{\times, \rho-1}(0, (m \cdot \circ \text{tr}_c \circ f)(j_b(u))) = \mathbb{F}_p^{\times, \rho-1}$, we have $B_{\tilde{t}}(n) = 1$, and, similarly, in $P^{\times, \rho-1}(0, 0) = \mathbb{F}_p^{\times, \rho-1}$, we have $C(n) = 1$. So, with apologies for the mix of additive and multiplicative notations, in $P^{\times, \rho-1}(\mathbb{F}_p)$ we have

$$(4.7) \quad D_{\tilde{t}}(n) = (1 +_2 1) +_1 (1 +_2 t) = t,$$

mapping to the following element in $(J \times J^{\vee 0, \rho-1})(\mathbb{F}_p)$:

$$(4.8) \quad \begin{aligned} & ((0, 0) +_2 ((0, (m \cdot \circ \text{tr}_c \circ f)(j_b(u)))) +_1 ((j_b(u), 0) +_2 (j_b(u), (m \cdot \circ \text{tr}_c \circ f)(j_b(u)))) \\ & = (j_b(u), (m \cdot \circ \text{tr}_c \circ f)(j_b(u))). \end{aligned}$$

We have proved our claim that $D_{\tilde{t}}(n) \in T(\mathbb{Z})_t$.

So we now have the map

$$(4.9) \quad \kappa_{\mathbb{Z}}: \mathbb{Z}^r \rightarrow T(\mathbb{Z})_t, \quad n \mapsto D_{\tilde{t}}((p-1)n).$$

The following theorem will be proved in Section 5.

4.10 Theorem *Let x_1, \dots, x_g be in $\mathcal{O}_{J, j_b(u)}$ such that together with p they form a system of parameters of $\mathcal{O}_{J, j_b(u)}$, and let $v_1, \dots, v_{\rho-1}$ be in $\mathcal{O}_{T, t}$ such that $p, x_1, \dots, x_g, v_1, \dots, v_{\rho-1}$ are parameters of $\mathcal{O}_{T, t}$. As in Section 3 these parameters, divided by p , give a bijection*

$$(4.10.1) \quad T(\mathbb{Z}_p)_t \longrightarrow \mathbb{Z}_p^{g+\rho-1}.$$

The composition of $\kappa_{\mathbb{Z}}$ with the map (4.10.1) is given by uniquely determined $\kappa_1, \dots, \kappa_{g+\rho-1}$ in $\mathcal{O}(\mathbb{A}_{\mathbb{Z}_p}^r)^{\wedge p} = \mathbb{Z}_p\langle z_1, \dots, z_r \rangle$. The images in $\mathbb{F}_p[z_1, \dots, z_r]$ of $\kappa_1, \dots, \kappa_g$ are of degree at most 1, and the images of $\kappa_{g+1}, \dots, \kappa_{g+\rho-1}$ are of degree at most 2. The map $\kappa_{\mathbb{Z}}$ extends uniquely to the continuous map

$$(4.10.2) \quad \kappa = (\kappa_1, \dots, \kappa_{g+\rho-1}): \mathbb{A}^r(\mathbb{Z}_p) = \mathbb{Z}_p^r \longrightarrow T(\mathbb{Z}_p)_t.$$

and the image of κ is $\overline{T(\mathbb{Z})_t}$.

Now the moment has come to confront $U(\mathbb{Z}_p)_u$ with $\overline{T(\mathbb{Z})_t}$. We have $\tilde{j}_b: U \rightarrow T$, whose tangent map $(\text{mod } p)$ at u is injective (here we use that $C_{\mathbb{F}_p}$ is smooth over \mathbb{F}_p). Then, as at the end of Section 3, $\tilde{j}_b: \widetilde{U}_u^p \rightarrow \widetilde{T}_t^p$ is, after reduction mod p , an affine linear embedding of codimension $g+\rho-2$, $\tilde{j}_b^*: \mathcal{O}(\widetilde{T}_t^p)^{\wedge p} \rightarrow \mathcal{O}(\widetilde{U}_u^p)^{\wedge p}$ is surjective and its kernel is generated by

elements $f_1, \dots, f_{g+\rho-2}$, whose images in $\mathbb{F}_p \otimes \mathcal{O}(\tilde{T}_t^p)$ are of degree at most 1, and such that f_1, \dots, f_{g-1} are in $\mathcal{O}(\tilde{J}_{jb(u)}^p)^{\wedge p}$. The pullbacks $\kappa^* f_i$ are in $\mathbb{Z}_p\langle z_1, \dots, z_r \rangle$; let I be the ideal in $\mathbb{Z}_p\langle z_1, \dots, z_r \rangle$ generated by them, and let

$$(4.11) \quad A := \mathbb{Z}_p\langle z_1, \dots, z_r \rangle / I.$$

Then the elements of \mathbb{Z}_p^r whose image is in $U(\mathbb{Z}_p)_u$ are zeros of I , hence morphisms of rings from A to \mathbb{Z}_p , and hence from the reduced quotient A_{red} to \mathbb{Z}_p .

4.12 Theorem For $i \in \{1, \dots, g+\rho-2\}$, let $\kappa^* \overline{f}_i$ be the image of $\kappa^* f_i$ in $\mathbb{F}_p[z_1, \dots, z_r]$, and let \overline{I} be the ideal of $\mathbb{F}_p[z_1, \dots, z_r]$ generated by them. Then $\kappa^* \overline{f}_1, \dots, \kappa^* \overline{f}_{g-1}$ are of degree at most 1, and $\kappa^* \overline{f}_g, \dots, \kappa^* \overline{f}_{g+\rho-2}$ are of degree at most 2. Assume that $\overline{A} := A/pA = \mathbb{F}_p[z_1, \dots, z_r]/\overline{I}$ is finite. Then \overline{A} is the product of its localisations \overline{A}_m at its finitely many maximal ideals m . The sum of the $\dim_{\mathbb{F}_p} \overline{A}_m$ over the m such that $\overline{A}/m = \mathbb{F}_p$ is an upper bound for the number of elements of \mathbb{Z}_p^r whose image under κ is in $U(\mathbb{Z}_p)_u$, and also an upper bound for the number of elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$.

Proof As every \overline{f}_i is of degree at most 1 in $x_1, \dots, x_g, v_1, \dots, v_{\rho-1}$, every $\kappa^* \overline{f}_i$ is an \mathbb{F}_p -linear combination of $\kappa_1, \dots, \kappa_{g+\rho-1}$, hence of degree at most 2. For $i < g$, \overline{f}_i is a linear combination of x_1, \dots, x_g , and therefore $\kappa^* \overline{f}_i$ is of degree at most 1.

We claim that A is p -adically complete. More generally, let R be a noetherian ring that is J -adically complete for an ideal J , and let I be an ideal in R . The map from R/I to its J -adic completion $(R/I)^\wedge$ is injective ([1, Thm.10.17]). As J -adic completion is exact on finitely generated R -modules ([1, Prop.10.12]), it sends the surjection $R \rightarrow R/I$ to a surjection $R = R^\wedge \rightarrow (R/I)^\wedge$ (see [1, Prop.10.5] for the equality $R = R^\wedge$). It follows that $R/I \rightarrow (R/I)^\wedge$ is surjective.

Now we assume that \overline{A} is finite. As A is p -adically complete, A is the limit of the system of its quotients by powers of p . These quotients are finite: for every $m \in \mathbb{Z}_{\geq 1}$, $A/p^{m+1}A$ is, as abelian group, an extension of A/pA by a quotient of $A/p^m A$. As \mathbb{Z}_p -module, A is generated by any lift of an \mathbb{F}_p -basis of \overline{A} . Hence A is finitely generated as \mathbb{Z}_p -module.

The set of elements of \mathbb{Z}_p^r whose image under κ is in $U(\mathbb{Z}_p)$ is in bijection with the set of \mathbb{Z}_p -algebra morphisms $\text{Hom}(A, \mathbb{Z}_p)$. As A is the product of its localisations A_m at its maximal ideals, $\text{Hom}(A, \mathbb{Z}_p)$ is the disjoint union of the $\text{Hom}(A_m, \mathbb{Z}_p)$. For each m , $\text{Hom}(A_m, \mathbb{Z}_p)$ has at most $\text{rank}_{\mathbb{Z}_p}(A_m)$ elements, and is empty if $\mathbb{F}_p \rightarrow A/m$ is not an isomorphism. This establishes the upper bound for the number of elements of \mathbb{Z}_p^r whose image under κ is in $U(\mathbb{Z}_p)$. By Theorem 4.10, the elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$ are in $\overline{T(\mathbb{Z})_t}$, and therefore of the form $\kappa(x)$ with $x \in \mathbb{Z}_p^r$ such that $\kappa(x)$ is in $U(\mathbb{Z}_p)_u$. This establishes the upper bound for the number of elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$. \square

We include some remarks to explain how Theorem 4.12 can be used, and what we hope that it can do.

4.13 Remark The $\kappa^* \overline{f}_i$ in Theorem 4.12 can be computed from the reduction $\mathbb{F}_p^r \rightarrow T(\mathbb{Z}/p^2\mathbb{Z})$ of $\kappa_{\mathbb{Z}}$ and (to get the \overline{f}_i) from $\tilde{j}_b: U(\mathbb{Z}/p^2\mathbb{Z})_u \rightarrow T(\mathbb{Z}/p^2\mathbb{Z})_t$. For this, one does not need to

treat T and J as schemes, one just computes with $\mathbb{Z}/p^2\mathbb{Z}$ -valued points. Now assume that $r \leq g + \rho - 2$. If, for some prime p , the criterion in Theorem 4.12 fails (that is, \overline{A} is not finite), then one can try the next prime. We hope (but also expect) that one quickly finds a prime p such that \overline{A} is finite for every U and for every u in $U(\mathbb{F}_p)$ such that $\tilde{j}_b(u)$ is in the image of $T(\mathbb{Z}) \rightarrow T(\mathbb{F}_p)$. By the way, note that our notation in Theorem 4.12 does not show the dependence on U and u of \tilde{j}_b , $\kappa_{\mathbb{Z}}$, κ and the \overline{f}_i .

Already for the case of classical Chabauty (working with J instead of T , and under the assumption that $r < g$), where everything is linear, the criterion of Theorem 4.12 can be useful; this is currently being worked out and implemented by Pim Spelier in his MSc thesis.

4.14 Remark If $r < g + \rho - 2$ then we think that it is likely (when varying p), for dimension reasons, that, for all $u \in U(\mathbb{F}_p)$, the upper bound in Theorem 4.12 for the number of elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$ is sharp.

4.15 Remark Suppose that $r = g + \rho - 2$. Then we expect, for dimension reasons, that it is likely (when varying p) that, for some $u \in U(\mathbb{F}_p)$, the upper bound in Theorem 4.12 for the number of elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$ is not sharp. Then, as in the classical Chabauty method, one must combine the information gotten from several primes, analogous to ‘Mordell-Weil sieving’. Suppose that we are given a subset B of $U(\mathbb{Z})$ that we want to prove to be equal to $U(\mathbb{Z})$. Let B' be the complement in $U(\mathbb{Z})$ of B . For every prime $p > 2$ not dividing n , Theorem 4.12 gives, interpreting \overline{A} as in the end of the proof of Theorem 4.12, a subset O_p of $J(\mathbb{Z})$, that is a union of cosets for the subgroup $p \cdot \ker(J(\mathbb{Z}) \rightarrow J(\mathbb{F}_p))$, that contains $j_b(B')$. Then one hopes that, taking a large enough finite set S of primes, that the intersection of the O_p for p in S is empty.

5 Parametrisation of integral points, and power series

In this section we give a proof of Theorem 4.10. The main tools here are the formal logarithm and formal exponential of a commutative smooth group scheme over a \mathbb{Q} -algebra ([5], Theorem 1): they give us identities as $n \cdot g = \exp(n \cdot \log g)$ that allow us to extend the multiplication to elements n of \mathbb{Z}_p .

The evaluation map from $\mathbb{Z}_p\langle z_1, \dots, z_n \rangle$ to the set of maps $\mathbb{Z}_p^n \rightarrow \mathbb{Z}_p$ is injective (induction on n , non-zero elements of $\mathbb{Z}_p\langle z \rangle$ have only finitely many zeros in \mathbb{Z}_p).

We say that a map $f: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^m$ is given by integral convergent power series if its coordinate functions are in $\mathbb{Z}_p\langle z_1, \dots, z_n \rangle = \mathcal{O}(\mathbb{A}_{\mathbb{Z}_p}^n)^{\wedge_p}$. This property is stable under composition: composition of polynomials over $\mathbb{Z}/p^k\mathbb{Z}$ gives polynomials.

5.1 Logarithm and exponential

Let p be a prime number, and let G be a commutative group scheme, smooth of relative dimension d over a scheme S smooth over \mathbb{Z}_p , with unit section e in $G(S)$. For any s in $S(\mathbb{F}_p)$, $G(\mathbb{Z}_p)_{e(s)}$ is a group fibred over $S(\mathbb{Z}_p)_s$. The fibres have a natural \mathbb{Z}_p -module structure: $G(\mathbb{Z}_p)_{e(s)}$ is the limit of the $G(\mathbb{Z}/p^n\mathbb{Z})_{e(s)}$ ($n \geq 1$), $S(\mathbb{Z}_p)_s$ is the limit of the $S(\mathbb{Z}/p^n\mathbb{Z})_s$, and for each

$n \geq 1$, the fibres of $G(\mathbb{Z}/p^n\mathbb{Z})_{e(s)} \rightarrow S(\mathbb{Z}/p^n\mathbb{Z})_s$ are commutative groups annihilated by p^{n-1} . Let $T_{G/S}$ be the relative (geometric) tangent bundle of G over S . Then its pullback $T_{G/S}(e)$ by e is a vector bundle on S of rank d .

5.1.1 Lemma *In this situation, and with n the relative dimension of S over \mathbb{Z}_p , the formal logarithm and exponential of G base changed to $\mathbb{Q} \otimes \mathcal{O}_{S,s}$ converge to maps*

$$\begin{aligned}\log: \tilde{G}_{e(s)}^p(\mathbb{Z}_p) &= G(\mathbb{Z}_p)_{e(s)} \rightarrow (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \\ \exp: \tilde{T}_{G/S}(e)_{0(s)}^p(\mathbb{Z}_p) &= (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \rightarrow G(\mathbb{Z}_p)_{e(s)},\end{aligned}$$

that are each others inverse and, after a choice of parameters for $G \rightarrow S$ at $e(s)$ as in (3.1), are given by $n + d$ elements of $\mathcal{O}(\tilde{G}_{e(s)}^p)^{\wedge p}$ and $n + d$ elements of $\mathcal{O}(\tilde{T}_{G/S}(e)_{0(s)}^p)^{\wedge p}$.

For a in \mathbb{Z}_p and g in $G(\mathbb{Z}_p)_{e(s)}$ we have $a \cdot g = \exp(a \cdot \log g)$, and, after a choice of parameters for $G \rightarrow S$ at $e(s)$, this map $\mathbb{Z}_p \times G(\mathbb{Z}_p)_{e(s)} \rightarrow G(\mathbb{Z}_p)_{e(s)}$ is given by $n + d$ elements of $\mathcal{O}(\mathbb{A}_{\mathbb{Z}_p}^1 \times_{\mathbb{Z}_p} \tilde{G}_{e(s)}^p)^{\wedge p}$. The induced morphism $\mathbb{A}_{\mathbb{F}_p}^1 \times (\tilde{G}_{e(s)}^p)_{\mathbb{F}_p} \rightarrow (\tilde{G}_{e(s)}^p)_{\mathbb{F}_p}$, where $(\tilde{G}_{e(s)}^p)_{\mathbb{F}_p}$ is viewed as the product $T_{S_{\mathbb{F}_p}}(s)$ and $T_{G/S}(e(s))$, is a morphism over $T_{S_{\mathbb{F}_p}}(s)$, bilinear in $\mathbb{A}_{\mathbb{F}_p}^1$ and $T_{G/S}(e(s))$.

Proof Let t_1, \dots, t_n be in $\mathcal{O}_{S,s}$ such that p, t_1, \dots, t_n are parameters at s . Then we have a bijection

$$(5.1.2) \quad \tilde{t}: S(\mathbb{Z}_p)_s \rightarrow \mathbb{Z}_p^n, \quad a \mapsto p^{-1} \cdot (t_1(a), \dots, t_n(a)).$$

Similarly, let x_1, \dots, x_d be generators for the ideal $I_{e(s)}$ of e in $\mathcal{O}_{G,e(s)}$. Then p , the t_i and the x_j together are parameters for $\mathcal{O}_{G,e(s)}$, and give the bijection

$$(5.1.3) \quad (t, x)^\sim: G(\mathbb{Z}_p)_{e(s)} \rightarrow \mathbb{Z}_p^{n+d}, \quad b \mapsto p^{-1} \cdot (t_1(b), \dots, t_n(b), x_1(b), \dots, x_d(b)).$$

The dx_i form an $\mathcal{O}_{S,s}$ -basis of $\Omega_{G/S}^1(e)_s$, and so give translation invariant differentials ω_i on $G_{\mathcal{O}_{S,s}}$. As G is commutative, for all i , $d\omega_i = 0$ ([5], Proposition 1.3). We also have the dual $\mathcal{O}_{S,s}$ -basis ∂_i of $T_{G/S}(e)$ and the bijection

$$(5.1.4) \quad (t, x)^\sim: (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \rightarrow \mathbb{Z}_p^{n+d}, \quad (a, \sum_i v_i \partial_i) \mapsto p^{-1} \cdot (t_1(a), \dots, t_n(a), v_1, \dots, v_d).$$

Then \log is given by elements \log_i in $(\mathbb{Q} \otimes \mathcal{O}_{S,s})[[x_1, \dots, x_d]]$ whose constant term is 0, uniquely determined (Proposition 1.1 in [5]) by the equality

$$(5.1.5) \quad d\log_i = \omega_i, \quad \text{in } \oplus_j \mathcal{O}_{S,s}[[x_1, \dots, x_d]] \cdot dx_j.$$

Hence the formula from calculus, $\log_i(x) - \log_i(0) = \int_0^1 (t \mapsto tx)^* \omega_i$, gives us that, with

$$(5.1.6) \quad \log_i = \sum_{J \neq 0} \log_{i,J} x^J \quad \text{and} \quad \log_{i,J} \in (\mathbb{Q} \otimes \mathcal{O}_{S,s}),$$

we have, for all i and J , with $|J|$ denoting the total degree of x^J ,

$$(5.1.7) \quad |J| \cdot \log_{i,J} \in \mathcal{O}_{S,s}.$$

The claim about convergence and definition of $\log: G(\mathbb{Z}_p)_{e(s)} \rightarrow (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)}$, is now equivalent to having an analytic bijection $\mathbb{Z}_p^{n+d} \rightarrow \mathbb{Z}_p^{n+d}$ given by

$$(5.1.8) \quad \begin{array}{ccc} G(\mathbb{Z}_p)_{e(s)} & \xrightarrow{\quad ? \quad} & (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \\ \downarrow (t,x)^\sim & & \downarrow (t,x)^\sim \\ \mathbb{Z}_p^{n+d} & \xrightarrow{\quad ? \quad} & \mathbb{Z}_p^{n+d} \end{array}$$

$$(a, b) \xrightarrow{\quad ? \quad} \left(a, p^{-1} \cdot \left(\sum_{J \neq 0} \log_{i,J}(\tilde{t}^{-1}(a))(pb)^J \right)_i \right).$$

We have, for each i ,

$$(5.1.9) \quad p^{-1} \cdot \sum_{J \neq 0} \log_{i,J}(\tilde{t}^{-1}(a))(pb)^J = \sum_{J \neq 0} \frac{p^{|J|-1}}{|J|} (|J| \log_{i,J})(\tilde{t}^{-1}(a))b^J.$$

For each i , this expression is an element of $\mathbb{Z}_p\langle \tilde{t}_1, \dots, \tilde{t}_n, \tilde{x}_1, \dots, \tilde{x}_d \rangle = \mathcal{O}(\tilde{G}_{e(s)}^p)^{\wedge_p}$, even when $p = 2$, because for each J , $|J| \log_{i,J}$ is in $\mathcal{O}_{S,s}$, which is contained in $\mathbb{Z}_p\langle \tilde{t}_1, \dots, \tilde{t}_n \rangle$, and the function $\mathbb{Z}_{\geq 1} \rightarrow \mathbb{Q}_p$, $r \mapsto p^{r-1}/r$ has values in \mathbb{Z}_p and converges to 0. The existence and analyticity of \log is now proved (even for $p = 2$). As $p > 2$, the image of (5.1.9) in $\mathbb{F}_p \otimes \mathcal{O}(\tilde{G}_{e(s)}^p)^{\wedge_p}$ is \tilde{x}_i , and on the first n coordinates, \log is the identity, so, by applying Hensel modulo powers of p , \log is invertible, and the inverse is also given by $n + d$ elements of $\mathcal{O}(\tilde{T}_{G/S}(e)_{0(s)}^p)^{\wedge_p}$.

The function $\mathbb{Z}_p \times G(\mathbb{Z}_p)_{e(s)} \rightarrow G(\mathbb{Z}_p)_{e(s)}$, $(a, g) \mapsto \exp(a \cdot \log g)$ is a composition of maps given by integral convergent power series, hence it is also of that form. \square

5.2 Parametrisation by power series

The assumptions are as in the beginning of Section 4, in particular, $p > 2$. We have a t in $T(\mathbb{F}_p)$, with image $j_b(u)$ in $J(\mathbb{F}_p)$, and a \tilde{t} in $T(\mathbb{Z})$ lifting t . For every Q in $T(\mathbb{Z})$ mapping to $j_b(u)$ in $J(\mathbb{F}_p)$ there are unique $\varepsilon \in \mathbb{Z}^{\times, \rho-1}$ and $n \in \mathbb{Z}^r$ such that $Q = \varepsilon \cdot D_{\tilde{t}}(n)$: the image of Q in $J(\mathbb{Z})$ is in $J(\mathbb{Z})_{j_b(u)}$, hence differs from the image $x_{\tilde{t}}$ in $J(\mathbb{Z})$ of \tilde{t} by an element of $J(\mathbb{Z})_0$ (with here $0 \in J(\mathbb{F}_p)$), $\sum_i n_i x_i$ for a unique $n \in \mathbb{Z}^r$, hence $D_{\tilde{t}}(n)$ and Q are in $T(\mathbb{Z})$ and have the same image in $J(\mathbb{Z})$, and that gives the unique ε . So we have a bijection

$$(5.2.1) \quad \mathbb{Z}^{\times, \rho-1} \times \mathbb{Z}^r \longrightarrow T(\mathbb{Z})_{j_b(u)} = \{Q \in T(\mathbb{Z}) : Q \mapsto j_b(u) \in J(\mathbb{F}_p)\}, \quad (\varepsilon, n) \mapsto \varepsilon \cdot D_{\tilde{t}}(n).$$

But a problem that we are facing is that the map $\mathbb{Z}^r \rightarrow T(\mathbb{F}_p)_{j_b(u)}$ sending n to the image of $D_{\tilde{t}}(n)$ depends on the (unkown) images of the $P_{i,j}$, $R_{i,\tilde{t}}$ and $S_{\tilde{t},j}$ from (4.1) in $P^{\times, \rho-1}(\mathbb{F}_p)$, and so we do not know for which n and ε the point $\varepsilon \cdot D_{\tilde{t}}(n)$ is in $T(\mathbb{Z})_t$. Luckily we have the $\mathbb{Z}_p^{\times, \rho-1}$ -action on $T(\mathbb{Z}_p)$. Using that $\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$ we have $\mathbb{F}_p^{\times, \rho-1}$ acting on $T(\mathbb{Z}_p)_{j_b(u)}$, compatibly with the torsor structure on $T(\mathbb{F}_p)_{j_b(u)}$. So, for every n in \mathbb{Z}^r there is a unique $\xi(n)$ in $\mathbb{F}_p^{\times, \rho-1}$ such that $\xi(n) \cdot D_{\tilde{t}}(n)$ is in $T(\mathbb{Z}_p)_t$. We define

$$(5.2.2) \quad D'(n) := \xi(n) \cdot D_{\tilde{t}}(n).$$

Then for all n in \mathbb{Z}^r ,

$$(5.2.3) \quad \kappa_{\mathbb{Z}}(n) = D_{\tilde{t}}((p-1) \cdot n) = D'((p-1) \cdot n),$$

because $D_{\tilde{t}}((p-1)\cdot n)$ maps to t in $T(\mathbb{F}_p)$. Moreover for every Q in $T(\mathbb{Z})_t$ there is a unique $n \in \mathbb{Z}^r$ and a unique $\varepsilon \in \mathbb{Z}^{\times, \rho-1}$ such that $Q = \varepsilon \cdot D_{\tilde{t}}(n) = \xi(n) \cdot D_{\tilde{t}}(n) = D'(n)$. Hence

$$(5.2.4) \quad T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r).$$

We will now show that, after any choice of parameters of $\mathcal{O}_{T,t}$ as in Theorem 4.10, D' is given by elements $\kappa'_1, \dots, \kappa'_{g+\rho-1}$ of $\mathcal{O}(\mathbb{A}_{\mathbb{Z}_p}^r)^{\wedge_p}$, and then $\kappa_{\mathbb{Z}}$ is given by $\kappa_1, \dots, \kappa_{g+\rho-1}$ with, for all $i \in \{1, \dots, g+\rho-1\}$ and all $a \in \mathbb{Z}_p^r$, $\kappa_i(a) = \kappa'_i((p-1)a)$.

We want a formula for $D'(n)$, so we introduce variants of the $P_{i,j}$, $R_{i,\tilde{t}}$, and $S_{\tilde{t},j}$ as follows. The images in $(J \times (J^{\vee 0})^{\rho-1})(\mathbb{F}_p)$ of these points are of the form $(0, *)$, $(0, *)$, and $(*, 0)$, respectively. Hence the fibers over them of $P^{\times, \rho-1}$ are rigidified, that is, equal to $\mathbb{F}_p^{\times, \rho-1}$. We define their variants $P'_{i,j}$, $R'_{i,\tilde{t}}$, and $S'_{\tilde{t},j}$ in $P^{\times, \rho-1}(\mathbb{Z}_p)$ to be the unique elements in their orbits under $\mathbb{F}_p^{\times, \rho-1}$ whose images in $P^{\times, \rho-1}(\mathbb{F}_p)$ are equal to the element 1 in $\mathbb{F}_p^{\times, \rho-1}$. Replacing, in (4.2) and (4.3), these $P_{i,j}$, $R_{i,\tilde{t}}$, and $S_{\tilde{t},j}$ by $P'_{i,j}$, $R'_{i,\tilde{t}}$, and $S'_{\tilde{t},j}$ gives variants A' , B' and C' , and using these in (4.4) gives a variant $D'_{\tilde{t}}(n)$ of 5.2.2. Then, for all n in \mathbb{Z}^r , $D'_{\tilde{t}}(n)$ and $D'(n)$ (as in (5.2.2)) are equal, because both are in $P^{\times, \rho-1}(\mathbb{Z}_p)_t$, and in the same $\mathbb{F}_p^{\times, \rho-1}$ -orbit. Hence we have, for all n in \mathbb{Z}^r :

$$(5.2.5) \quad \begin{aligned} A'(n) &= \sum_{j=1}^r n_j \cdot_2 S'_{\tilde{t},j}, \quad B'(n) = \sum_{i=1}^r n_i \cdot_1 R'_{i,\tilde{t}}, \\ C'(n) &= \sum_{i=1}^r n_i \cdot_1 \left(\sum_{j=1}^r n_j \cdot_2 P'_{i,j} \right), \\ D'(n) &= (C'(n) +_2 B'(n)) +_1 (A'(n) +_2 \tilde{t}). \end{aligned}$$

This shows how the map $n \mapsto D'(n)$ is built up from the two partial group laws $+_1$ and $+_2$ on $P^{\times, \rho-1}$, and the iterations \cdot_1 and \cdot_2 . Lemma 5.1.1 gives that the iterations are given by integral convergent power series. The functoriality in Section 3 gives that the maps induced by $+_1$ and $+_2$ on residue polydisks are given by integral convergent power series. Stability under composition then gives that $n \mapsto D'(n)$ is given by elements $\kappa'_1, \dots, \kappa'_{g+\rho-1}$ of $\mathbb{Z}_p\langle z_1, \dots, z_r \rangle$.

We call the κ'_i the coordinate functions of the extension $D': \mathbb{Z}_p^r \rightarrow T(\mathbb{Z}_p)_t = \mathbb{Z}_p^{g+\rho-1}$, and their images $\bar{\kappa}'_1, \dots, \bar{\kappa}'_{g+\rho-1}$ in $\mathbb{F}_p[z_1, \dots, z_r]$ the mod p coordinate functions, viewed as a morphism $\overline{D}'_{\mathbb{F}_p}: \mathbb{A}_{\mathbb{F}_p}^r \rightarrow \mathbb{A}_{\mathbb{F}_p}^{g+\rho-1}$.

The mod p coordinate functions of $A': \mathbb{Z}_p^r \rightarrow P^{\times, \rho-1}(\mathbb{Z}_p) = \mathbb{Z}_p^{\rho g + \rho - 1}$ (after choosing the necessary parameters) are all of degree at most 1. The same holds for B' . We define

$$(5.2.6) \quad C'_2: \mathbb{Z}^r \times \mathbb{Z}^r \longrightarrow P^{\times, \rho-1}(\mathbb{Z}_p), \quad C'_2(n, m) = \sum_{i=1}^r n_i \cdot_1 \left(\sum_{j=1}^r m_j \cdot_2 P'_{i,j} \right).$$

Then the mod p coordinate functions of C'_2 , elements of $\mathbb{F}_p[x_1, \dots, x_r, y_1, \dots, y_r]$, are linear in the x_i , and in the y_j . Hence of degree at most 2, and the same follows for the mod p coordinate functions of C' . However, as the first ρg parameters for $P^{\times, \rho-1}$ come from $J \times J^{\vee \rho-1}$, and the 1st and 2nd partial group laws there act on different factors, the first ρg mod p coordinate functions of C' are in fact linear. As D' is obtained by summing, using the partial group laws, the results of A' , B and C' , we conclude that $\bar{\kappa}'_1, \dots, \bar{\kappa}'_g$ are of degree at most 1, and the remaining $\bar{\kappa}_j$ are of degree at most 2. The same holds then for all $\bar{\kappa}_j$.

5.3 The p -adic closure

We know from (5.2.3) that $\kappa_{\mathbb{Z}}(\mathbb{Z}^r) = D'((p-1)\mathbb{Z}^r)$. From (4.9) we know that $\kappa_{\mathbb{Z}}(\mathbb{Z}^r) \subset T(\mathbb{Z})_t$. From (5.2.4) we know that $T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r)$. So together we have:

$$(5.3.1) \quad D'((p-1)\mathbb{Z}^r) = \kappa_{\mathbb{Z}}(\mathbb{Z}^r) \subset T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r).$$

We have extended D' to a continuous map $\mathbb{Z}_p^r \rightarrow T(\mathbb{Z}_p)_t$. As \mathbb{Z}_p^r is compact, $D'(\mathbb{Z}_p^r)$ is closed in $T(\mathbb{Z}_p)_t$. As \mathbb{Z}^r and $(p-1)\mathbb{Z}^r$ are dense in \mathbb{Z}_p^r , the closures of their images under D' are both equal to $D'(\mathbb{Z}_p^r)$, and equal to $\kappa(\mathbb{Z}_p^r)$. This finishes the proof of Theorem 4.10.

6 Explicit description of the Poincaré torsor

We give an explicit description of the Poincaré torsor on $J \times J^{\vee,0}$ and its partial group laws, in terms of divisors and invertible \mathcal{O} -modules on C , first over $\mathbb{Z}[1/n]$, where C is smooth, and then over \mathbb{Z} .

6.1 Norms

Let S be a scheme, $f: S' \rightarrow S$ be finite and locally free, say of rank n . Then $\mathcal{O}_{S'} = f_*\mathcal{O}_{S'}$ (we view $\mathcal{O}_{S'}$ as a sheaf on S) is an \mathcal{O}_S -algebra, locally free as \mathcal{O}_S -module of rank n , and $\mathcal{O}_{S'}^\times$ is a subsheaf of groups of $\mathrm{GL}_{\mathcal{O}_S}(\mathcal{O}_{S'})$. Then the norm morphism is the composition

$$(6.1.1) \quad \mathcal{O}_{S'}^\times \xrightarrow{\quad} \mathrm{GL}_{\mathcal{O}_S}(\mathcal{O}_{S'}) \xrightarrow{\det} \mathcal{O}_S^\times$$

For T an $\mathcal{O}_{S'}^\times$ -torsor (triviality locally on S and S' are equivalent, from the equivalence with invertible $\mathcal{O}_{S'}$ -modules), we let $\mathrm{Norm}_{S'/S}(T)$ be the \mathcal{O}_S^\times -torsor

$$(6.1.2) \quad \mathrm{Norm}_{S'/S}(T) := \mathcal{O}_S^\times \otimes_{\mathcal{O}_{S'}^\times} T = (\mathcal{O}_S^\times \times T) / \mathcal{O}_{S'}^\times,$$

with, for every open U of S , and every $u \in \mathcal{O}_{S'}^\times(U)$, u acting as $(v, t) \mapsto (v \cdot \mathrm{Norm}_{S'/S}(u), u^{-1} \cdot t)$. This is functorial in T : a morphism $\varphi: T_1 \rightarrow T_2$ induces an isomorphism $\mathrm{Norm}_{S'/S}(\varphi)$. It is also functorial for cartesian diagrams $(S'_2 \rightarrow S_2) \rightarrow (S'_1 \rightarrow S_1)$.

For $U \subset S$ open, T an $\mathcal{O}_{S'}^\times$ -torsor, and $t \in T(U)$, we have the isomorphism of $\mathcal{O}_{S'}^\times|_U$ -torsors $\mathcal{O}_{S'}^\times|_U \rightarrow T|_U$ sending 1 to t . Functoriality gives $\mathrm{Norm}_{S'/S}(t)$ in $(\mathrm{Norm}_{S'/S}(T))(U)$, also denoted $1 \otimes t$.

The norm functor (6.1.2) is multiplicative:

$$(6.1.3) \quad \mathrm{Norm}_{S'/S}(T_1 \otimes_{\mathcal{O}_{S'}} T_2) = \mathrm{Norm}_{S'/S}(T_1) \otimes_{\mathcal{O}_S} \mathrm{Norm}_{S'/S}(T_2),$$

such that, if $U \subset S$ is open and t_1 and t_2 are in $T_1(U)$ and $T_2(U)$, then

$$(6.1.4) \quad \mathrm{Norm}_{S'/S}(t_1 \otimes t_2) \mapsto \mathrm{Norm}_{S'/S}(t_1) \otimes \mathrm{Norm}_{S'/S}(t_2).$$

Let \mathcal{L} be an invertible $\mathcal{O}_{S'}$ -module; locally on S , it is free of rank 1 as $\mathcal{O}_{S'}$ -module. This gives us the $\mathcal{O}_{S'}^\times$ -torsor (on S) $\text{Isom}_{\mathcal{O}_{S'}}(\mathcal{O}_{S'}, \mathcal{L})$, which gives back \mathcal{L} as $\mathcal{L} = \mathcal{O}_{S'} \otimes_{\mathcal{O}_{S'}^\times} \text{Isom}_{\mathcal{O}_{S'}}(\mathcal{O}_{S'}, \mathcal{L})$. The norm of \mathcal{L} via $f: S' \rightarrow S$ is then defined as

$$(6.1.5) \quad \text{Norm}_{S'/S}(\mathcal{L}) := \mathcal{O}_S \otimes_{\mathcal{O}_S^\times} \text{Norm}_{S'/S}(\text{Isom}_{\mathcal{O}_{S'}}(\mathcal{O}_{S'}, \mathcal{L})) .$$

This construction is functorial for isomorphisms of invertible $\mathcal{O}_{S'}$ -modules.

6.2 Norms along finite relative Cartier divisors

This part is inspired by [6], section 1.1. Let S be a scheme, let $f: X \rightarrow S$ be an S -scheme of finite presentation. A finite effective relative Cartier divisor on $f: X \rightarrow S$ is a closed subscheme D of X that is finite and locally free over S , and whose ideal sheaf I_D is locally generated by a non-zero divisor (equivalently, I_D is locally free of rank 1 as \mathcal{O}_X -module). For such a D and an invertible \mathcal{O}_X -module \mathcal{L} , the norm of \mathcal{L} along D is defined, using (6.1.5), as

$$(6.2.1) \quad \text{Norm}_{D/S}(\mathcal{L}) := \text{Norm}_{D/S}(\mathcal{L}|_D) .$$

Then $\text{Norm}_{D/S}(\mathcal{L})$ is functorial for cartesian diagrams $(X' \rightarrow S', \mathcal{L}') \rightarrow (X \rightarrow S, \mathcal{L})$.

6.2.2 Lemma *Let $f: X \rightarrow S$ be a morphism of schemes that is of finite presentation. For D a finite effective relative Cartier divisor on f , the norm functor $\text{Norm}_{D/S}$ in (6.2.1) is multiplicative in \mathcal{L} :*

$$(6.2.3) \quad \text{Norm}_{D/S}(\mathcal{L}_1 \otimes \mathcal{L}_2) = \text{Norm}_{D/S}(\mathcal{L}_1) \otimes_{\mathcal{O}_S} \text{Norm}_{D/S}(\mathcal{L}_2) ,$$

with, for $U \subset S$ open, $V \subset X$ open, containing $f^{-1}U \cap D$ and $l_i \in \mathcal{L}_i(V)$ generating $\mathcal{L}_i|_V$,

$$(6.2.4) \quad \text{Norm}_{D/S}(l_1 \otimes l_2) = \text{Norm}_{D/S}(l_1) \otimes \text{Norm}_{D/S}(l_2) .$$

Let D_1 and D_2 be finite effective relative Cartier divisors on f . Then the ideal sheaf $I_{D_1}I_{D_2} \subset \mathcal{O}_X$ is locally free of rank 1, the closed subscheme $D_1 + D_2$ defined by it is a finite effective relative Cartier divisor on f . The norm functor in (6.2.1) is additive in D :

$$(6.2.5) \quad \text{Norm}_{(D_1+D_2)/S}(\mathcal{L}) = \text{Norm}_{D_1/S}(\mathcal{L}) \otimes_{\mathcal{O}_S} \text{Norm}_{D_2/S}(\mathcal{L}) ,$$

with, for $U \subset S$ open, $V \subset X$ open, containing $f^{-1}U \cap (D_1 + D_2)$ and $l \in \mathcal{L}(V)$ generating $\mathcal{L}|_{D_1+D_2}$,

$$(6.2.6) \quad \text{Norm}_{(D_1+D_2)/S}(l) = \text{Norm}_{D_1/S}(l) \otimes \text{Norm}_{D_2/S}(l) .$$

Proof Let D_1 and D_2 be as stated. If $V \subset X$ is open, and f_i generates $I_{D_i}|_V$, then f_1f_2 generates $(I_{D_1}I_{D_2})|_V$, and this element of $\mathcal{O}_X(V)$ is not a zero-divisor because f_1 and f_2 are not. To show that $D_1 + D_2$ is affine over S , we replace S by an affine open of it, and then reduce to the noetherian case, using the assumption that f is of finite presentation. Then,

$(D_1 + D_2)_{\text{red}}$ is the image of $D_{1,\text{red}} \coprod D_{2,\text{red}} \rightarrow X$, and therefore is proper. Hence $D_1 + D_2$ is proper over S , and quasi-finite over S , hence finite over S . The short exact sequence

$$(6.2.7) \quad \begin{array}{ccc} I_{D_2}/I_{D_1+D_2} & \hookrightarrow & \mathcal{O}_{D_1+D_2} \\ \parallel & & \\ (I_{D_2})|_{D_1} & & \end{array}$$

shows that $\mathcal{O}_{D_1+D_2}$ is locally free as \mathcal{O}_S -module, of rank the sum of the ranks of the \mathcal{O}_{D_i} . So $D_1 + D_2$ is a finite effective relative Cartier divisor on $X \rightarrow S$.

We prove (6.2.5), by proving the required statement about sheaves of groups. The diagram

$$(6.2.8) \quad \begin{array}{ccccc} & & \text{Norm}_{(D_1+D_2)/S} & & \\ & \swarrow & & \searrow & \\ \mathcal{O}_{D_1+D_2}^\times & \longrightarrow & \mathcal{O}_{D_1}^\times \times \mathcal{O}_{D_2}^\times & \xrightarrow{\text{Norm}_{D_1/S} \times \text{Norm}_{D_2/S}} & \mathcal{O}_S^\times \times \mathcal{O}_S^\times \longrightarrow \dots \longrightarrow \mathcal{O}_S^\times \\ u \longmapsto & & & & \rightarrow \text{Norm}_{D_1/S}(u)\text{Norm}_{D_2/S}(u). \end{array}$$

commutes, because multiplication by u on $\mathcal{O}_{D_1+D_2}$ preserves the short exact sequence (6.2.7), multiplying on the sub and quotient by its images in $\mathcal{O}_{D_1}^\times$ and in $\mathcal{O}_{D_2}^\times$; note that the sub is an invertible \mathcal{O}_{D_1} -module. \square

6.3 Explicit description of the Poincaré torsor of a smooth curve

Let g be in $\mathbb{Z}_{\geq 1}$, let S be a scheme, and $\pi: C \rightarrow S$ be a proper smooth curve, with geometrically connected fibres of genus g , with a section $b \in C(S)$. Let $J \rightarrow S$ be its jacobian. On $C \times_S J$ we have $\mathcal{L}^{\text{univ}}$, the universal invertible \mathcal{O} -module of degree zero on C , rigidified at b .

Let $d \geq 0$, and $C^{(d)}$ the d th symmetric power of $C \rightarrow S$ (we note that the quotient $C^d \rightarrow C^{(d)}$ is finite, locally free of rank $d!$, and commutes with base change on S). Then on $C \times_S C^{(d)}$ we have D , the universal effective relative Cartier divisor on C of degree d . Hence, on $C \times_S J \times_S C^{(d)}$ we have their pullbacks D_J and $\mathcal{L}_{C^{(d)}}^{\text{univ}}$, giving us

$$(6.3.1) \quad \mathcal{N}_d := \text{Norm}_{D_J/(J \times_S C^{(d)})}(\mathcal{L}_{C^{(d)}}^{\text{univ}}).$$

This invertible \mathcal{O} -module \mathcal{N}_d on $J \times_S C^{(d)}$, rigidified at the zero-section of J , gives us a morphism of S -schemes $C^{(d)}$ to $\text{Pic}_{J/S}$. The point db (the divisor d times the base point b) in $C^{(d)}(S)$ is mapped to 0, precisely because $\mathcal{L}^{\text{univ}}$ is rigidified at b , and 6.2.5. Hence there is a unique morphism $\square: C^{(d)} \rightarrow J^\vee = \text{Pic}_{J/S}^0$ such that the pullback of the Poincaré bundle P on $J \times J^\vee$ by $(\text{id}, \square): J \times C^{(d)} \rightarrow J \times J^\vee$, with its rigidifications, is the same as \mathcal{N}_d . The following proposition tells us what the morphism \square is, and the next section tells us what the induced isomorphism is between the fibres of \mathcal{N}_d at points of $J \times C^{(d)}$ with the same image in $J \times_S J$.

6.3.2 Proposition The pullback of P by $(j_b, j_b^{*, -1}): C \times_S J \rightarrow J \times_S J^\vee$ together with its rigidifications at b and 0 , is equal to $\mathcal{L}^{\text{univ}}$.

Let d be in $\mathbb{Z}_{\geq 0}$. The morphism $\square: C^{(d)} \rightarrow J^\vee = \text{Pic}_{J/S}^0$ is the composition of first $\Sigma: C^{(d)} \rightarrow J$, sending, for every S -scheme T and any D in $C^{(d)}(T)$ to the class of $\mathcal{O}_{C_T}(D - db)$ twisted by the pullback from T that makes it rigidified at b , followed by $j_b^{*, -1}: J \rightarrow J^\vee$. Summarised in a diagram, with $\mathcal{M} := (\text{id} \times j_b^{*, -1})^* P$:

$$(6.3.3) \quad \begin{array}{ccccccc} \mathcal{L}^{\text{univ}} & \xleftarrow{\hspace{1cm}} & P & \xrightarrow{\hspace{1cm}} & \mathcal{M} & \xrightarrow{\widetilde{\text{id} \times \Sigma}} & \mathcal{N}_d \\ C \times_S J & \xrightarrow{j_b \times j_b^{*, -1}} & J \times_S J^\vee & \xleftarrow{\text{id} \times j_b^{*, -1}} & J \times_S J & \xleftarrow{\text{id} \times \Sigma} & J \times_S C^{(d)}. \end{array}$$

Then \mathcal{M} , with its rigidifications at $\{0\} \times_S J$ and $J \times_S \{0\}$, is symmetric. For $T \rightarrow S$, x in $J(T)$ given by an invertible \mathcal{O} -module \mathcal{L} on C_T rigidified at b , and $y = \Sigma(D)$ in $J(T)$ given by an effective relative divisor D of degree d on C_T we have

$$(6.3.4) \quad P(x, j_b^{*, -1}(y)) = \mathcal{M}(x, y) = \text{Norm}_{D/T}(\mathcal{L}).$$

For c_1 and c_2 in $C(S)$, we have

$$(6.3.5) \quad \mathcal{M}(j_b(c_1), j_b(c_2)) = c_2^*(\mathcal{O}_C(c_1 - b)) \otimes b^*(\mathcal{O}_C(b - c_1)),$$

and, as invertible \mathcal{O} -modules on $C \times_S C$, with Δ the diagonal and $\text{pr}_\emptyset: C \times_S C \rightarrow S$ the structure morphism, we have

$$(6.3.6) \quad (j_b \times j_b)^* \mathcal{M} = \mathcal{O}(\Delta) \otimes \text{pr}_1^* \mathcal{O}(-b) \otimes \text{pr}_2^* \mathcal{O}(-b) \otimes \text{pr}_\emptyset^* b^* T_{C/S}.$$

For $d > 2g - 2$, $\widetilde{\text{id} \times \Sigma}$ gives \mathcal{N}_d a descent datum along $\text{id} \times \Sigma$ that gives \mathcal{M} on $J \times_S J$. For T an S -scheme, $x \in J(S)$ given by \mathcal{L} on C_T , rigidified at b , D_1 and D_2 in $C^{(d_1)}(S)$ and $C^{(d_2)}(S)$, the isomorphism

$$(6.3.7) \quad \mathcal{M}(x, \Sigma(D_1 + D_2)) = \mathcal{M}(x, \Sigma(D_1)) \otimes \mathcal{M}(x, \Sigma(D_2))$$

corresponds, via $\widetilde{\text{id} \times \Sigma}$, to

$$(6.3.8) \quad \begin{aligned} \mathcal{N}_{d_1+d_2}(x, D_1 + D_2) &= \text{Norm}_{(D_1+D_2)/T}(\mathcal{L}) = \text{Norm}_{D_1/T}(\mathcal{L}) \otimes \text{Norm}_{D_2/T}(\mathcal{L}) \\ &= \mathcal{N}_{d_1}(x, D_1) \otimes \mathcal{N}_{d_2}(x, D_2), \end{aligned}$$

using Lemma 6.2.2.

For T an S -scheme and x_1 and x_2 in $J(T)$ given by \mathcal{O} -modules \mathcal{L}_1 and \mathcal{L}_2 on C_T , rigidified at b , and D in $C^{(d)}(T)$, the isomorphism

$$(6.3.9) \quad \mathcal{M}(x_1 + x_2, \Sigma(D)) = \mathcal{M}(x_1, \Sigma(D)) \otimes \mathcal{M}(x_2, \Sigma(D))$$

corresponds, via $\widetilde{\text{id} \times \Sigma}$, to

$$(6.3.10) \quad \begin{aligned} \mathcal{N}_d(x_1 + x_2, D) &= \text{Norm}_{D/T}(\mathcal{L}_1 \otimes \mathcal{L}_2) = \text{Norm}_{D/T}(\mathcal{L}_1) \otimes \text{Norm}_{D/T}(\mathcal{L}_2) \\ &= \mathcal{N}_d(x_1, D) \otimes \mathcal{N}_d(x_2, D), \end{aligned}$$

using Lemma 6.2.2.

Proof Let T be an S -scheme, and x be in $J(T)$. Then x corresponds to the invertible \mathcal{O} -module $(\text{id} \times x)^* \mathcal{L}^{\text{univ}}$ on C_T , rigidified at b . Let $z := j_b^{*, -1}(x)$ in $J^\vee(T)$. Then $j_b^*(z) = x$, meaning that the pullback of $(\text{id} \times z)^* P$ on J_T rigidified at 0 by j_b equals $(\text{id} \times x)^* \mathcal{L}^{\text{univ}}$ on C_T rigidified at b . Taking $T := J$ and x the tautological point gives the first claim of the proposition.

The symmetry of \mathcal{M} with its rigidifications follows from [8], (2.7.1) and Lemma 2.7.5, and (2.7.7), using 2.9.

Now we prove (6.3.4). So let T and x be as above, and $y = \Sigma(D)$ in $J(T)$ given by a relative divisor D of degree d on C_T . As $C^d \rightarrow C^{(d)}$ is finite and locally free of rank $d!$, we may and do suppose that D is a sum of sections, say $D = \sum_{i=1}^d (c_i)$, with $c_i \in C(T)$. Then we have, functorially:

$$\begin{aligned} P(x, j_b^{*, -1}(y)) &= P(y, j_b^{*, -1}(x)) = P(\Sigma(D), j_b^{*, -1}(x)) \\ (6.3.11) \quad &= P\left(\sum_i j_b(c_i), j_b^{*, -1}(x)\right) = \bigotimes_i P(j_b(c_i), j_b^{*, -1}(x)) \\ &= \bigotimes_i \mathcal{L}^{\text{univ}}(c_i, x) = \bigotimes_i \mathcal{L}(c_i) = \text{Norm}_{D/T}(\mathcal{L}). \end{aligned}$$

Identities (6.3.5) and (6.3.6) follow directly from (6.3.4).

Now we prove the claimed compatibility between (6.3.9) and (6.3.10). We do this by considering the case where \mathcal{L} is universal, that is, base changing to J_T and x the universal point. Then, on J_T , we have 2 isomorphisms from $\text{Norm}_{(D_1+D_2)/J_T}(\mathcal{L})$ to $\text{Norm}_{D_1/J_T}(\mathcal{L}) \otimes \text{Norm}_{D_2/J_T}(\mathcal{L})$. These differ by an element of $\mathcal{O}(J_T)^\times = \mathcal{O}(T)^\times$. Hence it suffices to check that this element equals 1 at $0 \in J(T)$. This amounts to checking that the 2 isomorphisms are equal for $\mathcal{L} = \mathcal{O}_{C_T}$ with the standard rigidification at b . Then, both isomorphisms are the multiplication map $\mathcal{O}_T \otimes_{\mathcal{O}_T} \mathcal{O}_T \rightarrow \mathcal{O}_T$.

The compatibility between (6.3.7) and (6.3.8) is proved analogously. \square

6.3.12 Remark From Proposition 6.3.2 one easily deduces, in that situation, for T an S -scheme, x in $J(T)$ given by an invertible \mathcal{O} -module \mathcal{L} on C_T , and D_1 and D_2 effective relative Cartier divisors on C_T , of the same degree, a canonical isomorphism

$$(6.3.13) \quad \mathcal{M}(x, \Sigma(D_1) - \Sigma(D_2)) = \text{Norm}_{D_1/T}(\mathcal{L}) \otimes \text{Norm}_{D_2/T}(\mathcal{L})^{-1},$$

satisfying the analogous compatibilities as in Proposition 6.3.2. No rigidification of \mathcal{L} at b is needed. In fact, for \mathcal{L}_0 an invertible \mathcal{O}_T -module, we have $\text{Norm}_{D_1/T}(\pi^* \mathcal{L}_0) = \mathcal{L}_0^{\otimes d}$, where $\pi: C_T \rightarrow T$ is the structure morphism and d is the degree of D_1 . Hence the right hand side of (6.3.13) is independent of the choice of \mathcal{L} , given x .

6.4 Explicit isomorphism for norms along equivalent divisors

Let g be in $\mathbb{Z}_{\geq 1}$, let S be a scheme, and $p: C \rightarrow S$ be a proper smooth curve, with geometrically connected fibres of genus g , with a section $b \in C(S)$. Let D_1, D_2 be effective relative Cartier divisors of degree d on C , that we also view as elements of $C^{(d)}(S)$. Recall from Proposition 6.3.2 the morphism $\Sigma: C^{(d)} \rightarrow J$. Then $\Sigma(D_1) = \Sigma(D_2)$ if and only if D_1, D_2 are linearly equivalent

in the following sense: locally on S , there exists an f in $\mathcal{O}_C(U)^\times$, with $U := C \setminus (D_1 \cup D_2)$, such that $f: \mathcal{O}_U \rightarrow \mathcal{O}_U$ extends to an isomorphism $f: \mathcal{O}_C(D_1) \rightarrow \mathcal{O}_C(D_2)$. In this case, we define $\text{div}(f) = D_2 - D_1$. Proposition 6.3.2 gives us, for each invertible \mathcal{O} -module \mathcal{L} of degree 0 on C rigidified at b (viewed as an element of $J(S)$) specific isomorphisms

$$(6.4.1) \quad \begin{aligned} \text{Norm}_{D_1/S}(\mathcal{L}) &= \mathcal{N}_d(\mathcal{L}, D_1) = \mathcal{M}(\mathcal{L}, \Sigma(D_1)) = \mathcal{M}(\mathcal{L}, \Sigma(D_2)) = \mathcal{N}_d(\mathcal{L}, D_2) \\ &= \text{Norm}_{D_2/S}(\mathcal{L}). \end{aligned}$$

Now we describe explicitly this isomorphism $\text{Norm}_{D_1/S}(\mathcal{L}) \rightarrow \text{Norm}_{D_2/S}(\mathcal{L})$. To do so we first describe *an* isomorphism

$$(6.4.2) \quad \varphi_{\mathcal{L}, D_1, D_2}: \text{Norm}_{D_1/S}(\mathcal{L}) \longrightarrow \text{Norm}_{D_2/S}(\mathcal{L})$$

that is functorial for Cartesian diagrams $(C' \rightarrow S', \mathcal{L}', D'_1, D'_2) \rightarrow (C \rightarrow S, \mathcal{L}, D_1, D_2)$ and then we prove that *this* isomorphism is the one in (6.4.1).

We construct $\varphi_{\mathcal{L}, D_1, D_2}$ locally on S and the functoriality of the construction takes care of making it global. So, suppose that f is as above: $f \in \mathcal{O}_C(U)^\times$, and $f: \mathcal{O}_U \rightarrow \mathcal{O}_U$ extends to an isomorphism $f: \mathcal{O}_C(D_1) \rightarrow \mathcal{O}_C(D_2)$. Let $n \in \mathbb{Z}$ with $n > 2g - 2 + 2d$. Then $p_*(\mathcal{L}(nb)) \rightarrow p_*\mathcal{L}(nb)|_{D_1+D_2}$ and $p_*(\mathcal{O}_C(nb)) \rightarrow p_*\mathcal{O}_C(nb)|_{D_1+D_2}$ are surjective, and (still localising on S) $p_*(\mathcal{L}(nb))$ and $p_*(\mathcal{O}_C(nb))$ are free \mathcal{O}_S -modules and $\mathcal{L}(nb)|_{D_1+D_2}$ and $\mathcal{O}_C(nb)|_{D_1+D_2}$ are free $\mathcal{O}_{D_1+D_2}$ -modules of rank 1. Then we have l_0 in $(\mathcal{L}(nb))(C)$ and l_1 in $(\mathcal{O}_C(nb))(C)$ restricting to generators on $D_1 + D_2$. Let $D^- := \text{div}(l_1)$ and $D^+ := \text{div}(l_0)$, and let $V := C \setminus (D^+ + D^-)$. Note that V contains $D_1 + D_2$ and that U contains $D^+ + D^-$. Then, on V , $l := l_0/l_1$ is in $\mathcal{L}(V)$, generates $\mathcal{L}|_{D_1+D_2}$, and multiplication by l is an isomorphism $\cdot l: \mathcal{O}_C(D^+ - D^-) \rightarrow \mathcal{L}$, that is, $\text{div}(l) = D^+ - D^-$. Let

$$(6.4.3) \quad f(\text{div}(l)) = f(D^+ - D^-) := \text{Norm}_{D^+/S}(f|_{D^+}) \cdot \text{Norm}_{D^-/S}(f|_{D^-})^{-1} \in \mathcal{O}_S(S)^\times,$$

and let $\varphi_{\mathcal{L}, l, f}$ be the isomorphism, given in terms of generators

$$(6.4.4) \quad \begin{aligned} \varphi_{\mathcal{L}, l, f}: \text{Norm}_{D_1/S}(\mathcal{L}) &\longrightarrow \text{Norm}_{D_2/S}(\mathcal{L}) \\ \text{Norm}_{D_1/S}(l) &\longmapsto f(\text{div}(l))^{-1} \cdot \text{Norm}_{D_2/S}(l). \end{aligned}$$

Now suppose that we made other choices n' , l'_0 , l'_1 . Then we get D'^- , $D^{'+}$, V' , l' and $\varphi_{\mathcal{L}, l', f}$. Then there is a unique function $g \in \mathcal{O}_C(V \cap V')^\times$ such that $l' = gl$ in $\mathcal{L}(V \cap V')$. Then

$$(6.4.5) \quad \begin{aligned} \varphi_{\mathcal{L}, l', f}(\text{Norm}_{D_1/S}(l)) &= \varphi_{\mathcal{L}, l', f}(\text{Norm}_{D_1/S}(g^{-1}l')) \\ &= \varphi_{\mathcal{L}, l', f}(g^{-1}(D_1)\text{Norm}_{D_1/S}(l')) \\ &= g^{-1}(D_1) \cdot \varphi_{\mathcal{L}, l', f}(\text{Norm}_{D_1/S}(l')) \\ &= g^{-1}(D_1) \cdot f(\text{div}(l'))^{-1} \cdot \text{Norm}_{D_2/S}(l') \\ &= g^{-1}(D_1) \cdot f(\text{div}(gl))^{-1} \cdot \text{Norm}_{D_2/S}(gl) \\ &= g^{-1}(D_1) \cdot f(\text{div}(g) + \text{div}(l))^{-1} \cdot g(D_2) \cdot \text{Norm}_{D_2/S}(l) \\ &= g^{-1}(D_1) \cdot f(\text{div}(g))^{-1} \cdot g(D_2) \cdot f(\text{div}(l))^{-1} \cdot \text{Norm}_{D_2/S}(l) \\ &= g(\text{div}(f)) \cdot f(\text{div}(g))^{-1} \cdot \varphi_{\mathcal{L}, l, f}(\text{Norm}_{D_1/S}(l)) \\ &= \varphi_{\mathcal{L}, l, f}(\text{Norm}_{D_1/S}(l)), \end{aligned}$$

where, in the last step, we used Weil reciprocity, in a generality for which we do not know a reference. The truth in this generality is clear from the classical case by reduction to the universal case, in which the base scheme is integral: take a suitable level structure on J , then consider the universal curve with this level structure, and the universal 4-tuple of effective divisors with the necessary conditions. We conclude that $\varphi_{\mathcal{L},l,f} = \varphi_{\mathcal{L},l',f'}$.

Now suppose that f' is in $\mathcal{O}_C(U)^\times$ with $\text{div}(f') = \text{div}(f)$. Then there is a unique $u \in \mathcal{O}_S(S)^\times$ such that $f' = u \cdot f$, and since \mathcal{L} has degree 0 on C

$$\begin{aligned} \varphi_{\mathcal{L},l,f'}(\text{Norm}_{D_1/S}(l)) &= (u \cdot f)(\text{div}(l))^{-1} \cdot \text{Norm}_{D_2/S}(l) \\ (6.4.6) \quad &= u^{-\deg(\text{div}(l))} f(\text{div}(l))^{-1} \cdot \text{Norm}_{D_2/S}(l) \\ &= f(\text{div}(l))^{-1} \cdot \text{Norm}_{D_2/S}(l) = \varphi_{\mathcal{L},l,f}(\text{Norm}_{D_1/S}(l)). \end{aligned}$$

Hence $\varphi_{\mathcal{L},l,f'} = \varphi_{\mathcal{L},l,f}$. We define

$$(6.4.7) \quad \varphi_{D_1,D_2,\mathcal{L}}: \text{Norm}_{D_1/S}(\mathcal{L}) \longrightarrow \text{Norm}_{D_2/S}(\mathcal{L})$$

as the isomorphism $\varphi_{\mathcal{L},l,f}$ in (6.4.4) for any local choice of f and l .

We now prove that $\varphi_{\mathcal{L},D_1,D_2}$ is the same as the isomorphism in (6.4.1). We do this, as in the proof of Proposition 6.3.2, by considering the case of the universal \mathcal{L} , that is, we base change via $J \rightarrow S$, and then restricting to $0 \in J(S)$. This amounts to checking that the 2 isomorphisms are equal for $\mathcal{L} = \mathcal{O}_C$ with the standard rigidification at b . In this case, $\text{Norm}_{D_i/S}(\mathcal{O}_C) = \mathcal{O}_S$, with $\text{Norm}_{D_i/S}(1) = 1$. Hence $\varphi_{D_1,D_2,\mathcal{O}_C} = \varphi_{\mathcal{O}_C,1,f}$ is the identity on \mathcal{O}_S (use (6.4.4)). The other isomorphism is the identity on \mathcal{O}_S because of the rigidifications of \mathcal{M} and \mathcal{N}_d on $0 \times J$ and $0 \times C^{(d)}$.

6.5 Symmetry of the Norm for divisors on smooth curves

Let $C \rightarrow S$ be a proper and smooth curve with geometrically connected fibres. For D_1, D_2 effective relative Cartier divisors on C we define an isomorphism

$$(6.5.1) \quad \varphi_{D_1,D_2}: \text{Norm}_{D_1/S}(\mathcal{O}_C(D_2)) \longrightarrow \text{Norm}_{D_2/S}(\mathcal{O}_C(D_1))$$

that is functorial for cartesian diagrams $(C'/S', D'_1, D'_2) \rightarrow (C/S, D_1, D_2)$.

If suffices to define this isomorphism in the universal case, that is, over the scheme that parametrises all D_1 and D_2 . Let d_1 and d_2 be in $\mathbb{Z}_{\geq 0}$, and let $U := C^{(d_1)} \times_S C^{(d_2)}$, and let D_1 and D_2 be the universal divisors on C_U . Then we have the invertible \mathcal{O}_U -modules $\text{Norm}_{D_1/U}(\mathcal{O}_C(D_2))$ and $\text{Norm}_{D_2/U}(\mathcal{O}_C(D_1))$. The image of $D_1 \cap D_2$ in U is closed, let U^0 be its complement. Then, over U^0 , D_1 and D_2 are disjoint, and the restrictions of $\text{Norm}_{D_1/U}(\mathcal{O}_C(D_2))$ and $\text{Norm}_{D_2/U}(\mathcal{O}_C(D_1))$ are generated by $\text{Norm}_{D_1/U}(1)$ and $\text{Norm}_{D_2/U}(1)$, and there is a unique isomorphism $(\varphi_{D_1,D_2})_{U^0}$ that sends $\text{Norm}_{D_1/U}(1)$ to $\text{Norm}_{D_2/U}(1)$.

We claim that this isomorphism extends to an isomorphism over U . To see it, we base change by $U' \rightarrow U$, where $U' = C^{d_1} \times_S C^{d_2}$, then $U' \rightarrow U$ is finite, locally free of rank $d_1! \cdot d_2!$. Then $D_1 = P_1 + \dots + P_{d_1}$ and $D_2 = Q_1 + \dots + Q_{d_2}$ with the P_i and Q_j in $C(U')$. The complement of the inverse image U'^0 in U' of U^0 is the union of the pullbacks $D_{i,j}$ under $\text{pr}_{i,j}: U' \rightarrow C \times_S C$

of the diagonal, that is, the locus where $P_i = Q_j$. Each $D_{i,j}$ is an effective relative Cartier divisor on U' , isomorphic as S -scheme to $C^{d_1+d_2-1}$, hence smooth over S . Now

$$(6.5.2) \quad \text{Norm}_{D_1/U'}(\mathcal{O}(D_2)) = \bigotimes_{i,j} P_i^* \mathcal{O}(Q_j), \quad \text{Norm}_{D_2/U'}(\mathcal{O}(D_1)) = \bigotimes_{i,j} Q_j^* \mathcal{O}(P_i),$$

and, on U'^0 ,

$$(6.5.3) \quad \text{Norm}_{D_1/U'}(1) = \bigotimes_{i,j} 1, \quad \text{Norm}_{D_2/U'}(1) = \bigotimes_{i,j} 1, \quad \text{in } \mathcal{O}(U'^0).$$

The divisor on U' of the tensor-factor 1 at (i, j) , both in $\text{Norm}_{D_1/U'}(1)$ and in $\text{Norm}_{D_2/U'}(1)$, is $D_{i,j}$. Therefore, the isomorphism $(\varphi_{D_1, D_2})_{U^0}$ extends, uniquely, to an isomorphism φ_{D_1, D_2} over U' , which descends uniquely to U .

Our description of φ_{D_1, D_2} allows us to compute it in the trivial case where D_1 and D_2 are disjoint. One should be a bit careful in other cases. For example, when $d_1 = d_2 = 1$ and $P = Q$, we have $P^* \mathcal{O}_C(Q) = P^* \mathcal{O}_C(P)$ is the tangent space of $C \rightarrow S$ at P , and hence also at Q , but $\varphi_{P,Q}$ is multiplication by -1 on that tangent space. The reason for that is that the switch automorphism on $C \times_S C$ induces -1 on the normal bundle of the diagonal.

If b is an S -point on C , because of the symmetry in Proposition 6.3.2, using (6.3.13), for D_1, D_2 relative effective divisors on C of degree d_1, d_2 over S we have the following diagram of isomorphisms defining ψ_{D_1, D_2}

$$(6.5.4) \quad \begin{array}{ccc} \mathcal{M}(\Sigma(D_2), \Sigma(D_1)) & \xlongequal{\quad} & \text{Norm}_{D_1/S}(\mathcal{O}_C(D_2 - d_2 b)) \otimes b^* \mathcal{O}_C(D_2 - d_2 b)^{-d_1} \\ \parallel & & \downarrow \psi_{D_1, D_2} \\ \mathcal{M}(\Sigma(D_1), \Sigma(D_2)) & \xlongequal{\quad} & \text{Norm}_{D_2/S}(\mathcal{O}_C(D_1 - d_1 b)) \otimes b^* \mathcal{O}_C(D_1 - d_1 b)^{-d_2}. \end{array}$$

Then

$$(6.5.5) \quad \psi_{D_1, D_2} = \varphi_{D_1, D_2} \otimes \varphi_{D_1, d_2 b}^{-1} \otimes \varphi_{d_1 b, D_2}^{-1} \otimes \varphi_{d_1 b, d_2 b}.$$

It is enough to prove it in the universal case, that is when D_1 and D_2 are the universal divisors on C_U , and there we know that there exists a u in $\mathcal{O}_U(U)^\times = \mathcal{O}_S(S)^\times$ such that

$$(6.5.6) \quad u \cdot \psi_{D_1, D_2} = \varphi_{D_1, D_2} \otimes \varphi_{D_1, d_2 b}^{-1} \otimes \varphi_{d_1 b, D_2}^{-1} \otimes \varphi_{d_1 b, d_2 b}.$$

Since the symmetry in Proposition 6.3.2 is compatible with the rigidification at $(0, 0) \in (J \times J)(S)$ then $\psi_{d_1 b, d_2 b}$ is the identity on \mathcal{O}_U , as well as the right hand side of (6.5.5) when $D_i = d_i b$. Hence $u = u(d_1 b, d_2 b) = 1$, proving (6.5.5).

Moreover the isomorphisms φ_{D_1, D_2} , and consequently ψ_{D_1, D_2} , are compatible with addition of divisors, that is, under (6.3.10) and (6.3.8), for every triple D_1, D_2, D_3 of relative Cartier divisors on C we have

$$(6.5.7) \quad \varphi_{D_1+D_2, D_3} = \varphi_{D_1, D_3} \otimes \varphi_{D_2, D_3}, \quad \varphi_{D_1, D_2+D_3} = \varphi_{D_1, D_2} \otimes \varphi_{D_1, D_3}.$$

As for (6.5.5), it is enough to prove it in the universal case and then we can reduce to the case where $D_1 = d_1 b$, $D_2 = d_2 b$ and $D_3 = d_3 b$ for d_i positive integers where we have

$$(6.5.8) \quad \begin{aligned} \varphi_{d_1 b + d_2 b, d_3 b} &= \varphi_{d_1 b, d_3 b} \otimes \varphi_{d_2 b, d_3 b} = (-1)^{(d_1+d_2)d_3}, \\ \varphi_{d_1 b, d_2 b + d_3 b} &= \varphi_{d_1 b, d_2 b} \otimes \varphi_{d_1 b, d_3 b} = (-1)^{d_1(d_2+d_3)}. \end{aligned}$$

6.6 Explicit residue disks and partial group laws

Let C be a smooth curve over \mathbb{Z}/p^2 , let $b \in C(\mathbb{Z}/p^2)$, and let \mathcal{M} be as in Proposition 6.3.2. Let $D = D^+ - D^-$ and $E = E^+ - E^-$ be relative Cartier divisors of degree 0 on C . For each α in $\mathcal{M}^\times(\mathbb{F}_p)$ whose image in $(J \times J)(\mathbb{F}_p)$ is given by (D, E) we parametrise $\mathcal{M}^\times(\mathbb{Z}/p^2)_\alpha$, under the assumption that there exists a non-special split reduced divisor of degree g on $C_{\mathbb{F}_p}$.

Let b_1, \dots, b_g in $C(\mathbb{Z}/p^2)$ have distinct images \bar{b}_i in $C(\mathbb{F}_p)$ such that $h^0(C_{\mathbb{F}_p}, \bar{b}_1 + \dots + \bar{b}_g) = 1$, and let b_{g+1}, \dots, b_{2g} in $C(\mathbb{Z}/p^2)$ be such that the \bar{b}_{g+i} are distinct and $h^0(C_{\mathbb{F}_p}, \bar{b}_{g+1} + \dots + \bar{b}_{2g}) = 1$. Then the maps

$$(6.6.1) \quad \begin{aligned} f_1: C^g &\longrightarrow J, \quad (c_1, \dots, c_g) \longmapsto [\mathcal{O}_C(c_1 + \dots + c_g - (b_1 + \dots + b_g) + D)] \\ f_2: C^g &\longrightarrow J, \quad (c_1, \dots, c_g) \longmapsto [\mathcal{O}_C(c_1 + \dots + c_g - (b_{g+1} + \dots + b_{2g}) + E)], \end{aligned}$$

are étale respectively in the points $(b_1, \dots, b_g) \in C^g(\mathbb{F}_p)$ and $(b_{g+1}, \dots, b_{2g}) \in C^g(\mathbb{F}_p)$ and consequently give bijections $C^g(\mathbb{Z}/p^2)_{(b_1, \dots, b_g)} \rightarrow J(\mathbb{Z}/p^2)_{\overline{D}}$ and $C^g(\mathbb{Z}/p^2)_{(b_{g+1}, \dots, b_{2g})} \rightarrow J(\mathbb{Z}/p^2)_{\overline{E}}$. For each point $c \in C(\mathbb{F}_p)$ we choose $x_{D,c}$ a generator of $\mathcal{O}_C(-D)_c$ and $x_c \in \mathcal{O}_{C_{\mathbb{Z}/p}, c}$ so that p, x_c are parameters in c . For each $i = 1, \dots, 2g$ we choose x_{b_i} so that $x_{b_i}(b_i) = 0$. For each (\mathbb{Z}/p^2) -point $c \in C(\mathbb{Z}/p^2)$ with image \bar{c} in $C(\mathbb{F}_p)$ and for each $\lambda \in \mathbb{F}_p$ let c_λ be the unique point in $C(\mathbb{Z}/p^2)_{\bar{c}}$ with $x_{\bar{c}}(c_\lambda) = \lambda p$. Then the map $\lambda \mapsto c_\lambda$ is a bijection $\mathbb{F}_p \rightarrow C(\mathbb{Z}/p^2)_{\bar{c}}$ hence the maps f_1, f_2 induce bijections

$$(6.6.2) \quad \begin{aligned} \mathbb{F}_p^g &\longrightarrow J(\mathbb{Z}/p^2)_{\overline{D}}, \quad \lambda \longmapsto D_\lambda := D + (b_{1,\lambda_1} - b_1) + \dots + (b_{g,\lambda_g} - b_g) \\ \mathbb{F}_p^g &\longrightarrow J(\mathbb{Z}/p^2)_{\overline{E}}, \quad \mu \longmapsto E_\mu := E + (b_{g+1,\mu_1} - b_{g+1}) + \dots + (b_{2g,\mu_g} - b_{2g}). \end{aligned}$$

Hence $\mathcal{M}^\times(\mathbb{Z}/p^2)_{\overline{D}, \overline{E}}$ is the union of $\mathcal{M}^\times(D_\lambda, E_\mu)$ as λ and μ vary in \mathbb{F}_p^g and by Proposition 6.3.2 and Remark 6.3.12 we have

$$(6.6.3) \quad \begin{aligned} \mathcal{M}(D_\lambda, E_\mu) = & \text{Norm}_{E^+ / (\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda)) \otimes \text{Norm}_{E^- / (\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda))^{-1} \otimes \\ & \otimes \bigotimes_{i=1}^g (b_{g+i, \mu_i}^* \mathcal{O}_C(D_\lambda) \otimes b_{g+i}^* \mathcal{O}_C(D_\lambda)^{-1}). \end{aligned}$$

For each $i \in \{1, \dots, g\}$, $c \in C(\mathbb{Z}/p^2)$ and $\lambda \in \mathbb{F}_p$ we define $x_i(c, \lambda) := 1$ if $\bar{c} \neq \bar{b}_i$ and $x_i(c, \lambda) := x_{b_i} - \lambda p$ if $\bar{c} = \bar{b}_i$, so that $c^* x_i(c, \lambda)^{-1}$ generates $c^* \mathcal{O}(b_{i,\lambda})$. Then, for each $c \in C(\mathbb{Z}/p^2)$ and each $\lambda \in \mathbb{F}_p^g$,

$$(6.6.4) \quad c^* \left(x_{D,c}^{-1} \cdot \prod_{i=1}^g \frac{x_i(c, 0)}{x_i(c, \lambda_i)} \right) \text{ generates } c^* \mathcal{O}_C(D_\lambda).$$

We write $E^\pm = E^{0,\pm} + \dots + E^{g,\pm}$ so that $E^{0,\pm}$ is disjoint from $\{\bar{b}_1, \dots, \bar{b}_g\}$, and $E^{i,\pm}$, restricted to $C_{\mathbb{F}_p}$, is supported on \bar{b}_i . Let $x_{D,E}$ be a generator of $\mathcal{O}_C(-D)$ in a neighborhood of $E^+ \cup E^-$. Then, for each λ in \mathbb{F}_p^g ,

$$(6.6.5) \quad \text{Norm}_{E^{0,\pm} / (\mathbb{Z}/p^2)}(x_{D,E}^{-1}) \otimes \bigotimes_{i=1}^g \text{Norm}_{E^{i,\pm} / (\mathbb{Z}/p^2)} \left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p} \right)$$

generates $\text{Norm}_{E^\pm/(\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda))$. By (6.6.3), (6.6.4) and (6.6.5) we see that, for λ and μ in \mathbb{F}_p^g ,

(6.6.6)

$$\begin{aligned} s_{D,E}(\lambda, \mu) &:= \text{Norm}_{E^{0,+}/(\mathbb{Z}/p^2)}(x_{D,E}^{-1}) \otimes \bigotimes_{i=1}^g \text{Norm}_{E^{i,+}/(\mathbb{Z}/p^2)}\left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p}\right) \otimes \\ &\otimes \text{Norm}_{E^{0,-}/(\mathbb{Z}/p^2)}(x_{D,E}^{-1})^{-1} \otimes \bigotimes_{i=1}^g \text{Norm}_{E^{i,-}/(\mathbb{Z}/p^2)}\left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p}\right)^{-1} \otimes \\ &\otimes \bigotimes_{i=1}^g \left(b_{g+i, \mu_i}^* \left(x_{D,b_{g+i}}^{-1} \cdot \prod_{j=1}^g \frac{x_j(b_{g+i}, \mu_i, 0)}{x_j(b_{g+i}, \mu_i, \lambda_j)} \right) \otimes b_{g+i}^* \left(x_{D,b_{g+i}}^{-1} \cdot \prod_{j=1}^g \frac{x_j(b_{g+i}, 0)}{x_j(b_{g+i}, \lambda_j)} \right)^{-1} \right) \end{aligned}$$

generates the free rank one \mathbb{Z}/p^2 -module $\mathcal{M}(D_\lambda, E_\mu)$. The fibre $\mathcal{M}^\times(\overline{D}, \overline{E})$ over $(\overline{D}, \overline{E})$ in $(J \times J)(\mathbb{F}_p)$ is an \mathbb{F}_p^\times -torsor, containing $\overline{s_{D,E}(0,0)}$ are in bijection with the elements ξ in \mathbb{F}_p^\times and are exactly the points $\xi \cdot s_{D,E}(0,0)$. Using that $(\mathbb{Z}/p^2)^\times = \mathbb{F}_p^\times \times (1 + p\mathbb{F}_p)$, we parametrise, for each $\xi \in \mathbb{F}_p^\times$, the residue disk of $\xi \cdot \overline{s_{D,E}(0,0)}$ by the bijection

$$(6.6.7) \quad \mathbb{F}_p^g \times \mathbb{F}_p^g \times \mathbb{F}_p \longrightarrow \mathcal{M}^\times(\mathbb{Z}/p^2)_{\xi \cdot \overline{s_{D,E}(0,0)}}, \quad (\lambda, \mu, \tau) \longmapsto (1 + p\tau) \cdot \xi \cdot s_{D,E}(\lambda, \mu).$$

Using this parametrization it is easy to describe the two partial group laws on $\mathcal{M}^\times(\mathbb{Z}/p^2)$ when one of the two points we are summing lies over $(\overline{D}, \overline{E})$ and the other lies over $(\overline{D}, 0)$ or $(0, \overline{E})$. To compute the group law in $J(\mathbb{Z}/p^2)$ we notice that for each $c \in C(\mathbb{Z}/p^2)$ such that $x_c(c) = 0$ and for each $\lambda, \mu \in \mathbb{F}_p$ we have

$$(6.6.8) \quad \frac{x_c^2}{(x_c - \lambda p)(x_c - \mu p)} = \frac{x_c^2}{x_c^2 - \lambda p x_c - \mu p x_c} = \frac{x_c}{x_c - (\lambda + \mu)p}$$

and since these rational functions generate $\mathcal{O}_C(c_\lambda - c + c_\mu - c)$ and $\mathcal{O}_C(c_{\lambda+\mu} - c)$ in a neighborhood of c , we have the *equality* of relative Cartier divisors on C

$$(6.6.9) \quad (c_\lambda - c) + (c_\mu - c) = c_{\lambda+\mu} - c.$$

Hence, under the definition for $\lambda \in \mathbb{F}_p^g$ of

$$(6.6.10) \quad D_\lambda^0 := (b_{1,\lambda_1} - b_1) + \cdots + (b_{g,\lambda_g} - b_g), \quad E_\lambda^0 := (b_{g+1,\lambda_1} - b_{g+1}) + \cdots + (b_{2g,\lambda_g} - b_{2g}),$$

we have, for all $\lambda, \mu \in \mathbb{F}_p^g$, that $D_\lambda + D_\mu^0 = D_{\lambda+\mu}$ and $E_\lambda + E_\mu^0 = E_{\lambda+\mu}$. Definition 6.6.6, applied with $(D, 0)$ and $(0, E)$, with $x_{0,E} = 1$ and, for every $c \in C(\mathbb{F}_p)$, with $x_{0,c} = 1$, gives, for all λ, μ in \mathbb{F}_p^g , the elements

$$(6.6.11) \quad s_{D,0}(\lambda, \mu) \in \mathcal{M}^\times(D_\lambda, E_\mu^0), \quad s_{0,E}(\lambda, \mu) \in \mathcal{M}^\times(D_\lambda^0, E_\mu).$$

Then (6.6.8) and (6.6.9), together with the equivalence of (6.3.7) and (6.3.8) and the equivalence of (6.3.9) and (6.3.10) in Proposition 6.3.2, give that for all $\lambda, \lambda_1, \lambda_2, \mu, \mu_1, \mu_2$ in \mathbb{F}_p^g

$$\begin{aligned} (6.6.12) \quad s_{D,0}(\lambda, \mu_1) +_2 s_{D,E}(\lambda, \mu_2) &= s_{D,0}(\lambda, \mu_1) \otimes s_{D,E}(\lambda, \mu_2) = s_{D,E}(\lambda, \mu_1 + \mu_2) \\ s_{0,E}(\lambda_1, \mu) +_1 s_{D,E}(\lambda_2, \mu) &= s_{D,0}(\lambda_1, \mu) \otimes s_{D,E}(\lambda_2, \mu) = s_{D,E}(\lambda_1 + \lambda_2, \mu), \end{aligned}$$

and, consequently, for all $\tau_1, \tau_2 \in \mathbb{F}_p$ and $\xi_1, \xi_2 \in \mathbb{F}_p^\times$, that

$$(6.6.13) \quad \begin{aligned} \xi_1(1+\tau_1 p) \cdot s_{D,0}(\lambda, \mu_1) +_2 \xi_2(1+\tau_2 p) \cdot s_{D,E}(\lambda, \mu_2) &= \xi_1(1+\tau_1 p)\xi_2(1+\tau_2 p) \cdot s_{D,E}(\lambda, \mu_1 + \mu_2) \\ &= \xi_1\xi_2(1+(\tau_1+\tau_2)p) \cdot s_{D,E}(\lambda, \mu_1 + \mu_2), \\ \xi_1(1+\tau_1 p) \cdot s_{0,E}(\lambda_1, \mu) +_1 \xi_2(1+\tau_2 p) \cdot s_{D,E}(\lambda_2, \mu) &= \xi_1\xi_2(1+(\tau_1+\tau_2)p) \cdot s_{D,E}(\lambda_1 + \lambda_2, \mu). \end{aligned}$$

Let us now prove that the parametrization (6.6.7) is the inverse of a bijection given by parameters on \mathcal{M}^\times analogously to (3.1). Let \mathcal{Q} be the pullback of \mathcal{M} by $f_1 \times f_2$ with f_1 and f_2 as in (6.6.1). Then the lift $\widetilde{f_1 \times f_2}: \mathcal{Q}^\times \rightarrow \mathcal{M}^\times$ is étale at any point $\beta \in \mathcal{Q}(\mathbb{F}_p)$ lying over $\bar{b} = (b_1, \dots, b_{2g}) \in (C^{2g})(\mathbb{F}_p)$ and induces a bijection between $\mathcal{Q}^\times(\mathbb{Z}/p^2)_{\bar{b}}$ and $\mathcal{M}^\times(\mathbb{Z}/p^2)_{(\overline{D}, \overline{E})}$. In particular we can interpret $s_{D,E}(\lambda, \mu)$ as a section of $\mathcal{Q}(b_{1,\lambda_1}, \dots, b_{2g,\mu_g})$ and we can interpret (6.6.7) as a parametrization of $\mathcal{Q}^\times(\mathbb{Z}/p^2)_{\xi s_{D,E}(0,0)}$. It is then enough to prove that (6.6.7) is the inverse of a bijection given by parameters on \mathcal{Q}^\times . It comes from the definition of c_ν for $c \in C(\mathbb{Z}/p^2)$ and $\nu \in \mathbb{F}_p$, that the maps $\lambda_i \mu_i: C^{2g}(\mathbb{Z}/p^2)_{\bar{b}}$ are given by parameters in $\mathcal{O}_{C^{2g}, \bar{b}}$ divided by p . In order to see that also the coordinate $\tau: \mathcal{Q}^\times(\mathbb{Z}/p^2)_{\xi s_{D,E}(0)} \rightarrow \mathbb{F}_p$ is given by a parameter divided by p it is enough to prove that there is an open subset $U \subset C^{2g}$ containing \bar{b} and a section s trivializing $\mathcal{Q}|_U$ such that $s_{D,E}(\lambda, \mu) = s(b_{1,\lambda_1}, \dots, b_{2g,\mu_g})$. Remark 6.3.12 and (6.5.1) give that

$$(6.6.14) \quad \begin{aligned} \mathcal{Q} &= \bigotimes_{i,j=1}^g \left((\pi_i, \pi_{g+j})^* \mathcal{O}_{C \times C}(\Delta) \right) \\ &\otimes \bigotimes_{i=1}^g \left(\pi_i^* \mathcal{O}_C(E - (b_{g+1} + \dots + b_{2g})) \otimes \pi_{g+i}^* \mathcal{O}_C(D - (b_1 + \dots + b_g)) \right) \\ &\otimes \text{Norm}_{E/\mathbb{Z}/p^2}(\mathcal{O}_C(D - (b_1 + \dots + b_g))) \otimes \bigotimes_{i=1}^g b_{g+i}^* \mathcal{O}_C(D - (b_1 + \dots + b_g))^{-1} \end{aligned}$$

where $\Delta \subset C \times C$ is the diagonal and π_i is the i -th projection $C^g \times C^g \rightarrow C$. We can prove that there is an open subset $U \subset C^g \times C^g$ containing b and a section s trivializing $\mathcal{Q}|_U$ such that $s_{D,E}(\lambda, \mu) = s(b_{1,\lambda_1}, \dots, b_{2g,\mu_g})$, by trivializing each factor of the above tensor product in a neighborhood of b . Let us see it, for example, for the pieces of the form $(\pi_i, \pi_{g+j})^* \mathcal{O}_{C \times C}(\Delta)$. Let π_1, π_2 be the two projections $C \times C \rightarrow C$ and let us consider the divisor Δ : for each pair of points $c_1, c_2 \in C(\mathbb{F}_p)$ the invertible \mathcal{O} -module $\mathcal{O}_{C \times C}(-\Delta)$ is generated by the section $x_{\Delta, c_1, c_2} := 1$ in a neighborhood of (c_1, c_2) if $c_1 \neq c_2$, while it is generated by the section $x_{\Delta, c_1, c_2} := \pi_1^* x_{c_1} - \pi_2^* x_{c_2}$ in a neighborhood of (c_1, c_2) if $c_1 = c_2$. If we now take $c_1 = b_i, c_2 = b_{g+j} \in C(\mathbb{F}_p)$ we deduce there is a neighborhood U of (b_i, b_{g+j}) such that $x_{\Delta, b_i, b_{g+j}}^{-1}$ generates $\mathcal{O}_{C \times C}(\Delta)|_U$. For each $\lambda, \mu \in \mathbb{F}_p^g$ the point $(b_{i,\lambda_i}, b_{g+j,\mu_j})$ lies in $U(\mathbb{Z}/p^2)$ and the canonical isomorphism $(b_{i,\lambda_i}, b_{g+j,\mu_j})^* \mathcal{O}_{C \times C}(\Delta) = b_{g+j,\mu_j}^* \mathcal{O}(b_{i,\lambda_i})$ sends the generating section $(b_{i,\lambda_i}, b_{j,\mu_j})^* x_{\Delta, c_1, c_2}^{-1}$ to $b_{j,\mu_j}^* x_i(b_{g+j}, \lambda_i)^{-1}$, which is a factor in (6.6.6). This gives a section $s_{i,j}$ trivializing $(\pi_i, \pi_{g+j})^* \mathcal{O}_{C \times C}(\Delta)$ in a neighborhood of b . With similar choices we can find sections trivializing the other factors in (6.6.14) in a neighborhood of b and tensoring all such sections we get a section s such that $s_{D,E}(\lambda, \mu) = s(b_{1,\lambda_1}, \dots, b_{2g,\mu_g})$.

6.7 Extension of the Poincaré biextension over Néron models

Let C over \mathbb{Z} be a curve as in Section 2. Let q be a prime number that divides n . We also write C for $C_{\mathbb{Z}_q}$.

Let J be the Néron model over \mathbb{Z}_q of $\text{Pic}_{C/\mathbb{Q}_q}^0$, and J^0 its fibre-wise connected component of 0. On $(J \times_{\mathbb{Z}_q} J)_{\mathbb{Q}_q}$ we have \mathcal{M} as in Proposition 6.3.2, rigidified at $0 \times J_{\mathbb{Q}_q}$ and $J_{\mathbb{Q}_q} \times 0$. We claim that \mathcal{M} , with these rigidifications, extends uniquely to $J \times_{\mathbb{Z}_q} J^0$. We prove this. First of all, $J \times_{\mathbb{Z}_q} J^0$ is regular, hence Weil divisors and Cartier divisors are the same, and every invertible \mathcal{O} -module on $(J \times_{\mathbb{Z}_q} J^0)_{\mathbb{Q}_q}$ has an extension to an invertible \mathcal{O} -module on $J \times_{\mathbb{Z}_q} J^0$. So let \mathcal{M}' be an extension of \mathcal{M} . Any extension \mathcal{M}'' of \mathcal{M} is then of the form $\mathcal{M}'(D)$, with D a divisor on $J \times_{\mathbb{Z}_q} J^0$ with support in $(J \times_{\mathbb{Z}_q} J^0)_{\mathbb{F}_q}$. Such D are \mathbb{Z} -linear combinations of the irreducible components of the $D_i \times_{\mathbb{F}_q} J_{\mathbb{F}_q}^0$, where the D_i are the irreducible components of $J_{\mathbb{F}_q}$. Now $\mathcal{M}'|_{J \times 0}$ extends $\mathcal{M}|_{J_{\mathbb{Q}_q} \times 0}$, hence the rigidification of $\mathcal{M}|_{J_{\mathbb{Q}_q} \times 0}$ is a rational section of $\mathcal{M}'|_{J \times 0}$ whose divisor is a \mathbb{Z} -linear combination of the D_i . It follows that there is exactly one D as above such that the rigidification of \mathcal{M} extends to a rigidification of $\mathcal{M}'(D)$ on $J \times 0$. That rigidification is compatible with a unique rigidification of $\mathcal{M}'(D)$ on $0 \times J^0$. In what follows, we denote this extension $\mathcal{M}'(D)$ of \mathcal{M} to $J \times_{\mathbb{Z}_q} J^0$ by \mathcal{M} . Let us now prove that the \mathbb{G}_m -torsor \mathcal{M}^\times on $J \times_{\mathbb{Z}_q} J^0$ has a unique biextension structure, extending that over \mathbb{Q}_q . Over $J \times_{\mathbb{Z}_q} J \times_{\mathbb{Z}_q} J^0$ we have the invertible \mathcal{O} -modules whose fibres, at a point (x, y, z) (with values in some \mathbb{Z}_q -scheme) are $\mathcal{M}(x+y, z)$ and $\mathcal{M}(x, z) \otimes \mathcal{M}(y, z)$. The biextension structure over \mathbb{Q}_q gives an isomorphism between these, that differs from an isomorphism over \mathbb{Z}_q by a divisor with support over \mathbb{F}_q . But the compatibility with the rigidification of \mathcal{M} over $J \times_{\mathbb{Z}_q} 0$ proves that this divisor is zero. The other partial group law, and the required properties of them follow in the same way. We have now shown that \mathcal{M}^\times extends the Poincaré biextension.

6.8 Explicit description of the extended Poincaré bundle

Let C over \mathbb{Z} be a curve as in Section 2. Let q be a prime number that divides n . We also write C for $C_{\mathbb{Z}_q}$. By [7], Corollary 9.1.24, C is cohomologically flat over \mathbb{Z}_q , which means that for all \mathbb{Z}_q -algebras A , $\mathcal{O}(C_A) = A$. Another reference for this is [10], (6.1.4), (6.1.6) and (7.2.1).

The relative Picard functor $\text{Pic}_{C/\mathbb{Z}_q}$ sends a \mathbb{Z}_q -scheme T to the set of isomorphism classes of $(\mathcal{L}, \text{rig})$ with \mathcal{L} an invertible \mathcal{O} -module on C_T and rig a rigidification at b . By cohomological flatness, such objects are rigid. But if the action of $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on the set of irreducible components of $C_{\overline{\mathbb{F}}_q}$ is non-trivial, then $\text{Pic}_{C/\mathbb{Z}_q}$ is not representable by a \mathbb{Z}_q -scheme, only by an algebraic space over \mathbb{Z}_q (see [10], Proposition 5.5). Therefore, to not be annoyed by such inconveniences, we pass to $S := \text{Spec}(\mathbb{Z}_q^{\text{univ}})$, the maximal unramified extension of \mathbb{Z}_q . Then $\text{Pic}_{C/S}$ is represented by a smooth S -scheme, and on $C \times_S \text{Pic}_{C/S}$ there is a universal pair $(\mathcal{L}^{\text{univ}}, \text{rig})$ ([10], Proposition 5.5, and Section 8.0). We note that $\text{Pic}_{C/S} \rightarrow S$ is separated if and only if $C_{\overline{\mathbb{F}}_q}$ is irreducible.

Let $\text{Pic}_{C/S}^{[0]}$ be the open part of $\text{Pic}_{C/S}$ where $\mathcal{L}^{\text{univ}}$ is of total degree zero on the fibres of $C \rightarrow S$. It contains the open part $\text{Pic}_{C/S}^0$ where $\mathcal{L}^{\text{univ}}$ has degree zero on all irreducible components of $C_{\overline{\mathbb{F}}_q}$.

Let E be the closure of the 0-section of $\text{Pic}_{C/S}$, as in [10]. It is contained in $\text{Pic}_{C/S}^{[0]}$. By [10],

Proposition 5.2, E is represented by an S -group scheme, étale.

By [10], Theorem 8.1.4, or [4], Theorem 9.5.4, the tautological morphism $\mathrm{Pic}_{C/S}^{[0]} \rightarrow J$ is surjective (for the étale topology) and its kernel is E , and so $J = \mathrm{Pic}_{C/S}^{[0]}/E$. Also, the composition $\mathrm{Pic}_{C/S}^0 \rightarrow \mathrm{Pic}_{C/S}^{[0]} \rightarrow J$ induces an isomorphism $\mathrm{Pic}_{C/S}^0 \rightarrow J^0$.

Let C_i , $i \in I$, be the irreducible components of $C_{\overline{\mathbb{F}}_q}$. Then, as divisors on C , we have

$$(6.8.1) \quad C_{\overline{\mathbb{F}}_q} = \sum_{i \in I} m_i C_i.$$

For \mathcal{L} an invertible \mathcal{O} -module on $C_{\overline{\mathbb{F}}_q}$, its multidegree is defined as

$$(6.8.2) \quad \mathrm{mdeg}(\mathcal{L}): I \rightarrow \mathbb{Z}, \quad i \mapsto \deg_{C_i}(\mathcal{L}|_{C_i}),$$

and its total degree is then

$$(6.8.3) \quad \deg(\mathcal{L}) = \sum_{i \in I} m_i \deg_{C_i}(\mathcal{L}|_{C_i}).$$

The multidegree induces a surjective morphism of groups

$$(6.8.4) \quad \mathrm{mdeg}: \mathrm{Pic}_{C/S}(S) \rightarrow \mathbb{Z}^I.$$

Now let $d \in \mathbb{Z}^I$ be a sufficiently large multidegree so that every invertible \mathcal{O} -module \mathcal{L} on $C_{\overline{\mathbb{F}}_q}$ with $\mathrm{mdeg}(\mathcal{L}) = d$ satisfies $H^1(C_{\overline{\mathbb{F}}_q}, \mathcal{L}) = 0$ and has a global section whose divisor is finite. Let \mathcal{L}_0 be an invertible \mathcal{O} -module on C , rigidified at b , with $\mathrm{mdeg}(\mathcal{L}_0) = d$. Then over $C \times_S J^0$ we have the invertible \mathcal{O} -module $\mathcal{L}^{\mathrm{univ}} \otimes \mathcal{L}_0$, and its pushforward \mathcal{E} to J^0 . Then \mathcal{E} is a locally free \mathcal{O} -module on J^0 . Let E be the geometric vector bundle over J^0 corresponding to \mathcal{E} . Then over E , \mathcal{E} has its universal section. Let $U \subset E$ be the open subscheme where the divisor of this universal section is finite over J^0 . The J^0 -group scheme \mathbb{G}_m acts freely on U . We define $V := U/\mathbb{G}_m$. As the \mathbb{G}_m -action preserves the invertible \mathcal{O} -module and its rigidification, the morphism $U \rightarrow J^0$ factors through $U \rightarrow V$ and gives a morphism $\Sigma_{\mathcal{L}_0}: V \rightarrow J^0$. Then on $C \times_S V$ we have the universal effective relative Cartier divisor D^{univ} on $C \times_S V \rightarrow V$ of multidegree d , and $\mathcal{L}^{\mathrm{univ}} \otimes \mathcal{L}_0$ together its rigidification at b is (uniquely) isomorphic to $\mathcal{O}_{C \times_S V}(D^{\mathrm{univ}}) \otimes_{\mathcal{O}_V} b^* \mathcal{O}_{C \times_S V}(-D^{\mathrm{univ}})$ with its tautological rigidification at b , in a diagram:

$$(6.8.5) \quad \mathcal{L}^{\mathrm{univ}} \otimes \mathcal{L}_0 = \mathcal{O}_{C \times_S V}(D^{\mathrm{univ}}) \otimes_{\mathcal{O}_V} b^* \mathcal{O}_{C \times_S V}(-D^{\mathrm{univ}}).$$

Then $\Sigma_{\mathcal{L}_0}$ sends, for T an S -scheme, a T -point D on C_T to $\mathcal{O}_{C_T}(D) \otimes_{\mathcal{O}_T} b^* \mathcal{O}_{C_T}(-D) \otimes_{\mathcal{O}_C} \mathcal{L}_0^{-1}$ with its rigidification at b . Let s_0 be in $\mathcal{L}_0(C)$ such that its divisor D_0 is finite over S , and let $v_0 \in V(S)$ be the corresponding point.

On $\mathrm{Pic}_{C/S}^{[0]} \times_S V \times_S C$ we have the universal $\mathcal{L}^{\mathrm{univ}}$ from $\mathrm{Pic}_{C/S}^{[0]}$ with rigidification at b , and the universal divisor D^{univ} . Then on $\mathrm{Pic}_{C/S}^{[0]} \times_S V$ we have the invertible \mathcal{O} -module $\mathcal{N}_{q,d}$ whose fibre at a T -point $(\mathcal{L}, \mathrm{rig}, D)$ is $\mathrm{Norm}_{D/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D_0/T}(\mathcal{L})^{-1}$, canonically trivial on $\mathrm{Pic}_{C/S}^{[0]} \times_S v_0$:

$$(6.8.6) \quad \mathcal{N}_{q,d}: \left(\mathrm{Pic}_{C/S}^{[0]} \times_S V \right) (T) \ni (\mathcal{L}, \mathrm{rig}, D) \longmapsto \mathrm{Norm}_{D/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D_0/T}(\mathcal{L})^{-1}.$$

Any global regular function on the integral scheme $\mathrm{Pic}_{C/S}^{[0]} \times_S V$ is constant on the generic fibre, hence in $\mathbb{Q}_q^{\mathrm{unr}}$, and restricting it to $(0, v_0)$ shows that it is in $\mathbb{Z}_q^{\mathrm{unr}}$, and if it is 1 on $\mathrm{Pic}_{C/S}^{[0]} \times_S v_0$, it is equal to 1. Therefore trivialisations on $\mathrm{Pic}_{C/S}^{[0]} \times_S v_0$ rigidify invertible \mathcal{O} -modules on $\mathrm{Pic}_{C/S}^{[0]} \times_S V$.

The next proposition generalises [8], Corollary 2.8.6 and Lemma 2.7.11.2: there, $C \rightarrow S$ is nodal (but not necessarily regular), and the restriction of \mathcal{M} to $J^0 \times_S J^0$ is described.

6.8.7 Proposition *In the situation of Section 6.8, the pullback of the invertible \mathcal{O} -module \mathcal{M} on $J \times_{\mathbb{Z}_q^{\mathrm{unr}}} J^0$ to $\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V$ by the product of the quotient map $\mathrm{quot}: \mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \rightarrow J$ and the map $\Sigma_{\mathcal{L}_0}: V \rightarrow J^0$ is $\mathcal{N}_{q,d}$, compatible with their rigidifications at $J \times 0$ and $\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times v_0$. In a diagram:*

$$(6.8.8) \quad \begin{array}{ccccc} P^\times & \xleftarrow{\hspace{1cm}} & \mathcal{M}^\times & \xleftarrow{\hspace{1cm}} & \mathcal{N}_{q,d}^\times \\ \downarrow & & \downarrow & & \downarrow \\ J \times_{\mathbb{Z}_q^{\mathrm{unr}}} J^{\vee,0} & \xleftarrow[\mathrm{id} \times j_b^{*, -1}]{} & J \times_{\mathbb{Z}_q^{\mathrm{unr}}} J^0 & \xleftarrow[\mathrm{quot} \times \Sigma_{\mathcal{L}_0}]{} & \mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V. \end{array}$$

For T any $\mathbb{Z}_q^{\mathrm{unr}}$ -scheme, for x in $J(T)$ given by an invertible \mathcal{O} -module \mathcal{L} on C_T rigidified at b , and y in $J^0(T) = \mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^0(T)$ given by the difference $D = D^+ - D^-$ of effective relative Cartier divisors on C_T of the same multidegree, we have

$$P(x, j_b^{*, -1}(y)) = \mathcal{M}(x, y) = \mathrm{Norm}_{D^+/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D^-/T}(\mathcal{L})^{-1}.$$

Proof The scheme $\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V$ is smooth over $\mathbb{Z}_q^{\mathrm{unr}}$, hence regular, it is connected, hence integral, and since $V_{\overline{\mathbb{F}}_q}$ is irreducible, the irreducible components of $(\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V)_{\overline{\mathbb{F}}_q}$ are the $P^i \times_{\overline{\mathbb{F}}_q} V_{\overline{\mathbb{F}}_q}$, with P^i the irreducible components of $(\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]})_{\overline{\mathbb{F}}_q}$, with i in $\pi_0((\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]})_{\overline{\mathbb{F}}_q})$, which, by the way, equals the kernel of $\mathbb{Z}^I \rightarrow \mathbb{Z}$, $x \mapsto \sum_{j \in I} m_j x_j$.

We prove the first claim. Both $\mathcal{N}_{q,d}$ and the pullback of \mathcal{M} are rigidified on $\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times v_0$. Below we will give, after inverting q , an isomorphism α from $\mathcal{N}_{q,d}$ to the pullback of \mathcal{M} that is compatible with the rigidifications. Then there is a unique divisor D_α on $\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V$, supported on $(\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V)_{\overline{\mathbb{F}}_q}$, such that α is an isomorphism from $\mathcal{N}_{q,d}(D_\alpha)$ to the pullback of \mathcal{M} . Let i be in $\pi_0((\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]})_{\overline{\mathbb{F}}_q})$, and let x be in $\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]}(\mathbb{Z}_q^{\mathrm{unr}})$ specialising to an $\overline{\mathbb{F}}_q$ -point of P^i , then restricting α to (x_i, v_0) and using the compatibility of α (over $\mathbb{Q}_q^{\mathrm{unr}}$) with the rigidifications, gives that the multiplicity of $P^i \times V_{\overline{\mathbb{F}}_q}$ in D_α is zero. Hence D_α is zero.

Let us now give, over $(\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V)_{\mathbb{Q}_q^{\mathrm{unr}}}$, an isomorphism α from $\mathcal{N}_{q,d}$ to the pullback of \mathcal{M} . Note that $(\mathrm{Pic}_{C/\mathbb{Z}_q^{\mathrm{unr}}}^{[0]})_{\mathbb{Q}_q^{\mathrm{unr}}} = J_{\mathbb{Q}_q^{\mathrm{unr}}}$, and that $V_{\mathbb{Q}_q^{\mathrm{unr}}} = C_{\mathbb{Q}_q^{\mathrm{unr}}}^{(|d|)}$, where $|d| = \sum_i m_i d_i$ is the total degree given by the multidegree d . For T a $\mathbb{Q}_q^{\mathrm{unr}}$ -scheme, $x \in J(T)$ given by \mathcal{L} an invertible \mathcal{O}_{C_T} -module rigidified at b , and $v \in V(T)$ given by a relative Cartier divisor D of degree $|d|$ on C_T , we have, using Proposition 6.3.2 and (6.8.6), the following isomorphisms (functorial in T), respecting the rigidifications at $v = v_0$:

$$(6.8.9) \quad \begin{aligned} \mathcal{M}(x, \Sigma_{\mathcal{L}_0}(v)) &= \mathcal{M}(x, \Sigma(v) - \Sigma(v_0)) = \mathcal{M}(x, \Sigma(v)) \otimes \mathcal{M}(x, \Sigma(v_0))^{-1} \\ &= \mathrm{Norm}_{D/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D_0/T}(\mathcal{L})^{-1} = \mathcal{N}_{q,d}(x, v). \end{aligned}$$

This finishes the proof of the first claim of the Proposition. The second claim follows directly from the definition of $\mathcal{N}_{q,d}$, plus the compatibility at the end of Proposition 6.3.2. \square

6.9 Integral points of the extended Poincaré torsor

Let C over \mathbb{Z} be a curve as in Section 2. Given a point $(x, y) \in (J \times J^0)(\mathbb{Z})$ we want to describe explicitly the free \mathbb{Z} -module $\mathcal{M}(x, y)$ when x is given by an invertible \mathcal{O} -module \mathcal{L} of total degree 0 on C rigidified at b and y is given as a relative Cartier divisor D on C of total degree 0 with the property that there exists a unique divisor V whose support is disjoint from b and contained in the bad fibres of $C \rightarrow \text{Spec}(\mathbb{Z})$ such that $\mathcal{O}(D+V)$ has degree zero when restricted to every irreducible component of any fibre of $C \rightarrow \text{Spec}(\mathbb{Z})$. Since $\mathcal{M}(x, y)$ is a free \mathbb{Z} -module of rank 1 then it is a submodule of $\mathcal{M}(x, y)[1/n]$ and writing $D = D^+ - D^-$ as a difference of relative effective Cartier divisors, Proposition 6.3.2, with $S = \text{Spec}(\mathbb{Z}[1/n])$, gives

$$(6.9.1) \quad \mathcal{M}(x, y)[1/n] = (\text{Norm}_{D^+/\mathbb{Z}}(\mathcal{L}) \otimes_{\mathbb{Z}} \text{Norm}_{D^-/\mathbb{Z}}(\mathcal{L})^{-1}) [1/n]$$

and consequently there exist unique integers e_q , for q varying among the primes dividing n , such that, as submodules of $(\text{Norm}_{D^+/\mathbb{Z}}(\mathcal{L}) \otimes_{\mathbb{Z}} \text{Norm}_{D^-/\mathbb{Z}}(\mathcal{L})^{-1}) [1/n]$,

$$(6.9.2) \quad \mathcal{M}(x, y) = \left(\prod_{q|n} q^{e_q} \right) \cdot (\text{Norm}_{D^+/\mathbb{Z}}(\mathcal{L}) \otimes_{\mathbb{Z}} \text{Norm}_{D^-/\mathbb{Z}}(\mathcal{L})^{-1}) .$$

We write $V = \sum_{q|n} V_q$ where V_q is a divisor supported on $C_{\mathbb{F}_q}$. For every prime q dividing n let $C_{i,q}, i \in I_q$ the irreducible components of $C_{\mathbb{F}_q}$ with multiplicity $m_{i,q}$ and let $V_{i,q}$ be the integers so that $V_q = \sum_{i \in I_q} V_{i,q} C_{i,q}$.

For every q dividing n let H_q be an effective relative Cartier divisor on $C_{\mathbb{Z}_q}$ whose complement U_q is affine (recall that C is projective over \mathbb{Z} , take a high degree embedding and a hyperplane section that avoids chosen closed points $c_{i,q}$ on the $C_{i,q}$). The Chinese remainder theorem, applied to the $\mathcal{O}_C(U_q)$ -module $(\mathcal{O}_C(D+V))(U_q)$ and the (distinct) closed points $c_{i,q}$, provides an element f_q of $(\mathcal{O}_C(D+V))(U_q)$ that generates $\mathcal{O}_C(D+V)$ at all $c_{i,q}$. Let $D_q = D_q^+ - D_q^-$ be the divisor of f_q as rational section of $\mathcal{O}_C(D+V)$. Then D_q^+ and D_q^- are finite over \mathbb{Z}_q , and f_q is a rational function on $C_{\mathbb{Z}_q}$ with

$$(6.9.3) \quad \text{div}(f_q) = (D_q^+ - D_q^-) - (D + V) = (D_q^+ + D^-) - (D^+ + D_q^-) - V .$$

This linear equivalence, restricted to \mathbb{Q}_q , gives the isomorphism (6.4.7)

$$(6.9.4) \quad \varphi: \text{Norm}_{(D^+ + D_q^-)/\mathbb{Q}_q}(\mathcal{L}) \longrightarrow \text{Norm}_{(D_q^+ + D^-)/\mathbb{Q}_q}(\mathcal{L}) .$$

Tensoring with $\text{Norm}_{(D^- + D_q^-)/\mathbb{Q}_q}(\mathcal{L})^{-1}$ we obtain the isomorphism

$$(6.9.5) \quad \varphi \otimes \text{id}: \text{Norm}_{D^+/\mathbb{Q}_q}(\mathcal{L}) \otimes \text{Norm}_{D^-/\mathbb{Q}_q}(\mathcal{L})^{-1} \longrightarrow \text{Norm}_{D_q^+/\mathbb{Q}_q}(\mathcal{L}) \otimes \text{Norm}_{D_q^-/\mathbb{Q}_q}(\mathcal{L})^{-1}$$

using the identifications

$$(6.9.6) \quad \begin{aligned} \text{Norm}_{D^+/\mathbb{Q}_q}(\mathcal{L}) \otimes \text{Norm}_{D^-/\mathbb{Q}_q}(\mathcal{L})^{-1} &= \text{Norm}_{(D^+ + D_q^-)/\mathbb{Q}_q}(\mathcal{L}) \otimes \text{Norm}_{(D^- + D_q^-)/\mathbb{Q}_q}(\mathcal{L})^{-1} \\ \text{Norm}_{D_q^+/\mathbb{Q}_q}(\mathcal{L}) \otimes \text{Norm}_{D_q^-/\mathbb{Q}_q}(\mathcal{L})^{-1} &= \text{Norm}_{(D_q^+ + D^-)/\mathbb{Q}_q}(\mathcal{L}) \otimes \text{Norm}_{(D^- + D_q^-)/\mathbb{Q}_q}(\mathcal{L})^{-1} . \end{aligned}$$

Using the same method as for getting the rational section f_q of $\mathcal{O}_C(D + V)$, we get a rational section l of \mathcal{L} with the support of $\text{div}(l)$ finite over \mathbb{Z}_q and disjoint from the supports of D and D_q , and from the intersections of different $C_{i,q}$ and $C_{j,q}$. By Proposition 6.8.7, and the choice of l ,

$$(6.9.7) \quad \mathcal{M}(x, y)_{\mathbb{Z}_q} = \text{Norm}_{D_q^+/\mathbb{Z}_q}(\mathcal{L}) \otimes \text{Norm}_{D_q^-/\mathbb{Z}_q}(\mathcal{L})^{-1} = \mathbb{Z}_q \cdot \text{Norm}_{D_q^+/\mathbb{Z}_q}(l) \otimes \text{Norm}_{D_q^-/\mathbb{Z}_q}(l)^{-1},$$

and

$$(6.9.8) \quad \text{Norm}_{D^+/\mathbb{Z}_q}(\mathcal{L}) \otimes \text{Norm}_{D^-/\mathbb{Z}_q}(\mathcal{L})^{-1} = \mathbb{Z}_q \cdot \text{Norm}_{D^+/\mathbb{Z}_q}(l) \otimes \text{Norm}_{D^-/\mathbb{Z}_q}(l)^{-1}.$$

By (6.4.4), we have

$$(6.9.9) \quad \varphi \otimes \text{id}: \text{Norm}_{D^+/\mathbb{Q}_q}(l) \otimes \text{Norm}_{D^-/\mathbb{Q}_q}(l)^{-1} \mapsto f_q(\text{div}(l))^{-1} \cdot \text{Norm}_{D_q^+/\mathbb{Q}_q}(l) \otimes \text{Norm}_{D_q^-/\mathbb{Q}_q}(l)^{-1}.$$

Comparing with (6.9.2), we conclude that

$$(6.9.10) \quad e_q = v_q(f_q(\text{div}(l))).$$

We write $\text{div}(l) = \sum_j n_j D_j$ as a sum of prime divisors. These D_j are finite over \mathbb{Z}_q , disjoint from the support of the horizontal part of $\text{div}(f_q)$, that is of $D_q - D$, and each of them meets only one of the $C_{i,q}$, say $C_{s(j),q}$. Then, for each j , $f_q^{m_{s(j),q}}$ and $q^{-V_{s(j),q}}$ have the same multiplicity along $C_{s(j),q}$, and consequently they differ multiplicatively by a unit on a neighborhood of D_j .

Then we have

$$(6.9.11) \quad \begin{aligned} v_q(f_q(D_j)) &= \frac{v_q(f_q^{m_{s(j),q}}(D_j))}{m_{s(j),q}} = \frac{v_q(q^{-V_{s(j),q}}(D_j))}{m_{s(j),q}} = \frac{v_q(\text{Norm}_{D_j/\mathbb{Z}_q}(q^{-V_{s(j),q}}))}{m_{s(j),q}} \\ &= \frac{-V_{s(j),q} \deg_{\mathbb{Z}_q}(D_j)}{m_{s(j),q}} = \frac{-V_{s(j),q} \cdot (D_j \cdot C_{\mathbb{F}_q})}{m_{s(j),q}} = \frac{-V_{s(j),q} \cdot (D_j \cdot m_{s(j),q} C_{s(j),q})}{m_{s(j),q}} \\ &= -V_{s(j),q} (D_j \cdot C_{s(j)}) = -V_q \cdot D_j. \end{aligned}$$

We get

$$(6.9.12) \quad e_q = v_q(f_q(\text{div}(l))) = -V_q \cdot \text{div}(l) = -\sum_{i \in I_q} V_{i,q} (C_i \cdot \text{div}(l)) = -\sum_{i \in I_q} V_{i,q} \deg_{\mathbb{F}_q}(\mathcal{L}|_{C_{i,q}}).$$

7 Description of the map from the curve to the torsor

The situation is as in Section 2, see (2.12). We describe the morphism $\tilde{j}_b: U \rightarrow T$ in terms of invertible \mathcal{O} -modules on $C \times C^{\text{sm}}$. Since T is the product, over J , of the \mathbb{G}_{m} -torsors $T_i := (\text{id}, m \circ \text{tr}_{c_i} \circ f_i)^* P^\times$ this amounts to describing, for each i , the morphism $(\tilde{j}_b)_i: U \rightarrow T_i$. Note that $\text{tr}_{c_i} \circ f_i: J_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ is a morphism of groupschemes composed with a translation, and that all morphisms of schemes $\alpha: J_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ are of this form. From now on we fix one such i and omit it from our notation.

Let $\alpha: J_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ be a morphism of schemes, let \mathcal{L}_{α} be the pullback of \mathcal{M} (see (6.3.3)) to $C_{\mathbb{Q}} \times C_{\mathbb{Q}}$ via $j_b \times (\alpha \circ j_b)$, and let $T_{\alpha} := (\text{id}, \alpha)^* \mathcal{M}^{\times}$ on $J_{\mathbb{Q}}$:

$$(7.1) \quad \begin{array}{ccccc} & T_{\alpha} & \longrightarrow & \mathcal{M}^{\times} & \\ & \downarrow & & & \uparrow \\ C_{\mathbb{Q}} & \xrightarrow{j_b} & J_{\mathbb{Q}} & \xrightarrow{(\text{id}, \alpha)} & (J \times J)_{\mathbb{Q}} \\ \downarrow \text{diag} & & & & \uparrow j_b \times \text{id} \\ (C \times C)_{\mathbb{Q}} & \xrightarrow{\text{id} \times j_b} & (C \times J)_{\mathbb{Q}} & \xrightarrow{\text{id} \times \alpha} & (C \times J)_{\mathbb{Q}} \\ \uparrow & & & & \uparrow \\ \mathcal{L}_{\alpha}^{\times} & \longrightarrow & & & \mathcal{L}^{\text{univ}, \times}. \end{array}$$

Then $(b, \text{id})^* \mathcal{L}_{\alpha} = \mathcal{O}_{C_{\mathbb{Q}}}$, \mathcal{L}_{α} is of degree zero on the fibres of $\text{pr}_2: (C \times C)_{\mathbb{Q}} \rightarrow C_{\mathbb{Q}}$, and: $j_b^* T_{\alpha}$ is trivial if and only if $\text{diag}^* \mathcal{L}_{\alpha}$ is trivial. Note that diagram (7.1) without the \mathbb{G}_m -torsors is commutative.

Conversely, let \mathcal{L} be an invertible \mathcal{O} -module on $(C \times C)_{\mathbb{Q}}$, rigidified on $\{b\} \times C_{\mathbb{Q}}$, and of degree 0 on the fibres of $\text{pr}_2: (C \times C)_{\mathbb{Q}} \rightarrow C_{\mathbb{Q}}$. The universal property of $\mathcal{L}^{\text{univ}}$ gives a unique $\beta_{\mathcal{L}}: C_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ such that $(\text{id} \times \beta_{\mathcal{L}})^* \mathcal{L}^{\text{univ}} = \mathcal{L}$ (compatible with rigidification at b). The Albanese property of $j_b: C_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ then gives that $\beta_{\mathcal{L}}$ extends to a unique $\alpha_{\mathcal{L}}: J_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ such that $\alpha_{\mathcal{L}} \circ j_b = \beta_{\mathcal{L}}$. Then $j_b^* T_{\alpha_{\mathcal{L}}}$ is trivial if and only if $\text{diag}^* \mathcal{L}$ is trivial. Now assume that $\text{diag}^* \mathcal{L} = \mathcal{O}_{C_{\mathbb{Q}}}$ (compatible with rigidifications at b), and let

$$(7.2) \quad \ell \in (\text{diag}^* \mathcal{L}^{\times})(C_{\mathbb{Q}})$$

correspond to 1. Then $m \cdot \circ \alpha_{\mathcal{L}}$ extends over \mathbb{Z} to $m \cdot \circ \alpha_{\mathcal{L}}: J \rightarrow J^0$, and the restriction of $j_b^*(m \cdot \circ \alpha_{\mathcal{L}})^* \mathcal{M}$ on C^{sm} to U is trivial, giving a lift \tilde{j}_b , unique up to sign:

$$(7.3) \quad \begin{array}{ccccc} & T_{m \cdot \circ \alpha_{\mathcal{L}}} & \longrightarrow & \mathcal{M}^{\times} & \\ & \downarrow & & & \downarrow \\ U & \xrightarrow{\tilde{j}_b} & C^{\text{sm}} & \xrightarrow{j_b} & J \xrightarrow{(\text{id}, m \cdot \circ \alpha_{\mathcal{L}})} J \times J^0. \end{array}$$

The invertible \mathcal{O} -module \mathcal{L} on $(C \times C)_{\mathbb{Q}}$ with its rigidification of $(b, \text{id})^* \mathcal{L}$, extends uniquely to an invertible \mathcal{O} -module on $(C \times C)_{\mathbb{Z}[1/n]}$, still denoted \mathcal{L} . For S a $\mathbb{Z}[1/n]$ -scheme, d and e in $\mathbb{Z}_{\geq 0}$, $D \in C^{(d)}(S)$ and $E \in C^{(e)}(S)$, we claim that

$$(7.4) \quad \mathcal{M}(\Sigma(D), \alpha_{\mathcal{L}}(\Sigma(E))) = (\text{Norm}_{D/S}(\text{id}, b)^* \mathcal{L})^{\otimes(1-e)} \otimes \text{Norm}_{(D \times E)/S}(\mathcal{L}).$$

To prove this, we may and do assume (finite locally free base change on S) that we have x_i and y_j in $C(S)$, such that $D = \sum_i x_i$ and $E = \sum_j y_j$. Recall that, for $c \in C(S)$, $\beta_{\mathcal{L}}(c)$ in $J(S)$ is $(\text{id}, c)^* \mathcal{L}$ on C_S , with its rigidification at b . Then we have:

$$(7.4.1) \quad \begin{aligned} \mathcal{M}(\Sigma(D), \alpha_{\mathcal{L}}(\Sigma(E))) &= \mathcal{M}(\alpha_{\mathcal{L}}(\Sigma(E)), \Sigma(D)) \\ &= \mathcal{M}\left(\beta_{\mathcal{L}}(b) + \sum_j (\beta_{\mathcal{L}}(y_j) - \beta_{\mathcal{L}}(b)), \sum_i j_b(x_i)\right) \\ &= \left(\bigotimes_i \mathcal{L}(x_i, b)^{\otimes(1-e)}\right) \otimes \bigotimes_{i,j} \mathcal{L}(x_i, y_j). \end{aligned}$$

from which the desired equality follows.

For S a $\mathbb{Z}[1/n]$ -scheme and $x \in C(S)$, applying (7.4) with $D = E = x$ gives:

$$(7.5) \quad T_{m \cdot \alpha_{\mathcal{L}}}(j_b(x)) = \mathcal{M}^{\times}(j_b(x), m \cdot \alpha_{\mathcal{L}}(j_b(x))) = \mathcal{L}^{\otimes m}(x, x)^{\times} = (\mathbb{G}_m)_S,$$

with the last equality coming from the rigidification at b .

Now let \mathcal{L} be any extension of \mathcal{L} with its rigidification of $(b, \text{id})^* \mathcal{L}$ from $(C \times C)_{\mathbb{Z}[1/n]}$ to $C \times U$. For q dividing n , let W_q be the valuation along $U_{\mathbb{F}_q}$ of the rational section ℓ of $\text{diag}^* \mathcal{L}$ on U . Then ℓ , multiplied by the product, over the primes q dividing n , of q^{-W_q} , generates $\text{diag}^* \mathcal{L}$ on U :

$$(7.6) \quad \left(\prod_{q|n} q^{-W_q} \right) \cdot \ell \in (\text{diag}^* \mathcal{L}^{\times})(U).$$

There is a unique divisor V on $C \times U$ with support disjoint from $(b, \text{id})U$ and contained in the $(C \times U)_{\mathbb{F}_q}$ with q dividing n , such that

$$(7.7) \quad \mathcal{L}^m := \mathcal{L}^{\otimes m}(V) \quad \text{on } C \times U$$

has multidegree 0 on the fibres of $\text{pr}_2: C \times U \rightarrow U$. Then \mathcal{L}^m is the pullback of $\mathcal{L}^{\text{univ}}$ via $\text{id} \times (m \cdot \circ \alpha_{\mathcal{L}} \circ j_b): C \times U \rightarrow C \times J^0$. Its restriction $\mathcal{L}^m|_{C^{\text{sm}} \times U}$ is then the pullback of \mathcal{M} via $j_b \times (m \cdot \circ \alpha_{\mathcal{L}} \circ j_b): C^{\text{sm}} \times U \rightarrow J \times J^0$, because on $C^{\text{sm}} \times J^0$ the restriction of $\mathcal{L}^{\text{univ}}$ and $(j_b \times \text{id})^* \mathcal{M}$ are equal (both are rigidified after $(b, \text{id})^*$ and equal over $\mathbb{Z}[1/n]$; here we use that, for all $q|n$, $J_{\mathbb{F}_q}^0$ is geometrically connected). Hence, on U we have $j_b^* T_{m \cdot \alpha_{\mathcal{L}}} = \text{diag}^*(\mathcal{L}^{\otimes m}(V)^{\times})$, compatible with rigidifications at $b \in U(\mathbb{Z}[1/n])$. Our trivialisation \tilde{j}_b on U of $T_{m \cdot \alpha_{\mathcal{L}}}$ is therefore a generating section of $\mathcal{L}^{\otimes m}$, multiplied by the product over the q dividing n , of the factors q^{-V_q} , where V_q is the multiplicity in V of the prime divisor $(U \times U)_{\mathbb{F}_q}$. Then, for x and S as in (7.5), we have the following description of \tilde{j}_b :

$$(7.8) \quad \tilde{j}_b(x) = \left(\prod_{q|n} q^{-mW_q - V_q} \right) \cdot \ell^{\otimes m} \quad \text{in } (T_{m \cdot \alpha_{\mathcal{L}}}(j_b(x)))(S) = \mathcal{L}^{\otimes m}(x, x)^{\times}(S).$$

8 An example with genus 2, rank 2, and 14 points

Let C_0 be the curve over \mathbb{Z} obtained from the following closed subschemes of $\mathbb{A}_{\mathbb{Z}}^2$

$$\begin{aligned} V_1 : \quad & y^2 + y = x^6 - 3x^5 + x^4 + 3x^3 - x^2 - x, \\ V_2 : \quad & w^2 + z^3w = 1 - 3z + z^2 + 3z^3 - z^4 - z^5 \end{aligned}$$

by glueing the open subset of V_1 where x is invertible with the open subset of V_2 where z is invertible using the identifications $z = 1/x$, $w = y/x^3$. The scheme C_0 can be also described as a subscheme of the line bundle \mathcal{L}_3 associated to the invertible \mathcal{O} -module $\mathcal{O}_{\mathbb{P}_{\mathbb{Z}}^1}(3)$ on $\mathbb{P}_{\mathbb{Z}}^1$ with homogeneous coordinates X, Z : the map $\mathcal{O}_{\mathbb{P}_{\mathbb{Z}}^1}(3) \rightarrow \mathcal{O}_{\mathbb{P}_{\mathbb{Z}}^1}(6)$ sending a section Y to $Y \otimes Y + Z^3 \otimes Y$ induces a map φ from \mathcal{L}_3 to the line bundle \mathcal{L}_6 associated to $\mathcal{O}(6)$; then C_0 is isomorphic to the inverse image by φ of the section $s := X^6 - 3X^5Z + X^4Z^2 + 3X^3Z^3 - X^2Z^4 - XZ^5$ of \mathcal{L}_6 and

since the map φ is finite of degree 2 then C_0 is finite of degree 2 over $\mathbb{P}_{\mathbb{Z}}^1$. Hence C_0 is proper over \mathbb{Z} and it is moreover smooth over $\mathbb{Z}[1/n]$ with $n = 3 \cdot 43$. The generic fiber of C_0 is a curve of genus $g = 2$, labeled 5547.b.16641.1 on www.lmfdb.org. The only point where C_0 is not regular is the point $P_0 = (3, x - 2, y - 1)$ contained in V_1 and the blow up C of C_0 in P_0 is regular.

In the rest of the article we apply our geometric method to the curve C and we prove that $C(\mathbb{Z})$ contains exactly 14 elements. We use the same notation as in Sections 2 and 4.

The fiber $C_{\mathbb{F}_{43}}$ is absolutely irreducible while $C_{\mathbb{F}_3}$ is the union of two geometrically irreducible curves, a curve of genus 0 that lies above the point P_0 and that we call K_0 , and a curve of genus 1 that we call K_1 . We define $U_0 := C \setminus K_1$ and $U_1 := C \setminus K_0$ so that $C(\mathbb{Z}) = C^{\text{sm}}(\mathbb{Z}) = U_0(\mathbb{Z}) \cup U_1(\mathbb{Z})$ and both U_0 and U_1 satisfy the hypothesis of U in Section 2. We have $K_0 \cdot K_1 = 2$ and consequently the self-intersections of K_0 and K_1 are both equal to -2 . We deduce that all the fibers of J over \mathbb{Z} are connected except for $J_{\mathbb{F}_3}$ which has group of connected components equal to $\mathbb{Z}/2\mathbb{Z}$. Hence $m = 2$.

The automorphism group of C is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, generated by the automorphisms ι and η lifting the extension to C_0 of

$$\iota, \eta: V_1 \longrightarrow V_1, \quad \iota: (x, y) \longmapsto (x, -1 - y), \quad \eta: (x, y) \longmapsto (1 - x, -1 - y).$$

The quotients $E_1 := C_{\mathbb{Q}}/\eta$ and $E_2 := C_{\mathbb{Q}}/(\iota \circ \eta)$ are curves of genus 1 and the two projections $C \rightarrow E_i$ induce an isogeny $J \rightarrow \text{Pic}^0(E_1) \times \text{Pic}^0(E_2)$. The elliptic curves $\text{Pic}^0(E_i)$ are not isogenous and $\rho = 2$.

8.1 The torsor on the jacobian

Let $\infty, \infty_- \in C(\mathbb{Z})$ be the lifts of $(0, 1), (0, -1) \in V_2(\mathbb{Z}) \subset C_0(\mathbb{Z})$ and let us fix the base point $b = \infty$ in $C(\mathbb{Z})$. Following Section 7 we describe a \mathbb{G}_{m} -torsor $T \rightarrow J$ and maps $\widetilde{j_{b,i}}: U_i \rightarrow T$ using invertible \mathcal{O} -modules on $C \times C^{\text{sm}}$. Let Γ_{η} denote the graph of the map $\eta: C \rightarrow C$. Over $C_{\mathbb{Q}} \times C_{\mathbb{Q}}$ we consider

$$\mathcal{L} := \mathcal{O}_{C_{\mathbb{Q}} \times C_{\mathbb{Q}}}(\Gamma_{\eta, \mathbb{Q}} - \infty_- \times C_{\mathbb{Q}} - C_{\mathbb{Q}} \times \infty)$$

trivialised on $b \times C_{\mathbb{Q}}$ through the section

$$l_b := 2 \quad \text{in } ((b, \text{id})^* \mathcal{L})(C_{\mathbb{Q}}) = \mathcal{O}_{C_{\mathbb{Q}}}(\eta(b) - b)(C_{\mathbb{Q}}) = \mathcal{O}_{C_{\mathbb{Q}}}(C_{\mathbb{Q}}).$$

Notice that $(\text{id}, b)^* \mathcal{L}$ has degree 0 hence there exists a morphism of schemes $\alpha_{\mathcal{L}}: J_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$ such that \mathcal{L} , with its rigidification at $b \times C_{\mathbb{Q}}$, is the pull back of \mathcal{M} via $j_b \times (\alpha_{\mathcal{L}} \circ j_b)$. For every $\overline{\mathbb{Q}}$ -point Q on $C_{\mathbb{Q}}$ the invertible $\mathcal{O}_{C_{\overline{\mathbb{Q}}}}$ -module $(\text{id}, Q)^* \mathcal{L}$ is isomorphic to $\mathcal{O}_{C_{\overline{\mathbb{Q}}}}(\eta(Q) - \infty_-)$ hence

$$\alpha = \text{tr}_c \circ f, \quad \text{with } f = \eta_* \text{ and } c = [D_0], D_0 := \infty - \infty_-.$$

When restricted to the diagonal \mathcal{L} is trivial since, compatibly with the trivialisation at (b, b) ,

$$\text{diag}^* \mathcal{L} = \mathcal{O}_{C_{\mathbb{Q}}}(\infty_- + \infty - \infty_- - \infty) = \mathcal{O}_{C_{\mathbb{Q}}} = l \cdot \mathcal{O}_{C_{\mathbb{Q}}} \quad \text{with } l := 1.$$

Following Section 7 we choose the extension of \mathcal{L} over $C \times C^{\text{sm}}$

$$\mathcal{L} := \mathcal{O}(\Gamma_{\eta}|_{C \times C^{\text{sm}}} - \infty_- \times C^{\text{sm}} - C \times \infty)$$

trivialised along $b \times C^{\text{sm}}$ through the section $l_b = 2$ (the points ∞_- and b have a simple intersection over the prime 2). Following (7.5) the torsor $T := T_{m \cdot \alpha_L}$ on J satisfies, for S a $\mathbb{Z}[1/n]$ -scheme and x in $C(S)$, using the trivialisation given by l and l_b

$$\begin{aligned} (8.1.1) \quad T(j_b(x)) &= \mathcal{M}^\times(j_b(x), m \cdot \alpha_L(j_b(x))) = \mathcal{M}^\times(j_b(x), (\text{id}, x)^* \mathcal{L}^{\otimes m}) \\ &= x^*(\text{id}, x)^* \mathcal{L}^{\otimes m, \times} \otimes b^*(\text{id}, x)^* \mathcal{L}^{\otimes -m, \times} \\ &= \mathcal{L}^{\otimes m, \times}(x, x) \otimes \mathcal{L}^{\otimes m, \times}(b, x)^{-1} = \mathcal{L}^{\otimes m, \times}(x, x) = \mathcal{O}_S^\times. \end{aligned}$$

Since l generates $\text{diag}^*(\mathcal{L})$ on the whole C^{sm} then, we have $W_3 = W_{43} = 0$ in (7.6) when computing both $\widetilde{j}_{b,0}$ and $\widetilde{j}_{b,1}$.

The invertible \mathcal{O} -module $\mathcal{L}^{\otimes m}$ has multidegree 0 over all the fibers $C \times U_1 \rightarrow U_1$, hence in order to compute $\widetilde{j}_{b,1}$ we must take $V = 0$ in (7.7), giving $V_3 = V_{43} = 0$. Hence for S and x as in (8.1.1), assuming moreover that 2 is invertible on S ,

$$(8.1.2) \quad \widetilde{j}_{b,1}(x) = l^2 \otimes l_b^{-2} = \frac{1}{4}(x^* 1) \otimes (b^* 1)^{-1} \quad \text{in}$$

$$T(j_b(x)) = x^*(\text{id}, x)^* \mathcal{L}^{\otimes m, \times} \otimes b^*(\text{id}, x)^* \mathcal{L}^{\otimes -m, \times} = x^* \mathcal{O}_{C_S}(\eta(x) - \infty_-)^\times \otimes b^* \mathcal{O}_{C_S}(\eta(x) - \infty_-)^\times,$$

where the last equality in (8.1.2) makes sense if the image of x is disjoint from ∞, ∞_- in C_S .

The restriction $\mathcal{L}^{\otimes m}$ to $C \times U_0$ has multidegree 0 over all the fibers $C \times U_0 \rightarrow U_0$ of characteristic not 3, while if we consider a fiber of characteristic 3 it has degree 2 over K_0 and degree -2 over K_1 . Hence for computing $\widetilde{j}_{b,0}$ we take $V = K_0 \times (K_0 \cap U_0)$ in (7.7) giving $V_{43} = 0, V_3 = 1$. Hence for S and x as in (8.1.1), assuming moreover that 2 is invertible on S ,

$$(8.1.3) \quad \widetilde{j}_{b,0}(x) = \frac{1}{3}l^2 \otimes l_b^{-2} = \frac{1}{12}(x^* 1) \otimes (b^* 1)^{-1} \quad \text{in}$$

$$T(j_b(x)) = x^*(\text{id}, x)^* \mathcal{L}^{\otimes m, \times} \otimes b^*(\text{id}, x)^* \mathcal{L}^{\otimes -m, \times} = x^* \mathcal{O}_{C_S}(\eta(x) - \infty_-)^\times \otimes b^* \mathcal{O}_{C_S}(\eta(x) - \infty_-)^\times,$$

where the last equality in (8.1.3) makes sense if the image of x is disjoint from ∞, ∞_- in C_S .

8.2 Some integral points on the biextension

On C_0 we have the following integral points that lift uniquely to elements of $C(\mathbb{Z})$

$$\begin{aligned} \infty &= (0, 1), \quad \infty_- := (0, -1) \quad \text{in } V_2(\mathbb{Z}), \\ \alpha &:= (1, 0), \quad \beta := \eta(\alpha) = (0, -1), \quad \gamma := (2, 1), \quad \delta := \eta(\gamma) = (-1, -2) \quad \text{in } V_1(\mathbb{Z}). \end{aligned}$$

Computations in Magma confirm that $J(\mathbb{Z})$ is a free \mathbb{Z} -module of rank $r = 2$ generated by

$$G_1 := \gamma - \alpha, \quad G_2 := \alpha + \infty_- - 2\infty.$$

The points in $T(\mathbb{Z})$ are a subset of points of $\mathcal{M}^\times(\mathbb{Z})$ that can be constructed, using the two group laws, from the points in $\mathcal{M}^\times(G_i, m \cdot f(G_j))(\mathbb{Z})$ and $\mathcal{M}^\times(G_i, m \cdot D_0)(\mathbb{Z})$ for $i, j \in \{1, 2\}$. Let us compute in detail $\mathcal{M}^\times(G_1, m \cdot f(G_1))(\mathbb{Z})$. As explained in Section 6.9

$$\begin{aligned} \mathcal{M}(G_1, m \cdot f(G_1))^\times &= \mathcal{M}^\times(\gamma - \alpha, 2\delta - 2\beta) \\ &= 3^{e_3} 43^{e_{43}} \cdot \text{Norm}_{(2\delta)/\mathbb{Z}}(\mathcal{O}_C(\gamma - \alpha)) \otimes \text{Norm}_{(2\beta)/\mathbb{Z}}(\mathcal{O}(\gamma - \alpha))^{-1} \\ &= 3^{e_3} 43^{e_{43}} \cdot (2\delta - 2\beta)^* \mathcal{O}_C(\gamma - \alpha) \end{aligned}$$

where, given a scheme S , an invertible \mathcal{O} -module \mathcal{L} on C_S and a divisor $D_+ - D_- = \sum_i n_i P_i$ on C_S that is sum of S -points, we define the invertible \mathcal{O}_S -module

$$\left(\sum_i n_i P_i \right)^* \mathcal{L} := \bigotimes_i P_i^* \mathcal{L}^{n_i} = \text{Norm}_{D_+/S}(\mathcal{L}) \otimes \text{Norm}_{D_-/S}(\mathcal{L})^{-1}.$$

Since $C_{\mathbb{F}_{43}}$ is irreducible then $2f(G_1)$ has already multidegree 0 over 43, hence $e_{43} = 0$. If we look at $C_{\mathbb{F}_3}$ then $2f(G_1)$ does not have multidegree 0, while $2f(G_1) + K_0$ has multidegree 0; hence by (6.9.12)

$$e_3 = -\deg_{\mathbb{F}_3} \mathcal{O}_C(\gamma - \alpha)|_{K_0} = -1.$$

Notice that over $\mathbb{Z}[\frac{1}{2}]$ the divisor G_1 is disjoint from β and δ (to see that it is disjoint from $\delta = (-1, -2, 1)$ over the prime 3 one needs to look at local equations of the blow up) thus $\beta^* \mathcal{O}_C(\gamma - \alpha)$ and $\delta^* \mathcal{O}_C(\gamma - \alpha)$ are generated by $\beta^* 1$ and $\delta^* 1$ over $\mathbb{Z}[\frac{1}{2}]$. Thus there are integers e_β, e_δ such that $\beta^* \mathcal{O}_C(\gamma - \alpha)$ and $\delta^* \mathcal{O}_C(\gamma - \alpha)$ are generated by $\beta^* 2^{e_\beta}$ and $\delta^* 2^{e_\delta}$ over \mathbb{Z} . Looking at the intersections between β, γ, α and δ we compute that $e_\beta = -1$ $e_\delta = 1$ hence

$$\begin{aligned} \mathcal{M}(G_1, m \cdot f(G_1)) &= 3^{-1} \cdot (\delta^* 2)^2 \otimes (\beta^* 2^{-1})^{-2} \cdot \mathbb{Z} = 2^4 \cdot 3^{-1} \cdot (\delta^* 1)^2 \otimes (\beta^* 1) \cdot \mathbb{Z} \quad \text{and} \\ Q_{1,1} &:= \pm 2^4 \cdot 3^{-1} \cdot (\delta^* 1)^2 \otimes (\beta^* 1)^{-2} \in \mathcal{M}_{G_1, m \cdot f(G_1)}^\times(\mathbb{Z}). \end{aligned}$$

With analogous computations we see that

$$\begin{aligned} Q_{2,1} &:= 2^{-2} \cdot (\delta^* 1)^2 \otimes (\beta^* 1)^{-2} && \text{generates } \mathcal{M}_{G_2, m \cdot f(G_1)} \\ Q_{1,2} &:= 2^{-2} \cdot (\beta^* 1)^2 \otimes (\infty_-^* 1)^2 \otimes (\infty^* 1)^{-4} && \text{generates } \mathcal{M}_{G_1, m \cdot f(G_2)} \\ Q_{2,2} &:= 2^{18} \cdot (\beta^* 1)^2 \otimes (\infty_-^* x)^2 \otimes (\infty^* z^2)^{-4} && \text{generates } \mathcal{M}_{G_2, m \cdot f(G_2)} \\ Q_{1,2} &:= (\infty^* 1)^2 \otimes (\infty_-^* 1)^{-2} && \text{generates } \mathcal{M}_{G_1, m \cdot D_0} \\ Q_{2,0} &:= 2^{-12} \cdot (\infty^* z^2)^2 \otimes (\infty_-^* x)^{-2} && \text{generates } \mathcal{M}_{G_2, m \cdot D_0}. \end{aligned}$$

8.3 Some residue disks of the biextension

Let p be a prime of good reduction for C . Given the divisors

$$D := \alpha - \infty, \quad E := 2\beta - 2\infty_- = (m \cdot \circ \text{tr}_c \circ \eta_*)(D) \quad \text{in } \text{Div}(C_{\mathbb{Z}/p^2})$$

we apply Section 6.6 and we give parameters on the residue disks in $\mathcal{M}^\times(\mathbb{Z}/p^2)_{\overline{D}, \overline{E}}$ and $T(\mathbb{Z}/p^2)_{\overline{D}}$, with $\overline{D}, \overline{E}$ the images of D, E in $\text{Div}(C_{\mathbb{F}_p})$.

We choose the “base points” $b_1 = \alpha, b_2 = \infty, b_3 = \beta, b_4 = \infty$, so that $b_1 \neq b_2, b_3 \neq b_4$ and $h^0(C_{\mathbb{F}_p}, b_1 + b_2) = h^0(C_{\mathbb{F}_p}, b_3 + b_4) = 1$. As in Section 6.6 we define $x_\alpha = x - 1, x_\infty = z, x_\beta = x$ and $x_{D, \beta} = x_{D, \infty_-} = 1, x_{D, \infty} = z^{-1}$. For Q in $\{\infty, \beta, \alpha\}$ and $a \in \mathbb{F}_p$ let Q_a be the unique \mathbb{Z}/p^2 -point of C that is congruent to Q modulo p and such that $x_Q(Q_a) = ap \in \mathbb{Z}/p^2$. We have the bijections

$$\begin{aligned} \mathbb{F}_p^2 &\longrightarrow J(\mathbb{Z}/p^2)_{\overline{D}}, \quad \lambda \longmapsto D_\lambda := D + \alpha_{\lambda_1} - \alpha + \infty_{\lambda_2} - \infty = \alpha_{\lambda_1} + \infty_{\lambda_2} - 2\infty \\ \mathbb{F}_p^2 &\longrightarrow J(\mathbb{Z}/p^2)_{\overline{E}}, \quad \mu \longmapsto E_\mu := E + \beta_{\mu_1} - \beta + \infty_{\mu_2} - \infty = \beta + \beta_{\mu_1} + \infty_{\mu_2} - \infty - 2\infty_-. \end{aligned}$$

Following (6.6.6) for $\lambda, \mu \in \mathbb{F}_p^2$ we define

$$s_{D,E}(\lambda, \mu) := (\beta^* 1) \otimes (\beta_{\mu_1}^* 1) \otimes (\infty_{\mu_2}^* \frac{z^2}{z - \lambda_2 p}) \otimes (\infty^* \frac{z^2}{z - \lambda_2 p})^{-1} \otimes (\infty_-^* 1)^{-2}$$

that, by Proposition 6.3.2 and Remark 6.3.12, generates $E_\mu^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_\lambda) = \mathcal{M}_{D_\lambda, E_\mu}$. The points in $\mathcal{M}^\times(\mathbb{F}_p)$ projecting to $(\overline{D}, \overline{E})$ are in bijection with the elements ξ in \mathbb{F}_p^\times and are exactly the points $\xi \cdot s_{D,E}(0, 0)$. Using $(\mathbb{Z}/p^2)^\times = \mathbb{F}_p^\times \times (1+p\mathbb{F}_p)$, for each $\xi \in \mathbb{F}_p^\times$ we parametrise the residue disk of $\xi \cdot s_{D,E}(0, 0)$ using bijection (6.6.7)

$$\mathbb{F}_p^5 \longrightarrow \mathcal{M}^\times(\mathbb{Z}/p^2)_{\xi \cdot s_{D,E}(0,0)}, \quad (\lambda_1, \lambda_2, \mu_1, \mu_2, \tau) \longmapsto (1 + p\tau)\xi \cdot s_{D,E}((\lambda_1, \lambda_2), (\mu_1, \mu_2)).$$

Since $(m \cdot \circ \text{tr}_c \circ f)(D_\lambda) = E_{-2\lambda}$ then we have

$$T(\mathbb{Z}/p^2)_{\overline{D}} = \bigcup_{\lambda \in \mathbb{F}_p^2} T_{D_\lambda}(\mathbb{Z}/p^2) = \bigcup_{\lambda \in \mathbb{F}_p^2} \mathcal{M}_{D_\lambda, E_{-2\lambda}}^\times(\mathbb{Z}/p^2).$$

As ξ varies in \mathbb{F}_p^\times the point $\xi \cdot s_{D,E}(0, 0)$ varies in all the points in $\mathcal{M}^\times(\mathbb{F}_p)$ projecting to $(\overline{D}, \overline{E})$ and we have the following bijection induced by parameters in $\xi \cdot s_{D,E}(0, 0)$

$$(8.3.1) \quad \mathbb{F}_p^3 \longrightarrow T(\mathbb{Z}_p)_{\xi s_{D,E}(0,0)}, \quad (\lambda_1, \lambda_2, \tau) \longmapsto (1 + \tau p) \cdot \xi \cdot s_{D,E}((\lambda_1, \lambda_2), (-2\lambda_1, -2\lambda_2)).$$

If we apply (8.1.2) and (8.1.3) to $Q = \alpha_\lambda$ and we use the symmetry of the Poincaré torsor explained in Proposition 6.3.2 and made explicit in Section 6.5 we obtain the following description of $\widetilde{j_{b,i}}$ on $C(\mathbb{Z}/p^2)_{\alpha_{\mathbb{F}_p}}$ when $p \neq 2$

$$\widetilde{j_{b,1}}(\alpha_\lambda) = (1/4) \cdot s_{D,E}((\lambda, 0), (-2\lambda, 0)), \quad \widetilde{j_{b,0}}(Q) = (1/12) \cdot s_{D,E}((\lambda, 0), (-2\lambda, 0)).$$

If $p = 5$ then 18 and -1 are $(p-1)$ -th roots of unity in $(\mathbb{Z}/p^2)^\times$, thus $1/4 = (-1)(1+p)$ and $1/12 = 3(1+2p)$ in $(\mathbb{Z}/p^2)^\times = \mathbb{F}_p^\times \times (1+p\mathbb{F}_p)$, hence

$$(8.3.2) \quad \widetilde{j_{b,1}}(\alpha_\lambda) = -(1+p) \cdot s_{D,E}((\lambda, 0), (-2\lambda, 0)), \quad \widetilde{j_{b,0}}(Q) = 3 \cdot (1+2p) \cdot s_{D,E}((\lambda, 0), (-2\lambda, 0)).$$

Since it is useful for computing the map $\kappa_{\mathbb{Z}}$ in the residue disks of $T(\mathbb{Z}/p^2)$ projecting to \overline{D} , let us apply the recipe in Section 6.6 also to the residue disks of $\mathcal{M}^\times(\mathbb{Z}/p^2)$ lying over $(\overline{D}, 0)$, $(0, \overline{E})$ and $(0, 0)$. Hence for $\lambda, \mu \in \mathbb{F}_p^2$ we define the divisors on $C_{\mathbb{Z}/p^2}$

$$D_\lambda^0 := \alpha_{\lambda_1} - \alpha + \infty_{\lambda_2} - \infty, \quad E_\mu^0 := \beta_{\mu_1} - \beta + \infty_{\mu_2} - \infty$$

and the sections

$$\begin{aligned} s_{D,0}(\lambda, \mu) &:= (\beta_{\mu_1}^* 1) \otimes (\infty_{\mu_2}^* \frac{z^2}{z - \lambda_2 p}) \otimes (\beta^* 1)^{-1} \otimes (\infty^* \frac{z^2}{z - \lambda_2 p})^{-1} && \text{in } \mathcal{M}^\times(D_\lambda, E_\mu^0)(\mathbb{Z}/p^2) \\ s_{0,E}(\lambda, \mu) &:= (\beta^* 1) \otimes (\beta_{\mu_1}^* 1) \otimes (\infty_{\mu_2}^* \frac{z}{z - \lambda_2 p}) \otimes (\infty^* \frac{z}{z - \lambda_2 p})^{-1} \otimes (\infty_-^* 1)^{-2} && \text{in } \mathcal{M}^\times(D_\lambda^0, E_\mu)(\mathbb{Z}/p^2) \\ s_{0,0}(\lambda, \mu) &:= (\beta_{\mu_1}^* 1) \otimes (\infty_{\mu_2}^* \frac{z}{z - \lambda_2 p}) \otimes (\beta^* 1)^{-1} \otimes (\infty^* \frac{z}{z - \lambda_2 p})^{-1} && \text{in } \mathcal{M}^\times(D_\lambda^0, E_\mu^0)(\mathbb{Z}/p^2). \end{aligned}$$

8.4 Geometry mod p of integral points

From now on $p = 5$. Let $\overline{\alpha} \in C(\mathbb{Z}/p^2)$ be the image of $\alpha \in C(\mathbb{Z})$. In this subsection we compute the composition $\overline{\kappa}: \mathbb{Z}^2 \rightarrow T(\mathbb{Z}/p^2)_{\widetilde{j_{b,1}}(\overline{\alpha})}$ of the map $\kappa_{\mathbb{Z}}: \mathbb{Z}^2 \rightarrow T(\mathbb{Z}_p)_{\widetilde{j_{b,1}}(\overline{\alpha})}$ in (4.9) and the reduction map $T(\mathbb{Z}_p)_{\widetilde{j_{b,1}}(\overline{\alpha})} \rightarrow T(\mathbb{Z}/p^2)_{\widetilde{j_{b,1}}(\overline{\alpha})}$. With a suitable choice of parameters in $\mathcal{O}_{T, \widetilde{j_{b,1}}(\overline{\alpha})}$, the map $\kappa_{\mathbb{Z}}$ is described by integral convergent power series $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{Z}_p\langle z_1, z_2 \rangle$

and $\overline{\kappa}$, composed with the inverse of the parametrization (8.3.1), is given the images $\overline{\kappa_1}, \overline{\kappa_2}, \overline{\kappa_3}$ of $\kappa_1, \kappa_2, \kappa_3$ in $\mathbb{F}_p[z_1, z_2]$.

The divisor $j_b(\overline{\alpha})$ is equal to the image of

$$\widetilde{G}_t := e_{0,1}G_1 + e_{0,2}G_2 \text{ with } e_{0,1} := 6, e_{0,2} := 3$$

in $J(\mathbb{F}_p)$ and

$$\tilde{t} := Q_{1,0}^6 \otimes Q_{2,0}^3 \otimes Q_{1,1}^{6 \cdot 6} \otimes Q_{1,2}^{6 \cdot 3} \otimes Q_{2,1}^{3 \cdot 6} \otimes Q_{2,2}^{3 \cdot 3} \text{ in } \mathcal{M}^\times(\widetilde{D}_1, m \cdot (D_0 + \eta_* \widetilde{G}_t))(\mathbb{Z})$$

is a lift of $j_{b,1}(\overline{\alpha})$. The kernel of $J(\mathbb{Z}) \rightarrow J(\mathbb{F}_p)$ is a free \mathbb{Z} -module generated by

$$\widetilde{G}_1 := e_{1,1}G_1 + e_{1,2}G_2, \quad \widetilde{G}_2 := e_{2,1}G_1 + e_{2,2}G_2, \text{ with } e_{1,1} := 16, e_{1,2} := 2, e_{2,1} := 0, e_{2,2} := 5.$$

Let $\widetilde{G}_{t,2}$ be the divisor $m(D_0 + \eta_*(\widetilde{G}_t))$ representing $(m \cdot \text{otr}_c \circ f)(\widetilde{G}_t) \in J^0(\mathbb{Z})$. Following (4.1) for $i, j \in \{1, 2\}$ we define

$$\begin{array}{ccc} P_{i,j} := \bigotimes_{m,l=1}^2 Q_{l,m}^{e_{i,l} \cdot e_{j,m}} & R_{i,\tilde{t}} := \bigotimes_{l=1}^2 Q_{l,0}^{e_{i,l}} \otimes \bigotimes_{m,l=1}^2 Q_{l,m}^{e_{i,l} \cdot e_{0,m}} & S_{\tilde{t},j} := \bigotimes_{m,l=1}^2 Q_{l,m}^{e_{0,l} \cdot e_{j,m}} \\ \downarrow & \downarrow & \downarrow \\ (\widetilde{G}_i, f(m\widetilde{G}_j)) & (\widetilde{G}_i, \widetilde{G}_{t,2}) & (\widetilde{G}_t, f(m\widetilde{G}_j)). \end{array}$$

Computations in $C_{\mathbb{Z}/p^2}$ show the following linear equivalences of divisors

$$\widetilde{G}_t \sim D_{0,3}, \quad \widetilde{G}_1 \sim D_{4,0}^0, \quad \widetilde{G}_2 \sim D_{0,3}^0$$

and applying Section 6.4 and the functoriality of the norm we compute

(8.4.1)

$$\begin{aligned} P_{1,1} &= (1+4p) \cdot s_{0,0}((4,0), (2,0)) && \text{in } \mathcal{M}^\times(\widetilde{G}_1, \widetilde{G}_1)(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{4,0}^0, E_{2,0}^0)(\mathbb{Z}/p^2), \\ P_{1,2} &= (1+4p) \cdot s_{0,0}((4,0), (0,4)) && \text{in } \mathcal{M}^\times(\widetilde{G}_1, \widetilde{G}_2)(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{4,0}^0, E_{0,4}^0)(\mathbb{Z}/p^2), \\ P_{2,1} &= (1+4p) \cdot s_{0,0}((0,3), (2,0)) && \text{in } \mathcal{M}^\times(\widetilde{G}_2, \widetilde{G}_1)(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{0,3}^0, E_{2,0}^0)(\mathbb{Z}/p^2), \\ P_{2,2} &= (-1) \cdot (1+2p) \cdot s_{0,0}((0,3), (0,4)) && \text{in } \mathcal{M}^\times(\widetilde{G}_2, \widetilde{G}_2)(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{0,3}^0, E_{0,4}^0)(\mathbb{Z}/p^2), \\ R_{1,\tilde{t}} &= s_{0,E}((4,0), (0,4)) && \text{in } \mathcal{M}^\times(\widetilde{G}_1, \widetilde{G}_{t,2})(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{4,0}^0, E_{0,4})(\mathbb{Z}/p^2), \\ R_{2,\tilde{t}} &= (1+4p) \cdot s_{0,E}((0,3), (0,4)) && \text{in } \mathcal{M}^\times(\widetilde{G}_2, \widetilde{G}_{t,2})(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{0,3}^0, E_{0,4})(\mathbb{Z}/p^2), \\ S_{\tilde{t},1} &= s_{D,0}((0,3), (2,0)) && \text{in } \mathcal{M}^\times(\widetilde{G}_t, \widetilde{G}_1)(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{0,3}, E_{2,0}^0)(\mathbb{Z}/p^2), \\ S_{\tilde{t},2} &= (-1)(1+4p) \cdot s_{D,0}((0,3), (0,4)) && \text{in } \mathcal{M}^\times(\widetilde{G}_t, \widetilde{G}_2)(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{0,3}, E_{0,4}^0)(\mathbb{Z}/p^2), \\ \tilde{t} &= (-1) \cdot (1+2p) \cdot s_{D,E}((0,3), (0,4)) && \text{in } \mathcal{M}^\times(\widetilde{G}_t, \widetilde{G}_{t,2})(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{0,3}, E_{0,4})(\mathbb{Z}/p^2). \end{aligned}$$

We now show these computations in the cases of \widetilde{G}_t and \tilde{t} . The Riemann-Roch space relative to the divisor $\widetilde{G}_t + \infty + \alpha - D$ on $C_{\mathbb{Z}/p^2}$ is generated by the inverse of the rational function

$$h_1 := \frac{x^9 - 5x^8 - 2x^7 + 7x^6 - 9x^5 - 5x^4 + 14x^3 + 7x^2 + 13x + 1 + (x^6 + 9x^5 - 5x^4 + 15x^3 - 5x^2 + 4x + 14)y}{15x^5 - x^4 + 4x^3 + 19x^2 + 4x + 9}$$

and indeed

$$\text{div}(h_1) = \widetilde{G}_t - D_{0,3} = (6\gamma + 3\infty_- - 3\alpha - 6\infty) - (\alpha + \infty_3 - 2\infty) \text{ in } \text{Div}(C_{\mathbb{Z}/p^2}).$$

Hence multiplication by h_1 gives an isomorphism $\mathcal{O}_{C_{\mathbb{Z}/p^2}}(\widetilde{G}_t) \rightarrow \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3})$ and by functoriality of the norm we get

$$\begin{aligned} \delta^* \mathcal{O}_C(\widetilde{G}_t) &\rightarrow \delta^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}), & \delta^* 1 &\mapsto \delta^*(h_1) = h_1(\delta) \cdot \delta^* 1 = 12 \cdot \delta^* 1, \\ \beta^* \mathcal{O}_C(\widetilde{G}_t) &\rightarrow \beta^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}), & \beta^* 1 &\mapsto \beta^*(h_1) = h_1(\beta) \cdot \beta^* 1 = 18 \cdot \beta^* 1, \\ \infty^* \mathcal{O}_C(\widetilde{G}_t) &\rightarrow \infty^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}), & \infty^* z^6 &\mapsto \infty^*(z^6 h_1) = 13 \cdot \infty^* \frac{z^2}{z-3p}, \\ \infty_-^* \mathcal{O}_C(\widetilde{G}_t) &\rightarrow \infty_-^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}), & \infty_-^* z^{-3} &\mapsto \infty_-^*(z^{-3} h_1) = (z^{-3} h_1)(\infty_-) \cdot \infty_-^* 1 = 6 \cdot \infty_-^* 1. \end{aligned}$$

Since $\widetilde{G}_{t,2} = 12\delta + 4\infty_- - 6\beta - 10\infty$, the above isomorphisms, tensored with the exponents, give the canonical isomorphism

$$(8.4.2) \quad \mathcal{M}(\widetilde{G}_t, \widetilde{G}_{t,2}) = \widetilde{G}_{t,2}^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(\widetilde{G}_t) \rightarrow \widetilde{G}_{t,2}^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}) = \mathcal{M}(D_{0,3}, \widetilde{G}_{t,2})$$

$$\tilde{t} = 14 \cdot (\delta^* 1)^{12} \otimes (\beta^* 1)^{-6} \otimes (\infty^* z^6)^{-10} \otimes (\infty_-^* z^{-3})^4 \mapsto 14 \cdot (\delta^* 1)^{12} \otimes (\beta^* 1)^{-6} \otimes (\infty^* \frac{z^2}{z-3p})^{-10} \otimes (\infty_-^* 1)^4.$$

The Riemann-Roch space relative to the divisor $\widetilde{G}_{t,2} + \infty + \alpha - E$ on $C_{\mathbb{Z}/p^2}$ is generated by the inverse of the rational function

$$h_2 := \frac{x^{17} - 8x^{16} + x^{15} - 4x^{14} + 7x^{13} + 4x^{12} + 12x^{11} + x^{10} + 2x^9 - 5x^8 + x^7 + 3x^6 + 12x^5 - 6x^4 - 6x^3 + 4x^2 - 6}{20x^8 - 6x^7}$$

$$+ \frac{10x^2 + (x^{15} + 6x^{14} - 5x^{13} - x^{12} - 2x^{11} + 14x^{10} - 4x^9 + 14x^8 + 3x^7 + 8x^6 - 6x^5 - 3x^4 + 4x^3 + 13x^2 - x - 7)y}{20x^9 - 6x^8}$$

and indeed

$$\text{div}(h_2) = \widetilde{G}_{t,2} - E_{0,4} = (12\delta + 4\infty_- - 6\beta - 10\infty) - (2\beta + \infty_4 - \infty - \infty_-) \quad \text{in } \text{Div}(C_{\mathbb{Z}/p^2}).$$

Following the recipe in Section 6.4 we consider the following rational section of $\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3})$

$$l := \frac{10x^4 + x^3 + 17x + 14 + (15x + 9)y}{10x^4 + 16x^3 + 7x^2 + 7x + 10}.$$

since it generates $\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3})$ in a neighborhood of the supports of $\widetilde{G}_{t,2}$ and $E_{0,4}$. Then

$$\text{div}(l) = 3 \cdot (-1, 1) + (17, 23) + (15, 10) - 2 \cdot (12, 23) - 2 \cdot (5, 20) - (0, 1) \quad \text{in } \text{Div}(V_{1, \mathbb{Z}/p^2}) \subset \text{Div}(C_{\mathbb{Z}/p^2}).$$

Hence by (6.4.4) the canonical isomorphism

$$\mathcal{M}(D_{0,3}, \widetilde{G}_{t,2}) = \widetilde{G}_{t,2}^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}) \longrightarrow E_{0,4}^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}) = \mathcal{M}(D_{0,3}, E_{0,4})$$

described in Section 6.4 is characterised by

$$(8.4.3) \quad \widetilde{G}_{t,2}^* l \longmapsto h_2(\text{div}(l)) \cdot E_{0,4}^* l = 14 \cdot E_{0,4}^* l.$$

where

$$\begin{aligned} \widetilde{G}_{t,2}^* l &:= (\delta^* l)^{12} \otimes (\beta^* l)^{-6} \otimes (\infty^* l)^{-10} \otimes (\infty_-^* l)^4 = -(\delta^* 1)^{12} \otimes (\beta^* 1)^{-6} \otimes (\infty^* \frac{z^2}{z-3p})^{-10} \otimes (\infty_-^* 1)^4, \\ E_{0,4}^* l &:= (\beta^* l)^2 \otimes (\infty_4^* l) \otimes (\infty^* l)^{-1} \otimes (\infty_-^* l)^{-2} = 16 \cdot (\beta^* 1)^2 \otimes (\infty_4^* \frac{z^2}{z-3p}) \otimes (\infty^* \frac{z^2}{z-3p})^{-1} \otimes (\infty_-^* 1)^{-2}. \end{aligned}$$

Equations (8.4.2) and (8.4.3) imply that $\tilde{t} = -(1 + 2p) \cdot s_{D,E}((0, 3), (0, 4))$.

Let $\overline{A}_{\tilde{t}}$, $\overline{B}_{\tilde{t}}$, \overline{C} and $\overline{D}_{\tilde{t}}$ be the compositions of the reduction map $\mathcal{M}^{\times}(\mathbb{Z}_p) \rightarrow \mathcal{M}(\mathbb{Z}/p^2)$ and respectively $A_{\tilde{t}}$, $B_{\tilde{t}}$, C and $D_{\tilde{t}}$, defined in (4.2), (4.3) and (4.4). Using (6.6.13) and (8.4.1) we get, for n in \mathbb{Z}^2 ,

$$(8.4.4) \quad \begin{aligned} \overline{A}_{\tilde{t}}(n) &= (-1)^{n_2}(1 + (4n_2)t) \cdot s_{D,0}((0, 3), (2n_1, 4n_2)), \\ \overline{B}_{\tilde{t}}(n) &= (1 + (4n_2)p)s_{0,E}((4n_1, 3n_2), (0, 4)), \\ \overline{C}(n) &= (-1)^{n_2^2}(1 + (4n_1^2 + (4+4)n_1n_2 + 2n_2^2)p) \cdot s_{0,0}((4n_1, 3n_2), (2n_1, 4n_2)), \\ \overline{D}_{\tilde{t}}(n) &= -(1 + (4n_1^2 + 3n_1n_2 + 2n_2^2 + 3n_2 + 2)p) \cdot s_{D,E}((4n_1, 3 + 3n_2), (2n_1, 4 + 4n_2)), \\ \overline{\kappa}(n) &= -(1 + (4n_1^2 + 3n_1n_2 + 2n_2^2 + 2n_2 + 2)p) \cdot s_{D,E}((n_1, 3 + 2n_2), (3n_1, 4 + n_2)), \end{aligned}$$

hence, using the bijection (8.3.1),

$$(8.4.5) \quad \overline{\kappa_1} = z_1, \quad \overline{\kappa_2} = 3 + 2z_2, \quad \overline{\kappa_3} = 4z_1^2 + 3z_1z_2 + 2z_2^2 + 2z_2 + 2.$$

8.5 The rational points with a specific image mod 5.

By 8.4.4 the image in $T(\mathbb{F}_p)$ of a point $\pm \overline{D}_{\tilde{t}}(n)$ for $n \in \mathbb{Z}^2$ is always of the form $\pm s_{D,E}(0, 0)$, hence, looking at (8.1.3) we see that there is no point $T(\mathbb{Z})$ with reduction $\widetilde{j}_{b,0}(\overline{\alpha}) \in T(\mathbb{F}_p)$. Hence $C(\mathbb{Z})_{\overline{\alpha}} = U_1(\mathbb{Z})_{\overline{\alpha}}$.

Let $f_1, f_2 \in \mathcal{O}(\widetilde{T}_t^p)^{\wedge p}$ be generators of the kernel of $\widetilde{j}_{b-1}^*: \mathcal{O}(\widetilde{T}_t^p)^{\wedge p} \rightarrow \mathcal{O}(\widetilde{U}_u^p)^{\wedge p}$ as in Section 4. The bijection (8.3.1) gives an isomorphism $\mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p) = \mathbb{F}_p[\lambda_1, \lambda_2, \tau]$ and since the images $\overline{f_1}, \overline{f_2}$ of f_1, f_2 in $\mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p)$ are generators of the kernel of $\widetilde{j}_{b,1}^*: \mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p)^{\wedge p} \rightarrow \mathbb{F}_p \otimes \mathcal{O}(\widetilde{U}_u^p)^{\wedge p}$ we can suppose that

$$\overline{f_1} = \lambda_2, \quad \overline{f_2} = \tau - 1.$$

By (8.4.5) we have

$$\kappa^* \overline{f_1} = \overline{\kappa_2} = 3 + 2z_2, \quad \kappa^* \overline{f_2} = \overline{\kappa_3} - 1 = 4z_1^2 + 3z_1z_2 + 2z_2^2 + 2z_2 + 1.$$

Let A be $\mathbb{Z}_p\langle z_1, z_2 \rangle / (\kappa^* f_1, \kappa^* f_2)$. Then the ring

$$(8.5.1) \quad \overline{A} := A/pA = \mathbb{F}_p[z_1, z_2] / (\kappa^* \overline{f_1}, \kappa^* \overline{f_2}) = \mathbb{F}_p[z_1, z_2] / (z_2 - 1, 4z_1^2 + 3z_1)$$

has dimension 2 over \mathbb{F}_p , hence by Theorem 4.12 $U(\mathbb{Z})_{\overline{\alpha}}$ contains at most 2 points. Since both

$$\alpha \quad \text{and} \quad (12/7, 20/7) \in V_1(\mathbb{Z}[1/7])$$

reduce to $\overline{\alpha}$ we deduce that $C(\mathbb{Z})_{\overline{\alpha}} = U_1(\mathbb{Z})_{\overline{\alpha}}$ is made of the these two points.

8.6 Determination of all rational points

Denoting $(3, -1) \in V_1(\mathbb{F}_p) \subset C(\mathbb{F}_p)$ as ε we have

$$C(\mathbb{F}_p) = \{\overline{\infty}, \overline{\infty_-}, \overline{\alpha}, \iota(\overline{\alpha}), \eta(\overline{\alpha}), (\iota \circ \eta)(\overline{\alpha}), \overline{\gamma}, \iota(\overline{\gamma}), \eta(\overline{\gamma}), (\iota \circ \eta)(\overline{\gamma}), \varepsilon, \iota(\varepsilon)\}.$$

Using that for any point Q in $C(\mathbb{F}_p)$ the condition $T(\mathbb{Z})_{\widetilde{j}_{b,i}(Q)} = \emptyset$ implies $U_i(\mathbb{Z})_Q = \emptyset$ we get

$$U_0(\mathbb{Z})_{\overline{\infty}} = U_0(\mathbb{Z})_{\overline{\infty_-}} = U_1(\mathbb{Z})_{\varepsilon} = U_1(\mathbb{Z})_{\iota(\varepsilon)} = U_1(\mathbb{Z})_{\overline{\gamma}} = U_1(\mathbb{Z})_{\eta(\overline{\gamma})} = U_1(\mathbb{Z})_{\iota\eta(\overline{\gamma})} = \emptyset.$$

Applying our method to $\overline{\infty}$ we discover that $U_1(\mathbb{Z})_{\overline{\infty}}$ contains at most 2 points and the same holds for $U_1(\mathbb{Z})_{\overline{\infty_-}}$. Moreover the action of $\langle \eta, \iota \rangle$ on $C(\mathbb{Z})$ tells that $U_1(\mathbb{Z})_{\iota(\overline{\alpha})}$, $U_1(\mathbb{Z})_{\eta(\overline{\alpha})}$ and $U_1(\mathbb{Z})_{\eta\iota(\overline{\alpha})}$ are sets containing exactly 2 elements. Hence

$$U_1(\mathbb{Z}) = U_1(\mathbb{Z})_{\overline{\alpha}} \cup U_1(\mathbb{Z})_{\iota(\overline{\alpha})} \cup U_1(\mathbb{Z})_{\eta(\overline{\alpha})} \cup U_1(\mathbb{Z})_{\eta\iota(\overline{\alpha})} \cup U_1(\mathbb{Z})_{\overline{\infty_-}} \cup U_1(\mathbb{Z})_{\overline{\infty}}$$

contains at most 12 elements. Looking at the orbits of the action of $\langle \eta, \iota \rangle$ on $U_1(\mathbb{Z})$ we see that $\#U_1(\mathbb{Z}) \equiv 2 \pmod{4}$, hence $\#U_1(\mathbb{Z}) \leq 10$. Since $U_1(\mathbb{Z})$ contains ∞, ∞_- and all the images by $\langle \eta, \iota \rangle$ of $U_1(\mathbb{Z})_{\overline{\alpha}}$ we conclude that $\#U_1(\mathbb{Z}) = 10$.

Applying our method to the point $\overline{\gamma}$ we see that $U_0(\mathbb{Z})_{\overline{\gamma}}$ contains at most two points, one of them being γ . Moreover solving the equations $\kappa^* \overline{f_i} = 0$ we see that if there is another point γ' in $U_0(\mathbb{Z})_{\overline{\gamma}}$ then there exist $n_1, n_2 \in \mathbb{Z}$ such that

$$j_b(\gamma') = 39G_1 + 17G_2 + 5n_1 \widetilde{G}_1 + 5n_2 \widetilde{G}_2.$$

Confronting this information with the image of the map $j_b: C(\mathbb{F}_7) \rightarrow J(\mathbb{F}_7)$ we derive a contradiction, hence $U_0(\mathbb{Z})_{\overline{\gamma}} = \{\gamma\}$. Applying our method to ε we see that $U_0(\mathbb{Z})_{\varepsilon}$ contains at most 2 points corresponding to two different solutions to the equations $\kappa^* \overline{f_i} = 0$. We can see that one of the two solutions does not lift to a point in $U_0(\mathbb{Z})_{\varepsilon}$ in the same way we excluded the existence of $\gamma' \in U_0(\mathbb{Z})_{\overline{\gamma}}$. Hence $U_0(\mathbb{Z})_{\varepsilon}$ has cardinality at most 1. Using that for every $Q \in C(\mathbb{F}_p)$ and every automorphism ω of C we have $\#U_0(\mathbb{Z})_Q = \#U_0(\mathbb{Z})_{\omega(Q)}$, we deduce that

$$U_0(\mathbb{Z}) = U_0(\mathbb{Z})_{\overline{\gamma}} \cup U_0(\mathbb{Z})_{\iota(\overline{\gamma})} \cup U_0(\mathbb{Z})_{\eta(\overline{\gamma})} \cup U_0(\mathbb{Z})_{\eta\iota(\overline{\gamma})} \cup U_0(\mathbb{Z})_{\varepsilon} \cup U_0(\mathbb{Z})_{\iota(\varepsilon)}$$

contains at most 6 points. Looking at the orbits of the action of $\langle \eta, \iota \rangle$ on $U_0(\mathbb{Z})$ we see that $\#U_0(\mathbb{Z}) \equiv 0 \pmod{4}$, hence $\#U_0(\mathbb{Z}) \leq 4$, and since $U_0(\mathbb{Z})$ contains the orbit of γ we conclude that $\#U_0(\mathbb{Z}) = 4$. Finally

$$\#C(\mathbb{Z}) = \#U_0(\mathbb{Z}) + \#U_1(\mathbb{Z}) = 4 + 10 = 14.$$

Author contributions This project started with an idea of Edixhoven in December 2017. From then on Edixhoven and Lido worked together on the project. Section 8 is due entirely to Lido.

Acknowledgements We thank Steffen Müller, Netan Dogra, Jennifer Balakrishnan, Kamal Khuri-Makdisi and Jan Vonk for discussions and correspondence we had with them, and Michael Stoll for suggesting the title of this article.

References

- [1] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*. Addison–Wesley Publishing Co., Reading, Mass.–London–Don Mills, Ont. 1969
- [2] J. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*. Ann. of Math. (2) 189 (2019), no. 3, 885–944.

- [3] D. Bertrand, B. Edixhoven, *Pink's conjecture on unlikely intersections and families of semi-abelian varieties.*
<https://arxiv.org/abs/1904.01788>
- [4] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 21. Springer-Verlag, Berlin, 1990.
- [5] T. Honda, *On the theory of commutative formal groups*. Journal of the Mathematical Society of Japan Vol. 22 No. 2 (1970).
<https://projecteuclid.org/euclid.jmsj/1259942752>
- [6] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*. Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985.
- [7] Q. Liu, *Algebraic geometry and arithmetic curves*. Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002.
- [8] L. Moret-Bailly, *Métriques permises*. Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). Astérisque No. 127 (1985), 29–87.
http://www.numdam.org/article/AST_1985__127__29_0.pdf
- [9] L. Moret-Bailly, *Pinceaux de variétés abéliennes*. Astérisque No. 129 (1985).
http://www.numdam.org/item/AST_1985__129__1_0/
- [10] M. Raynaud, *Spécialisation du foncteur de Picard*. Inst. Hautes Études Sci. Publ. Math. No. 38 1970, 27–76.
http://www.numdam.org/article/PMIHES_1970__38__27_0.pdf
- [11] *Groupes de monodromie en géométrie algébrique. I*. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D.S. Rim. Lecture Notes in Mathematics, Vol 288. Springer-Verlag, Berlin–New York, 1972.