

# $p$ -adic heights on Jacobians of hyperelliptic curves II

Jennifer Balakrishnan

University of Oxford

PIMS Summer School  
on Explicit Methods for Abelian Varieties  
University of Calgary  
June 17, 2016

# Coleman-Gross $p$ -adic heights

We've seen the following:  $p$ -adic heights on elliptic curves over number fields beyond  $\mathbf{Q}$  require a choice of idele class character.

However, going from elliptic curves to Jacobians of higher genus curves requires an additional choice: in particular, if our  $p$ -adic height is to be symmetric, we must choose a certain direct sum decomposition of

$$H_{dR}^1(X) = H^0(X, \Omega^1) \oplus W,$$

i.e., a choice of  $W$  such that  $W$  is isotropic with respect to the cup product pairing.

Since we have chosen  $p$  to be an ordinary prime, there is a canonical choice of  $W$ : the unit root subspace for the action of Frobenius.

# Coleman-Gross $p$ -adic height pairing



Then the Coleman-Gross  $p$ -adic height pairing is a symmetric bilinear pairing

$$h : \text{Div}^0(X) \times \text{Div}^0(X) \rightarrow \mathbf{Q}_p, \quad \text{where}$$

- ▶  $h$  can be decomposed into a sum of local height pairings  $h = \sum_v h_v$  over all finite places  $v$  of  $\mathbf{Q}$ .
- ▶  $h_v(D, E)$  is defined for  $D, E \in \text{Div}^0(X \times \mathbf{Q}_v)$  with disjoint support.
- ▶ We have  $h(D, \text{div}(\beta)) = 0$  for  $\beta \in k(X)^\times$ , so  $h$  is well-defined on  $J \times J$ .
- ▶ The local pairings  $h_v$  can be extended (non-uniquely) such that  $h(D) := h(D, D) = \sum_v h_v(D, D)$  for all  $D \in \text{Div}^0(X)$ .
- ▶ We fix a certain extension and write  $h_v(D) := h_v(D, D)$ .

We consider the global height pairing  $h$  as a sum of (finitely many) local height pairings  $h = \sum h_v$ ; Coleman-Gross achieve a description of these local heights solely in terms of the curve.

Construction of  $h_v$  depends on whether  $v = p$  or  $v \neq p$ .

- ▶  $v \neq p$ : arithmetic intersection theory, as in Müller's lectures
- ▶  $v = p$ : logarithms, Coleman integration of normalized differentials of the third kind ( $p$ -adic Green's functions); in particular,

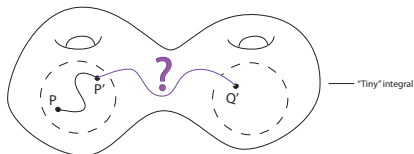
$$h_p(D, E) = \int_E \omega_D$$

for  $\omega_D$  a certain differential of the third kind with  $\text{Res}(\omega_D) = D$ . This is a Coleman integral.

# Coleman integration

# $p$ -adic line integrals

A Coleman integral is a  $p$ -adic *line integral*.



$p$ -adic line integration is difficult – how do we construct the correct path?

- ▶ We can construct local (“tiny”) integrals easily, but extending them to the entire space is challenging.
- ▶ Coleman’s solution: *analytic continuation along Frobenius*, giving rise to a theory of  $p$ -adic line integration satisfying the usual nice properties

# Notation and setup

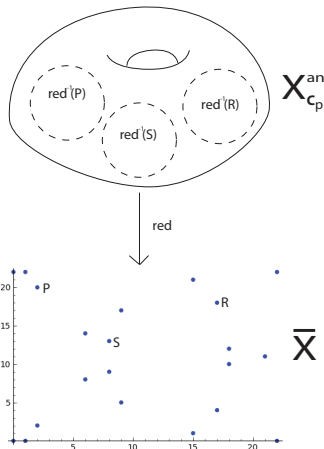
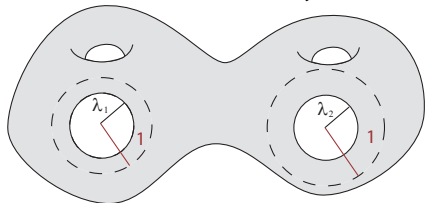


- ▶  $X$ : genus  $g$  hyperelliptic curve (of the form  $y^2 = f(x)$ ,  $f$  monic of degree  $2g + 1$ ) over  $K = \mathbf{Q}_p$
- ▶  $\bar{X}$ : special fibre of  $X$
- ▶  $X_{\mathbf{C}_p}^{\text{an}}$ : generic fibre of  $X$  (as a rigid analytic space)



# Notation and setup, in pictures

- ▶ There is a natural reduction map from  $X_{\mathbb{C}_p}^{\text{an}}$  to  $\bar{X}$ ; the inverse image of any point of  $\bar{X}$  is a subspace of  $X_{\mathbb{C}_p}^{\text{an}}$  isomorphic to an open unit disk. We call such a disk a *residue disk* of  $X$ .
- ▶ A *wide open subspace* of  $X_{\mathbb{C}_p}^{\text{an}}$  is the complement in  $X_{\mathbb{C}_p}^{\text{an}}$  of the union of a finite collection of disjoint closed disks of radius  $\lambda_i < 1$ :



# Warm-up: Computing “tiny” integrals



We refer to any Coleman integral of the form  $\int_P^Q \omega$  in which  $P, Q$  lie in the same residue disk (so  $P \equiv Q \pmod{p}$ ) as a *tiny integral*. To compute such an integral:

- ▶ Construct a linear interpolation from  $P$  to  $Q$ . For instance, in a non-Weierstrass residue disk, we may take

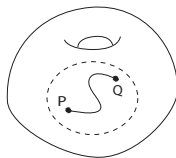
$$x(t) = (1 - t)x(P) + tx(Q)$$

$$y(t) = \sqrt{f(x(t))},$$

where  $y(t)$  is expanded as a formal power series in  $t$ .

- ▶ Formally integrate the power series in  $t$ :

$$\int_P^Q \omega = \int_0^1 \omega(x(t), y(t)) dt.$$



Coleman formulated an integration theory, allowing us to define  $\int_P^Q \omega$  whenever  $\omega$  is a meromorphic 1-form on  $X$ , and  $P, Q \in X(\mathbf{Q}_p)$  are points where  $\omega$  is holomorphic.

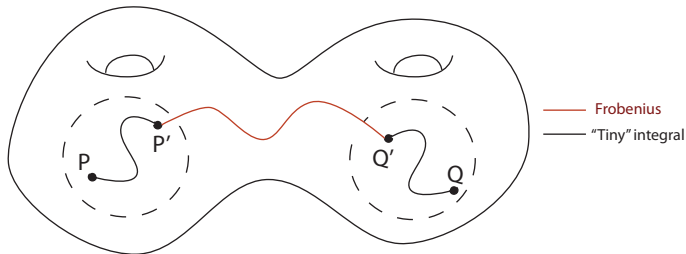
Properties of the Coleman integral include:

## Theorem (Coleman)

- ▶ *Linearity:*  $\int_P^Q (\alpha\omega_1 + \beta\omega_2) = \alpha \int_P^Q \omega_1 + \beta \int_P^Q \omega_2$ .
- ▶ *Additivity:*  $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$ .
- ▶ *Change of variables:* if  $X'$  is another such curve, and  $f : U \rightarrow U'$  is a rigid analytic map between wide opens, then
$$\int_P^Q f^* \omega = \int_{f(P)}^{f(Q)} \omega.$$
- ▶ *Fundamental theorem of calculus:*  $\int_P^Q df = f(Q) - f(P)$ .

# Coleman's construction

How do we integrate if  $P, Q$  aren't in the same residue disk?  
Coleman's key idea: use Frobenius to move between different residue disks (Dwork's "analytic continuation along Frobenius")



So we need to calculate the action of Frobenius on differentials.

# Frobenius, MW-cohomology



- ▶  $X'$ : affine curve ( $X - \{\text{Weierstrass points of } X\}$ )
- ▶  $A$ : coordinate ring of  $X'$

To discuss the differentials we will be integrating, we recall:  
The *Monsky-Washnitzer (MW) weak completion* of  $A$  is the ring  $A^\dagger$  consisting of infinite sums of the form

$$\left\{ \sum_{i=-\infty}^{\infty} \frac{B_i(x)}{y^i}, B_i(x) \in K[x], \deg B_i \leq 2g \right\},$$

further subject to the condition that  $v_p(B_i(x))$  grows faster than a linear function of  $i$  as  $i \rightarrow \pm\infty$ . We make a ring out of these using the relation  $y^2 = f(x)$ .

These functions are holomorphic on wide opens, so we will integrate 1-forms

$$\omega = g(x, y) \frac{dx}{2y}, \quad g(x, y) \in A^\dagger.$$

# Using the basis differentials



Any odd differential  $\omega = h(x, y) \frac{dx}{2y}$ ,  $h(x, y) \in A^\dagger$  can be written as

$$\omega = df_\omega + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1},$$

where  $f_\omega \in A^\dagger$ ,  $c_i \in \mathbf{Q}_p$  and

$$\omega_i = \frac{x^i dx}{2y} \quad (i = 0, \dots, 2g - 1).$$

The set  $\{\omega_i\}_{i=0}^{2g-1}$  forms a basis of the odd part of the de Rham cohomology of  $A^\dagger$ .

By linearity and the fundamental theorem of calculus, we reduce the integration of  $\omega$  to the integration of the  $\omega_i$ .

Let  $\phi$  denote a lift of  $p$ -power Frobenius:

- ▶ On a hyperelliptic curve  $y^2 = f(x)$ ,

$$\phi : (x, y) \mapsto (x^p, \sqrt{f(x^p)}).$$

- ▶ A *Teichmüller point* of  $X$  is a point  $P$  fixed by Frobenius:  
 $\phi(P) = P$ .

One way to compute Coleman integrals  $\int_P^Q \omega_i$ :

- ▶ Find the Teichmüller points  $P', Q'$  in the residue disks of  $P, Q$ .

- ▶ Use Frobenius to compute  $\int_{P'}^{Q'} \omega_i$ .

- ▶ Use additivity in endpoints to recover the integral:

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



# The Frobenius step (Kedlaya's algorithm)



We have a  $p$ -power lift of Frobenius  $\phi$  on  $A^\dagger$ :

$$\phi(x) = x^p,$$

$$\phi(y) = y^p \left( 1 + \frac{f(x^p) - f(x)^p}{f(x)^p} \right)^{1/2} = y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}$$

Now we use it on  $H_{MW}^1(X')^-$ ; let  $\omega_i = \frac{x^i dx}{2y}$ .

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

where  $f_i \in A^\dagger$ .

# Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))



- ▶ Use Kedlaya's algorithm to calculate the action of Frobenius  $\phi$  on each basis differential, letting

$$\phi^* \omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij} \omega_j.$$

- ▶ Compute  $\int_{P'}^{Q'} \omega_j$  by solving a linear system

$$\int_{P'}^{Q'} \omega_i = \int_{\phi(P')}^{\phi(Q')} \omega_i = \int_{P'}^{Q'} \phi^* \omega_i = \int_{P'}^{Q'} \left( df_i + \sum_{j=0}^{2g-1} M_{ij} \omega_j \right)$$

$$\int_{P'}^{Q'} \omega_i = f_i(Q') - f_i(P') + \sum_{j=0}^{2g-1} M_{ij} \int_{P'}^{Q'} \omega_j.$$

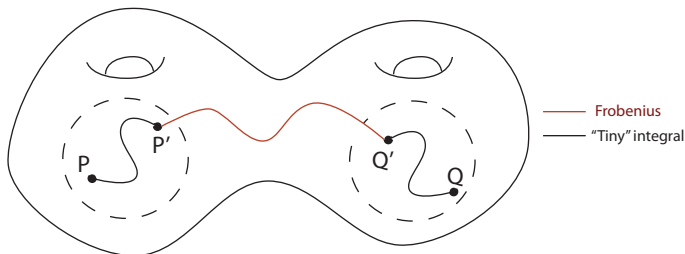
- ▶ The eigenvalues of  $M$  have  $\mathbf{C}$ -norm  $p^{1/2} \neq 1$ , so  $M - I$  is invertible; solve the system to obtain the integrals  $\int_{P'}^{Q'} \omega_i$ .

# Integrals via Teichmüller, continued



- ▶ The linear system gives us the integral between different residue disks.
- ▶ Then putting it all together, we have

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



# Iterated Coleman integrals



There is a generalization to  $n$ -fold iterated line integrals:

$$\int_P^Q \omega_n \cdots \omega_1 = \int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \cdots f_1(t_1) dt_n \cdots dt_1$$

and an algorithm using Frobenius (B., 2013) to compute iterated Coleman integrals.

These iterated Coleman integrals play a key role in Kim's nonabelian Chabauty program.

We focus on the case  $n = 2$ , and we use the convention

$$\int_P^Q \omega_i \omega_j := \int_P^Q \omega_i(R) \int_P^R \omega_j$$

“Tiny” double integration (points  $P, Q$  in the same non-Weierstrass residue disk)

- ▶ Compute local coordinate  $(x(t), y(t))$  at  $P$ .
- ▶ Let  $R = (a + x(Q), \sqrt{f(a + x(Q))})$ .
- ▶ Write

$$\begin{aligned}\int_P^Q \omega_i \omega_j &= \int_P^Q \omega_i(R) \int_P^R \omega_j \\ &= \int_0^{x(Q)-x(P)} \left( \int_0^a \frac{x(t)^j dx(t)}{2y(t)} \right) \frac{x(R(a))^i dx(R(a))}{2y(R(a)) da}.\end{aligned}$$

# Moving between different disks



As before, we can link integrals between non-Weierstrass points via Frobenius.

To compute the integrals  $\int_P^Q \omega_i \omega_k$  when  $P, Q$  are in different disks:

- ▶ Compute Teichmüller points  $P', Q'$  in the disks of  $P, Q$ .
- ▶ Use Frobenius to calculate  $\int_{P'}^{Q'} \omega_i \omega_k$ .
- ▶ Recover the double integral:

$$\int_P^Q \omega_i \omega_k = \int_{P'}^{Q'} \omega_i \omega_k - \int_{P'}^P \omega_i \omega_k - \left( \int_P^Q \omega_i \right) \left( \int_{P'}^P \omega_k \right) - \left( \int_Q^{Q'} \omega_i \right) \left( \int_{P'}^{Q'} \omega_k \right) + \int_{Q'}^Q \omega_i \omega_k.$$

Suppose  $P, Q$  are Teichmüller. We have

$$\int_P^Q \omega_i \omega_k = \int_{\Phi(P)}^{\Phi(Q)} \omega_i \omega_k$$

$$\int_P^Q \omega_i \omega_k = \int_P^Q (\Phi^* \omega_i)(\Phi^* \omega_k)$$

$$\int_P^Q \omega_i \omega_k = \int_P^Q \left( df_i + \sum_{j=0}^{2g-1} M_{ij} \omega_j \right) \left( df_k + \sum_{j=0}^{2g-1} M_{kj} \omega_j \right)$$

# The linear system

For all  $0 \leq i, k \leq 2g - 1$ , define the constants  $c_{ik}$ :

$$\begin{aligned} c_{ik} = & \int_P^Q df_i(R)(f_k(R)) - f_k(P)(f_i(Q) - f_i(P)) \\ & + \int_P^Q \sum_{j=0}^{2g-1} M_{ij} \omega_j(R)(f_k(R) - f_k(P)) \\ & + f_i(Q) \int_P^Q \sum_{j=0}^{2g-1} M_{kj} \omega_j - \int_P^Q f_i(R) \left( \sum_{j=0}^{2g-1} M_{kj} \omega_j(R) \right). \end{aligned}$$

Then

$$\begin{pmatrix} \int_P^Q \omega_0 \omega_0 \\ \int_P^Q \omega_0 \omega_1 \\ \vdots \\ \int_P^Q \omega_{2g-1} \omega_{2g-1} \end{pmatrix} = (I_{4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} c_{00} \\ \vdots \\ c_{2g-1, 2g-1} \end{pmatrix}.$$



# Quadratic Chabauty

# Kim's nonabelian Chabauty program



The aim is to generalize the Chabauty-Coleman method, which says that for a curve  $X/\mathbf{Q}$  with rank  $J(\mathbf{Q}) < g$ , we have

$$X(\mathbf{Q}_p)_1 := \left\{ z \in X(\mathbf{Q}_p) : \int_b^z \omega = 0 \right\}$$

for some  $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega_X^1)$ . Kim's program is to give further *iterated*  $p$ -adic integrals vanishing on rational or integral points on curves by studying *Selmer varieties*, with the hope of *precisely* cutting out rational or integral points.

Explicit examples have been worked out in the case of

- ▶  $\mathbf{P}^1 \setminus \{0, 1, \infty\}$  (Dan-Cohen–Wewers, Dan-Cohen)
- ▶ Elliptic curve  $E \setminus \{O\}$ ,  $\text{rk } E(\mathbf{Q})$  is 0, 1 (Kim, B.–Kedlaya–Kim, B.–Besser, B.–Dan-Cohen–Kim–Wewers, B.–Dogra)
- ▶ Genus  $g$  hyperelliptic curve  $C \setminus \{\infty\}$  or  $C$ , where we have  $\text{rank } J = g$  (B.–Besser–Müller, B.–Dogra)

Let  $X/\mathbf{Q}$  be a genus  $g$  hyperelliptic curve. Given a global  $p$ -adic height pairing  $h$ , we want to study it on integral points:

$$\underbrace{h}_{\text{quadratic form, rewrite as a } p\text{-adic analytic function using Coleman integrals}} = \underbrace{h_p}_{\text{\(p\)-adic analytic function via double Coleman integral}} + \underbrace{\sum_{v \neq p} h_v}_{\text{takes on finite number of values on integral points}}$$

Given a global  $p$ -adic height pairing  $h$ , we want to study it on integral points:

$$\underbrace{h}_{\text{quadratic form, rewrite as a } p\text{-adic analytic function using Coleman integrals}} = \underbrace{h_p}_{\text{\textit{p}-adic analytic function via double Coleman integral}} + \underbrace{\sum_{v \neq p} h_v}_{\text{takes on finite number of values on integral points}}$$

# Local height at $p$



By Coleman-Gross, the local height  $h_p$  is given in terms of Coleman integration: for  $D, E \in \text{Div}^0(X)$  of disjoint support,

$$h_p(D, E) = \int_E \omega_D.$$

## Theorem (B.-Besser-Müller)

If  $P \in X(\mathbf{Q}_p)$ , then  $h_p(P - \infty) := h_p(P - \infty, P - \infty)$  is equal to a double Coleman integral

$$\tau(P) := h_p(P - \infty) = \sum_{i=0}^{g-1} \int_{\infty}^P \omega_i \bar{\omega}_i,$$

where  $\{\bar{\omega}_0, \dots, \bar{\omega}_{g-1}\}$  forms a dual basis to  $\{\omega_0, \dots, \omega_{g-1}\}$  with respect to the cup product pairing on  $H_{dR}^1(X/\mathbf{Q}_p)$ .

# Local heights away from $p$



If  $q \neq p$  then  $h_q$  is defined in terms of arithmetic intersection theory on a regular model of  $X$  over  $\text{Spec}(\mathbf{Z})$ .

There is an explicitly computable finite set  $T \subset \mathbf{Q}_p$  such that

$$-\sum_{q \neq p} h_q(P - \infty) \in T$$

for integral points  $P \in X(\mathbf{Q})$ .

# Strategy of Quadratic Chabauty



Consider the  $\mathbf{Q}_p$ -valued functionals  $f_i = \int_O \omega_i$  for  $0 \leq i \leq g-1$  on  $J(\mathbf{Q})$ .

Idea when  $\text{rk}(J(\mathbf{Q})) = r = g$ :

- ▶ Suppose the  $f_i$  are linearly independent functionals on  $J(\mathbf{Q})$ .
- ▶ Then  $\{f_i f_j\}_{i \leq j \leq g-1}$  is a natural basis of the space of  $\mathbf{Q}_p$ -valued quadratic forms on  $J(\mathbf{Q})$ .
- ▶ The  $p$ -adic height  $h$  is also a quadratic form, so there must exist  $\alpha_{ij} \in \mathbf{Q}_p$  such that

$$h = \sum_{i \leq j \leq g-1} \alpha_{ij} f_i f_j$$

- ▶ Linear algebra gives us the global  $p$ -adic height in terms of products of Coleman integrals.

# Quadratic Chabauty



We use these double and single Coleman integrals to rewrite the global  $p$ -adic height pairing  $h$  and to study it on integral points:

$$\underbrace{h}_{\text{quadratic form, rewrite as a } p\text{-adic analytic function using Coleman integrals}} = \underbrace{h_p}_{\text{\(p\)-adic analytic function via double Coleman integral}} + \underbrace{\sum_{v \neq p} h_v}_{\text{takes on finite number of values on integral points}}$$

$$\underbrace{h_p}_{\text{\(p\)-adic analytic function via double Coleman integral}} - \underbrace{h}_{\text{quadratic form, rewrite as a } p\text{-adic analytic function using Coleman integrals}} = - \underbrace{\sum_{v \neq p} h_v}_{\text{takes on finite number of values on integral points}}$$



## Theorem (B.-Besser-Müller)

If  $r = g \geq 1$  and the  $f_i$  are independent, then there is an explicitly computable finite set  $T \subset \mathbf{Q}_p$  and explicitly computable constants  $\alpha_{ij} \in \mathbf{Q}_p$  such that

$$\rho(P) := \tau(P) - \sum_{0 \leq i < j \leq g-1} \alpha_{ij} f_i f_j(P)$$

takes values in  $T$  on integral points.

Main strategy of quadratic Chabauty:

$p$ -adic heights  $\rightsquigarrow$   $p$ -adic integrals  $\rightsquigarrow$   $p$ -adic power series (set equal to a finite set of constants)

Then solve and produce a finite set of points containing integral points!

# Rational points for bielliptic genus 2 curves



Let  $K$  be  $\mathbf{Q}$  or a quadratic imaginary number field,  $X/K$  be given by

$$y^2 = x^6 + ax^4 + bx^2 + c$$

and let

$$E_1 : y^2 = x^3 + ax^2 + bx + c \qquad E_2 : y^2 = x^3 + bx^2 + acx + c^2,$$

with maps

$$f_1 : \begin{array}{ccc} X & \longrightarrow & E_1 \\ (x, y) & \mapsto & (x^2, y) \end{array} \qquad f_2 : \begin{array}{ccc} X & \longrightarrow & E_2 \\ (x, y) & \mapsto & (cx^{-2}, cyx^{-3}). \end{array}$$

## Theorem (B.-Dogra '16)

*Let  $X/K$  be as above and suppose  $E_1$  and  $E_2$  each have rank 1. We can carry out quadratic Chabauty to recover a finite set of  $p$ -adic points containing  $X(K)$ .*

# Details (all the $p$ -adic heights)



## Theorem (B.-Dogra '16)

Then  $X/K$  be a genus 2 bielliptic curve as before. Then  $X(K)$  is contained in the finite set of  $z$  in  $X(K_p)$  satisfying

$$\begin{aligned} \rho(z) = & 2h_{E_{2,p}}(f_2(z)) - h_{E_{1,p}}(f_1(z) + (0, \sqrt{c})) - h_{E_{1,p}}(f_1(z) + (0, -\sqrt{c})) \\ & - 2\alpha_2 \log_{E_2}(f_2(z))^2 + 2\alpha_1 (\log_{E_1}(f_1(z)))^2 + \log_{E_1}((0, \sqrt{c}))^2 \\ & \in \Omega, \end{aligned}$$

where  $\Omega$  is the finite set of values

$$\left\{ \sum_{v \nmid p} (h_{E_{1,v}}(f_1(z) + (0, \sqrt{c})) + h_{E_{1,v}}(f_1(z) + (0, -\sqrt{c})) - 2h_{E_{2,v}}(f_2(z))) \right\},$$

for  $(z_v)$  in  $\prod_{v \nmid p} X(K_v)$ , and where  $\alpha_i = \frac{h_{E_i}(P_i)}{[K:\mathbf{Q}] \log_{E_i}(P_i)^2}$ .

## Example : Computing $X_0(37)(\mathbf{Q}(i))$



Consider

$$X_0(37) : y^2 = -x^6 - 9x^4 - 11x^2 + 37.$$

We have  $\text{rk}(J_0(37)(\mathbf{Q}(i))) = 2$ .

Change models and use

$$X : y^2 = x^6 - 9x^4 + 11x^2 + 37,$$

which is isomorphic to  $X_0(37)$  over  $K = \mathbf{Q}(i)$ ; we have  $\text{rk}(J(\mathbf{Q})) = \text{rk}(J(\mathbf{Q}(i))) = 2$ .

Define

$$E_1 : y^2 = x^3 - 16x + 16 \qquad E_2 : y^2 = x^3 - x^2 - 373x + 2813$$

and maps from  $X$

$$f_1 : X \longrightarrow E_1 \qquad f_2 : X \longrightarrow E_2 \\ (x, y) \mapsto (x^2 - 3, y) \qquad (x, y) \mapsto (37x^{-2} + 4, 37yx^{-3}).$$

Take  $P_1$  and  $P_2$  to be points of infinite order in  $E_1(\mathbf{Q})$  and  $E_2(\mathbf{Q})$ .

We compute

$$\begin{aligned}\rho(z) &= 2h_{E_2,p}(f_2(z)) - h_{E_1,p}(f_1(z) + (-3, \sqrt{37})) \\ &\quad - h_{E_1,p}(f_1(z) + (-3, -\sqrt{37})) \\ &\quad - 2\alpha_2 h_{E_2}(f_2(z)) + 2\alpha_1(h_{E_1}(f_1(z))) + \log_{E_1}((-3, \sqrt{37}))^2\end{aligned}$$

and find that points  $z \in X(\mathbf{Q}(i))$  satisfy

$$\rho(z) = \frac{4}{3} \log_p(37).$$

Taking  $p = 41, 73, 101$ , we use  $\rho$  to produce points in  $X(\mathbf{Q}_{41}), X(\mathbf{Q}_{73}), X(\mathbf{Q}_{101})$ .

# Recovered points in $X(\mathbf{Q}_{41})$



$X(\mathbf{F}_{41})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$(1, 9)$	$1 + 16 \cdot 41 + 23 \cdot 41^2 + 5 \cdot 41^3 + 23 \cdot 41^4 + O(41^5)$	$(2, 1)$
$(2, 1)$	$1 + 6 \cdot 41 + 23 \cdot 41^2 + 30 \cdot 41^3 + 14 \cdot 41^4 + O(41^5)$	
$(4, 18)$	$2 + O(41^5)$	
$(5, 12)$	$2 + 19 \cdot 41 + 36 \cdot 41^2 + 15 \cdot 41^3 + 26 \cdot 41^4 + O(41^5)$	
$(6, 1)$	$5 + 25 \cdot 41 + 26 \cdot 41^2 + 26 \cdot 41^3 + 31 \cdot 41^4 + O(41^5)$	
$(7, 15)$	$5 + 14 \cdot 41 + 12 \cdot 41^3 + 33 \cdot 41^4 + O(41^5)$	$(i, 4)$
$(9, 4)$	$6 + 18 \cdot 41^2 + 31 \cdot 41^3 + 6 \cdot 41^4 + O(41^5)$	
$(12, 5)$	$6 + 30 \cdot 41 + 35 \cdot 41^2 + 11 \cdot 41^3 + O(41^5)$	
$(13, 19)$	$9 + 9 \cdot 41 + 34 \cdot 41^2 + 22 \cdot 41^3 + 24 \cdot 41^4 + O(41^5)$	
$(16, 1)$	$9 + 39 \cdot 41 + 14 \cdot 41^2 + 6 \cdot 41^3 + 17 \cdot 41^4 + O(41^5)$	
$(17, 20)$	$13 + 10 \cdot 41 + 2 \cdot 41^2 + 15 \cdot 41^3 + 29 \cdot 41^4 + O(41^5)$	$\infty^+$
$(18, 20)$	$13 + 7 \cdot 41 + 8 \cdot 41^2 + 32 \cdot 41^3 + 14 \cdot 41^4 + O(41^5)$	
$(19, 3)$	$16 + 13 \cdot 41 + 6 \cdot 41^3 + 18 \cdot 41^4 + O(41^5)$	
$(20, 6)$	$16 + 12 \cdot 41 + 8 \cdot 41^2 + 9 \cdot 41^3 + 32 \cdot 41^4 + O(41^5)$	
$(\infty^+)$	$17 + 24 \cdot 41 + 37 \cdot 41^2 + 16 \cdot 41^3 + 28 \cdot 41^4 + O(41^5)$	
$(0, 18)$	$17 + 19 \cdot 41 + 20 \cdot 41^2 + 7 \cdot 41^3 + 7 \cdot 41^4 + O(41^5)$	
	$18 + 3 \cdot 41 + 7 \cdot 41^2 + 9 \cdot 41^3 + 38 \cdot 41^4 + O(41^5)$	
	$18 + 41 + 34 \cdot 41^2 + 3 \cdot 41^3 + 32 \cdot 41^4 + O(41^5)$	
	$20 + 7 \cdot 41 + 40 \cdot 41^2 + 22 \cdot 41^3 + 7 \cdot 41^4 + O(41^5)$	
	$20 + 23 \cdot 41 + 26 \cdot 41^2 + 17 \cdot 41^3 + 22 \cdot 41^4 + O(41^5)$	
	$\infty^+$	
	$32 \cdot 41 + 13 \cdot 41^2 + 16 \cdot 41^3 + 8 \cdot 41^4 + O(41^5)$	
	$9 \cdot 41 + 27 \cdot 41^2 + 24 \cdot 41^3 + 32 \cdot 41^4 + O(41^5)$	

# Recovered points in $X(\mathbf{Q}_{73})$



$X(\mathbf{F}_{73})$	recovered $x(z)$ in residue disk	$z \in X(K)$ (or $X(\mathbf{Q}(\sqrt{3}))$ )	
$(2, 1)$	$2 + 61 \cdot 73 + 50 \cdot 73^2 + 71 \cdot 73^3 + 56 \cdot 73^4 + O(73^5)$	$(2, 1)$	
$(5, 26)$	$2 + O(73^5)$		
$(7, 16)$	$5 + 63 \cdot 73 + 4 \cdot 73^2 + 42 \cdot 73^3 + 25 \cdot 73^4 + O(73^5)$		
$(9, 34)$	$5 + 39 \cdot 73 + 65 \cdot 73^2 + 33 \cdot 73^3 + 60 \cdot 73^4 + O(73^5)$		
$(10, 30)$	$7 + 62 \cdot 73 + 31 \cdot 73^2 + 33 \cdot 73^3 + 44 \cdot 73^4 + O(73^5)$		
$(18, 17)$	$7 + 29 \cdot 73 + 67 \cdot 73^2 + 69 \cdot 73^3 + 17 \cdot 73^4 + O(73^5)$		
$(19, 2)$	$10 + 53 \cdot 73 + 35 \cdot 73^2 + 21 \cdot 73^3 + 67 \cdot 73^4 + O(73^5)$		
$(20, 15)$	$10 + 39 \cdot 73 + 40 \cdot 73^2 + 17 \cdot 73^3 + 59 \cdot 73^4 + O(73^5)$		
$(21, 4)$	$21 + 17 \cdot 73 + 70 \cdot 73^2 + 42 \cdot 73^3 + 18 \cdot 73^4 + O(73^5)$		$(\sqrt{3}, 4)$
$(23, 31)$	$21 + 52 \cdot 73 + 67 \cdot 73^2 + 20 \cdot 73^3 + 27 \cdot 73^4 + O(73^5)$		
$(25, 25)$	$23 + 18 \cdot 73 + 59 \cdot 73^2 + 23 \cdot 73^3 + 2 \cdot 73^4 + O(73^5)$		
$(27, 4)$	$23 + 70 \cdot 73 + 53 \cdot 73^2 + 21 \cdot 73^3 + 50 \cdot 73^4 + O(73^5)$	$(i, 4)$	
$(29, 8)$	$27 + 62 \cdot 73 + 28 \cdot 73^2 + 56 \cdot 73^3 + 58 \cdot 73^4 + O(73^5)$		
$(30, 20)$	$27 + 24 \cdot 73 + 30 \cdot 73^2 + 20 \cdot 73^3 + 65 \cdot 73^4 + O(73^5)$		
$(36, 17)$	$29 + 70 \cdot 73 + 21 \cdot 73^2 + 56 \cdot 73^3 + 5 \cdot 73^4 + O(73^5)$		
$\infty^+$	$29 + 34 \cdot 73 + 42 \cdot 73^2 + 19 \cdot 73^3 + 54 \cdot 73^4 + O(73^5)$	$\infty^+$	
$(0, 16)$	$36 + 70 \cdot 73 + 19 \cdot 73^2 + 11 \cdot 73^3 + 54 \cdot 73^4 + O(73^5)$		
	$36 + 32 \cdot 73 + 23 \cdot 73^2 + 23 \cdot 73^3 + 28 \cdot 73^4 + O(73^5)$		
	$\infty^+$		
	$61 \cdot 73 + 63 \cdot 73^2 + 51 \cdot 73^3 + 16 \cdot 73^4 + O(73^5)$		
	$12 \cdot 73 + 9 \cdot 73^2 + 21 \cdot 73^3 + 56 \cdot 73^4 + O(73^5)$		

# Recovered points in $X(\mathbf{Q}_{101})$

$X(\mathbf{F}_{101})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$(2, 1)$	$2 + O(101^7)$	$(2, 1)$
$(8, 36)$	$2 + 38 \cdot 101 + 11 \cdot 101^2 + 99 \cdot 101^3 + 26 \cdot 101^4 + O(101^5)$	$(i, 4)$
$(10, 4)$	$8 + 90 \cdot 101 + 39 \cdot 101^2 + 80 \cdot 101^3 + 70 \cdot 101^4 + O(101^5)$	
$(12, 7)$	$8 + 40 \cdot 101 + 84 \cdot 101^2 + 74 \cdot 101^3 + 15 \cdot 101^4 + O(101^5)$	
$(14, 21)$	$10 + 5 \cdot 101 + 29 \cdot 101^2 + 66 \cdot 101^3 + 10 \cdot 101^4 + O(101^5)$	
$(15, 11)$	$10 + 49 \cdot 101 + 80 \cdot 101^2 + 74 \cdot 101^3 + 8 \cdot 101^4 + O(101^5)$	
$(17, 18)$	$12 + 12 \cdot 101 + 95 \cdot 101^2 + 55 \cdot 101^3 + 48 \cdot 101^4 + O(101^5)$	
$(18, 45)$	$12 + 36 \cdot 101 + 62 \cdot 101^2 + 97 \cdot 101^3 + 27 \cdot 101^4 + O(101^5)$	
$(20, 47)$	$14 + 62 \cdot 101 + 62 \cdot 101^2 + 41 \cdot 101^3 + 51 \cdot 101^4 + O(101^5)$	
$(22, 3)$	$14 + 80 \cdot 101 + 72 \cdot 101^2 + 32 \cdot 101^3 + 75 \cdot 101^4 + O(101^5)$	
$(24, 19)$	$17 + 65 \cdot 101 + 37 \cdot 101^2 + 80 \cdot 101^3 + 45 \cdot 101^4 + O(101^5)$	
$(27, 39)$	$17 + 50 \cdot 101 + 61 \cdot 101^2 + 89 \cdot 101^3 + 61 \cdot 101^4 + O(101^5)$	
$(28, 37)$	$22 + 59 \cdot 101 + 78 \cdot 101^2 + 43 \cdot 101^3 + 53 \cdot 101^4 + O(101^5)$	
	$22 + 96 \cdot 101 + 29 \cdot 101^2 + 43 \cdot 101^3 + 86 \cdot 101^4 + O(101^5)$	
	$28 + 30 \cdot 101 + 83 \cdot 101^2 + 5 \cdot 101^3 + 23 \cdot 101^4 + O(101^5)$	
	$28 + 37 \cdot 101 + 24 \cdot 101^2 + 78 \cdot 101^3 + 35 \cdot 101^4 + O(101^5)$	



# Recovered points in $X(\mathbf{Q}_{101})$ , continued



$X(\mathbf{F}_{101})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$(30, 46)$		
$(31, 23)$	$31 + 23 \cdot 101 + 11 \cdot 101^2 + 67 \cdot 101^3 + 39 \cdot 101^4 + O(101^5)$	
	$31 + 29 \cdot 101 + 68 \cdot 101^2 + 29 \cdot 101^3 + 24 \cdot 101^4 + O(101^5)$	
$(34, 45)$	$34 + 91 \cdot 101 + 46 \cdot 101^2 + 28 \cdot 101^3 + 34 \cdot 101^4 + O(101^5)$	
	$34 + 51 \cdot 101 + 73 \cdot 101^2 + 34 \cdot 101^3 + 14 \cdot 101^4 + O(101^5)$	
$(37, 22)$		
$(38, 28)$		
$(39, 46)$	$39 + 76 \cdot 101 + 86 \cdot 101^2 + 18 \cdot 101^3 + 64 \cdot 101^4 + O(101^5)$	
	$39 + 31 \cdot 101 + 43 \cdot 101^2 + 10 \cdot 101^3 + 48 \cdot 101^4 + O(101^5)$	
$(46, 6)$		
$(47, 32)$		
$(48, 27)$	$48 + 43 \cdot 101 + 100 \cdot 101^2 + 47 \cdot 101^3 + 19 \cdot 101^4 + O(101^5)$	
	$48 + 21 \cdot 101 + 38 \cdot 101^2 + 80 \cdot 101^3 + 95 \cdot 101^4 + O(101^5)$	
$(50, 5)$	$50 + 59 \cdot 101 + 19 \cdot 101^2 + 64 \cdot 101^3 + 36 \cdot 101^4 + O(101^5)$	
	$50 + 74 \cdot 101 + 69 \cdot 101^2 + 80 \cdot 101^3 + 21 \cdot 101^4 + O(101^5)$	
$\infty^+$	$\infty^+$	$\infty^+$
$(0, 21)$		

# Putting it together and computing $X_0(37)(\mathbf{Q}(i))$



Steffen Müller carried out the Mordell-Weil sieve on the sets of points found in  $X(\mathbf{Q}_{41})$ ,  $X(\mathbf{Q}_{73})$ , and  $X(\mathbf{Q}_{101})$ ; conclusion:

$$X(\mathbf{Q}(i)) = \{(\pm 2 : \pm 1 : 1), (\pm i : \pm 4 : 1), (1 : \pm 1 : 0)\},$$

or in other words,

$$X_0(37)(\mathbf{Q}(i)) = \{(\pm 2i : \pm 1 : 1), (\pm 1 : \pm 4 : 1), (i : \pm 1 : 0)\}.$$

Note: the computation of points in  $X(\mathbf{Q}_{73})$  recovered the points  $(\pm \sqrt{-3}, \pm 4) \in X_0(37)(\mathbf{Q}(\sqrt{-3}))$  as well!