COleman integration and its Uses in Number Theory, COUNT

Alex J. Best
King's College London
3/3/23

Coleman integration: Let X/K be a smooth projective and geometrically integral curve over a number field.

When $g = \mathrm{genus}(X) \geq 2$ we have $\#X(K) < \infty$ by **Faltings' theorem**.

Classic Chabauty


Bourbaki in Dieulefit

Let p be a prime of good reduction for X assume we have a $\mathbf{Q}_p$-linear assignment $\int_b^x : \Omega^1_X \otimes \mathbf{Q}_p \to \mathbf{Q}_p$ for which:

$$\mathrm{d} \circ \int_b^x = \mathrm{id}, \quad \text{“FTC”}$$

$$\int_b^x \circ \, \mathrm{d} = \mathrm{id}$$

let $J = \mathrm{Jac}(X)$

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, hook] & X(\mathbf{Q}_p) \arrow[d, hook] \arrow[dr] & \\
J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \arrow[r] & \mathrm{Lie}\, J(\mathbf{Q})
\end{tikzcd}$$

We have

$$\overline{J(\mathbf{Q})} \cap X(\mathbf{Q}_p) \supseteq X(\mathbf{Q})$$

now if

$$r = \mathrm{rank}(J(\mathbf{Q})) < g$$

then this intersection is finite! If we can compute these logarithm functions we can potentially find the intersection explicitly

Problem: There are too many functions satisfying all the conditions above, so computing one of them on the nose is hard

Coleman's idea: impose that the integral pullback along rigid analytic maps, including for a chosen lift of Frobenius

$$\int_b^x \phi^* \omega = \phi^* \int_b^x \omega \quad \text{“Frobenius equivariance”}$$

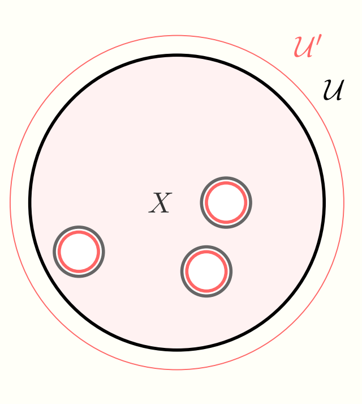
We **can** compute the abelian integrals needed for Chabauty by multiplying points on our curve till they lie in the same residue disk on the Jacobian.

But we would also like for some applications to compute iterated integrals, using Coleman integrals as coefficient functions for 1-forms and iterating again.

To do this, we cannot allow arbitrary rigid functions on our space, but must remove a finite union of disks and consider overconvergent functions:
For example in this way p-adic polylogarithms may be defined

$$\mathrm{li}_n(z) = \int \mathrm{li}_{n-1}(z) \frac{\mathrm{d}z}{z}, \ \mathrm{li}_1(z) = -\log(1-z)$$

Algorithms to compute these are due to Besser and de Jeu.



Applications of this theory:

Coleman integration can be used to define p-adic regulators, p-adic heights, p-adic periods.

Of these, p-adic heights have played a big role in the huge effort of several authors that enables the non-abelian Chabauty of Kim to be made effective and computable, some highlights:

Theorem 1 (Balakrishnan–Dogra–Müller–Tuitman–Vonk)**.** *The (non-)split Cartan modular curve of level 13 is a genus 3 curve which can be given as*

$$X_s(13)\colon y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0$$

its Jacobian has rank 3, and Picard rank 3. Then quadratic Chabauty shows that there are exactly 7 rational points on this curve.

Theorem 2 (Balakrishnan–B.–Bianchi–Lawrence–Müller–Triantafillou–Vonk)**.** *The number of rational points on the Atkin–Lehner quotient modular curves $X_0(N)^+ := X_0(N)/w_N$, all of genus 2, rank 2 and Picard rank 2 for $N \in \{67, 73, 103\}$ are as follows:*

$$\#X_0(67)^+(\mathbf{Q}) = 10, \quad \#X_0(73)^+(\mathbf{Q}) = 10, \quad \#X_0(103)^+(\mathbf{Q}) = 8.$$

This involves non-abelian Chabauty and Mordell–Weil sieving at 31 and 137 in the $N = 67$ case.

Theorem 3 (Balakrishnan–Dogra–Müller–Tuitman–Vonk)**.** *The non-split Cartan modular curve of level 17 is a genus 6 curve, its Jacobian has rank 6. Quadratic Chabauty shows that there are exactly 7 rational points on this curve.*

Many authors by now use quadratic Chabauty computations for interesting questions in rational points, Adžaga, Arul, Beneish, Chen, Chidambaram, Keller, and Wen Arul and Müller, Chidambaram, Keller, and Padurariu, and more ...

Anatomy of a p-adic integral computation: after Balakrishnan-Bradshaw-Kedlaya

1. Pick a lift of the Frobenius map
2. Compute Frobenius action on H^1
3. Evaluate primitives for at least one point in each disk
4. Compute integrals between nearby points
5. Solve a linear system

Authors	Capabilities	System	Runtime
Balakrishnan-Bradshaw-Kedlaya	Odd hyperelliptic curves / $\mathbf{Q}_p$	Sage	pN^2g^2
Balakrishnan-Tuitman (BT)	General curves with a map to $\mathbf{P}^1$ / ramified	Magma	$pd_x^4 d_y^2 \, (N^2 + d_x d_y N)$
B.	Superelliptic curves / unramified (some restriction on p)	Julia/Nemo	$g^3 \sqrt{p} n N^{5/2}$
B.-Kaya-Keller(+CMM) (after BT)	General curves with a map to $\mathbf{P}^1$ / mixed	Magma	????

Note: also Chabauty code due to e.g. Stoll, Siksek

In the algorithm of Balakrishnan-Tuitman and BKK we work with almost any plane model of a curve, over a number field K, of the form

$$X \colon Q(x, y) = 0.$$

(For now we assume p inert in K and take the completion $K_p \simeq \mathbf{Q}_{p^n}$)

We consider this together with a map $X \overset{x}{\mapsto} \mathbf{P}^1$.

We work in the ring $R^\dagger/K_p$ of overconvergent p-adic functions away from the ramification locus.

Then using prior work of Tuitman we can find a Frobenius lift

$$\phi \colon R^\dagger \to R^\dagger$$

$$x \mapsto x^p$$

$$c \mapsto \sigma(c) \text{ for } c \in \mathbf{Q}_{p^n},$$

a vector of primitives and the matrix capturing the Frobenius action on cohomology

$$(\phi^* \omega_i)_i = M(\omega_i)_i + \underbrace{(\mathrm{d} f_i)_i}_{=0} \in H^1_{rig}(X \otimes K_p).$$

these can be computed for a basis $(\omega_i)_i$ of 1-forms p-adically integral on the complement of the ramification locus.

Roughly, these algorithms (based on Kedlaya's) approximate the Frobenius lift applied to differentials, then try to iteratively reduce the degree of the resulting series by subtracting appropriately chosen exact differentials. Generally need to consider many terms!

Over extension fields: In order to integrate over $\mathbf{Q}_{p^n}$ we start with the known data above. Assuming we want to integrate between two points of $X(\mathbf{Q}_{p^n})$.

We define the action of ϕ on $X(\overline{\mathbf{Q}}_{p^n})$ via

$$\phi(x_0, y_0) = (\sigma^{-1}(\phi(x)(x_0, y_0)), \sigma^{-1}(\phi(y)(x_0, y_0))).$$

On functions $f \colon X(\overline{\mathbf{Q}}_{p^n}) \to \overline{\mathbf{Q}}_{p^n}$ the action of ϕ is then

$$\phi(f)(P) = \sigma f(\phi(P)).$$

The action the nth power of Frobenius on the basis differentials is given by

$$\phi^{*n}(\omega_i)_i = \sum_{t=n-1,\ldots,0} \left(\prod_{s=n-1,\ldots,t+1} \phi^s(M) \right) \phi^{*t}(\mathrm{d} f_i)_i + \prod_{s=n-1,\ldots,0} \phi^s(M)(\omega_i)_i.$$

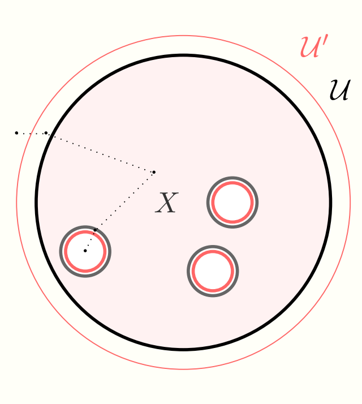
so that

$$\left(1 - \prod_{s=n-1,\ldots,0} \phi^s(M)\right) \left(\int_P^Q \omega_i\right)_i = \left(\int_P^{\phi^n P} \omega_i\right)_i + \left(\int_{\phi^n Q}^Q \omega_i\right)_i + \sum_{t=n-1,\ldots,0} \left(\prod_{s=n-1,\ldots,t+1} \phi^s(M) \right) \sigma^t \left(f_i(\phi^t Q) - f_i(\phi^t P)\right)_i.$$

As we can compute the RHS and the matrix M we can compute the integrals of basis differentials.

The primitives f_i must be evaluated at at least one point in each disk, and at Frobenius images of these points.

This forces us to pass to a totally ramified extension on top of the unramified one we started with. We simply choose ϕ to be an element of the Galois group of this extension that extends the usual Frobenius on the unramified extension.



In the algorithm for superelliptic curves the superelliptic automorphism is used to conclude that integrals between the bad points all vanish and avoid passing to additional ramified extensions.

Conclusion: The algorithm of Balakrishnan-Tuitman can be extended to completely general p-adic fields, but remains quite time consuming.

We have a working implementation, and will soon release a preprint with proofs of correctness and complexity analysis. The Coleman integral is Galois equivariant, which is convenient to check that the implementation is correct, but doesn't seem to help yet when computing.

Do you have interesting examples for us (curves over $\mathbf{Q}(\sqrt{-163})$)!?

Time for something completely different: A Wieferich prime is one for which

$$2^{p-1} \equiv 1 \pmod{p^2},$$

only 2 are known, unlikely p-adic closeness.

Katz (2015) reinterprets this as the fact that $2^{\#\mathbf{G}_m(\mathbf{F}_p)}$ is closer to the identity p-adically than it is forced to be.

If we assume that this happens no more often that it would randomly we get a heuristic for the distribution of Wieferich primes.

Generalizing we consider an abelian variety A and select an integral model of the Lie algebra of the Neron model and a point P of infinite order, consider

$$W_P \colon \{p : p \text{ prime}, p \text{ good}\} \to \mathbf{Lie}(\mathcal{A}/\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{R}/\mathbf{Z}) \cong (\mathbf{R}/\mathbf{Z})^d$$

$$p \mapsto \left(\left(\int_0^{\#\mathcal{A}_{\mathbf{F}_p}(\mathbf{F}_p) P} \omega_i \right) / p \mod p \right)_i$$

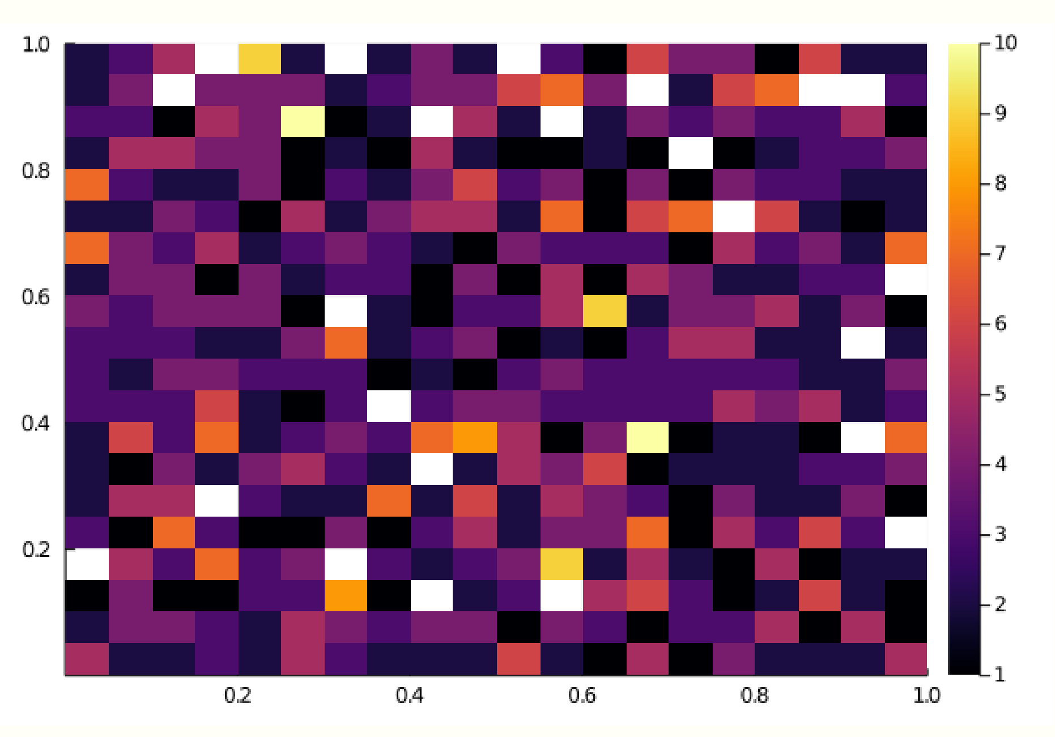
we call this quantity $W_P(p)$ the **Wieferich quotient**, the “first digit” of the integral.

Katz conjectures that as long as P generates a Zariski dense subgroup, if we take larger p the Wieferich quotients equidistribute.

The genus 2 curve

$$X \colon y^2 = 4x^5 - 8x^4 + 8x^3 - 4x^2 + 1$$

997.b.997.1, has a rational point $x = (0, 1)$ such that the class $P = [x - \infty] \in \mathrm{Jac}(X)(\mathbf{Q})$ is of infinite order. A histogram of Wieferich quotients of the Coleman integrals of invariant 1-forms is as follows:

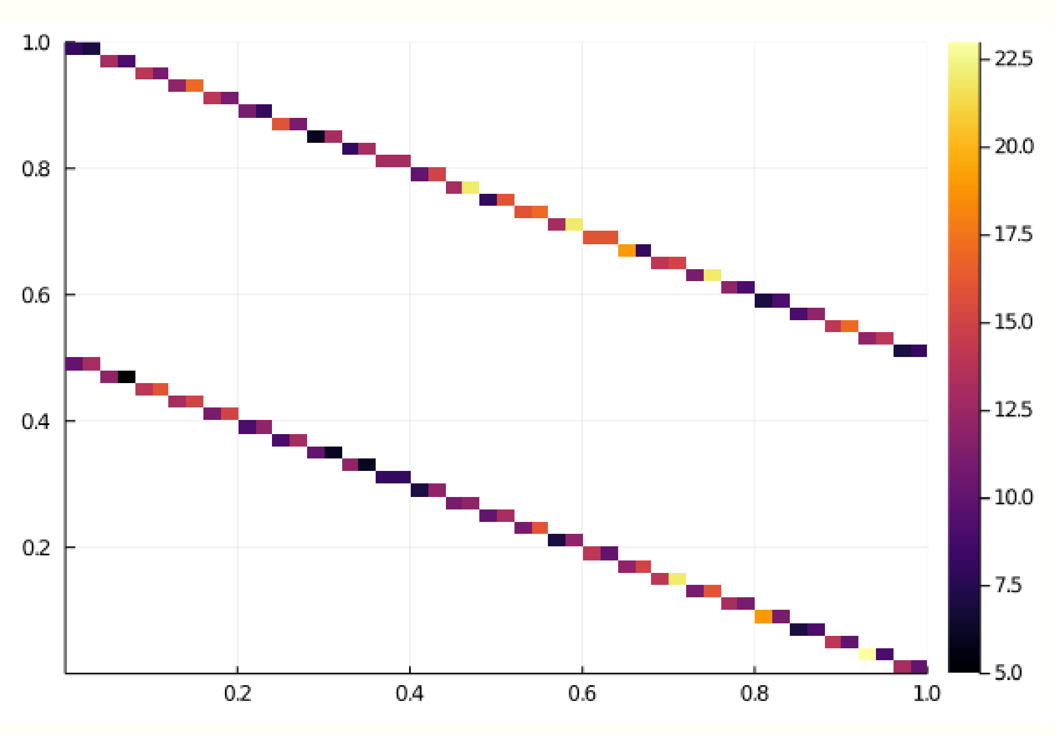


for the Wieferich quotients $W_P(p)$ for all primes $15 < p < 10000$, and $p \neq 997$.

However for the genus 2 curve

$$X \colon y^2 = 4x^5 - 8x^4 + 8x^3 - 4x^2 + 1$$

2080.a.4160.2, with $P = [(0, 1) - \infty] \in \mathrm{Jac}(X)(\mathbf{Q})$ of infinite order, the Wieferich quotients $W_P(p)$ for all primes $15 < p < 10000$.



This curve has Jacobian over $\mathbf{Q}$ isogenous the product of elliptic curves 32.a and 65.a. As 32.a is rank 0, the point P will not generate a Zariski dense subgroup of the Jacobian in this case.

We see that the annihilating differential is (mod p)

$$\frac{\mathrm{d}x}{y} + 2x \frac{\mathrm{d}x}{y}$$

for all these p, so almost certainly a global annihilating differential.

Doing these computations type of we gain some evidence for Katz's conjecture, even in cases where other things might interfere, e.g. CM.

A worked example

Coleman's work

The above approach is known as **effective Chabauty** and is due to Coleman. Coleman described how to compute these integrals using **analytic continuation along Frobenius** and proved the following theorem

Theorem 4 (Coleman's effective Chabauty)**.** *If $p > 2g$ then*

$$|X(\mathbf{Q})| \leq |X(\mathbf{F}_p)| + 2g - 2$$

The proof goes over each disk, estimating the number of zeroes of the integral on each disk.

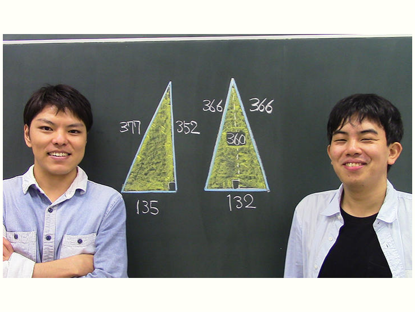
This bound is sometimes sharp! For instance:

Theorem 5 (Hirakawa–Matsumura)**.** *There exists a unique pair of a rational right triangle, and a rational isosceles triangle with equal areas and equal perimeters.*

Proof. The problem reduces to finding rational points on the genus 2 rank 1 curve

$$r^2 = (-3w^2 + 2w^2 - 6w + 4)^2 - 8w^6.$$

which has good reduction at 5, and 8 points over $\mathbf{F}_5$. Moreover we can find 10 rational points, most of which do not correspond to non-degenerate triangles. ☐



Nevertheless it is still often necessary to actually compute these integrals.

Computing Coleman integrals

Coleman's theory makes use of a **lift of Frobenius**, an analytic morphism of an affine curve over $\mathbf{Q}_p$ that reduces to the Frobenius morphism over $\mathbf{F}_p$.

Example 6. *For*

$$X \colon y^2 = f(x)$$

a hyperelliptic curve, we can take $\phi \colon x \mapsto x^p$ which forces

$$(\phi(y))^2 = f(x^p) = f(x^p) - f(x)^p + f(x)^p = f(x^p) - f(x)^p + y^{2p}$$

hence

$$\phi(y) = y^p \sqrt{1 + \frac{f(x^p) - f(x)^p}{y^p}}$$

on the locus away from $y = 0$.

The property of Coleman integrals that makes the theory uniquely defined, is that we ask the integrals to be equivariant for some (any) lift of Frobenius.

We pick a lift of the Frobenius map, on some affine subvariety A of X, $\phi^* \colon A \to A$, and write $A^\dagger$ (resp. $A_{\mathrm{loc}}(X)$) for overconvergent (resp. locally analytic) functions on A.

Theorem 7 (Coleman)**.** *There is a (unique) $\mathbf{Q}_p$-linear map $\int_b^x \colon \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p \to A_{\mathrm{loc}}(X)$ for which:*

$$\mathrm{d} \circ \int_b^x = \mathrm{id} \colon \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p \to \Omega^1_{loc} \quad \text{“FTC”}$$

$$\int_b^x \circ \, \mathrm{d} = \mathrm{id} \colon A^\dagger \hookrightarrow A_{\mathrm{loc}}$$

$$\int_b^x \phi^* \omega = \phi^* \int_b^x \omega \quad \text{“Frobenius equivariance”}$$

- Balakrishnan–Bradshaw–Kedlaya reduce the problem of computing all Coleman integrals of basis differentials ω_i of $H^1_{\mathrm{dR}}(X)$ between $\infty \in X$ and a point $x \in X(\mathbf{Q}_p)$ on an odd degree hyperelliptic curve, to:
  1. Finding “tiny integrals” between nearby points,
  2. Writing $\phi^* \omega_i - \mathrm{d} f_i = \sum_j a_{ij} \omega_j$ and evaluating the primitive f_i for a point P near x, for each i.
- Balakrishnan–Tuitman gave a more general version of this procedure that works on a very large class of curves.
- B. gave a computationally more efficient method for superelliptic curves, using work of Harvey and Minzlaff, that also works over unramified extensions of $\mathbf{Q}_p$.

Number field Chabauty

If we work over a fixed number field K one can make sense of all of the above, and sometimes one can do better following ideas of Siksek and Wetherell.

If X/K is a curve over a number field K of degree d then $\mathrm{Res}_{K/\mathbf{Q}}(X)$ is a d-dimensional projective variety such that

$$V = \mathrm{Res}_{K/\mathbf{Q}}(X)(\mathbf{Q}) \leftrightarrow X(K)$$

and

$$A = \mathrm{Res}_{K/\mathbf{Q}}(\mathrm{Jac}(X))$$

is a gd-dimensional abelian variety. Then the analogous Chabauty diagram is

$$\begin{tikzcd}
V(\mathbf{Q}) \arrow[r, hook] \arrow[d, hook] & V(\mathbf{Q}_p) \arrow[d, hook] \arrow[dr] & \\
A(\mathbf{Q}) \arrow[r, hook] & A(\mathbf{Q}_p) \arrow[r] & \mathrm{Lie}\, A(\mathbf{Q})
\end{tikzcd}$$

where now

$$\dim \overline{A(\mathbf{Q})} = \mathrm{rank}(J(K)),\ \dim V(\mathbf{Q}) = d$$

If $d + r \leq gd$ then we might **hope** that the intersection of these two subspaces is finite, and we can therefore cut out $X(K)$ whenever $r \leq (g-1)[K : \mathbf{Q}]$.

Warning 8. *The intersection is not always finite! This was noted by Siksek, but even Siksek's guess for a sufficient condition also turned out to be false, as shown by Dogra, with the example of a genus 3 hyperelliptic curve over* $\mathbf{Q}(\sqrt{33})$.

Nevertheless in practice this approach is quite useful, Siksek gives an explicitly checkable condition that can be used to verify that rational points are alone in their residue disk.

Theorem 9 (Siksek). *For every K-rational point Q of X/K there is an effectively computable matrix $M_p(Q)$ defined using the integrals of holomorphic 1-forms against a basis of a free subgroup of finite index in $J(K)$, and the local behaviour of the basis of 1-forms such that if the reduction of $M_p(Q)$ has rank d then Q is the only K-rational point of the curve in a p-adic unit ball around Q.*

Example 10 (B.–Dahmen). *Consider $X\colon x^{13} + y^{13} = z^5$, one of the generalized Fermat curves, then there exists a covering map*

$$X \to C\colon y^2 = 4x^5 + 1677\alpha^2 - 2769\alpha + 637/K$$

where

$$K = \mathbf{Q}(\alpha) = \mathbf{Q}[x]/(x^3 - x^2 - 4x - 1)$$

is the unique cubic subfield of $\mathbf{Q}(\zeta_{13})$. This curve has rank 2 over K and genus 2, so regular Chabauty does not apply. Nevertheless Siksek's techniques using the prime 47 *suffice to show that there are only five K-rational points on C.*

Removing extra points – the Mordell–Weil sieve

This is a technique that first appears in the work of Scharaschkin, that is extremely useful to rule extra points that appear in the Chabauty method.

In the example above we had a zero of our integrals that didn't appear to correspond to a rational solution. Once again fixing a rational base point $b \in X(\mathbf{Q})$ for simplicity we have:

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook, "\mathrm{AJ}"] \arrow[d, hook, "\mathrm{red}_X"] & J(\mathbf{Q}) \arrow[d, hook, "\mathrm{red}_J"] \\
X(\mathbf{F}_\ell) \arrow[r, "\mathrm{AJ}_\ell"] & J(\mathbf{F}_\ell)
\end{tikzcd}$$

where now the image of any rational point lands in the union of cosets $\mathrm{red}_J^{-1}(\mathrm{AJ}_\ell(X(\mathbf{F}_\ell)))$.

In order to prove non-rationality of certain p-adic points we make use of the p-adic filtration on J, points of $X(\mathbf{Q})$ whose difference lies in a group of large p-power order of the Jacobian are p-adically close on the Jacbian, and hence on the curve itself.

By varying ℓ over primes such that a power of p divides $|J(\mathbf{F}_\ell)|$ we increasingly place restrictions on how p-adically close any putative rational point must be to one of our known rational points.

Using just the sieve on its own we always cut out a union of p-adic balls, which is infinite if non-empty, but coupled with finiteness from Chabauty we can often determine exactly the set of rational points.

The question remains, what if $r \geq g$?

Chabauty–Kim

Minhyong Kim has extended the core idea of Chabauty, inspired in part by the **section conjecture** of Grothendieck that

$$X(\mathbf{Q}) \simeq H^1(G, \pi_1^{\text{ét}}(\overline{X}, b)).$$

Kim considers the $\mathbf{Q}_p$-pro-unipotent étale fundamental group, denoted U, this has a descending central series filtration $U = U^1 \supset U^2 \supset \cdots$, for which the quotients $U_i = U/U^i$ get increasingly non-abelian as $i \gg 1$. Kim defines local and global **Selmer schemes** that fit into an analogous diagram as before, for each n

$$\begin{tikzcd}
X(\mathbf{Z}[1/S]) \arrow[r, hook] \arrow[d] & X(\mathbf{Z}_p) \arrow[d] \arrow[dr] & \\
H^1_f(G, U_n) \arrow[r, "loc_p"] & H^1_f(G_p, U_n) \arrow[r] & U_n^{DR}/F^0
\end{tikzcd}$$

The bottom horizontal maps are algebraic, and the vertical maps are transcendental.

Kim conjectures that for some **depth** n we always have that the image of loc_p is not Zariski dense and so a Chabauty-like argument applies to show finiteness of rational points. Kim also expects that for $n \gg 1$ this method will cut out precisely the set of rational points, with no extra transcendental points like we had before.

In depth 1 this gives us a diagram which is essentially the original Chabauty diagram.

Quadratic Chabauty

Work of Balakrishnan–Dogra makes Chabauty–Kim more effective in the case that the rank of the Neron–Severi group of the Jacobian is at least 2. This allows them to find a more approachable quotient of the group U_2 and make a connection with p-adic heights to get a handle on the functions appearing

Applications to modular curves

Integral points and connection with the S-unit equation

In addition to answering questions about rational points, Chabauty techniques can also be used to determine or bound integral points, by considering punctured curves:

Letting $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ and fixing a finite set of rational primes S we have

$$X(\mathbf{Z}[1/S]) = \{(u, v) \in (\mathbf{Z}[1/S]^\times)^2 : u + v = 1\}$$

the solutions to the S-**unit equation**.

The Chabauty diagram in this case involves the **generalised Jacobian**, for a prime $p \notin S$

$$\begin{tikzcd}
X(\mathbf{Z}[1/S]) \arrow[r, hook] \arrow[d, hook] & X(\mathbf{Z}_p) \arrow[d, hook] \arrow[dr] & \\
\mathbf{G}_m(\mathbf{Z}[1/S])^2 \arrow[r] & \mathbf{G}_m(\mathbf{Z}_p)^2 \arrow[r] & \mathbf{Z}_p^2
\end{tikzcd}$$

from this we see that the rank < genus condition is almost never satisfied.

But passing to non-abelian Chabauty in depth 2 we obtain the diagram

$$\begin{tikzcd}
X(\mathbf{Z}[1/S]) \arrow[r, hook] \arrow[d, hook] & X(\mathbf{Z}_p) \arrow[d, hook] \\
\mathbf{A}^{2|S|} \arrow[r] & \mathbf{A}^3
\end{tikzcd}$$

where $\mathrm{Li}_2(z) = \int \frac{\log(1-w)}{w}\, \mathrm{d}w$ is an **iterated Coleman integral**. Defined near zero by the series

$$\sum_{i=0}^{\infty} \frac{z^i}{i^2}.$$

The bottom horizontal arrow is more mysterious. In joint work with Betts–Kumptisch–Lüdtke–McAndrew–Qian–Studnia–Xu we study the S_3-equivariance of this set-up. We also apply **refined non-abelian Chabauty–Kim** to reduce the dimension of the bottom left entry and apply this extension of Chabauty when $|S| = 2$.

Other applications

Integral points

Torsion points

General fields

with E. Kaya & T. Keller

Following Balakrishnan-Tuitman