Coleman integration and its Uses in Number Theory

Alex J. Best
King's College London
9/3/23

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

When $g = \operatorname{genus}(X) \geq 2$ 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 $J = \operatorname{Jac}(X)$

$$\begin{array}{ccccc} X(\mathbf{Q}) & \hookrightarrow & X(\mathbf{Q}_p) & \searrow & \\ \downarrow & & \downarrow & & \\ J(\mathbf{Q}) & \hookrightarrow & J(\mathbf{Q}_p) & \longrightarrow & \operatorname{Lie} J(\mathbf{Q}_p) \end{array}$$

We have

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

now if

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

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

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 $\operatorname{Res}_{K/\mathbf{Q}}(X)$ is a d-dimensional projective variety such that

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

and

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

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

$$\begin{array}{ccccc} V(\mathbf{Q}) & \hookrightarrow & V(\mathbf{Q}_p) & \searrow & \\ \downarrow & & \downarrow & & \\ A(\mathbf{Q}) & \hookrightarrow & A(\mathbf{Q}_p) & \longrightarrow & \operatorname{Lie} A(\mathbf{Q}_p) \end{array}$$

where now

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

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 1. *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 (Siksek)**.** *For every X/K and $Q \in X(K)$ 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 (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.

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

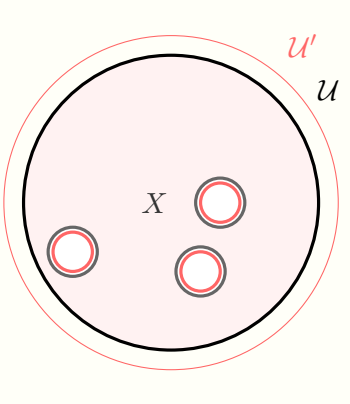
Coleman's idea: impose that the integral pullback along rigid analytic maps, including for a chosen lift of Frobenius

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

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



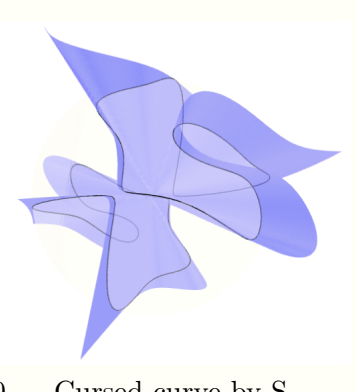
$$\operatorname{li}_n(z) = \int \operatorname{li}_{n-1}(z) \frac{\mathrm{d}z}{z},\ \operatorname{li}_1(z) = -\log(1-z)$$

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 can be expressed in terms of double integrals and have played a big role in the effort of several authors that enables the non-abelian Chabauty of Kim to be made effective and computable, some highlights:



Cursed curve by S. Hashimoto

Theorem (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 (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 (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 ...

Over number fields? work of Balakrishnan-Besser-Bianchi-Muller caries out explicit quadratic Chabauty over number fields

Goal: extend explicit computational tools to general curves over general p-adic fields, to enable experiments and explicit proofs.

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
Balakrishnan-Bradshaw-Kedlaya	Odd hyperelliptic curves / $\mathbf{Q}_p$	Sage
Balakrishnan-Tuitman (BT)	General curves with a map to $\mathbf{P}^1$ / ramified	Magma
B.	Superelliptic curves / $\mathbf{Q}_{p^n}$ (some restriction on p)	Julia/Nemo
B.-Kaya-Keller(+CMM) (after BT)	General curves with a map to $\mathbf{P}^1$ / mixed	Magma

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

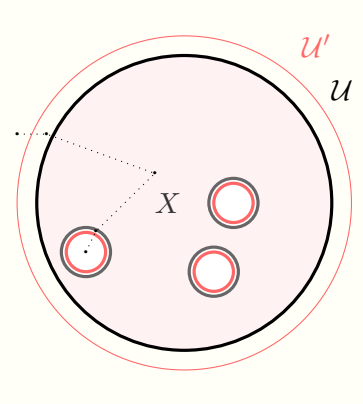
$$\phi(f)(P) = \sigma f(\phi(P)).$$

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

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

so that

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



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.

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

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

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

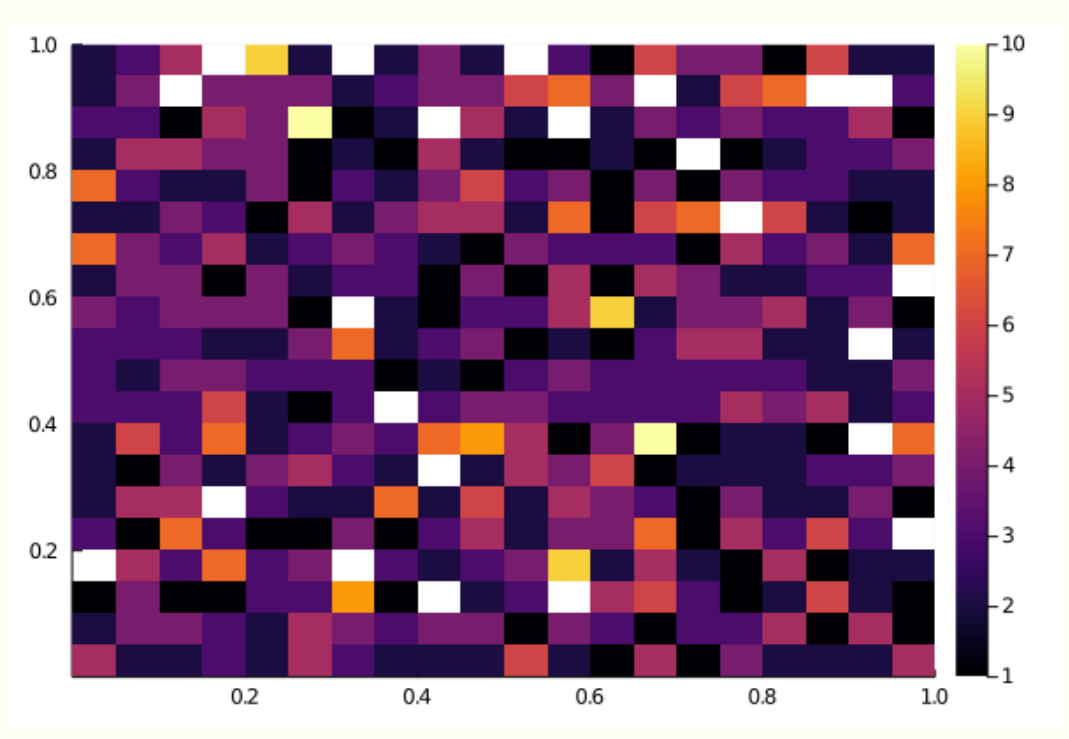
we call this quantity $W_P(p)$ the **Wieferich quotient**, the “first digit” of the integral.

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 $P = [x - \infty] \in \operatorname{Jac}(X)(\mathbf{Q})$ is of infinite order. A histogram of Wieferich quotients of the Coleman integrals of invariant 1-forms is as follows:

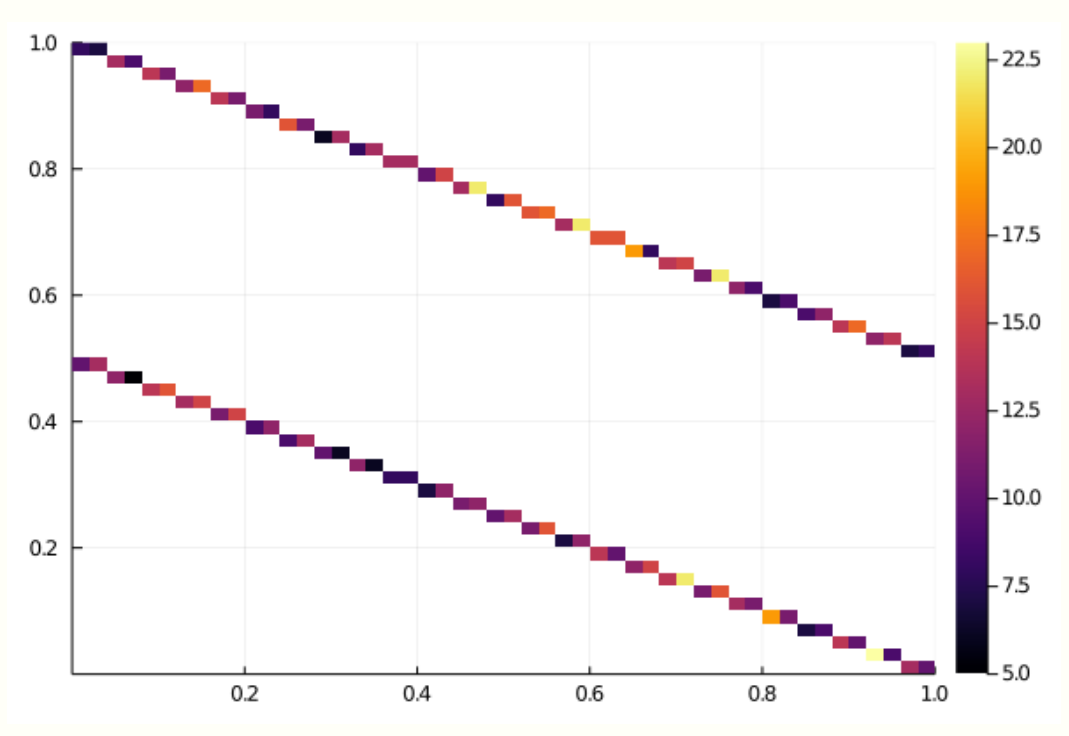


for the Wieferich quotients $W_P(p)$ for all primes $15 < p < 10000$, and $p \neq 997$.

However for the genus 2 curve

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

2080.a.4160.2, with $P = [(0, 1) - \infty] \in \operatorname{Jac}(X)(\mathbf{Q})$ 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.