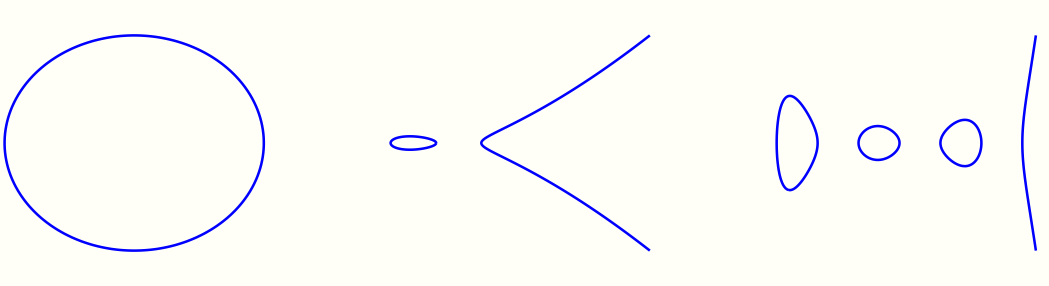
A Guided Tour of Chabauty Methods

Alex J. Best
Vrije Universiteit Amsterdam

12/7/21

On the menu: A summary of different Chabauty methods, when they apply, and some applications.

Let $X/\mathbf{Q}$ be a smooth projective and geometrically integral curve, e.g.



We are interested in the set $X(\mathbf{Q})$, especially when $|X(\mathbf{Q})| < \infty$ we hope to provably determine this set.

This is always the case when $g = \mathrm{genus}(X) \geq 2$ by **Faltings' theorem**.

Classic Chabauty

Given a curve X we can choose a prime p of good reduction for X, let $J = \mathrm{Jac}(X)$ and fix a base point $b \in X(\mathbf{Q})$ and look at:

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

We have

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

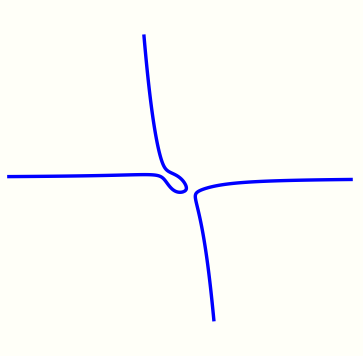
now if

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

then this intersection is finite!

From now on we assume this condition on the rank.

A worked example



The genus 2 curve with smallest conductor and positive rank is conjecturally given by

$$X\colon y^2 + (x^3 + x + 1)y = -x^2 - x$$

Taking $P = (0, -1)$, $b = \infty^+$ we can integrate

$$\int_P^b \frac{\mathrm{d}x}{y} = -79 \cdot 3 + O(3^{14}), \quad \int_P^b \frac{x\,\mathrm{d}x}{y} = -7010 \cdot 3^3 + O(3^{14})$$

hence

$$\int_P^b (-7010 \cdot 3^3 + 79 \cdot 3x)\frac{\mathrm{d}x}{y} = O(3^{14})$$

so any other rational point $Q \in X(\mathbf{Q})$ will also have the property that

$$\int_Q^b (-7010 \cdot 3^3 + 79 \cdot 3x)\frac{\mathrm{d}x}{y} = O(3^{14})$$

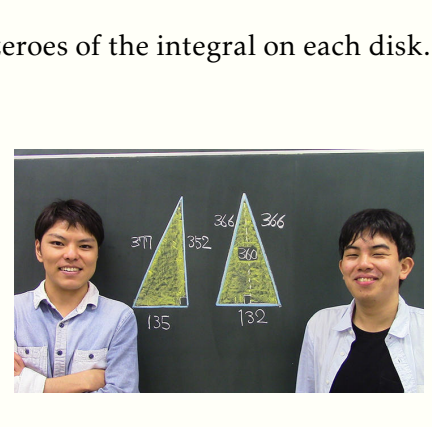
p-adically locally this integral can be expressed as a power series in a local parameter t. Near $(0,1) \in X(\mathbf{Q})$ we may take $t = x$ and calculate the integrals to be:

$$\begin{aligned} \int_{Q(t)}^b \omega = {} & O(3^{15}) + (7010 \cdot 3^3 + O(3^{14})) \cdot t + (797122 \cdot 3 + O(3^{14})) \cdot t^2 + (126101 + O(3^{13})) \cdot t^3 \\ & - (382828 \cdot 3^2 + O(3^{15})) \cdot t^4 + (356687 \cdot 3^2 + O(3^{15})) \cdot t^5 - (576544 \cdot 3 + O(3^{14})) \cdot t^6 \\ & + (54032 \cdot 3^3 + O(3^{16})) \cdot t^7 + (1162 \cdot 3^6 + O(3^{14})) \cdot t^8 - (130775 \cdot 3^{-1} + O(3^{12})) \cdot t^9 \\ & + (158450 \cdot 3^2 + O(3^{14})) \cdot t^{10} + (352786 \cdot 3 + O(3^{14})) \cdot t^{11} + (432610 \cdot 3^2 + O(3^{15})) \cdot t^{12} \\ & - (167738 \cdot 3^4 + O(3^{16})) \cdot t^{13} + (701429 \cdot 3^3 + O(3^{16})) \cdot t^{14} + O(t^{15}) \end{aligned}$$

As we are looking for roots near $(0,1)$ we can substitute $t = pt$ and find the roots of the resulting series. The roots of this series are

$$O(3^{12}),\ -106289 + O(3^{12}),\ -182670 + O(3^{12})$$

which give x-coordinates 0, $-12/5$, and some wild looking p-adic number! We can verify that 0, $-12/5$ are indeed coordinates of points on the curve.



We see from this example that things work best when we have a rational point in each **residue disk**, which we can recover as the root 0 and then have no other roots.

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

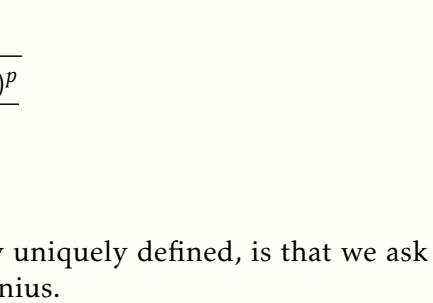
Theorem 1 (Coleman's effective Chabauty). *If $p > 2g$ then*

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

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 2 (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 3. *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 4 (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 $\mathbf{Q}_p$.

Stoll's work

If $r < g - 1$ then the dimension of

$$\left\{\omega : \forall D \in J(\mathbf{Q}), \int_D \omega = 0\right\}$$

is larger than one, hence we have a choice of which ω to use in each residue disk.

Theorem 5 (Stoll). *If $p > 2g$ then*

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

Note that if $r = 0$ this says $|X(\mathbf{Q})| \leq |X(\mathbf{F}_p)|$, which also follows from the fact that rational torsion of the Jacobian injects into torsion of the reduction.

Remark 6. *One can reverse this type of theorem to create families of curves with a given rank, just write down a curve with a lot of rational points reducing to the same point in $\mathbf{F}_p$ and it will be forced to have large rank!*

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

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

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 7. *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 8 (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 9 (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:

$$\begin{array}{ccc} X(\mathbf{Q}) & \xhookrightarrow{\mathrm{AJ}} & J(\mathbf{Q}) \\ \downarrow{\scriptstyle \mathrm{red}_X} & & \downarrow{\scriptstyle \mathrm{red}_J} \\ X(\mathbf{F}_\ell) & \xrightarrow{\mathrm{AJ}_\ell} & J(\mathbf{F}_\ell) \end{array}$$

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

$$\begin{array}{ccccc} X(\mathbf{Z}[1/S]) & \hookrightarrow & X(\mathbf{Z}_p) & & \\ \downarrow & & \downarrow & \searrow & \\ H^1_f(G, U_n) & \xrightarrow{loc_p} & H^1_f(G_p, U_n) & \longrightarrow & U_n^{DR}/F^0 \end{array}$$

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

Theorem 10 (Balakrishnan–Dogra–Müller–Tuitman–Vonk). *Consider the (non-)split Cartan modular curve of level 13, this is a genus 3 curve which can be given as*

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

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

Theorem 11 (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.

Recently Balakrishnan–Dogra–Müller–Tuitman–Vonk have extended their work to even more interesting 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 $X = \mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$ 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 $p \notin S$

$$\begin{array}{ccccc} X(\mathbf{Z}[1/S]) & \hookrightarrow & X(\mathbf{Z}_p) & & \\ \downarrow & & \downarrow & \searrow & \\ \mathbf{G}_m(\mathbf{Z}[1/S])^2 & \longrightarrow & \mathbf{G}_m(\mathbf{Z}_p)^2 & \longrightarrow & \mathbf{Z}_p^2 \end{array}$$

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

$$\begin{array}{ccc} X(\mathbf{Z}[1/S]) & \hookrightarrow & X(\mathbf{Z}_p) \\ \downarrow & & \downarrow \\ \mathbf{A}^{2|S|} & \longrightarrow & \mathbf{A}^3 \end{array}$$

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 $|S| = 2$.