Chabauty Quadràtic

Xavier Xarles

24 de Gener de 2019

Detesto l'infinit,
és massa llarg i ample,
però m'agrada perquè el trobo fet
un vuit tombat de panxa enlaire,
com un escarabat vençut injustament
per la física.

Detesto l'infinit, no sona a pluja
ni a cargol de mar ni a vent ni a
campana ni a ocell matiner:
sempre m'ha fet por,
la por perfecta,
el clos d'on vaig sortir
vestit de rosa.

Màrius Sampere Passerell

General notations

p a prime number.
K number field.
$\wp$ a prime ideal (of residual characteristics p).
$K_\wp$ the completion of K at $\wp$.
X smooth projective curve of genus $g \geq 2$ over K.
We will suppose $X(K) \neq \emptyset$, and fix $b \in X(K)$.
J the Jacobian of X over K.
$\iota : X \to J$ the Abel-Jacobi map given by the point b:
so $\iota(x) = x - b$ and $\iota(b) = 0$.

Chabauty-Coleman idea

We have a pairing of p-adic integration.

$$\int : J(K_\wp) \times H^0(J_\wp, \Omega^1_J) \to K_\wp$$

equivalently, $\int_D \omega = \log_J(D)(\omega)$, where

$$\log_J : J(K_\wp) \to H^0(J_\wp, \Omega^1_J)^*$$

is the logarithm obtained from the formal group).
Consider the $K_\wp$-subspace

$$W := \{\omega \in H^0(J, \Omega^1_J) \mid \int_D \omega = 0 \ \forall D \in J(K)\}.$$

If $W \neq 0$, then the set

$$X(K_\wp)_1 := \{x \in X(K_\wp) \mid \int_b^x \omega = 0 \ \forall \omega \in W\}$$

is finite (and computable).

Kim's Idea

There is a descending filtration

$$X(K) \subset \cdots \subset X(K_\wp)_n \subset X(K_\wp)_{n-1} \subset \cdots \subset X(K_\wp)$$

given by information obtained from the maximal n-unipotent quotient of the $\mathbb{Q}_p$-étale fundamental group of X with base point b and analogously with the de Rham fundamental group.

Conjecture

If $K = \mathbb{Q}$ and X a curve of genus $g \geq 2$, there exist an n such that $X(\mathbb{Q}_p)_n$ is finite.

One version of this conjecture (suggested by N. Dogra in a private communication) could be

Guess

For any K and X a curve of genus $g \geq 2$, there exist an n such that $X(\prod_{v|p} K_v)_n$ is finite.

Some conjectures that imply this conjecture

The conjecture is implied for any the following conjectures.

- The Bloch-Kato conjecture:

  $$K^{(r)}_{2r-n-1}(X^n) \otimes \mathbb{Q}_p \cong H^1_g(\mathrm{Gal}(\overline{K}/K), H^n(\overline{X}^n, \mathbb{Q}_p(r)))$$

  given by the Chern character, and in particular it is zero if $n > 2r - 1$.
- A (sightly generalize version of) the Fontaine-Mazur conjecture: a continuous irreducible $\mathbb{Q}_p$-representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that is unramified at almost all places and potentially semi-stable at p is motivic. An extension of two such is then conjectured to be a $\mathbb{Q}_p$-linear combination of motivic representations in a suitable Ext group.

Some positive general results

- Coates-Kim: The conjecture is true if the jacobian of X has CM.
- Ellenberg-Hast: The conjecture is true for all twists of some unramified covering of the solvable Galois covers of $\mathbb{P}^1$.
- (Balakrishnan-Dogra) If $K = \mathbb{Q}$ (or quadratic imaginary), $\rho := \mathrm{rank}_{\mathbb{Z}}(NS(J))$ the rank of the Néron-Severi group of J over K, $r := \mathrm{rank}_{\mathbb{Z}}(J(K))$, and $r < g + \rho - 1$, then $X(K_\wp)_2$ is finite.

Note that $\rho = 1$ "generically", so in this case we don't get more than the Chabauty result. But $\rho > 1$ for some interesting curves, like the bielliptic curves and most modular curves.
Note also that elements of the Néron-Severi group of J are directly related to certain correspondences in X^2: the more correspondences we have, the more conditions we have.

Coleman-Gross p-adic Heigh pairing

The Coleman-Gross p-adic height pairing is a symmetric bilinear pairing

$$h : Div^0(X) \times Div^0(X) \to \mathbb{Q}_p,$$

where

- h can be decomposed into a sum of local height pairings $h = \sum_v h_v$ over all finite places v of K_v.
- $h_v(D, E)$ is defined for $D, E \in Div^0(X \otimes K_v)$ with disjoint support.
- We have $h(D, div(\alpha)) = 0$ for $\alpha \in k(X)^\times$, so h is well-defined on $J(F) \times J(F)$.
- 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 $D \in \mathrm{Div}^0(X)$.

We fix a certain extension and write $h_v(D) := h_v(D, D)$.

Local height functions

- For $v \nmid p$, the local height function $h_v(x-b, x-b)$ can be computed using intersection theory on a regular model of X .
- For $v \nmid p$ and of potentially good reduction, the local height function $h_v(D, D') = 0$ for all D, D' with disjoint support.
- For $v \mid p$ the local height function $h_p(D, D')$ can be computed using (iterated) Coleman integration and is locally analytic. It depends (among other things) on an splitting

  $$s : H^1_{\mathrm{dR}}(X/K_\wp)/\operatorname{Fil}^1 \to H^1_{\mathrm{dR}}(X/K_\wp) \text{ where } \operatorname{Fil}^1(H^1_{\mathrm{dR}}(X/K_\wp)) = H^1(X \otimes K_\wp, \Omega^1)$$

  via the natural map.
- Explicitly, if $v \mid p$ and D and E have disjoint support, then

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

  were ω_D is a differential of third kind on $X \otimes K_\wp$ such that $\operatorname{Res}(\omega_D) = D$ and ω_D is normalized with respect to the above splitting.

Quadratic Chabauty for integral Points (Balakrishnan-Besser-Müller)

$X_{\mathbb{Q}}$ an hyperelliptic with a Weierstrass point ∞, $Y = X \setminus \{\infty\}$. p good reduction prime.
The set of values $\Upsilon \subset \mathbb{Q}_p$ taken by

$$-\sum_{v \text{ bad reduction}} h_v(z_v - \infty, z_v - \infty) \text{ where } (z_v) \in \prod Y(\mathbb{Z}_v)$$

is finite and computable ($\Upsilon = \{0\}$ if the X is everywhere pot. good reduction).
Suppose that $g = \mathrm{rank}_{\mathbb{Z}}(J(\mathbb{Q}))$ and we know a basis of $J(\mathbb{Q}) \otimes \mathbb{Q}$. The p-adic height pairing h determines a bilinear symmetric paring

$$B\colon J(\mathbb{Q}) \otimes \mathbb{Q}_p \times J(\mathbb{Q}) \otimes \mathbb{Q}_p \to \mathbb{Q}_p.$$

Then $Y(\mathbb{Z})$ is contained in the **finite** and **computable** set of points $z \in Y(\mathbb{Z}_p)$ verifying that

$$h_p(z - \infty, z - \infty) - B(z - \infty, z - \infty) \in \Upsilon.$$

Nice correspondences

A correspondence $Z \in \text{Pic}(X \times X)$ is

- Symmetric if $\tau_* Z = Z + \pi_1^* Z_1 + \pi_2^* Z_2$ for some $Z_i \in \text{Pic}(X)$ $i = 1, 2$, where π_i are the projections and $\tau : X^2 \to X^2$ the involution.
- Nice if it is non-trivial, symmetric and the corresponding $\xi_Z \in \text{End}(H^1(X))$ has trace 0.
- If J is absolutely simple, then Z is nice if and only if the image of this class in $H^2(X)(1)$ under the cup product is zero.

Such a nice correspondence Z gives a (non-trivial) element in the Néron-Severi group of J which produces hence a condition on the points in $X(K_\wp)_2$.
If $\rho > 1$, then there exists nice correspondences.

Construction of a special divisor

Consider $b \neq z \in X(K)$.
Denote by

$$\delta, i_1, i_2 \colon X \to X \times X$$

the diagonal embedding $\delta(x) = (x, x)$, the vertical embedding $i_1(x) = (b, x)$ and the horizontal embedding $i_2(x) = (x, z)$. Denote by Δ, X_1 and X_2 the codimension 1 cycles giving the respective images.
Given any cycle Z in $\mathrm{Pic}(X \times X)$, we define

$$\tilde{D}_Z(b, z) := \delta^* Z - i_1^* Z - i_2^* Z \in \mathrm{Div}(X)$$

whose degree is $\deg(\tilde{D}_Z(b, z)) = Z \cdot (\Delta - X_1 - X_2)$.
By choosing a base point x_0 we get a degree 0 divisor

$$D_Z(b, z) := \tilde{D}_Z(b, z) - \deg(\tilde{D}_Z(b, z))x_0.$$

This type of divisors were considered before by Schoen and by Darmon-Rotger-Sols, among others.

Quadratic Chabauty for rational points (Balakrishnan-Dogra)

X of genus $g \geq 2$, $X' := X \setminus \delta^{-1}(|Z|)$, $\wp$ good reduction above p, $b \in X'(K)$.
$\Upsilon \subset \mathbb{Q}_p$ the finite explicit computable set of values taken by

$$- \sum_{v \text{ bad reduction } , v \nmid p} h_v(z_v - b, D_Z(b, z_v)) \text{ where } (z_v) \in \prod X'(\mathbb{Q}_v)$$

($\Upsilon = \{0\}$ in the pot. good reduction case).
Suppose that $g = \mathrm{rank}_{\mathbb{Z}}(J(K))$, $\overline{J(K)}$ has finite index in $J(K_\wp)$ (so Chabauty does not apply) and that we know a basis of $J(K) \otimes \mathbb{Q}$.
The p-adic height pairing h determines a bilinear symmetric paring

$$B \colon J(K_\wp) \otimes \mathbb{Q} \times J(K_\wp) \otimes \mathbb{Q} \to \mathbb{Q}_p.$$

Then $X'(K) \subset X(K)_2 \cap X'(K_\wp)$ is contained in the **finite** and **computable** set of points $z \in X'(K_\wp)$ verifying that

$$h_\wp(z - \infty, D_Z(b, z)) - B(z - \infty, D_Z(b, z)) \in \Upsilon.$$

Comments on the theorem.

1. By moving the cycle Z to a rationally equivalent Z' to cover the part of the curve X not in X'.
2. One key point that allows to show results on rational points instead of just integral points is that for $v \nmid p$, the height $h_v(z_v - b, D_Z(b, z_v))$ takes only a finite number of points for $X'(\mathbb{Q}_v)$, and this is not true for $h_v(z_v - b, z_v - b)$.
3. We can use the integration map

$$J(K) \otimes K_\wp \cong J(K_\wp) \otimes K_\wp \cong H^0(X, \Omega^1_X)^*$$

(where we used $g = \mathrm{rank}_{\mathbb{Z}}(J(K))$ and that $J(K) \otimes K_\wp \cong J(K_\wp) \otimes K_\wp$) in order to give the pairing B as

$$B\colon H^0(X, \Omega^1_X)^* \times H^0(X, \Omega^1_X)^* \to \mathbb{Q}_p.$$

Comments on the theorem II

In order to make explicit the result above one needs

- to compute the vales Υ (which will depend on how bad the reduction of X can be),
- to describe $h_{\wp}(z-\infty, D_Z(b,z))$ as a locally analytic function (via, for example, iterated integrals)
- to compute the values of $h(D_i, D_j)$ for a basis $D_1, \dots, D_g$ of $J(K) \otimes \mathbb{Q}$.
- to express $D_Z(b,z)$ in terms of the basis $D_1, \dots, D_g$.

This last item one cannot hope to do it in general, but it can be done for bielliptic curves and Z coming from the bielliptic involution.

Special cases.

Balakrishnan and Dogra makes explicit height in the case Z is given by the hyperelliptic involution (which is not nice):

$$h_v(z-b, D_Z(z,b)) = h_v(z-\infty) + h_v(b - infty)$$

When X is a bielliptic genus 2 curve, and Z is a nice correspondence given by a combination of the hyperelliptic involution and bielliptic involution, then the height $h_v(z-b, D_Z(z,b))$ can be express in terms of the “classical” p-adic heights of elliptic curves (there is an algorithm of Mazur, Stein, and Tate).
One gets a version of the theorem in the case K is $\mathbb{Q}$ or a quadratic imaginary extension, and that both elliptic quotients E_i have rank 1, in terms of the p-adic heights of generators of $E_i(K)\otimes\mathbb{Q}$ and of the local p-adic heights of the E_i.
The key point is a description of $D_Z(z,b)$ in this case in terms of the bielliptic and hyperelliptic involutions.

Bielliptic curves (Balakrishnan-Dogra)

Let X be a bielliptic genus 2 curve over $\mathbb{Q}$ and $f_i : X \to E_i$ $i = 1, 2$ be the elliptic quotients given. Take $Q_i \in E_i(\overline{\mathbb{Q}})$ the branch points of f_i. p a prime of good reduction.

Then, when $((z_v)) \in \prod_{v \nmid p} X(\mathbb{Q}_v)$, the functions

$$-\sum_{v \nmid p} h_{E_i,v}(f_i(z_v) + Q_i) + h_{E_i,v}(f_i(z_v) - Q_i) - 2h_{E_{3-i},v}(f_{3-i}(z_v))$$

takes only a finite number of values Υ_i for $i = 1, 2$.

Suppose that $E_i(\mathbb{Q})$ have rank 1 and $P_i \in E_i(\mathbb{Q})$ are points of infinite order. Denote by

$$\alpha_i := \frac{h_{E_i}(P_i)}{\log_{E_i}(P_i)^2}.$$

Then $X(\mathbb{Q})$ is contained in the **finite** subset of points z in $X(\mathbb{Q}_p)$ such that

$$2h_{E_{3-i},v}(f_{3-i}(z)) - h_{E_i,p}(f_i(z) + Q_i) - h_{E_i,p}(f_i(z) - Q_i)$$

$$-2\alpha_{3-i} \log_{E_{3-i}}(f_{3-i}(z))^2 - 2\alpha_i \left(\log_{E_i}(f_i(z))^2 + \log_{E_i}(Q_i)^2\right) \in \Upsilon_i$$

The method explicitly in the modular case

In the following we suppose that $K = \mathbb{Q}$ (by simplicity), and that

- $\mathrm{End}(J) \otimes \mathbb{Q} = L$ is a field with $[L : \mathbb{Q}] = g$ (as it often happens in the modular case).
- there exists points $P_1, \ldots, P_g \in X(\mathbb{Q})$ such that

  $$\log_J(\iota(P_i)) \otimes \log_J(D_Z(P_i, b)) \in H^0(X_{\mathbb{Q}_p}, \Omega^1_X) \otimes_{L \otimes \mathbb{Q}_p} H^0(X_{\mathbb{Q}_p}, \Omega^1_X) := \mathcal{E}$$

  generates $\mathcal{E}$ as a $\mathbb{Q}_p$-vector space.
- the Hodge filtration we need for the height paring L-equivariant, so the height paring is L-equivariant: $h(\lambda D_1, D_2) = h(D_1, \lambda D_2)$.
- the curve X has potentially good reduction everywhere (as it happens for $X_s(13)$).

  Then $h(z - b, D_Z(b, z)) = \theta(z) = h_p(z - b, D_Z(b, z))$, and we only need the expression of $\theta(z)$ as a power series in every residue disc:

  $$]z[:= \{x \in C(K_\wp) | red_\wp(x) = red_\wp(z)\}$$

Then for every rational point $z \in X(\mathbb{Q})$ we have that $\iota_b(z) \otimes D_Z(b, z) \in \mathcal{E}$ is a $\mathbb{Q}_p$-linear combination of the $\iota(P_i) \otimes D_Z(P_i, b)$, so one can use this and the fact that the pairing is L-equivariant to construct a locally analytic function that is zero for the rational points.

Cohomological nice correspondence

Instead of $Z \in \mathrm{Pic}(X \times X)$, we want the corresponding $Z \in H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X)(1)$ (given as a matrix $Z = \sum_{i,j} Z_{i,j}\omega_i \otimes \omega_j$ for a basis ω_i of $H^1_{\mathrm{dR}}(X)$).
The conditions that needs to verify are

- Z maps to zero under the cup product

$$\cup : H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X) \to H^2_{\mathrm{dR}}(X)$$

- Z maps to zero under the symmetrisation

$$\cup : H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X) \to \mathrm{Sym}^2(H^1_{\mathrm{dR}}(X))$$

- $Z \in (H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X))^{\phi = p}$ where ϕ is the Frobenius.
- $Z \in \mathrm{Fil}^1(H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X))$ where Fil is the Hodge Filtration.

Any nice correspondence gives such a class, and all of them are (essentially) of this form.
Hence, if $\rho(J) > 1$, there exist such a class.
In the modular case, they will be constructed from Hecke operators.

The logarithm of the cycle D_Z.

Recall that we can describe the height paring as a paring

$$B\colon H^0(X,\Omega^1_X)^* \times H^0(X,\Omega^1_X)^* \to \mathbb{Q}_p$$

by using the integration/logarithm map.

This is useful when we are considering Z not as a correspondence, but as a cohomology class $Z \in H^0(X,\Omega^1_X) \otimes H^0(X,\Omega^1_X)$. We have

$$\log_J(D_Z(b,s)) = E_Z((z-b)) + c_{Z,b}$$

where $c_{Z,b} \in H^0(X,\Omega^1_X)^*$ is independent of z and

$$E_Z : J(\mathbb{Q}_p) \to H^0(X,\Omega^1_X)^*$$

is the map

$$E_Z(z-b) = E_Z(\log_J(z-b))$$

given by a natural associated homomorphism

$$E_Z \in \mathrm{Hom}(H^0(X,\Omega^1_X)^*, H^0(X,\Omega^1_X)^*).$$

The local pairing cohomologically

Now, the main objective is to show that $h_p(z-\infty, D_Z(b,z))$ can be described cohomologically. The idea is the following:

- $h_p(z-\infty, D_Z(b,z))$ can be described as a natural number associated to a certain mixed motive $\mathcal{M}_Z(b,z)$ (via Nekovář's paring).
- This number can be computed once we know the structure of its de Rham cohomology $M_Z(b,z)$, as filtered module and the Frobenius action.
- These structures can be computed from z, b and $Z \in H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X)$.

Explicit construction

The motive $\mathcal{M}_Z(b,z)$ can be constructed in general for given two elements in D_1 and $D_2 \in \mathrm{Div}^0(X)$ with disjoint support as a subquotient of $H^1(\overline{X} \setminus |D_1|; |D_2|)(1)$ as follows: we have a short exact sequence

$$0 \to \mathrm{Ker}\left(H^2_{|D_1|}(\overline{X}) \to H^2(\overline{X})\right)(1) \to H^1(\overline{X} \setminus |D_1|; |D_2|)(1) \to$$

$$\to \mathrm{Ker}\left(H^2_{|D_1|}(\overline{X}) \to H^2(\overline{X})\right)^* \to 0.$$

We consider then the pull-back (and push-out) for the cycle class map (and its dual)

$$cl_{D_i} : \mathbb{Q}_p \to \mathrm{Ker}\left(H^2_{|D_i|}(\overline{X}) \to H^2(\overline{X})(1)\right).$$

The important point is that $M_Z(b,z)$ can also be described from the a certain finite-dimensional quotient of the universal enveloping algebra of $\pi_1^{dR}(X,b)$ by using the theory of Maltsev completion, by using a result of Beilinson; or, more abstractly, as certain quotient of the universal 2-unipotent object on a certain categories of vector bundles with connections (which give us the de Rham structure) and overconvergent isocrystals with connections (which gives the Frobenius structure).

Explicit construction

The de Rham cohomology $M = M_Z(b, z)$ of the motive has a filtration

$$0 = M_3 \subset M_2 \subset M_1 \subset M_0 = M$$

such that $M_2 \cong \mathbb{Q}_p(1)$, $M_1/M_2 \cong H^1_{\mathrm{dR}}(X)^*$ and $M_0/M_1 \cong \mathbb{Q}_p$.
It can be described by fixing a basis of $\mathbb{Q}_p$-vector spaces giving a splitting of the filtration

$$s_0 : M \cong \mathbb{Q}_p \oplus H^1_{\mathrm{dR}}(X)^* \oplus \mathbb{Q}_p(1),$$

and two matrices

$$A_\phi := \begin{pmatrix} 1 & 0 & 0 \\ \alpha_\phi & 1 & 0 \\ \gamma_\phi & \beta_\phi & 1 \end{pmatrix} \quad A_{\mathrm{Fil}} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\mathrm{Fil}} & \beta_{\mathrm{Fil}} & 1 \end{pmatrix}$$

such that $s_0 A_\phi$ is Frobenius equivariant and $s_0 A_{\mathrm{Fil}}$ respects the filtration (the first one is unique, the second depends of a choice).
Here $\alpha : \mathbb{Q}_p \to H^1_{\mathrm{dR}}(X)^*$, $\gamma : \mathbb{Q}_p \to \mathbb{Q}_p(1)$ and $\beta : H^1_{\mathrm{dR}}(X)^* \to \mathbb{Q}_p(1)$.
The elements in A_{Fil} are “easily” computed by solving some differential equations.
The ones of A_ϕ use Tuitman’s algorithm to compute the action of Frobenius in the cohomology by Teichmüller liftings.

The local height paring explicitly

The construction of the local height paring needs the choice of a splitting $s : H^1_{\mathrm{dR}}(X)^* / \operatorname{Fil}^1 \to H^1_{\mathrm{dR}}(X)^*$, and an isomorphism $\chi : \mathbb{Q}_p(1) \to \mathbb{Q}_p$.

The splitting determines idempotents $s_1, s_2 : H^1_{\mathrm{dR}}(X)^* \to H^1_{\mathrm{dR}}(X)^*$ projecting to $H^1_{\mathrm{dR}}(X)^* / \operatorname{Fil}^1$ and Fil^1 respectively.

Then

$$\theta(z) := h_p(z - b, D_Z(b, z)) = h_p(M) = \chi(\gamma_\phi - \gamma_{\mathrm{Fil}} - \beta_\phi(s_1(\alpha_\phi)) - \beta_{\mathrm{Fil}}(s_2(\alpha_\phi)))$$

where recall that $\beta_? : H^1_{\mathrm{dR}}(X)^* \to \mathbb{Q}_p(1)$ and $s_i(\alpha_\phi) \in H^1_{\mathrm{dR}}(X)^*$, so $\beta_?(s_i(\alpha_\phi)) \in \mathbb{Q}_p(1)$.

The cursed curve

The 5 authors paper by

Jennifer S. Balakrishnan, Netan Dogra, Jan Steffen Müller, Jan Tuitman and Jan Vonk

proved that the rational points of $X_s(13) \cong X_{ns}(13)$ are the ones already known, hence completing the description of all the $X_s(p)$, p a prime.
They proved that it has potentially good reduction everywhere (i.e. at $p = 13$) and that the conditions we wrote above apply.
This curve had resisted the different approaches and it was the only one remaining after the work by Bilu, Parent and Rebolledo.
The used all the techniques explained above (plus much other ones).

No puc afegir res més
a la veritat que porto dintre.

Joan Brossa