Rational points on hyperelliptic curves via the Chabauty-Kim method

Netan Dogra
joint work with Jennifer Balakrishnan, Steffen Müller and Alex Betts

September 8, 2017

Diophantine geometry of hyperelliptic curves

- $y^2 = f(x)$ a hyperelliptic curve of genus g.
- How do we find the rational number solutions to this equation?
- Answer is hidden in the equation

$$\phi^* \omega_i = \sum M_{ij} \omega_j + df_i.$$

  and the stable models at primes of bad reduction.
- Sometimes.

Chabauty-Coleman revisited

Fix p a prime of good reduction, and $b \in X(\mathbb{Q})$. Let J denote the Jacobian, and r the rank of J.

- Recall the idea of the Chabauty-Coleman method: we have g functions $\int_b \omega_i$. If the rank of J is less than g, then on rational points there is a nontrivial linear relation $\sum \lambda_i \int_b \omega_i = 0$ between these functions.
- However the map

$$\left(\int_b \omega_0, \ldots, \int_b \omega_{g-1}\right) : X(\mathbb{Q}_p) \to \mathbb{Q}_p^g,$$

restricted to each residue disk, has Zariski dense image and is given by a power series.

Hence $X(\mathbb{Q})$ is contained in the finite set $\{z \in X(\mathbb{Q}_p) : \sum \lambda_j \int_b^z \omega_i = 0\}$.

Quadratic Chabauty: The idea

What happens when the rank is equal to the genus?
Suppose we can find

- a function $F : X(\mathbb{Q}_p) \to \mathbb{Q}_p$
- An endomorphism $E \in \mathrm{End}(J(\mathbb{Q}_p), J(\mathbb{Q}_p)) \otimes \mathbb{Q}_p$.
- a vector $c \in J(\mathbb{Q}_p) \widehat{\otimes} \mathbb{Q}_p$,
- a bilinear map $B : J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \to \mathbb{Q}_p$
- A finite set $\Omega \subset \mathbb{Q}_p$

such that

- For all $z \in X(\mathbb{Q})$, $F(z) - B(z - b, E(z - b) + c) \in \Omega$.
- For all $x \in X(\mathbb{F}_p)$, $(\int_b \omega_0, \dots, \int_b \omega_{g-1}, F)$, restricted to $]x[$, has Zariski dense image and is given by power series.

Then $X(\mathbb{Q})$ is contained in the finite set $\{F(z) - B(z - b, E(z - b) + c) \in \Omega\} \subset X(\mathbb{Q}_p)$. Call (F, Ω) a *quadratic Chabauty pair*.

An example: Quadratic Chabauty for integral points on hyperelliptic curves

Theorem (Balakrishnan, Besser, Müller)

Let X be a hyperelliptic curve with a monic odd degree model, and define $Y = X - \infty$. Let Ω be the finite set

$$\{\sum_{v \nmid p} h_v(P_v) : (P_v) \in \prod_{v \nmid p} Y(\mathbb{Z}_v)\}.$$

Then (h_p, Ω) is a quadratic Chabauty pair for $Y(\mathbb{Z})$.

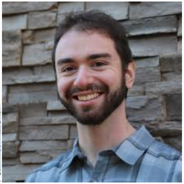
This generalised previous work of Balakrishnan, Kedlaya and Kim on integral points on elliptic curves.

Generalisations

Goal of this talk: explain how to use quadratic Chabauty to find rational points on curves.

This is just the simplest nontrivial case of using Kim's nonabelian Chabauty method: the generalisation of $\int \omega_i, F$ is given by an analytic map $X(\mathbb{Q}_p) \to H^1_f(G_p, U_n)$, and the analogue of this map satisfying nontrivial polynomial relations on $X(\mathbb{Q})$ is the nondominance of the localisation map $\mathrm{Sel}(U_n) \to H^1_f(G_p, U_n)$.

By a theorem of Ellenberg and Hast, the Chabauty-Kim method explains finiteness of all hyperelliptic curves over $\mathbb{Q}$.



Example 1: $J \sim E_1 \times E_2, r = g = 2$

(joint with Balakrishnan, Müller)

$$X = X_0(37)/\mathbb{Q}(i) : y^2 = x^6 - 9x^4 + 11x^2 + 37.$$

with maps f_i to E_i where

$$\begin{array}{cc} E_1 : y^2 = x^3 - 16x + 16 & E_2 : y^2 = x^3 - x^2 - 373x + 2813. \\ f_1(x,y) = (x^2 - 3, y) & f_2(x,y) = (37x^{-2} + 4, 37x^{-3}) \end{array}$$

F can be taken to be

$$2h_{E_2,\mathfrak{p}}(f_2(z)) - h_{E_1,\mathfrak{p}}(f_1(z) + (-3, \sqrt{37})) - h_{E_1,\mathfrak{p}}(f_1(z) + (-3, -\sqrt{37}))$$

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

We find $X(\mathbb{Q}(i)) = \{(\pm 2 : \pm 1), (\pm i, \pm 4), \infty^{\pm}\}$.

Example 2: $\mathrm{End}^0(J) \simeq \mathbb{Q}(\sqrt{5})$, $r = g = 2$

$$X : y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1.$$

Then we may take

$$F(z) = -4x(z) - 4 + \sum_{0 \le i,j \le 3} Z_{ij} \int_b^z \omega_i \omega_j - \sum_{0 \le i \le 1, 0 \le j \le 3} Z_{ij} \left(\int_b^z \omega_i\right)\left(\int_{w(b)}^z \omega_j\right)$$

and $\Omega = \{0, \frac{4}{3}\log(2), \frac{8}{3}\log(2)\}$, where

$$Z = \begin{pmatrix} 0 & -6 & 8 & -6 \\ 6 & 0 & -6 & 12 \\ -8 & 6 & 0 & 0 \\ 6 & -12 & 0 & 0 \end{pmatrix}$$

Then $X(\mathbb{Q}) = \{(0, \pm 1), (1, \pm 1), (-1, \pm 1), (2, \pm 5), (4, \pm 29), \infty\}$.
In practice to compute this we worked with a different choice of F so that the associated bilinear form is K-linear.

(A nonhyperelliptic example) $\mathrm{End}^0(J) = \mathbb{Q}(\zeta_7)^+$, $r = g = 3$

(joint work with Balakrishnan, Müller, Jan Tuitman, Jan Vonk).
$X = X_s^+(13)$: smooth plane quartic

$$Y^4 + 5X^4 - 6X^2Y^2 + 6X^3Z + 26X^2YZ + 10XY^2Z - 10Y^3Z - 32X^2Z^2$$
$$- 40XYZ^2 + 24Y^2Z^2 + 32XZ^3 - 16YZ^3 = 0$$

- J has rank 3.
- Potential good reduction everywhere.
- There are two quadratic Chabauty pairs $(F_1, \{0\})$ and $(F_2, \{0\})$, which can be computed using Tuitman's algorithm.

We find $X_s^+(13) = \{(1:1:1), (1:1:2), (0:0:1), (-3:3:2), (1:1:0), (0:2:1), (-1:1:0)\}$.

What's going on?

Now suppose we have a hyperelliptic curve with an odd degree model. Suppose $\rho(J_{\mathbb{Q}}) = \rho(J_{\mathbb{Q}_p}) > 1$. The function F is constructed by first finding an element $Z = \sum Z_{ij}[\omega_i] \otimes [\omega_j] \in H^1(X_{\mathbb{Q}_p}) \otimes H^1(X_{\mathbb{Q}_p})$ be in the image of the cycle class map (we also need this Z to satisfy $\sum Z_{ij}[\omega_i] \cup [\omega_j] = 0$ and $Z \neq Z^t$).

- The p-adic Lefschetz (1,1) theorem implies the image of the cycle class map is exactly equal to $(F^1(H^1 \otimes H^1)) \cap (H^1 \otimes H^1)^{\phi = p}$.
- Let $\mathcal{A}$ denote the vector bundle $\mathcal{O}_Y^8$, with connection $d + \Lambda$, where

$$\Lambda = \begin{pmatrix} 0 & 0 & 0 \\ \boldsymbol{\omega} & 0 & 0 \\ 0 & \boldsymbol{\omega}^t Z & 0 \end{pmatrix}$$

This connection carries a canonical F-structure (once you fix a basepoint), which can be computed using Kedlaya's algorithm.

From $\mathcal{A}$ to F

By computing the F-structure (and a certain canonical filtration) on $\mathcal{A}$, we get away to associate to each $z \in X(\mathbb{Q}_p)$ a $\mathbb{Q}_p$-vector space equipped with a filtration and an automorphism (a *filtered ϕ-module*).
To get F, we apply Nekovar's p-adic height function on categories of Galois representations/filtered ϕ-modules:

$$J \rightsquigarrow \rho_V$$

$$D \in J(\mathbb{Q}) \rightsquigarrow \begin{pmatrix} 1 & 0 \\ * & \rho_V \end{pmatrix}$$

$$D_1, D_2 \in \mathrm{Div}^0(X) \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ * & \rho_V & 0 \\ * & * & \chi \end{pmatrix}$$

Kim's theory + Nekovar's theory implies that $F + \Omega$ is bilinear, giving the quadratic Chabauty pair. The set Ω is the image of $\prod_{v \neq p} X(\mathbb{Q}_v)$ under a sum of local height functions $\sum F_v$, which are locally constant and trivial at primes of good reduction.

A theorem

Theorem (Balakrishnan, D.)

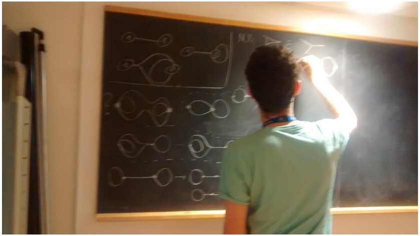
Suppose $\mathrm{NS}(J_{\mathbb{Q}}) > 1$*,* $r = g$*,* p *is a prime of good reduction, and the* p*-adic closure of* $J(\mathbb{Q})$ *in* $J(\mathbb{Q}_p)$ *is finite index. Define* $F : z \mapsto h_p(A(z))$*. Then there are locally constant functions* $F_v : X(\mathbb{Q}_v) \to \mathbb{Q}_p$ *which are identically zero for all prime of potential good reduction for* X *such that* $(F, (\sum F_v) \prod_{v \neq p}) X(\mathbb{Q}_v)$ *is a quadratic Chabauty pair.*

Another characterisation is that $F_v(z) = h_v(z - b, C \cap (\Delta_X - X \times \{b\} - \{z\} \times X))$, where C is a correspondence with cycle class Z.

Local computations at v prime to p.

(joint work with Alex Betts)

It remains to describe how to compute F_v in general. It turns out this can be reduced to computing a stable model!



Lemma (Betts, D.)

The local maps $F_v : X(\mathbb{Q}_v) \to \mathbb{Q}_p$ factor through the irreducible components of a regular semistable model.

Also get a recipe for computing the functions in terms of a graph of groups canonically associated the dual graph.

Thank you!