

2020/05/26, 10:00 CEST, Bas Edixhoven, 50 minutes + questions. ☺.
Number Theory Web Seminar.

Geometric Quadratic Chabauty, joint work with

(\exists pdf document with some links on my homepage, under "Talks".)

Guido Lido.

Problem to be addressed: proving that a given list of solutions in \mathbb{Q}^2 of a polynomial equation $f(x, y) = 0$ is complete.

a.k.a. $X_{(13)_5}^+$ and $X_{(13)_{ns}}^+$

Example: the "cursed curve" given by:

$$-(y+1) \cdot x^3 + (2y^2+y) \cdot x^2 + (-y^3+y^2-2y+1) \cdot x + (2y^2-3y) \cdot 1 = 0,$$

and the list: $(0, 0)$, $(1, 0)$, $(-1, 0)$, $(0, \frac{3}{2})$,

$(1:0:0)$, $(1:1:0)$ and $(0:1:0)$.

This curve was number 1 on the "most wanted list".

It resisted all attackers, whatever tools they brought, until 2017 (Annals of math. 2019), when Balakrishnan, Dogra, Müller, Tuitman & Vonk applied their newest weapon, "quadratic Chabauty", the simplest non-linear case of Minhyong Kim's "non-abelian Chabauty method".

Aim of this talk: give a geometric description of that method.

Note: on July 16 Balakrishnan gives a talk in this seminar, maybe on a closely related subject.

Setup for Chabauty's method.

1

$C :=$ a non-singular projective curve over \mathbb{Q} , geometrically irreducible, with a point $b \in C(\mathbb{Q})$, genus $g \geq 2$.

Faltings: $C(\mathbb{Q})$ is finite. But his proof is hard to use for showing that a list of known points is complete.

What to do? Linearise! Use the jacobian J of C .

J is an abelian variety over \mathbb{Q} . \swarrow lattice \searrow g -dim'l \mathbb{C} -vec.sp.

As complex analytic variety: $H_1(C(\mathbb{C}), \mathbb{Z}) \hookrightarrow \mathbb{C} \otimes_{\mathbb{Q}} \Omega^1(C)^{\vee} \twoheadrightarrow J(\mathbb{C})$.
 $[\gamma] \mapsto \left(\omega \mapsto \int_{\gamma} \omega \right)$

Abel-Jacobi map: $C(\mathbb{C}) \xrightarrow{j_b} J(\mathbb{C})$, embedding.
 $P \mapsto \left[\left(\omega \mapsto \int_b^P \omega \right) \right]$.

J as an algebraic variety / \mathbb{Q} .

\swarrow degree 0 divisors on $C_{\overline{\mathbb{Q}}}$

$\overline{\mathbb{Q}} \subset \mathbb{C}$ algebraic closure of \mathbb{Q} .

$J(\overline{\mathbb{Q}}) = \left\{ D: C(\overline{\mathbb{Q}}) \rightarrow \mathbb{Z} : \sum_{P \in C(\overline{\mathbb{Q}})} D(P) = 0 \right\}$
for almost all $P \in C(\overline{\mathbb{Q}}): D(P) = 0$

principal divisors: for f a non-zero rat. function on $C_{\overline{\mathbb{Q}}}$: $P \mapsto \text{ord}_P(f)$.

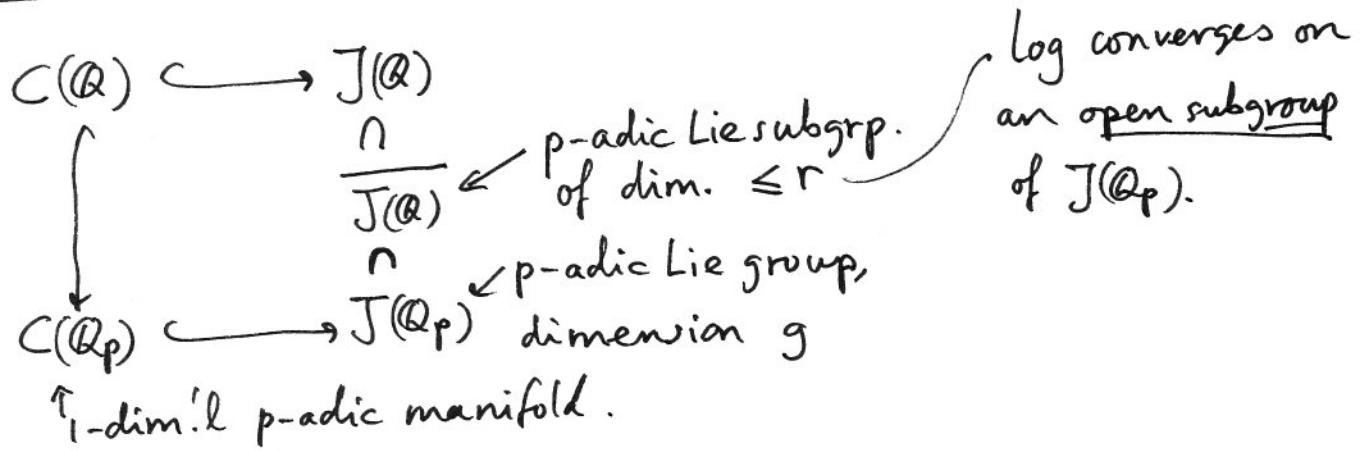
Then $C(\overline{\mathbb{Q}}) \xrightarrow{j_b} J(\overline{\mathbb{Q}})$, $P \mapsto [P - b]$.

Mordell-Weil group: $J(\mathbb{Q})$. Mordell-Weil Thm: $J(\mathbb{Q})$ is finitely generated.
Mordell-Weil rank: $r_0 = \cong \mathbb{Z}^r \oplus \text{finite}$

New problem: decide which $P \in J(\mathbb{Q})$ are in $C(\mathbb{Q})$.

2.

Chabauty's idea: take a prime p , use \mathbb{Q}_p .
in case $r < g$.



If $r < g$ then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ finite, contains $C(\mathbb{Q})$, can do computations with finite p-adic precision, and if necessary vary p (Mordell-Weil sieve...).

What to do if $r \geq g$? (For cursed curve: $r = g = 3$.)

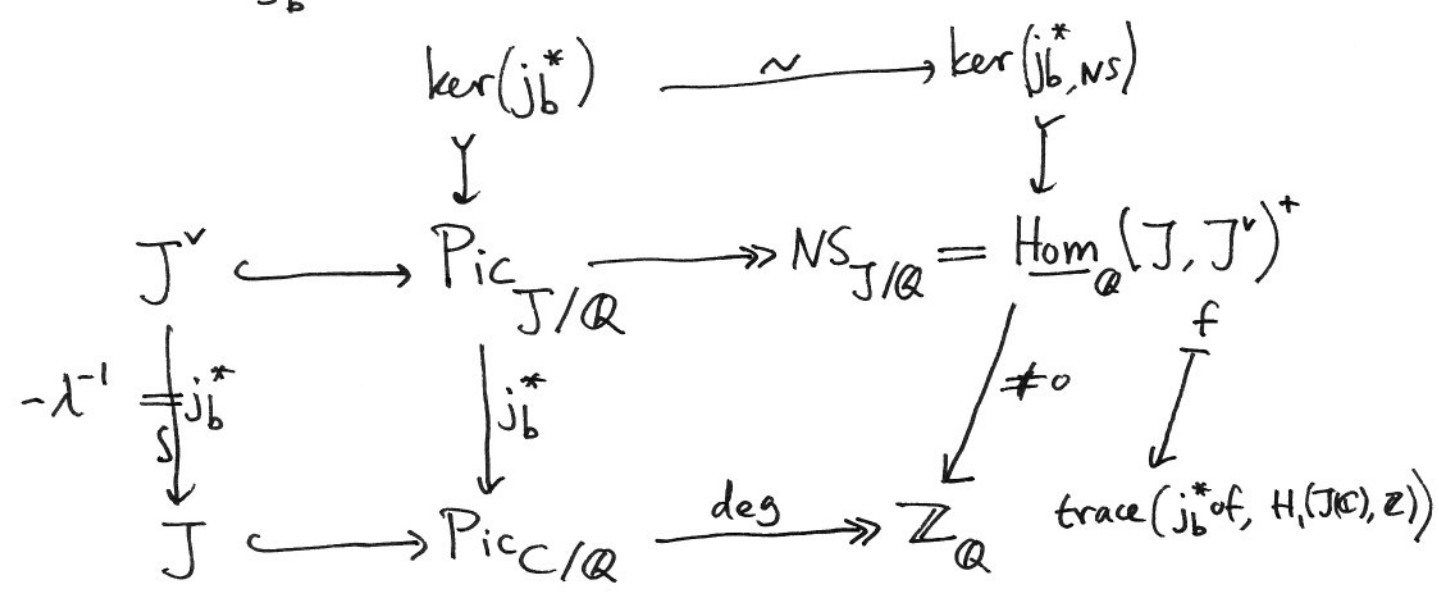
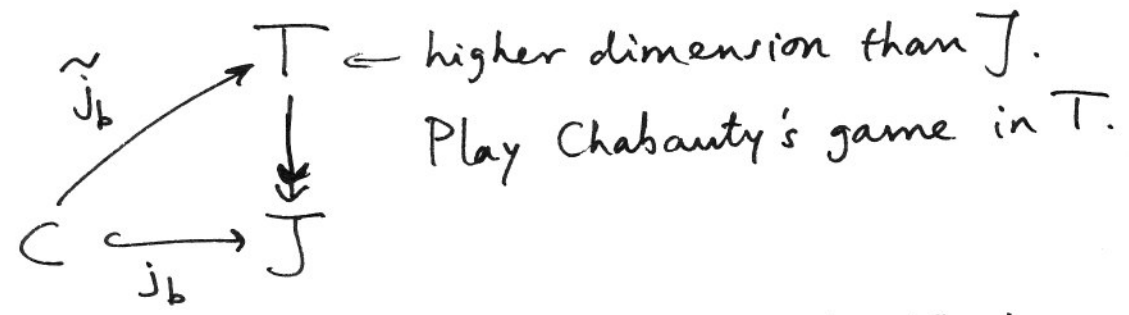
Minhyong Kim: well, J corresp. to $H_1(C(\mathbb{C}), \mathbb{Z}) = \pi_1(C(\mathbb{C}))^{ab}$; one should use non-abelian quotients of $\pi_1(C(\mathbb{C}))$, think of descending central series $G/[G, G]$, $G/[G, [G, G]]$,

Approach 1: abandon J ("J is bad"), and use (non-abelian) p-adic Hodge theory and all that.

Approach 2: improve J !

How to improve J?

Take G_m -torsors on J : line bundles minus the zero-section.



Picard number of J : ρ , with $NS_{J/Q}(\mathbb{Q}) = \text{Hom}_{\mathbb{Q}}(J, J^v)^+ \cong \mathbb{Z}^{\rho}$.

So: $\ker(j_{b,NS}^*)(\mathbb{Q}) \cong \mathbb{Z}^{\rho-1}$.

Take a basis of this: $f_1, \dots, f_{\rho-1}$.

One also gets $c_1, \dots, c_{\rho-1}$ in $J^v(\mathbb{Q})$.

And G_m -torsors $T_1, \dots, T_{\rho-1}$ on J that are trivial on C .

Then $T :=$ the product of $T_1, \dots, T_{\rho-1}$, over J , a $G_m^{\rho-1}$ -torsor.

$$\dim(T) = g + \rho - 1.$$

Hope: if $r < g + \rho - 1$, then can successfully play Chabauty's game.

But there is a problem: $T(\mathbb{Q})$ is a $\mathbb{Q}^{\times, p^{-1}}$ -torsor, 4.
 \downarrow
 $J(\mathbb{Q})$ $T(\mathbb{Q})$ is awfully big!

Solution: do everything over \mathbb{Z} . As $\mathbb{Z}^{\times, p^{-1}} = \{\pm 1\}^{p-1}$ is finite, we can hope that $T(\mathbb{Z}) \subset \overline{T(\mathbb{Z})} \subset T(\mathbb{Z}_p)$
 \uparrow
 p -adic manifold $\dim. \leq r$.

Thm. 4.10 of the arxiv preprint "GQC" gives local parametrisations $\mathbb{Z}_p^r \xrightarrow{\kappa} \overline{T(\mathbb{Z})} \subset T(\mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p^{g+p-1}$
 \uparrow locally \uparrow locally

This uses very much the biextension structure of the Poincaré $\widehat{\mathbb{G}_m}$ -torsor on $J \times J^\vee$.

Thm. 4.12 says how to use this to bound the fibres of $C(\mathbb{Q}) = C(\mathbb{Z}) \rightarrow C(\mathbb{F}_p)$, using only computations involving $C(\mathbb{Z}/p^2\mathbb{Z})$, $T(\mathbb{Z}/p^2\mathbb{Z})$, (2-digits of p -adic precision).

Remarks 4.13 - 4.15 say that we hope and expect that this gives sharp "upper bounds" for $C(\mathbb{Q})$, if $r < g + p - 1$.

§ 6-7 make the whole process explicit, for computer computations.

§ 8 is an example ($g = r = p = 2$) by Guido.
 (bielliptic)

Back to $\pi_1(C(\mathbb{C})) =: G$.

Which quotient of it have we now used?

(After Arizona Winter School, Mazur made me think about this.)

$$\begin{array}{ccccc}
 G/[G, G] & \longleftarrow & G/[G, [G, G]] & \longleftarrow & \frac{[G, G]}{[G, [G, G]]} \\
 \parallel & & & & \parallel \\
 H_1(J(\mathbb{C}), \mathbb{Z}) & & & & \frac{H_2(J(\mathbb{C}), \mathbb{Z})}{H_2(C(\mathbb{C}), \mathbb{Z})} \\
 \parallel & & \mathbb{Z} \binom{2g}{2}^{-1} \cong & \nearrow & \\
 H_1(K(\mathbb{C}), \mathbb{Z}) & & & &
 \end{array}$$

has a Hodge structure of weight 0 (do Tate twist), we use the largest quotient that has type (0,0) and trivial Galois action.

Thank you for your attention!

Questions?