2020/05/26, 10:00 CEST, Bas Edixhoven, 50 minutes + questions. 0.

Number Theory Web Seminar.

Geometric Quadratic Chabauty, joint work with Guido Lido.

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

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. $X(13)_s^+$ 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: $(0,0)$, $(1,0)$, $(-1,0)$, $(0,3/2)$,

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

This curve was number 1 on the "most wanted list". It resisted all attackers, whatever tools the 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.

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

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 $\mathbb{Q}$.

$$\underset{\text{lattice}}{H_1(C(\mathbb{C}),\mathbb{Z})} \hookrightarrow \underset{g\text{-dim'l } \mathbb{C}\text{-vect.sp.}}{\mathbb{C}\otimes_{\mathbb{Q}} \Omega^1(C)^\vee} \twoheadrightarrow J(\mathbb{C}).$$

As complex analytic variety:

$$[\gamma] \longmapsto \left(\omega \mapsto \int_\gamma \omega\right)$$

Abel-Jacobi map: $C(\mathbb{C}) \xhookrightarrow{j_b} J(\mathbb{C})$, embedding.

$$P \longmapsto \left[\left(\omega \mapsto \int_b^P \omega\right)\right].$$

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

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

$$J(\overline{\mathbb{Q}}) = \frac{\underbrace{\left\{ D : C(\overline{\mathbb{Q}}) \to \mathbb{Z} : \begin{array}{l} \text{for almost all } P\in C(\overline{\mathbb{Q}}): D(P)=0 \\ \sum_{P\in C(\overline{\mathbb{Q}})} D(P) = 0 \end{array} \right\}}_{\text{degree 0 divisors on } C_{\overline{\mathbb{Q}}}}}{\text{principal divisors: for } f \text{ a non-zero rat. function on } C_{\overline{\mathbb{Q}}}:\ P \mapsto \mathrm{ord}_P(f).}$$

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 $\cong \mathbb{Z}^r \oplus$ finite

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

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

$$
\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook] \arrow[dd] & J(\mathbb{Q}) \arrow[d, phantom, "\cap"] \\
 & \overline{J(\mathbb{Q})} \arrow[d, phantom, "\cap"] \\
C(\mathbb{Q}_p) \arrow[r, hook] & J(\mathbb{Q}_p)
\end{tikzcd}
$$

p-adic Lie subgrp. of dim. $\leq r$

log converges on an <u>open subgroup</u> of $J(\mathbb{Q}_p)$.

p-adic Lie group, dimension g

1-dim'l p-adic manifold.

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 $r \geqslant g$? (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 $\mathbb{G}_m$-torsors on J: line bundles minus the zero-section.

$$\begin{tikzcd}
 & T \arrow[d, two heads] \\
C \arrow[ur, "\tilde{j}_b"] \arrow[r, hook, "j_b"'] & J
\end{tikzcd}$$

T ← higher dimension than J.
Play Chabauty's game in T.

$$\begin{tikzcd}
 & \ker(j_b^*) \arrow[rr, "\sim"] \arrow[d, tail] & & \ker(j_{b,NS}^*) \arrow[d, tail] & \\
J^\vee \arrow[r, hook] \arrow[d, "j_b^*", "-\lambda^{-1} \ \wr"'] & \mathrm{Pic}_{J/\mathbb{Q}} \arrow[rr, two heads] \arrow[d, "j_b^*"] & & NS_{J/\mathbb{Q}} = \underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+ \arrow[d, "\neq 0"] & f \arrow[d, mapsto] \\
J \arrow[r, hook] & \mathrm{Pic}_{C/\mathbb{Q}} \arrow[rr, two heads, "\deg"] & & \mathbb{Z}_{\mathbb{Q}} & \mathrm{trace}(j_b^* \circ f, H_1(J(\mathbb{C}), \mathbb{Z}))
\end{tikzcd}$$

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

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

Take a basis of this: $f_1, \ldots, f_{\rho-1}$.
One also gets $c_1, \ldots, c_{\rho-1}$ in $J^\vee(\mathbb{Q})$.
And $\mathbb{G}_m$-torsors $T_1, \ldots, T_{\rho-1}$ on J that are trivial on C.
Then $T :=$ the product of $T_1, \ldots, T_{\rho-1}$, over J, a $\mathbb{G}_m^{\rho-1}$-torsor.

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

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

But there is a problem: $\begin{array}{c} T(\mathbb{Q}) \\ \downarrow \\ J(\mathbb{Q}) \end{array}$ is a $\mathbb{Q}^{\times,\rho-1}$-torsor, $T(\mathbb{Q})$ is awfully big!

Solution: do everything over $\mathbb{Z}$. As $\mathbb{Z}^{\times,\rho-1} = \{\pm 1\}^{\rho-1}$ 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 $\mathbb{Z}_p^r \xrightarrow{\kappa} \overline{T(\mathbb{Z})} \subset T(\mathbb{Z}_p) \underset{\text{locally}}{\simeq} \mathbb{Z}_p^{g+\rho-1}$

$\uparrow$ locally.

This uses very much the biextension structure of the Poincaré torsor on $J \times J^\vee$.

$\mathbb{G}_m$

Thm. 4.12 says how to use this to bound the fibres of $C(\mathbb{Q}) = C(\mathbb{Z}) \longrightarrow C(\mathbb{F}_p)$, 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 $r < g+\rho-1$.

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

§ 8 is an example ($g = r = \rho = 2$) 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.)

$$\begin{array}{ccccc}
G/[G,G] & \twoheadleftarrow & G/[G,[G,G]] & \hookleftarrow & \dfrac{[G,G]}{[G,[G,G]]} \\
\| & & & & \| \\
H_1(J(\mathbb{C}),\mathbb{Z}) & & \mathbb{Z}^{\binom{2g}{2}-1} & \cong & \dfrac{H_2(J(\mathbb{C}),\mathbb{Z})}{H_2(C(\mathbb{C}),\mathbb{Z})} \\
\| & & & & \\
H_1(C(\mathbb{C}),\mathbb{Z}) & & & &
\end{array}$$

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?