Generalised Symmetric Chabauty for cubic points on modular curves with infinitely many quadratic points

Stevan Gajović (University of Groningen/MPIM Bonn)
Joint work with Josha Box (at the time, University of Warwick) and Pip Goodman (at the time, University of Bristol)

Rational Points 2022,
29/03/2022

Introduction

- Let X be a nice curve (smooth, projective, geometrically irreducible algebraic variety of dimension 1) defined over $\mathbb{Q}$ of genus g (or g_X if we specify a curve).
- Denote by $X^{(d)} := X^d/S_d$ the dth symmetric power of X.
- $\{\mathbb{Q}$-rational points on $X^{(d)}\} \simeq \{\mathbb{Q}$-rational effective degree d divisors on $X\}$.
- In other words:

$$X^{(d)}(\mathbb{Q}) = \{Q_1 + \cdots + Q_d : Q_1, \ldots, Q_d \in X(\overline{\mathbb{Q}}),$$
$$(\forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))\ \sigma(Q_1 + \cdots + Q_d) = Q_1 + \cdots + Q_d\}.$$

- If $X^{(d)}(\mathbb{Q})$ is finite (and in some other cases), knowing $X^{(d)}(\mathbb{Q}) \implies$ knowing all points $X(L)$ for all extensions $L/\mathbb{Q}$ of degree d.

Motivation

- Study points on symmetric powers of modular curves.

(1) Extending Mazur's results on classifying potential torsion subgroups and isogenies of elliptic curves defined over $\mathbb{Q}$ to number fields.

- Determine non-cuspidal points on modular curves $X_0(N)$ and $X_1(N)$;
- Work of Banwait, Bruin, Derickx, Etropolski, Kamienny, Michaud-Jacobs, Momose, Morrow, Najman, Stein, Stoll, van Hoeij, Vukorepa, Zureick-Brown, ...

(2) Extending modularity statements from $\mathbb{Q}$ to number fields:

- Freitas, Le Hung, Siksek - real quadratic fields;
- Derickx, Najman, Siksek - totally real cubic fields;
- Box - quartic fields not containing $\sqrt{5}$.

Symmetric Chabauty

- Klassen, "Algebraic points of low degree on curves of low rank", PhD thesis (1993)
- Siksek, "Chabauty for symmetric powers of curves" (2009)
- Let p be a prime of good reduction for curve X.
- Denote the reduction modulo p map by red_p of by a tilde on points.
- Let $\widetilde{\mathcal{Q}} \in X^{(d)}(\mathbb{F}_p)$. Its inverse image under red_p, denoted by $D(\widetilde{\mathcal{Q}}) \subseteq X^{(d)}(\mathbb{Q}_p)$, is called a residue class of $\widetilde{\mathcal{Q}}$.
- Similarly, for $\mathcal{Q} \in X^{(d)}(\mathbb{Q}_p)$ we denote $D(\mathcal{Q}) := D(\widetilde{\mathcal{Q}})$.
- Let $J(X)$ be the Jacobian of X. Denote by r (or r_X when we specify a curve) the rank of $J(X)(\mathbb{Q})$.
- Assume there is $\mathcal{Q} \in X^{(d)}(\mathbb{Q})$. Use $\mathcal{Q}$ to define an Abel-Jacobi map $\iota \colon X^{(d)} \to J(X)$, $\mathcal{P} \mapsto \mathcal{P} - \mathcal{Q}$.

The diagram of symmetric Chabauty

$$\begin{tikzcd} D(\widetilde{\mathcal{P}}) \cap X^{(d)}(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(X)(\mathbb{Q}) \arrow[d] \\ D(\widetilde{\mathcal{P}}) \arrow[r, "\iota"] & J(X)(\mathbb{Q}_p) \end{tikzcd}$$

- To determine $X^{(d)}(\mathbb{Q})$ it suffices to determine its intersection with each of its residue classes.
- If the condition $r + d \leq g$ is satisfied, then we can hope for finitely many points of $X^{(d)}(\mathbb{Q})$.
- When $d = 1$, using the classical method of Chabauty and Coleman, the set $\iota(D(\widetilde{\mathcal{P}})) \cap \overline{J(X)(\mathbb{Q})}$ is finite and we can determine it.
- Problem: Even if $r + d \leq g$, the set $\iota(D(\widetilde{\mathcal{P}})) \cap \overline{J(X)(\mathbb{Q})}$ might not be finite when $d \geq 2$.

However

- Consider a hyperelliptic curve $X : y^2 = f(x)$.
- Denote $\rho : X \to \mathbb{P}^1$, $\rho(x, y) = x$.
- For all $x_0 \in \mathbb{P}^1(\mathbb{Q})$, we have

$$\rho^*(x_0) = (x_0, \sqrt{f(x_0)}) + (x_0, -\sqrt{f(x_0)}) \in X^{(2)}(\mathbb{Q})!$$

$\implies$ We see that $X^{(2)}(\mathbb{Q})$ can be infinite regardless of r!

- There is a morphism $X \to \mathbb{P}^1$ or $X \to E$ of degree at most d, where $E/\mathbb{Q}$ is an elliptic curve of rank $r \geq 1 \implies X^{(d)}(\mathbb{Q})$ is infinite.
- $P \in X^{(d)}(\mathbb{Q})$ not coming from the previous maps, and such that $\iota(P)$ does not lie in any translate of a positive rank abelian subvariety of $J(X)$ contained in $\iota(X^{(d)})$ is called an isolated point.

Theorem (Bourdon, Ejder, Liu, Odumodu, Viray (2019))

There are finitely many isolated points.

What then we do?

- Studying $X^{(d)}(\mathbb{Q})$ amounts to:

(1) Describe all infinite subsets of $X^{(d)}(\mathbb{Q})$;

(2) Find the finite set of isolated points of $X^{(d)}(\mathbb{Q})$.

- There is a subspace $\mathcal{V} \subset H^0(X, \Omega_{X/\mathbb{Q}})$, $\dim(\mathcal{V}) \geq g - r$, such that for all $\omega \in \mathcal{V}$, we have (the integral is Coleman integral)

$$\int_D \omega = 0 \text{ for all } D \in \overline{J(\mathbb{Q})}.$$

- $\mathcal{V}$ is called the space of vanishing differentials.
- In principle, if $r + d \leq g$, get d equations on a d-dimensional space.
- Siksek: A criterion whether $\mathcal{Q} \in X^{(d)}(\mathbb{Q})$ is alone in its residue class, i.e., if $D(\mathcal{Q}) \cap X^{(d)}(\mathbb{Q}) = \{\mathcal{Q}\}$.

- Assume there is a morphism of curves $\rho : X \to C$ over $\mathbb{Q}$ of degree d.
  - It induces the trace map $\mathrm{Tr}_\rho : H^0(X, \Omega_{X/\mathbb{Q}}) \to H^0(C, \Omega_{C/\mathbb{Q}})$.
  - There is an abelian variety $A/\mathbb{Q}$ such that $J(X) \sim J(C) \times A$.
- Define $\mathcal{W} := \mathcal{V} \cap \ker(\mathrm{Tr}_\rho)$ the space of vanishing differentials with trace zero.
- Use this space to "disregard" C, and replace the $J(X)$ to A in the Chabauty diagram, obtain the rank condition $r_X - r_C \leq g_X - g_C - d$.
- Siksek: A criterion whether a residue class of $\mathcal{Q} \in \rho^*(C^{(d)}(\mathbb{Q})) \subseteq X^{(d)}(\mathbb{Q})$ consists only of the pull-back points, i.e., if $D(\mathcal{Q}) \cap X^{(d)}(\mathbb{Q}) \subseteq \rho^*(C^{(d)}(\mathbb{Q}))$.
- For $d' > d$, such that $X^{(d'-d)}(\mathbb{Q}) \neq \emptyset$, we also have that $X^{(d')}(\mathbb{Q})$ is infinite. Consider $\mathcal{Q} = \mathcal{Q}_1 + \mathcal{Q}_2$, such that $\mathcal{Q}_1 \in X^{(d'-d)}(\mathbb{Q})$ and $\mathcal{Q}_2 \in \rho^*(C^{(d)}(\mathbb{Q}))$. There was no known criterion to describe $D(\mathcal{Q}) \cap X^{(d)}(\mathbb{Q})$.

Our concrete case

Theorem (Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown (2020))

Completed the classification of the finite groups which appear as a torsion subgroup of $E(K)$ for K a cubic number field and E/K an elliptic curve.

- In their work they wanted to determine $X_1(65)^{(3)}(\mathbb{Q})$.
- We could use the knowledge of $X_0(65)^{(3)}(\mathbb{Q})$ to determine $X_1(65)^{(3)}(\mathbb{Q})$.
- We know that $X_0(65)(\mathbb{Q}) = \{\text{four cusps}\}$.
- ω_{65} is the Atkin-Lehner involution of $X_0(65)$.
- Denote $X_0(65)^+ := X_0(65)/\omega_{65}$, and $\rho_{65} : X_0(65) \to X_0(65)^+$ the quotient map.
- $\rho_{65} : X_0(65) \to X_0(65)^+$ is a map of degree 2.

Our concrete case

- $X_0(65)^+$ is an elliptic curve of rank 1 over $\mathbb{Q}$.
- $\implies X_0(65)^{(2)}(\mathbb{Q})$ is infinite!

Theorem (Box (2020))

$X_0(65)^{(2)}(\mathbb{Q}) = \rho_{65}^*(X_0(65)(\mathbb{Q})^+) +$ *sums of cusps.*

Question (David Zureick-Brown, AWS 2020)

Can you determine $X_0(65)^{(3)}(\mathbb{Q})$ despite the fact that $X_0(65)^{(2)}(\mathbb{Q})$ is infinite?

Main theorem, special case, setup

Theorem (Box-G.-Goodman, 2022)

- *$\rho : X \to C$ morphism of curves defined over $\mathbb{Q}$.*
- $\deg(\rho) \leq 3$, $\#C(\mathbb{Q}) = \infty$.
- *$p \geq 11$ prime of good reduction.*
- *Denote by $\omega_1, \ldots, \omega_s$ the basis of $\mathcal{W}$.*
- *Let $\mathcal{Q} = Q_1 + Q_2 + Q_3 \in X^{(3)}(\mathbb{Q})$.*
- *For each i, let t_{Q_i} be a well-behaved uniformiser at Q_i.*
- *$\mathcal{K} := \mathbb{Q}_p(Q_1, Q_2, Q_3)$, π any generator of the maximal ideal in $\mathcal{K}$.*
- *The expansion of ω_j at $\widetilde{Q_i} := Q_i$ reduced modulo π is*

$$\omega_j = \sum_{l=0}^{\infty} \widetilde{a}_l(\omega_j, i)\widetilde{t}_{Q_i}^{l} d\widetilde{t}_{Q_i}.$$

Main theorem, special case, cases

Theorem (Box-G.-Goodman, 2022)

- *There are pull-back divisors in $\mathcal{Q}$, $\deg(\rho) = 2$ (generalisation of the case from Siksek, 2009).*

(a) *Assume $\widetilde{Q_1} \neq \widetilde{Q_2}$, $Q_1 + Q_3 = \rho^*(R)$ for some $R \in C(\mathbb{Q})$, and that the matrix*

$$\begin{pmatrix} \widetilde{a}_0(\omega_1, 1) & \widetilde{a}_0(\omega_1, 2) \\ \widetilde{a}_0(\omega_2, 1) & \widetilde{a}_0(\omega_2, 2) \end{pmatrix}$$

has rank 2.

- *Let $\mathcal{P} \in X^{(3)}(\mathbb{Q})$ be in a residue class of $\mathcal{Q}$.*
- *We conclude that $\mathcal{P} = Q_2 + \rho^*(R')$, for some $R' \in C(\mathbb{Q})$.*

Sketch of the proof

Proof.

- Let $\mathcal{P} = P_1 + P_2 + P_3 \in D(\mathcal{Q})$. Then, $\int_{\mathcal{Q}}^{\mathcal{P}} \omega = 0$, for all $\omega \in \mathcal{W}$.
- Denote $\rho^*(\rho(P_3)) = P_3 + P_3'$, then $\int_{Q_1+Q_3}^{P_3+P_3'} \omega = 0$.
- $0 = \int_{Q_1+Q_2+Q_3}^{P_1+P_2+P_3} \omega = \int_{Q_1+Q_3}^{P_3+P_3'} \omega + \int_{P_3'}^{P_1} \omega + \int_{Q_2}^{P_2} \omega = \int_{P_3'}^{P_1} \omega + \int_{Q_2}^{P_2} \omega$.
- Denote $t_{Q_1}(P_1) = z_1$, $t_{Q_1}(P_3') = z_1'$, $t_{Q_2}(P_2) = z_2 \implies$

$$a_0(\omega,1)(z_1 - z_1') + \frac{a_1(\omega,1)}{2}({z_1}^2 - {z_1'}^2) + \cdots + a_0(\omega,2)z_2 + \frac{a_1(\omega,2)}{2}{z_2}^2 + \cdots = 0.$$

- Note $\mathrm{ord}_\pi(z_1), \mathrm{ord}_\pi(z_1'), \mathrm{ord}_\pi(z_2) > 0$. We want to prove $z_1 = z_1'$, $z_2 = 0$, i.e., $P_2 = Q_2$ and $P_3' = P_1$.
- $z_1 - z_1' \neq 0$ or $z_2 \neq 0 \implies$ that all higher terms have the property of higher divisibility by π.
- Repeat this for at least two differentials until we get the matrix from the previous slide of rank 2.
- This increases divisibility by π of at least one of $z_1 - z_1'$ and z_2. Contradiction!

□

Main theorem, special case, cases

Theorem (Box-G.-Goodman, 2022)

- *There are pull-back divisors in $\mathcal{Q}$,* $\deg(\rho) = 2$ *(generalisation of the case from Siksek, 2009).*

(b) *Assume* $\widetilde{Q_1} = \widetilde{Q_2}$, $Q_1 + Q_2 = \rho^*(R)$ *for some* $R \in C(\mathbb{Q})$*, and that the matrix*

$$\begin{pmatrix} \widetilde{a}_0(\omega_1, 1) & \frac{\widetilde{a}_1(\omega_1,1)}{2} \\ \widetilde{a}_0(\omega_2, 1) & \frac{\widetilde{a}_1(\omega_2,1)}{2} \end{pmatrix}$$

has rank 2.

- *Let* $\mathcal{P} \in X^{(3)}(\mathbb{Q})$ *be in a residue class of* $\mathcal{Q}$*.*
- *We conclude that* $\mathcal{P} = Q_3 + \rho^*(R')$*, for some* $R' \in C(\mathbb{Q})$*.*

Summary

- Generalised criteria from Siksek's paper.
- Found a new, "more in depth" criterion to deal with some situations when matrices from the theorem do not have sufficiently large rank.
- Our method has already contributed to (1) in work of Banwait and Derickx and (2) in work of Box.
- Using Mordell-Weil sieve and previous theorems we managed to compute cubic points on the curves

$$X_0(53),\ X_0(57),\ X_0(65),\ X_0(61),\ X_0(67) \text{ and } X_0(73).$$

- Only truly cubic points on $X_0(65)$ are defined over $\mathbb{Q}(\alpha)$, $\alpha^3 - \alpha^2 + \alpha - 2 = 0$.
- Determined the quartic points on $X_0(65)$.

The end

Thank you for your attention!

Question

Any questions?