Cubic points on modular curves via Chabauty

Joint work with Josha Box and Stevan Gajović

Pip Goodman

Cubic points on $X_0(65)$

David Zureick-Brown (DZB) and his collaborators had recently finished proving the analogue of Mazur's Theorem on torsion subgroups for elliptic curves over cubic fields.

For $X_1(65)$, they had tried using the natural map $X_1(65) \to X_0(65)$ to reduce the question to computing cubic points on $X_0(65)$. But they were unable to do so!

DZB: is it possible to determine the finitely many cubic points on $X_0(65)$?

How do we deal with cubic points?

We study points on $X^{(n)}$ the n-th symmetric power of the curve X. Points on $X^{(n)}$ are unordered n-tuples $P_1 + \ldots + P_n$ with $P_i \in X$.

Example

$X^{(2)}(\mathbb{Q}) = \{P + Q | P, Q \in X(\mathbb{Q})\} \cup \{P + P^\sigma | P \in X(K), [K : \mathbb{Q}] = 2\}$

There could be infinitely many points on $X^{(n)}(\mathbb{Q})$ regardless of X's genus!

A hyperelliptic curve $X/\mathbb{Q}$ has a rational degree two map $\rho \colon X \to \mathbb{P}^1$. Thus by pulling back rational points, we get infinitely many points in $X^{(2)}(\mathbb{Q})$.

For $X \colon y^2 = f(x)$, we have $\{(x, y) + (x, -y) | x \in \mathbb{Q}\} \subseteq X^{(2)}(\mathbb{Q})$.

Back to the cubic points on $X_0(65)$

The jacobian $J_0(65)(\mathbb{Q})$ has positive rank, so we're going to try looking for a Chabauty method to classify the points on $X_0(65)^{(3)}(\mathbb{Q})$.

What do we want from such a method?

Let $\tilde{\mathcal{P}} \in X^{(n)}(\mathbb{F}_p)$. We want information on its inverse image $D(\tilde{\mathcal{P}})$, the *residue class* of $\tilde{\mathcal{P}}$, in $X^{(n)}(\mathbb{Q}_p)$.

Given $\mathcal{Q} \in X^{(n)}(\mathbb{Q}) \cap D(\tilde{\mathcal{P}})$, we want to know

- is $\mathcal{Q}$ the only such point?
- If $\mathcal{Q} \in \rho^* C(\mathbb{Q})$, is $X^{(n)}(\mathbb{Q}) \cap D(\tilde{\mathcal{P}}) \subseteq \rho^* C(\mathbb{Q})$, i.e., does it just consist of pullbacks (via ρ).

Theorem (Siksek's Symmetric Chabauty method), '09
Explicit conditions, depending on p, to determine if $X^{(n)}(\mathbb{Q}) \cap D(\tilde{\mathcal{P}})$ consists of just one point, or pullbacks via ρ.

What's the problem with $X_0(65)^{(3)}(\mathbb{Q})$?

We have a degree two map $\rho\colon X_0(65) \to X_0^+(65)$ defined over $\mathbb{Q}$ (quotient by the Atkin-Lehner involution).

The set $X_0(65)(\mathbb{Q})$ contains 4 rationals points (the cusps) and the curve $X_0^+(65)$ is a rank one elliptic curve.

In particular, $X_0(65)^{(3)}(\mathbb{Q}) \supseteq c + \rho^* X_0^+(65)(\mathbb{Q})$ where $c \in X_0(65)(\mathbb{Q})$, is an infinite set not consisting of pullbacks!

Theorem (Box, Gajović, G. '22)
Let d, e, f and $n = f + de \neq 0$ be non-negative integers, $\rho\colon X \to C$ a morphism of degree d defined over $\mathbb{Q}$, and $\mathcal{Q} \in X^{(f)}(\mathbb{Q})$.

Explicit conditions, depending on p, to determine if $X^{(n)}(\mathbb{Q}) \cap D(\tilde{\mathcal{P}})$ is contained in $\mathcal{Q} + \rho^* C^{(e)}(\mathbb{Q})$.

Cubic and quartic points on modular curves

Theorem (Box, Gajović, G. '22)
The set of cubic points for each of the curves

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

is finite and listed in our paper. The quartic points on $X_0(65)$ form an infinite set. These points consist of those coming from $\rho^* X_0^+(65)^{(2)}(\mathbb{Q})$ and a finite set of points listed in our paper.

Our new method also plays a crucial role in Box's result:

Theorem (Box '22)
Let K be a totally real quartic field, not containing $\sqrt{5}$. Then any elliptic curve E/K is modular.

Symmetric Chabauty

Consider $\widetilde{\mathcal{Q}} \in X^{(n)}(\mathbb{F}_p)$ and its inverse image $D(\widetilde{\mathcal{Q}}) \subseteq X^{(n)}(\mathbb{Q}_p)$ under the reduction map.

Fixing an Abel-Jacobi map $\iota \colon X^{(n)} \to \mathrm{Jac}(X)$, we obtain a commutative diagram:

$$\begin{array}{ccc} D(\widetilde{\mathcal{Q}}) \cap X^{(n)}(\mathbb{Q}) & \xrightarrow{\quad \iota \quad} & \mathrm{Jac}(X)(\mathbb{Q}) \\ \downarrow & & \downarrow \\ D(\widetilde{\mathcal{Q}}) & \xrightarrow{\quad \iota \quad} & \mathrm{Jac}(X)(\mathbb{Q}_p) \end{array}$$

In classical Chabauty, we look to determine $\iota(D(\widetilde{\mathcal{Q}})) \cap \overline{\mathrm{Jac}(X)(\mathbb{Q})}$.

The problem is that even if the analogous Chabauty condition $r_X < g_X - (n-1)$ is satisfied, this set might not be finite.

Non finiteness of $\iota(D(\widetilde{\mathcal{Q}})) \cap \overline{\mathrm{Jac}(X)(\mathbb{Q})}$

If $\mathcal{Q} = P + \rho^*(Q) \in D(\widetilde{\mathcal{Q}})$ with $P \in X(\mathbb{Q})$, $Q \in C(\mathbb{Q})$, then the family

$$P + \rho^* C(\mathbb{Q}) \subseteq X^{(n)}(\mathbb{Q})$$

often leads to infinitely many points in $D(\widetilde{\mathcal{Q}})$.

To remedy this, we need to 'kill' the pullbacks. There is an abelian variety A such that $J(X) \sim J(C) \times A$. Let $\pi_A : J(X) \to A$ be the quotient map. The image

$$\pi_A(\iota(P + \rho^* C(\mathbb{Q})))$$

is now a single point on A. Hence we should try determining $\iota(D(\widetilde{\mathcal{Q}})) \cap \overline{A(X)(\mathbb{Q})}$, when $r_X - r_C < g_X - g_C - (n-1)$ is satisfied.

In general, this allows to deduce information about $D(\widetilde{\mathcal{Q}}) \cap X^{(n)}(\mathbb{Q})$ relative to $C(\mathbb{Q})$.

What could possibly go wrong?

In practice, we need to use information from several primes. The relevant technique here is the Mordell–Weil sieve.

There are algorithms for computing MW groups of curves with genus at most two. But our examples have genus 4 or 5.

Taking pullbacks, we can compute subgroups with index dividing a known quantity (the degree of our maps) and usually this is enough. But it wasn't for the quartic points on $X_0(65)$.

So, we proved the following:

Theorem (Box, Gajović, G. '22)
$J_0(65)(\mathbb{Q})$ is generated by $\rho^* J_0^+(65)(\mathbb{Q})$ and $J_0(65)(\mathbb{Q})_{tors}$.

(Where $J_0^+(65)$ is the elliptic curve that was causing problems earlier.)

Computing the full Mordell–Weil group

Suppose for a second $J(X)(\mathbb{Q})$ is torsion. We can try using

$$J(X)(\mathbb{Q}) \hookrightarrow J(X)(\mathbb{F}_p)$$

for several primes of good reduction to bound $J(X)(\mathbb{Q})$.

But there's no guarantee this bound will be sharp.

So, instead it's reasonable to compute $J(X)(K)_{tors}$ for some extension $K/\mathbb{Q}$ and then take Galois invariants.

Suppose $J(X)(\mathbb{Q})$ has positive rank, with $G \subseteq J(X)(\mathbb{Q})$ index dividing, say, two.

We then check if $D \in G$ is a double in $J(X)(\mathbb{Q})$ by either

- reducing mod p; or
- computing a preimage $\frac{1}{2}D \in J(X)(K)$ and looking for rational points in $\frac{1}{2}D + J(X)(K)[2]$.

Rough form of our Chabauty conditions

Given $\mathcal{Q} \in X^{(n)}(\mathbb{Q})$ we associate to it a matrix $\mathcal{A}_{\mathcal{Q}}$, built from fixing some local coordinate t and then taking the first few coefficients modulo p of the expansion of certain differentials around t.

We also assume we know integers n, d, e such that $\mathcal{Q} \in \mathcal{P} + \rho^* C^{(e)}(\mathbb{Q})$ for some $\mathcal{P} \in X^{(n-de)}(\mathbb{Q})$.

From this we cook up a rank condition on $\mathcal{A}_{\mathcal{Q}}$, which if satisfied shows $X^{(n)}(\mathbb{Q}) \cap D(\tilde{\mathcal{Q}}) \subseteq \mathcal{P} + \rho^* C^{(e)}(\mathbb{Q})$.

Sometimes these rank conditions are not satisfied. But this is usually for a "good reason".

The problem with $X_0(73)$

Let c_0, c_∞ denote the cusps on $X_0(73)$. They are exchanged by the Atkin-Lehner involution, i.e., $w(c_0) = c_\infty$.

We expect $3c_0, 3c_\infty \in X_0(73)^{(3)}(\mathbb{Q})$ to be alone in their residue classes, and thus their corresponding matrices $\mathcal{A}_0, \mathcal{A}_\infty$ would have to have full rank ($= 3$ here).

The matrix corresponding to $3c_0 + 3c_\infty$ is given by $\mathcal{A} = (\mathcal{A}_0 | \mathcal{A}_\infty)$.

Owing to the fact $w(c_0) = c_\infty$, we find $\mathcal{A}_0 = -\mathcal{A}_\infty$ and thus $\mathcal{A}$ has rank $\mathrm{rk}(\mathcal{A}_0)$.

However, our theorem also tells us that if $\mathcal{A}$ had rank $= 3$, then the residue class of $3c_0 + 3c_\infty$ would be contained in $\rho^* X_0^+(73)^{(3)}(\mathbb{Q})$.

However, this is not the case as there exists $f \in L(3c_0 + 3c_\infty)$ of degree 6 such that $w^* f \neq f$.

We provide other Chabauty conditions to deal with such novelties.

Thank you for listening!