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.

Due to previous work, they only had to compute the cubic points on the modular curves $X_1(N)$ for finitely many N, all of which had finitely many such points.

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!

How do we deal with cubic points?

We study points on $X^{(d)}$ the d-th symmetric power of the curve X. Points on $X^{(d)}$ are unordered d-tuples $P_1 + \ldots + P_d$ 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 $X^{(d)}(\mathbb{Q})$ 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 $\{(x, y) + (x, -y) | x \in \mathbb{Q}\} \subseteq X^{(2)}(\mathbb{Q})$.

If all but finitely many rational points on $X^{(d)}$ ($X/\mathbb{Q}$ not necessarily hyperelliptic) arise as the pullbacks of a degree d map, then in principle, the degree d points on X may be computed using Siksek's symmetric Chabauty method.

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

Note: if $X^{(d_0)}(\mathbb{Q})$ is infinite and $X(\mathbb{Q}) \neq \emptyset$, then $X^{(d)}(\mathbb{Q})$ is infinite for $d \geq d_0$. Furthermore, for $d > d_0$, there are infinitely many rational points on $X^{(d)}(\mathbb{Q})$ which are not pullbacks.

This is the case for $X_0(65)$, which has a rational degree two map to a rank one elliptic curve.

In particular, Siksek's methods cannot be applied to $X_0^{(3)}(65)(\mathbb{Q})$.

For this reason, DZB asked: can one determine the finitely many cubic points on $X_0(65)$ despite its infinitely many quadratic points?

Generalised symmetric Chabauty

Together with Josha Box and Stevan Gajović, we developed a generalised symmetric Chabauty method.

This allowed us to answer DZB's question affirmatively. Moreover, we prove the following:

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

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

is finite and known. The quartic points on $X_0(65)$ form an infinite set. We describe an infinite family and list a finite set of remaining points.

Our new method played 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

Let p be a prime of good reduction for our curve X. To determine $X^{(d)}(\mathbb{Q})$ it suffices to determine each of its residue discs.

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

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

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

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 $r_X < g_X - (d-1)$ is satisfied, this set might not be finite.

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

Recall: maps $\rho\colon X \to C$ can give rise to infinitely many points in $X^{(d)}(\mathbb{Q})$.

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

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

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 $r_X - r_C < g_X - g_C - (d-1)$ is satisfied.

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

For example, here we find conditions to guarantee $\mathcal{D} \subseteq P + \rho^* C(\mathbb{Q})$.

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 $\frac{1}{2}D + J(X)(K)[2]$.

What else could go wrong?

Our Chabauty conditions are given in terms of (certain) differentials of X. In fact, they depend on the rank of a matrix constructed from the first few coefficients of these differentials.

(Slightly) more precisely
Given $\mathcal{Q} \in X^d(\mathbb{Q})$ we associate to it a matrix $\mathcal{A}_{\mathcal{Q}}$.

We also assume that we know something about $\mathcal{Q}$.

For example $\mathcal{Q} \in \rho^* C^{d/e}(\mathbb{Q})$ for some quotient $\rho\colon X \to C$ of degree e, or perhaps $\mathcal{Q} \in \mathcal{P} + \rho^* C(\mathbb{Q})$ for some $\mathcal{P} \in X^{(d-e)}(\mathbb{Q})$.

From this we cook up a rank condition on $\mathcal{A}_{\mathcal{Q}}$, which if satisfied means all points in the residue disc of $\mathcal{Q}$ have the same form.

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

The problem with $X_0(73)$

Example

Let c_0, c_∞ denote the cusps on $X_0(73)$. We have $w_{73}(c_0) = c_\infty$, thus $c_0 + c_\infty \in \rho^* X_0^+(73)(\mathbb{Q})$, i.e., their sum is a pullback.

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) if we want to apply our earlier criteria.

However, since their sum is a pullback, these matrices satisfy $\mathcal{A}_0 = -\mathcal{A}_\infty$.

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

However, our theorem tells us that if the reduction of $\mathcal{A}$ modulo p 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 one may verify by computing the Riemann-Roch space $L(3c_0 + 3c_\infty)$.

Thanks for listening!