Rational points on Atkin–Lehner quotients of geometrically hyperelliptic Shimura curves

Oana Păduraru (MPIM Bonn)
joint work with Ciaran Schembri

Modular Curves and Galois Representations, Zagreb

September 21st, 2023

Overview

- Rational points on curves
- Hasse principle
- Shimura curves
- A database of geometrically hyperelliptic Shimura curves and their Atkin–Lehner quotients

Rational points on curves

Given a curve $C/\mathbb{Q}$ of arbitrary genus $g \geq 0$ we would like to answer the following:

1. Is $C(\mathbb{Q})$ non-empty?
2. If $C(\mathbb{Q})$ is non-empty, then what is $C(\mathbb{Q})$?

Both of these questions are deep and difficult to answer in general, and the answers depend on the genus g of the curve.

Genus trichotomy

1. For a genus 0 curve $C/\mathbb{Q}$, the set $C(\mathbb{Q})$ is either infinite or empty, and if a rational point on the curve exists it is straightforward to explicitly parameterize all of the rational points.
2. For a genus 1 curve $C/\mathbb{Q}$, the set $C(\mathbb{Q})$ is either empty or $C/\mathbb{Q}$ is an elliptic curve. If $C(\mathbb{Q})$ is non-empty, then $C(\mathbb{Q})$ has the group structure of a finitely generated abelian group:
$$C(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r.$$
3. Faltings proved in 1983 that $|C(\mathbb{Q})| < \infty$ whenever $g \geq 2$. His proof was not constructive, and there is no algorithm that is guaranteed to provably compute $C(\mathbb{Q})$. If J is the Jacobian of C, then
$$J(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r.$$

Hasse principle

- Hasse local to global principle: study a problem over $\mathbb{Q}$ by studying it over $\mathbb{R}$ and over all $\mathbb{Q}_p$.
- For curves: if a curve has points defined over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes p, does it necessarily have a point defined over $\mathbb{Q}$?
- Curves of genus 0 satisfy the Hasse principle.
- In genus 1 we find violations of the Hasse principle, e.g.

$$3x^3 + 4y^3 + 5z^3 = 0.$$

Shimura curves

As with modular curves, Shimura curves arise naturally as moduli spaces.

Before defining them, we need to introduce some notions related to quaternion algebras.

Quaternion algebras

Definition

Let K be a field with $\mathrm{char}(K) \neq 2$. Given $a, b \in K^*$, the quaternion K-algebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ is the K-algebra with K-basis $\{1, i, j, k\}$ with the rules $i^2 = a, j^2 = b, ij = -ji = k$.

Example

$$M_2(\mathbb{Q}) \simeq \left(\frac{1, -1}{\mathbb{Q}}\right)$$

with $\mathbb{Q}$-basis

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Shimura curves

Let B be an indefinite quaternion algebra over $\mathbb{Q}$ of discrimiant $D > 1$. For $N \in \mathbb{Z}_{\geq 1}$ with $\gcd(D, N) = 1$, one defines a group O_N^1 similar to the group $\Gamma_0(N)$ for modular curves.

The Shimura curve associated to B of level N is defined as the quotient:

$$X_0(D, N) := O_N^1 \backslash \mathcal{H}.$$

Shimura curves arise naturally as moduli spaces of abelian surfaces with quaternionic multiplication.

It is well known that Shimura curves have no real points, i.e.

$$X_0(D, N)(\mathbb{R}) = \emptyset.$$

Atkin–Lehner quotients

Definition

We say that $d|N$ is a Hall divisor of N if $\gcd(d, N/d) = 1$. We write $d \parallel N$.

For every Hall divisor m of DN, there exists an Atkin–Lehner involution w_m. The full group of Atkin–Lehner involutions is

$$W(D,N) = \{\ w_m\ :\ m \geq 1,\ m \parallel DN\ \}.$$

There is an identification

$$W(D,N) \simeq (\mathbb{Z}/2\mathbb{Z})^{\omega(DN)}.$$

For every subgroup $W \leq W(D,N)$ we consider the quotient curve

$$X_0(D,N)/W.$$

Equations

Guo–Yang computed a complete list of Shimura curves $X_0(D, N)$ which are hyperelliptic over $\overline{\mathbb{Q}}$ plus their Atkin–Lehner involutions. In total there are 44 such curves.

Theorem (P-Schembri)

Let $X_0(D, N)$ be a Shimura curve which is hyperelliptic over $\overline{\mathbb{Q}}$ and W a subgroup of Atkin–Lehner involutions.

Then defining equations for the Atkin–Lehner quotient curve $X_0(D, N)/W$ have been computed and in the case that the quotient curve has finitely many rational points the set $(X_0(D, N)/W)(\mathbb{Q})$ is given explicitly.

Furthermore, when the level N is 1 and the quotient curve has finitely many rational points it is known which of these points are CM.

Methods used for computing rational points

- Not everywhere locally solvable
- Two–cover descent
- Chabauty–Coleman method
- Pullback of rational points

For the rank = genus = 2 cases, we were able to use

- exceptional isomorphisms between quotients of Shimura curves and modular curves:

$$X_0(91,1)/\langle w_{91}\rangle \simeq X_0(91)/\langle w_{91}\rangle,$$
$$X_0(93,1)/\langle w_{93}\rangle \simeq X_0(93)/\langle w_3, w_{31}\rangle,$$

- bielliptic quadratic Chabauty:

$$X_0(10,19)/\langle w_{190}\rangle \simeq X_0(190)/\langle w_5, w_{19}\rangle.$$

New examples of violations of the Hasse principle

genus 2:

$$X_0(87,1)/\langle w_3\rangle, \quad X_0(6,29)/\langle w_6\rangle, \quad X_0(6,37)/\langle w_3\rangle,$$

genus 3:

$$X_0(93,1)/\langle w_3\rangle, \quad X_0(39,2)/\langle w_{78}\rangle,$$

genus 4:

$$X_0(119,1)/\langle w_7\rangle.$$

Hvala!