Odd degree isolated points on $X_1(N)$ with rational j-invariant

Lori Watson
Wake Forest
Joint with Abbey Bourdon, David R. Gill, and Jeremy Rouse

VaNTAGe Seminar
June 08, 2021

The question "When can a curve have infinitely many rational points?" was answered in Faltings's celebrated theorem.

Theorem (Faltings)

Let K be a number field. If C is a curve over K of genus $g \geq 2$, then there are only finitely many K-rational points.

Given a curve C over $\mathbb{Q}$, we know that $C(\mathbb{Q})$ can be infinite only if the genus g of C is 0 or 1 (this is unchanged if we consider $C(K)$ for any number field K).

By the degree of a closed point $z \in C(\bar{K})$, we mean $[K(z) : K]$, the degree of the residue field of z over K.

Example: Let C be the curve defined by $y^2 = x^5 + x^2 + 1$. Then the closed point $\{(1, \sqrt{3}), (1, -\sqrt{3})\}$ is a degree 2 point over $\mathbb{Q}$.

Faltings's Theorem tells us that for any curve C of genus $g > 1$ and any number field K, the set of degree 1 points is finite.

The story can change drastically when we consider points of degree $d \geq 2$.

Example 1: Consider again the curve C defined by $y^2 = x^5 + x^2 + 1$. This is a curve of genus 2, so there are only finitely many degree 1 points. If we fix $a \in \mathbb{Q}$, however, then $\{(a, \pm\sqrt{a^5 + a^2 + 1})\}$ is a closed point over the field $K_a = \mathbb{Q}(\sqrt{a^5 + a^2 + 1})$.

For most $a \in \mathbb{Q}$, $a^5 + a^2 + 1$ is not a square, so $[K_a : \mathbb{Q}] = 2$. Letting a run through the rationals, we obtain infinitely many degree 2 closed points of C.

At work is the existence of a degree 2 morphism $\pi : C \to \mathbb{P}^1$ defined over $\mathbb{Q}$. (The morphism in this case is defined by $\pi(x, y) = x$.) We have infinitely-many degree 2 points $\pi^{-1}(a)$ coming from the infinitely many degree 1 points $a \in \mathbb{P}^1$.

This works for $d > 2$ as well: if we have a degree d morphism $f : C \to \mathbb{P}^1$, then there will be infinitely many degree 1 points $a \in \mathbb{P}^1$ such that $f^{-1}(a)$ is a degree d point of C.

There is another way in which we can obtain infinitely many degree d points.

Example 2: Let C be the curve defined by $y^2 = x^9 + x^3 + 1$. As before, C admits a degree 2 morphism to $\mathbb{P}^1$, and so we expect infinitely many degree 2 points. But C also admits a degree 3 map to the elliptic curve $E : y^2 = x^3 + x + 1$, $f : C \to E$, $f(x, y) = (x^3, y)$. We can therefore expect cubic points $f^{-1}(a, b)$ of C. As $E(\mathbb{Q})$ has rank 1, there will be infinitely many such points.

So far, our examples have involved infinitely many degree d points parameterized by either $\mathbb{P}^1$, or a positive rank elliptic curve.

Debarre and Fahlaoui provided examples of curves C that admitted infinitely many degree d points, yet had no maps of degree $\leq d$ to $\mathbb{P}^1$ or an elliptic curve. Instead, their construction involves the dth symmetric product $C^{(d)}$.

Let C/K be a curve (and assume $C(K) \neq \emptyset$). A closed point $x \in C$ of degree d gives a K-rational point of $C^{(d)}$, and there is a natural map $\phi : C^{(d)} \to J(C)$.

If this natural map is not injective then there is a dominant morphism $f : C \to \mathbb{P}^1$ of degree d.

Otherwise, Faltings's Theorem implies that there are finitely many K-rational abelian subvarieties $A_i \subset J(C)$ and K-rational points $x_i \in \mathrm{im}\phi$ such that

$$(\mathrm{im}\phi)(K) = \bigcup_{i=1}^{n} [x_i + A_i(K)].$$

Consequently, one of the A_i must have positive rank.

In order for C to admit infinitely many degree d closed points over K, one of two things must occur:

(i) C admits a dominant morphism of degree d to $\mathbb{P}^1$, or

(ii) The degree d points of C inject into the set of K-rational points of a translate of a positive rank abelian subvariety of the Jacobian $J(C)$.

This does not, however, tell the whole story of degree d points.

Example 3: Let C be the curve $C : y^2 = x^8 + 8x^6 - 2x^4 + 8x^2 + 1 = F(x)$. Since C is hyperelliptic, we expect C to have infinitely many quadratic points. Most of these are of the form $(a, \pm\sqrt{F(a)})$ with $a \in \mathbb{Q}$, but there is a point that does not arise in this fashion.

The point $(i, \pm 4i)$ is a quadratic point of C, but as the x-coordinate is not rational, this point does not come from the dominant degree 2 morphism $C \to \mathbb{P}^1$.

Nor is it part of an infinite family of quadratic points of a abelian subvariety of $J(C)$ – the rank of its Jacobian is 0.

The point $(i, \pm 4i)$ is an example of an *isolated point*.

Definition

Let C be a curve defined over a number field K and let $x \in C$ be a closed point of degree d. We say x is **isolated** *if it does not belong to an infinite family of degree d points parametrized by $\mathbb{P}^1$ or a translate of a positive rank abelian subvariety of the curve's Jacobian.*

The term isolated points was first defined in a paper of Bourdon, Ejder, Liu, Odumodu, and Viray, where the focus was on modular curves (though the construction had been studied earlier).

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

Let C be a curve over a number field.
There are infinitely many degree d points on C if and only if there is a degree d point on C that is not isolated.

Sporadic Points on Modular Curves

There is a type of point that is guaranteed to be isolated.

Definition

Let C be a curve defined over a number field K and let $x \in C$ be a closed point of degree $\deg(x)$. We say that x is **sporadic** *if there are only finitely many closed points y with $\deg(y) \leq \deg(x)$.*

Some of the isolated points on modular curves first observed were sporadic points.

Modular Curves

For fixed $N \in \mathbb{Z}^+$, the modular curve $X_1(N)$ is an algebraic curve which can be defined over $\mathbb{Q}$. Each noncuspidal K-rational point on the curve corresponds up to isomorphism to a pair $[E, P]$, where E is an elliptic curve and P is a distinguished point of order N defined over K.

The noncuspidal K-rational points on the modular curve $X_0(N)$ correspond up to isomorphism to a pair $[E, \langle P \rangle]$, where E is an elliptic curve and $\langle P \rangle$ is a cyclic subgroup of order N.

Examples

- CM points on $X_1(\ell)$ for all sufficiently large primes ℓ (Clark, Cook, and Stankewicz).
- A point of degree 6 on $X_1(37)$ (van Hoeij)
- A point of degree 3 on $X_1(21)$ (Najman)

Example (Najman): The curve $X_1(21)$ has an isolated point of degree 3. The degree 3 point corresponds to an elliptic curve E with j-invariant $-3^2 \cdot 5^5/2^3$ which has a point of order 21 over the field $\mathbb{Q}(\zeta_9^+)$.

For a fixed curve C, there are only finitely many isolated points of degree d, and when $d \geq g + 1$, no point of degree d is isolated. Thus, for a fixed integer N, there are only finitely many isolated points on $X_1(N)$.

On the other hand, the Clark, Cook, Stankewicz result shows the set of isolated points on all $X_1(N)$ for all $N \in \mathbb{Z}^+$ is infinite (and there are CM elliptic curves with rational j-invariant that give rise to isolated points of arbitrarily large degree).

It is expected that only finitely many rational j-invariants correspond to isolated points on $X_1(N)$.

Isolated Points on Modular Curves

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

Let $\mathcal{I}$ denote the set of all isolated points on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$. Assume Serre's Uniformity Conjecture. Then $j(\mathcal{I}) \cap \mathbb{Q}$ is finite.

Conjecture (Uniformity Conjecture)

There exists a constant M such that for all non-CM elliptic curves $E/\mathbb{Q}$ and for all primes $p > M$, the mod p Galois representation

$$\rho_{E,p} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to Aut(E[p]) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$$

is surjective.

By adding an assumption on the degree of an isolated point, we obtain the following unconditional result:

Main Result

Theorem (Bourdon, Gill, Rouse, W.)

Let $\mathcal{I}_{odd}$ denote the set of all isolated points of odd degree on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$. Then $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ contains at most the j-invariants in the following list:

non-CM j-invariants	CM j-invariants
$-3^2 \cdot 5^6/2^3$	$-2^{18} \cdot 3^3 \cdot 5^3$
$3^3 \cdot 13/2^2$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

Conversely, $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ contains $-3^2 \cdot 5^6/2^3$ and $3^3 \cdot 13/2^2$.

Connection with rational cyclic isogenies

The key advantage in adding the hypothesis that $\deg(x)$ is odd for $x \in X_1(N)$ is that it allows us to establish a connection with rational cyclic isogenies.

In particular, we show that if x is a point of odd degree on $X_1(N)$ with $p|N$ an odd prime and $3^3 \cdot 5 \cdot 7^5/2^7 \neq j(x) \in \mathbb{Q}$, then there is some $y \in X_0(p)(\mathbb{Q})$ with $j(x) = j(y)$.

In addition, $p \in \{3, 5, 7, 11, 13, 19, 43, 67, 163\}$ and $N = 2^a p^b q^c$ (with bounds on a).

We treat CM and non-CM points (mostly) separately in the paper.

One key result, which we use throughout the paper, is again due to Bourdon, Ejder, Liu, Odumodu, and Viray.

Theorem

Let $f : C \to D$ be a finite map of curves and let $x \in C$ be an isolated point. If $\deg(x) = \deg(f(x)) \cdot \deg(f)$, then $f(x)$ is an isolated point of D.

This theorem gives one approach for identifying isolated points on $X_1(N)$: use the natural map $f : X_1(N) \to X_1(m)$ for some $m|N$.

To this end, we use results of Greenberg and Greenberg, Rubin, Silverberg, and Stoll on the images of p-adic Galois representations for primes $p \geq 5$ with cyclic p-isogenies to determine values of m for which the degree condition on residue fields holds.

Example: To show that there are no non-CM isolated points of odd degree on $X_1(2 \cdot 7^b)$ with rational j-invariant for any $b \geq 1$, we show that an such odd degree isolated point on $X_1(2 \cdot 7^b)$ would map to a non-cuspidal isolated point on $X_1(14)$. By Mazur, there are no non-cuspidal $\mathbb{Q}$-rational points on $X_1(14)$, so a non-cuspidal odd degree point must have degree ≥ 3, and hence cannot be isolated.

Though the techniques for addressing specific N vary, the approach (broadly speaking) is to push isolated points on $X_1(N)$ down to isolated points on other curves which are either known to have no isolated points, or which are amenable to computations.

Example: Let $x \in X_1(2^a 3^b)$ be an isolated point of odd degree corresponding to a non-CM elliptic curve with $j(x) \in \mathbb{Q}$. Then x maps to an isolated point on either $X_1(54)$ or $X_1(162)$. We show that these curves have no non-CM isolated points of odd degree using the 3-adic classification due to Rouse, Sutherland, and Zureick-Brown, as well as a characterization of certain elliptic curves $E/\mathbb{Q}$ with "entanglement" of torsion point fields.

If $E/\mathbb{Q}$ has CM by an order $\mathcal{O}$, then the discriminant Δ of $\mathcal{O}$ is one of only 13 integers.

We show that there is no isolated point $x \in X_1(N)$ of odd degree corresponding to an elliptic curve with CM by the order of discriminant

$$\Delta \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28\}.$$

The remaining three discriminants are $-43, -67, -163$, and it is the j-invariants corresponding to these discriminants that appear in the main theorem.

To complete the classification of odd degree isolated points, it remains to determine whether these points are isolated. These j-invariants are in $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ if and only if they correspond to isolated points of degree 21, 33, and 81 on $X_1(43)$, $X_1(67)$ and $X_1(163)$, respectively... unfortunately the Jacobians of each of these curves has positive rank.

Remaining Problems/Questions

- Unconditional results for isolated points of even degree on $X_1(N)$.
- Are there non-CM j-invariants giving rise to infinitely many isolated points?
- What is the proportion of non-CM to CM isolated j-invariants?

Thank you!

References

- Bourdon, Ejder, Liu, Odumodu, Viray. *On the level of modular curves that give rise to isolated j-invariants*.
- Bourdon, Gill, Rouse, Watson. *Odd degree isolated points on* $X_1(N)$ *with rational j-invariant*.