On Isolated Points of Odd Degree

Abbey Bourdon, David R. Gill, Jeremy Rouse, Lori D. Watson

Wake Forest University

August 31, 2020

Introduction

Question: If C is a curve defined over a number field k, is $C(k)$ finite or infinite?

Introduction

Question: If C is a curve defined over a number field k, is $C(k)$ finite or infinite?

- genus 0: If $C(k) \neq \emptyset$, then $C \cong \mathbb{P}^1$ and $C(k)$ is infinite.
- genus 1: If $C(k) \neq \emptyset$, then C is an elliptic curve and $C(k)$ is a finitely generated abelian group.
- genus ≥ 2: $C(k)$ is finite by Faltings's theorem

Introduction

Let $d \in \mathbb{Z}^+$.

Question: If C is a curve defined over a number field k, is the collection of closed points of degree d finite or infinite?

Introduction

Let $d \in \mathbb{Z}^+$.

Question: If C is a curve defined over a number field k, is the collection of closed points of degree d finite or infinite?

- $f : C \to \mathbb{P}^1$, degree $d \implies$ infinitely many points of degree d

Introduction

Let $d \in \mathbb{Z}^+$.

Question: If C is a curve defined over a number field k, is the collection of closed points of degree d finite or infinite?

- $f : C \to \mathbb{P}^1$, degree $d \implies$ infinitely many points of degree d

Debarre and Fahlaoui ('93): Can have infinitely many degree d points even without a map of degree $\leq d$ onto $\mathbb{P}^1$ or an elliptic curve.

Introduction

Suppose $P_0 \in C(k)$ and $x \in C$ is a closed point of degree d.

Introduction

Suppose $P_0 \in C(k)$ and $x \in C$ is a closed point of degree d.

$$\Phi_d : \operatorname{Sym}^d C \to \operatorname{Jac}(C)$$

$$x = P_1 + P_2 + \cdots + P_d \mapsto [P_1 + \cdots + P_d - dP_0]$$

Introduction

Suppose $P_0 \in C(k)$ and $x \in C$ is a closed point of degree d.

$$\Phi_d : \mathrm{Sym}^d C \to \mathrm{Jac}(C)$$

$$x = P_1 + P_2 + \cdots + P_d \mapsto [P_1 + \cdots + P_d - dP_0]$$

If C has infinitely many closed points of degree d, then one of following is true:

Introduction

Suppose $P_0 \in C(k)$ and $x \in C$ is a closed point of degree d.

$$\Phi_d : \mathrm{Sym}^d C \to \mathrm{Jac}(C)$$

$$x = P_1 + P_2 + \cdots + P_d \mapsto [P_1 + \cdots + P_d - dP_0]$$

If C has infinitely many closed points of degree d, then one of following is true:

- $\Phi_d(x) = \Phi_d(y)$ for distinct $y \in (\mathrm{Sym}^d C)(k)$. $\exists f \in k(C)^\times$ with $\mathrm{div}(f) = x - y$, and $f : C \to \mathbb{P}^1$ has degree d.

Introduction

Suppose $P_0 \in C(k)$ and $x \in C$ is a closed point of degree d.

$$\Phi_d : \mathrm{Sym}^d C \to \mathrm{Jac}(C)$$

$$x = P_1 + P_2 + \cdots + P_d \mapsto [P_1 + \cdots + P_d - dP_0]$$

If C has infinitely many closed points of degree d, then one of following is true:

- $\Phi_d(x) = \Phi_d(y)$ for distinct $y \in (\mathrm{Sym}^d C)(k)$. $\exists f \in k(C)^\times$ with $\mathrm{div}(f) = x - y$, and $f : C \to \mathbb{P}^1$ has degree d.
- Φ_d is injective on degree d points. By Faltings ('94), there must be an infinite family of degree d points parametrized by a positive rank abelian subvariety of $\mathrm{Jac}(C)$.

Isolated Points

$$\Phi_d : \mathrm{Sym}^d C \to \mathrm{Jac}(C)$$

Definition

1. A closed point $x \in C$ of degree d is $\mathbb{P}^1$**-parametrized** if there exists distinct $x' \in (\mathrm{Sym}^d C)(k)$ such that $\Phi_d(x) = \Phi_d(x')$.

Isolated Points

$$\Phi_d : \operatorname{Sym}^d C \to \operatorname{Jac}(C)$$

Definition

1. A closed point $x \in C$ of degree d is **$\mathbb{P}^1$-parametrized** if there exists distinct $x' \in (\operatorname{Sym}^d C)(k)$ such that $\Phi_d(x) = \Phi_d(x')$.
2. A closed point $x \in C$ of degree d is **AV-parametrized** if there exists a positive rank abelian subvariety $A \subset \operatorname{Jac}(C)$ such that $\Phi_d(x) + A \subset \operatorname{im}(\Phi_d)$.

Isolated Points

$$\Phi_d : \operatorname{Sym}^d C \to \operatorname{Jac}(C)$$

Definition

1. A closed point $x \in C$ of degree d is $\mathbb{P}^1$**-parametrized** if there exists distinct $x' \in (\operatorname{Sym}^d C)(k)$ such that $\Phi_d(x) = \Phi_d(x')$.
2. A closed point $x \in C$ of degree d is **AV-parametrized** if there exists a positive rank abelian subvariety $A \subset \operatorname{Jac}(C)$ such that $\Phi_d(x) + A \subset \operatorname{im}(\Phi_d)$.
3. A closed point $x \in C$ of degree d is **isolated** if it is neither $\mathbb{P}^1$-parametrized nor AV-parametrized.

Isolated Points

A closed point $x \in C$ of degree d is **isolated** if it is neither $\mathbb{P}^1$-parametrized nor AV-parametrized.

Isolated Points

A closed point $x \in C$ of degree d is **isolated** if it is neither $\mathbb{P}^1$-parametrized nor AV-parametrized.

Theorem (B., Ejder, Liu, Odumodu, Viray - BELOV, '19)

Let C be a curve over a number field.

1. *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.*
2. *There are only finitely many isolated points on C.*

Isolated Points on Modular Curves

Isolated Points on Modular Curves

$X_1(N)/\mathbb{Q}$: Noncuspidal points parametrize pairs $(E, P)/\sim$

Isolated Points on Modular Curves

$X_1(N)/\mathbb{Q}$: Noncuspidal points parametrize pairs $(E, P)/\sim$

$j : X_1(N) \to X_1(1) \cong \mathbb{P}^1$ sends $x = [E, P]$ to $j(E)$

Isolated Points on Modular Curves

$X_1(N)/\mathbb{Q}$: Noncuspidal points parametrize pairs $(E, P)/\sim$

$j : X_1(N) \to X_1(1) \cong \mathbb{P}^1$ sends $x = [E, P]$ to $j(E)$

Theorem (BELOV, '19)

Let $\mathcal{I}$ denote the set of all isolated points on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$. Suppose there exists a constant $C = C(\mathbb{Q})$ such that for all non-CM elliptic curves $E/\mathbb{Q}$, the mod p Galois representation associated to E is surjective for primes $p > C$. Then $j(\mathcal{I}) \cap \mathbb{Q}$ is finite.

Isolated Points on Modular Curves

$X_1(N)/\mathbb{Q}$: Noncuspidal points parametrize pairs $(E, P)/\sim$

$j : X_1(N) \to X_1(1) \cong \mathbb{P}^1$ sends $x = [E, P]$ to $j(E)$

Theorem (BELOV, '19)

Let $\mathcal{I}$ denote the set of all isolated points on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$. Suppose there exists a constant $C = C(\mathbb{Q})$ such that for all non-CM elliptic curves $E/\mathbb{Q}$, the mod p Galois representation associated to E is surjective for primes $p > C$. Then $j(\mathcal{I}) \cap \mathbb{Q}$ is finite.

We call $j \in j(\mathcal{I})$ an **isolated j-invariant**.

Isolated Points on Modular Curves

Let $\mathcal{I}$ denote the set of all isolated points on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$.

Isolated Points on Modular Curves

Let $\mathcal{I}$ denote the set of all isolated points on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$.

- Can the (likely finite) set $j(\mathcal{I}) \cap \mathbb{Q}$ be made explicit?

Isolated Points on Modular Curves

Let $\mathcal{I}$ denote the set of all isolated points on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$.

- Can the (likely finite) set $j(\mathcal{I}) \cap \mathbb{Q}$ be made explicit?
- What can be said about the proportion of CM versus non-CM j-invariants in $j(\mathcal{I}) \cap \mathbb{Q}$?

Isolated Points on Modular Curves

Let $\mathcal{I}$ denote the set of all isolated points on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$.

- Can the (likely finite) set $j(\mathcal{I}) \cap \mathbb{Q}$ be made explicit?
- What can be said about the proportion of CM versus non-CM j-invariants in $j(\mathcal{I}) \cap \mathbb{Q}$?
- Can the condition on Serre's Uniformity Conjecture be removed?

Restriction to Odd Degree

Restriction to Odd Degree

Theorem (B., Gill, Rouse, Watson, '20)

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 $3^3 \cdot 13/2^2$.

Restriction to Odd Degree

Theorem (B., Gill, Rouse, Watson, '20)

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 $3^3 \cdot 13/2^2$.

- Najman, '16: $\exists x \in X_1(21)$ of degree 3 with $j(x) = -3^2 \cdot 5^6/2^3$

Restriction to Odd Degree

Theorem (B., Gill, Rouse, Watson, '20)

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 $3^3 \cdot 13/2^2$.

- Najman, '16: $\exists x \in X_1(21)$ of degree 3 with $j(x) = -3^2 \cdot 5^6/2^3$
- $\exists x \in X_1(28)$ of degree 9 and $j(x) = 3^3 \cdot 13/2^2$

Restriction to Odd Degree

Theorem (B., Gill, Rouse, Watson, '20)

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 $3^3 \cdot 13/2^2$.

CM points - are they AV-parametrized?

Restriction to Odd Degree

Theorem (B., Gill, Rouse, Watson, '20)

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 $3^3 \cdot 13/2^2$.

CM points - are they AV-parametrized?

- degree 21 on $X_1(43)$, degree 33 on $X_1(67)$, and degree 81 on $X_1(163)$, respectively

Characterization of Odd Degree Points

Let $x \in X_1(n)$ be a point of odd degree with $j(x) \in \mathbb{Q}$.

Characterization of Odd Degree Points

Let $x \in X_1(n)$ be a point of odd degree with $j(x) \in \mathbb{Q}$.

- Suppose $j(x) \neq 3^3 \cdot 5 \cdot 7^5/2^7$.
- Suppose $j(x) \neq j(z)$ for all $z \in X_0(21)(\mathbb{Q})$.

Characterization of Odd Degree Points

Let $x \in X_1(n)$ be a point of odd degree with $j(x) \in \mathbb{Q}$.

- Suppose $j(x) \neq 3^3 \cdot 5 \cdot 7^5/2^7$.
- Suppose $j(x) \neq j(z)$ for all $z \in X_0(21)(\mathbb{Q})$.

Theorem (B., Gill, Rouse, Watson, '20)

If p is an odd prime dividing n, then there exists $y \in X_0(p)(\mathbb{Q})$ with $j(x) = j(y)$. Moreover,

$$n = 2^a p^b$$

for $p \in \{3, 5, 7, 11, 13, 19, 43, 67, 163\}$ and nonnegative integers a, b with $a \leq 3$. If $b > 0$, then $a \leq 2$.

$E/\mathbb{Q}$ with isogenies

For a fixed prime p, let m be the maximum integer such that an elliptic curve $E/\mathbb{Q}$ possesses a $\mathbb{Q}$-rational cyclic p^m-isogeny.

$E/\mathbb{Q}$ with isogenies

For a fixed prime p, let m be the maximum integer such that an elliptic curve $E/\mathbb{Q}$ possesses a $\mathbb{Q}$-rational cyclic p^m-isogeny.

Theorem (Greenberg, '12 & Greenberg, Rubin, Silverberg, Stoll, '14)

If $E/\mathbb{Q}$ is a non-CM elliptic curve with a rational p-isogeny for some prime $p \geq 5$, then $\operatorname{im} \rho_{E,p^\infty}$ is the complete pre-image of $\operatorname{im} \rho_{E,p^m}$ in $\mathrm{GL}_2(\mathbb{Z}_p)$.

$E/\mathbb{Q}$ with isogenies

For a fixed prime p, let m be the maximum integer such that an elliptic curve $E/\mathbb{Q}$ possesses a $\mathbb{Q}$-rational cyclic p^m-isogeny.

Theorem (Greenberg, '12 & Greenberg, Rubin, Silverberg, Stoll, '14)

If $E/\mathbb{Q}$ is a non-CM elliptic curve with a rational p-isogeny for some prime $p \geq 5$, then $\operatorname{im} \rho_{E,p^\infty}$ is the complete pre-image of $\operatorname{im} \rho_{E,p^m}$ in $\mathrm{GL}_2(\mathbb{Z}_p)$.

Theorem (BELOV, '19)

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.

Proof Outline: Nice Cases

Proof Outline: Nice Cases

Let $x \in X_1(N)$ be an isolated point of odd degree with $j(x) \in \mathbb{Q}$.

Proof Outline: Nice Cases

Let $x \in X_1(N)$ be an isolated point of odd degree with $j(x) \in \mathbb{Q}$.

- No $E/\mathbb{Q}$ with rational 21-isogeny and $j(E) = j(x)$
  $\implies N = 2^a p^b$ with $a \leq 2$.

Proof Outline: Nice Cases

Let $x \in X_1(N)$ be an isolated point of odd degree with $j(x) \in \mathbb{Q}$.

- No $E/\mathbb{Q}$ with rational 21-isogeny and $j(E) = j(x)$
  $\implies N = 2^a p^b$ with $a \leq 2$.
- If $p > 5$, then Greenberg, Rubin, Silverberg, Stoll + BELOV
  $\implies f(x) \in X_1(2^a p)$ is isolated, with finite exceptions.

Proof Outline: Nice Cases

Let $x \in X_1(N)$ be an isolated point of odd degree with $j(x) \in \mathbb{Q}$.

- No $E/\mathbb{Q}$ with rational 21-isogeny and $j(E) = j(x)$
  $\implies N = 2^a p^b$ with $a \leq 2$.
- If $p > 5$, then Greenberg, Rubin, Silverberg, Stoll + BELOV
  $\implies f(x) \in X_1(2^a p)$ is isolated, with finite exceptions.
- Demonstrate $f(x)$ is isolated, or argue no such isolated point can exist.

What about rational cyclic 21-isogenies?

What about rational cyclic 21-isogenies?

Let $x \in X_1(N)$ be an isolated point of odd degree with $j(x) \in \mathbb{Q}$. Suppose $j(x) = j(E)$ for some $E/\mathbb{Q}$ with rational cyclic 21-isogeny.

- $N = 2^a 3^b 7^c$

What about rational cyclic 21-isogenies?

Let $x \in X_1(N)$ be an isolated point of odd degree with $j(x) \in \mathbb{Q}$. Suppose $j(x) = j(E)$ for some $E/\mathbb{Q}$ with rational cyclic 21-isogeny.

- $N = 2^a 3^b 7^c$
- $\mathbb{Q}(\zeta_9)^+ \subseteq \mathbb{Q}(E[7]) \cap \mathbb{Q}(E[9])$ - “entanglement” occurs

What about rational cyclic 21-isogenies?

Let $x \in X_1(N)$ be an isolated point of odd degree with $j(x) \in \mathbb{Q}$. Suppose $j(x) = j(E)$ for some $E/\mathbb{Q}$ with rational cyclic 21-isogeny.

- $N = 2^a 3^b 7^c$
- $\mathbb{Q}(\zeta_9)^+ \subseteq \mathbb{Q}(E[7]) \cap \mathbb{Q}(E[9])$ - "entanglement" occurs

For fixed m, BELOV ('19) gives explicit (uniform) bound on level of m-adic Galois representation.

What about rational cyclic 21-isogenies?

Let $x \in X_1(N)$ be an isolated point of odd degree with $j(x) \in \mathbb{Q}$. Suppose $j(x) = j(E)$ for some $E/\mathbb{Q}$ with rational cyclic 21-isogeny.

- $N = 2^a 3^b 7^c$
- $\mathbb{Q}(\zeta_9)^+ \subseteq \mathbb{Q}(E[7]) \cap \mathbb{Q}(E[9])$ - "entanglement" occurs

For fixed m, BELOV ('19) gives explicit (uniform) bound on level of m-adic Galois representation.

These bounds can be improved when entanglement occurs!

What about $p = 3$?

What about $p = 3$?

The case of possible isolated points $x \in X_1(2^a 3^b)$ is difficult to analyze because possible entanglement is much harder to control.

What about $p = 3$?

The case of possible isolated points $x \in X_1(2^a 3^b)$ is difficult to analyze because possible entanglement is much harder to control.

Proposition (B., Gill, Rouse, Watson, '20)

There are no odd degree isolated points on $X_1(54)$ or $X_1(162)$ associated to a non-CM elliptic curve E with $j(E) \in \mathbb{Q}$.

What about $p = 3$?

The case of possible isolated points $x \in X_1(2^a 3^b)$ is difficult to analyze because possible entanglement is much harder to control.

Proposition (B., Gill, Rouse, Watson, '20)

There are no odd degree isolated points on $X_1(54)$ or $X_1(162)$ associated to a non-CM elliptic curve E with $j(E) \in \mathbb{Q}$.

For example:

- Any elliptic curve $E/\mathbb{Q}$ for which $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[27])$ is an S_3-extension gives a rational point on an explicit curve $C/\mathbb{Q}$.

What about $p = 3$?

The case of possible isolated points $x \in X_1(2^a 3^b)$ is difficult to analyze because possible entanglement is much harder to control.

Proposition (B., Gill, Rouse, Watson, '20)

There are no odd degree isolated points on $X_1(54)$ or $X_1(162)$ associated to a non-CM elliptic curve E with $j(E) \in \mathbb{Q}$.

For example:

- Any elliptic curve $E/\mathbb{Q}$ for which $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[27])$ is an S_3-extension gives a rational point on an explicit curve $C/\mathbb{Q}$.
- Can reduce to case of a single $C/\mathbb{Q}$ of genus 4.

What about $p = 3$?

The case of possible isolated points $x \in X_1(2^a 3^b)$ is difficult to analyze because possible entanglement is much harder to control.

Proposition (B., Gill, Rouse, Watson, '20)

There are no odd degree isolated points on $X_1(54)$ or $X_1(162)$ associated to a non-CM elliptic curve E with $j(E) \in \mathbb{Q}$.

For example:

- Any elliptic curve $E/\mathbb{Q}$ for which $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[27])$ is an S_3-extension gives a rational point on an explicit curve $C/\mathbb{Q}$.
- Can reduce to case of a single $C/\mathbb{Q}$ of genus 4.
- Since C maps to a genus 1 curve, can show has no non-cuspidal points.

Main Theorem

Theorem (B., Gill, Rouse, Watson, '20)

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 $3^3 \cdot 13/2^2$.

Thank you!