$\mathbb{Q}$-curves over odd degree number fields and sporadic points

Filip Najman

University of Zagreb

joint with Abbey Bourdon (Wake Forest) and John Cremona (Warwick)

VaNTAGe
a virtual math seminar on open conjectures in number theory and arithmetic geometry

June 29th 2021.

Definitions

Definition

An isogeny of elliptic curves is a surjective homomorphism with finite kernel

We say that an isogeny $\phi : E_1 \to E_2$ is defined over K if E_1, E_2 and ϕ are all defined over K.

An isogeny (if no field is stated) is in this talk defined over $\overline{\mathbb{Q}}$.

Definition

An elliptic curve is called a $\mathbb{Q}$-*curve* if it is isogenous to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.

If E/K is a $\mathbb{Q}$-curve, it is not necessarily isogenous over K to its conjugates.

Galois representations attached to elliptic curves

Let E/K be an elliptic curve, K a number field and p a prime. Define

$$E[p] := \left\{R \in E(\overline{K}) \mid pR = O\right\},$$

$G_K := \mathrm{Gal}(\overline{K}/K)$ acts on $E[p]$.

This induces

$$\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p),$$

the mod p Galois representation attached to E.

Serre's uniformity question/conjecture: Does there exist a $C > 0$ such that for all primes $p > C$ and for all elliptic curves $E/\mathbb{Q}$ without CM we have $\rho_{E,p}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_p)$?

$\mathbb{Q}$-curves are the modular curves over number fields

Ribet (1992) (assuming Serre's conjecture which was later proved): $\mathbb{Q}$-curves are exactly the elliptic curves over number fields that are modular, in the sense of being quotients of $J_1(N)$ for some N.

$\mathbb{Q}$-curves have been extensively used in the "modular method" to solve Fermat-type equations. It is often crucial to understand their Galois representations.

Which curves are $\mathbb{Q}$-curves?

An elliptic curve defined over $\mathbb{Q}$ is a $\mathbb{Q}$-curve.

A base change of a $\mathbb{Q}$-curve is a $\mathbb{Q}$-curve.

A twist of a $\mathbb{Q}$-curve is a $\mathbb{Q}$-curve.

An elliptic curve E with $j(E) \in \mathbb{Q}$ is a $\mathbb{Q}$-curve.

A curve that is isogenous to a $\mathbb{Q}$-curve is a $\mathbb{Q}$-curve.

Any CM elliptic curve is a $\mathbb{Q}$-curve.

Let $\mathcal{E}$ be the set of all elliptic curves.

$$\mathcal{E} \supset \{\mathbb{Q} - \text{curves}\} \supset \{E \text{ isogenous to } E_1 \mid j(E_1) \in \mathbb{Q}\} \supset$$

$$\supset \{E \mid j(E) \in \mathbb{Q}\} \supset \{E/\mathbb{Q}\}.$$

Questions, questions

$$\begin{aligned}
\mathcal{QC} &:= \{\mathbb{Q}-\text{curves}\}\\
\mathcal{IJ} &:= \{E \text{ isogenous to } E_1 \mid j(E_1)\in\mathbb{Q}\}\\
\mathcal{J} &:= \{E \mid j(E)\in\mathbb{Q}\},\\
\mathcal{B} &:= \{E/\mathbb{Q}\},
\end{aligned}$$

Important tower of sets: $\mathcal{E} \supset \mathcal{QC} \supset \mathcal{IJ} \supset \mathcal{J} \supset \mathcal{B}$.

Which statements about Galois representaions of elliptic curves in each of these sets can we prove?

In particular are degrees of isogenies and sizes of torsion groups bounded?

I will not talk about CM elliptic curves. Their Galois representations are now well understood (Bourdon, Clark & collaborators, Lozano-Robledo).

Our tower of sets: $\mathcal{E} \supset \mathcal{QC} \supset \mathcal{IJ} \supset \mathcal{J} \supset \mathcal{B}$.

For each of these sets S and for $d \in \mathbb{Z}_+$ denote by $S(d)$ the set of all such elliptic curves defined over all number fields of degree d.

$T(S) :=$ set of all possible torsion groups of elliptic curves in S.

Obviously $\mathcal{E}(1) = \mathcal{QC}(1) = \mathcal{IJ}(1) = \mathcal{J}(1) = \mathcal{B}(1)$.

Mazur (1977):
$T(\mathcal{E}(1)) = \{C_n : n = 1, \ldots, 10, 12\} \cup \{C_2 \times C_{2m} : m = 1, \ldots, 4\}$

Torsion groups over quadratic fields

Our tower of sets: $\mathcal{E} \supset \mathcal{QC} \supset \mathcal{IJ} \supset \mathcal{J} \supset \mathcal{B}$.

$T(\mathcal{E}(2)) = \{C_n : n = 1, \dots, 16, 18\} \cup \{C_2 \times C_{2n} : n = 1, \dots, 6\}$
$\cup \{C_3 \times C_{3n}, n = 1, 2\} \cup \{C_4 \times C_4\}$(Kenku,Momose '88,Kamienny '92).

$T(\mathcal{B}(2)) = T(\mathcal{E}(2)) \backslash \{C_n, n = 11, 13, 14, 18\}$. (N. (2014)).

$T(\mathcal{J}(2)) = T(\mathcal{B}(2)) \cup \{C_{13}\}$ (Tzortzakis (2018), Gužvić (2019)).

$T(\mathcal{QC}(2)) = T(\mathcal{J}(2)) \cup \{C_{14}, C_{18}\}$. (Le Fourn, N. (2018)).

Le Fourn (2013): over any imaginary quadratic field Serre's uniformity conjecture is true for curves in $\mathcal{QC} \backslash (\mathcal{IJ} \cup \mathcal{CM})$.

Where do torsion groups and isogenies appear?

Our tower of sets: $\mathcal{E} \supset \mathcal{QC} \supset \mathcal{IJ} \supset \mathcal{J} \supset \mathcal{B}$.

Where do elliptic curves over quadratic fields with certain torsion groups and isogenies appear?

Curves with C_{13} torsion are in $\mathcal{J} \backslash \mathcal{B}$. (Bosman, Bruin, Dujella, N. (2014))

Curves wit C_{18} torsion are in $\mathcal{QC} \backslash \mathcal{IJ}$. (Bosman, Bruin, Dujella, N. (2014))

Curves wit C_{16} torsion are in $\mathcal{B}$ (Bruin, N. (2016).)

Similar results about elliptic curves with n-isogenies, for various n, over quadratic fields have been by Bruin, N. (2014), Ozman, Siksek(2016) and Box (2018).

Torsion groups over cubic fields

Our tower of sets: $\mathcal{E} \supset \mathcal{QC} \supset \mathcal{IJ} \supset \mathcal{J} \supset \mathcal{B}$.

Derickx, Etropolski, van Hoeij, Morrow and Zureick-Brown (2020):
$T(\mathcal{E}(3)) = \{C_n : n = 1, \ldots, 16, 18, 21\} \cup \{C_2 \times C_{2n} : n = 1, \ldots, 7\}$.

N. (2014): $T(\mathcal{B}(3)) = \{C_n : n = 1, \ldots, 10, 12, 13, 14, 18, 21\}$
$\cup \{C_2 \times C_{2n} : n = 1, \ldots, 4, 7\}$.

Gužvić (2019): $T(\mathcal{J}(3)) = T(\mathcal{B}(3))$.

Open problem: Determine $T(\mathcal{QC}(3))$ (this is equal to $T(\mathcal{IJ}(3))$, as will be seen).

Torsion bounds over general number fields

Our tower of sets: $\mathcal{E} \supset \mathcal{QC} \supset \mathcal{IJ} \supset \mathcal{J} \supset \mathcal{B}$.

Order of groups in $T(\mathcal{E}(d))$ is bounded by some B_d. (Merel (1996))

Order of groups in $T(\mathcal{B}(d))$ for d not divisible by primes ≤ 7 is bounded by 16. (Gonzalez-Jimenez and N. (2016))

Order of groups in $T(\mathcal{J}(p))$, for p prime is bounded by 28. (Gužvić (2019))

Theorem (Cremona, N. (2020))

Order of groups in $T(\mathcal{QC}(p))$ for $p > 7$ prime is bounded by 16.

If one includes $p = 2, 3, 5, 7$ then the correct bound is almost certainly 28.

No such absolute bound can exist for $T(\mathcal{E}(d))$ when d runs through any infinite set of positive integers.

Isogeny bounds

Our tower of sets: $\mathcal{E} \supset \mathcal{QC} \supset \mathcal{IJ} \supset \mathcal{J} \supset \mathcal{B}$.

$I(S) :=$ set of all possible cyclic isogeny degrees of elliptic curves in S.

Note $I(\mathcal{J}(d)) = I(\mathcal{B}(d))$.

Mazur (1978) and Kenku (1980s) determined $I(\mathcal{B}(1))$.

N. (2015) - the largest prime in $I((\mathcal{IJ} \backslash \mathcal{CM})(d))$ is bounded by $3d - 1$ (and by $d - 1$ if we assume a weaker version of Serre's uniformity conjecture, which has been proven by Le Fourn and Lemos (2020)).

Theorem (Cremona, N. (2020))

Let $L = \{2, 3, 5, 7, 11, 13, 17, 37\}$.

a) *The primes in* $I((\mathcal{QC} \backslash \mathcal{CM})(d))$ *for odd* d *are contained in* L.

b) *If* d *is not divisible by any prime* $\ell \in L$, *then* $\max I((\mathcal{QC} \backslash \mathcal{CM})(d)) = 37$.

c) *For odd* d, $\max I(\mathcal{QC}(d)) \leq B_d$ *for some constant* B_d *depending only on* d.

Fields of defintion: Removing the bar

Theorem (Elkies(1994))

Every non-CM $\mathbb{Q}$-curve over a number field K is $\overline{K}$-isogenous to an elliptic curve defined over a polyquadratic field F.

Theorem (Cremona, N. (2020))

Every non-CM $\mathbb{Q}$-curve over a number field K is K-isogenous to an elliptic curve with j-invariant in a polyquadratic field F.

So $F \subseteq K$ and moreover $\mathbb{Q}$-curve over an odd degree number field is isogenous to an elliptic curve with $j(E) \in \mathbb{Q}$.

Conjecturally (Elkies), the degree of the field F can be bounded by an absolute constant.

Proving these results

This means that for odd d we have $\mathcal{QC}(d) = \mathcal{IJ}(d)$ and the Galois representations of curves in $\mathcal{IJ}(d)$ are comparatively well understood and this allows us to obtain our results.

We also develop a quick algorithm to test whether a given curve E/K is a $\mathbb{Q}$-curve. It works (in the worst case) by computing the K-isogeny class.

Previously it was necessary to compute the K'-isogeny class, where K' is the Galois closure of K over $\mathbb{Q}$.

Sporadic points

Definition

We say that a point x of degree d on a curve X is **sporadic** if there are only finitely many points of degree $\leq d$.

When trying to determine $T(\mathcal{E}(d))$ and $I(\mathcal{E}(d))$ it is determining what the "sporadic groups" (those that appear finitely many times) are that is the hardest obstacle.

The groups that appear infinitely often in $T(\mathcal{E}(d))$ are known for $d \leq 6$: $d = 3$ proved by Jeon, Kim, Schweizer (2004), $d = 4$ by Jeon, Kim, Park (2006) and $d = 5, 6$ by Derickx, Sutherland (2016).

The sporadic groups in $T(\mathcal{E}(d))$ are known only for $d \leq 3$.

The degrees that appear infinitely often in $I(\mathcal{E}(d))$ are known for $d = 2$ (Bars, 1999) and $d = 3$ (Jeon, 2021), while the sporadic ones are known only for $d = 1$.

CM sporadic points

For large N and large degrees there is an abundance of CM sporadic points on $X_1(N)$.

Theorem (Clark, Genao, Pollack, Saia, 2019)

For all $N \geq 721$, the curve $X_1(N)$ has a sporadic CM point.

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

Let E be a CM elliptic curve. Then E corresponds to a sporadic point on $X_1(N)$ for infinitely many N.

So every CM j-invariant is a "sporadic j-invariant."

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

Assuming Serre's Uniformity Conjecture, there are only finitely many rational j-invariants giving rise to a sporadic point in $\cup_{N\in\mathbb{Z}_+} X_1(N)$.

The set of "sporadic j-invariants" in $\mathbb{Q}$ contains $-3^2 \cdot 5^6/2^3$, $-7 \cdot 11^3$ and all CM j-invariants.

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

Suppose there is a point $x \in X_1(N)$ *with*

$$\deg(x) < \frac{7}{1600}[\mathbb{PSL}_2(\mathbb{Z}) : \Gamma_1(N)].$$

Then x *is sporadic and for any positive integer* d *and any point* $y \in X_1(dN)$ *with* $\pi(y) = x$, *the point* y *is sporadic, where* π *denotes the natural map* $X_1(dN) \to X_1(N)$.

Sporadic points of small degree

N. 2012: The elliptic curve $E : y^2 + xy + y = x^3 - x^2 - 5x + 5$ with $j = -3^2 \cdot 5^6/2^3$ and LMFDB label 162.c3 has a point of order 21 over the cubic field $\mathbb{Q}(\zeta_9)^+$, while $X_1(21)$ has finitely many points of degree ≤ 3.

This is the least degree of sporadic point on $X_1(N)$ for any N.

There exists a positive finite number of elliptic curves (up to $\overline{\mathbb{Q}}$-isomorphism) with n-isogenies over $\mathbb{Q}$ for

$$n = 11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163.$$

So the lowest degree of a sporadic point on $X_0(n)$ is 1.

Bourdon, Gill, Rouse and Watson (2020): $j = -3^2 \cdot 5^6/2^3$ is the unique non-CM rational j-invariant giving rise to a sporadic point of odd degree on $X_1(N)$.

van Hoeij has a huge list of sporadic points on $X_1(N)$ for $N \leq 80$.

There are no sporadic points of degree 1 and 2, while there exist sporadic points of degree 3 and all $5 \leq d \leq 30$ (follows also from Derickx and van Hoeij's results on gonality of $X_1(N)$, 2014).

Question

Are there any sporadic points on $X_1(N)$ (or more generally $X_1(M, N)$) of degree 4?

Theorem (Bourdon, N., 2021)

Suppose that all non-CM $\mathbb{Q}$-curves corresponding to sporadic points on $X_1(p^2)$ lie in finitely many isogeny classes, as p varies through all primes. Then Serre's Uniformity Conjecture holds.

- Suppose $E/\mathbb{Q}$ is non-CM and $\rho_{E,p}$ non-surjective for $p > 37$. Then $\operatorname{im} \rho_{E,p} \leq C_{ns}^{+}(p)$, so $F := \mathbb{Q}(E[p])$ is of degree dividing $2(p^2 - 1)$.
- E has two independent p-isogenies over F, and so is F-isogenous to an elliptic curve E' with a F-rational cyclic p^2-isogeny and a F-rational point of order p which is in the kernel of this isogeny.
- E' has a point of order p^2 over an extension F'/F of degree dividing p, so at most $2p(p^2 - 1)$.
- For large enough p is always sporadic by Abramovich's bound.

Relationship to Serre's Uniformity Conjecture

Basically the same argument also proves:

Theorem (Bourdon, N., 2021)

Suppose that there are finitely many sporadic non-CM points on $X(p)$ corresponding to elliptic curves defined over $\mathbb{Q}$, as p varies through all primes. Then Serre's Uniformity Conjecture holds.

Odd degree sporadic points on $\mathbb{Q}$-curves

Question (Bourdon, N. (2021))

Does there exist only finitely many (isogeny classes of) non-CM $\mathbb{Q}$-curves giving rise to sporadic points on $X_1(N)$ for some N?

If yes, this would imply Serre's uniformity conjecture.

Theorem (Bourdon, N., 2021)

All the odd degree sporadic points on $X_1(N)$ corresponding to non-CM $\mathbb{Q}$-curves lie in the isogeny classes of $j = -3^2 \cdot 5^6/2^3$.

Theorem (Bourdon, N., 2021)

Let p be a prime. If $x = [E, P] \in X_1(p^k)$ is a sporadic point of odd degree corresponding to a $\mathbb{Q}$-curve, then E has CM.

Isogeny classes giving infinitely many sporadic points

Proposition (Bourdon, N. 2021)

Suppose that there is a non-CM point $x = [E, P] \in X_1(N)$ corresponding to a $\mathbb{Q}$-curve with

$$\deg(x) < \frac{7}{1600}[\mathbb{PSL}_2(\mathbb{Z}) : \Gamma_1(N)]. \qquad (1)$$

Then there exists infinitely many sporadic points $x' = (E', P')$ on the curves $X_1(dN)$ (with d varying), such that E' is isogenous to E and that all the $j(E')$ are pairwise distinct. If $\deg(x)$ is odd, we can obtain infinitely many sporadic points such x' such that $\deg(x')$ is odd.

The sporadic j-invariant $-7 \cdot 11^3$, which corresponds to a degree 6 point on $X_1(37)$ (which is of gonality 18) almost satisfies this.

If an elliptic curve with this j-invariant was non-surjective at any other prime apart from 37, it would satisfy (1).

Questions

Question

Does there exist a non-CM j-invariant that satisfies (1)?

Question

Does there exist a non-CM isogeny class with infinitely many sporadic points on $\cup_{N\in\mathbb{Z}_+} X_1(N)$*?*

Question

Does every non-CM isogeny class that has 1 sporadic point in $\cup_{N\in\mathbb{Z}_+} X_1(N)$ *have infinitely many?*

Question

What can we say about sporadic points on $X_1(N)$ *(or* $X_1(p^2)$*) of even degree?*

The end

Thanks for listening!