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

Filip Najman

University of Zagreb

joint with John Cremona (Warwick)

Modern Breakthroughs in Diophantine Problems
Online, 31. August 2020.

Definitions

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

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.

$\mathbb{Q}$-curves in Diophantine equations

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

Ellenberg (2004) + Bennett, Ellenberg and Ng (2010): Solved about $A^4 + B^2 = C^p$ and $A^4 + 2B^2 = C^p$ using $\mathbb{Q}$-curves.

Dieulefait (2004): results about $x^4 + y^4 = z^p$ using $\mathbb{Q}$-curves

Dieulefait and Freitas (2011): Solved $x^5 + y^5 = 2z^p$ or $3z^p$ using $\mathbb{Q}$-curves

Bennett and Chen (2012): Solved $a^2 + b^6 = c^p$ or $3c^p$ using $\mathbb{Q}$-curves

Chen (2012): Results $a^2 - 2b^6 = c^p$ using $\mathbb{Q}$-curves

Bennett, Chen, Dahmen and Yazdani (2014): results about $a^3 + b^{3n} = c^2$ using $\mathbb{Q}$-curves

Why else do we care about $\mathbb{Q}$-curves

Ribet (2004) (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.

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

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

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.

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

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

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

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

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

Also

$$\{\mathbb{Q} - \text{curves}\} \supset \{E \in \mathcal{E} \mid E \text{ has CM}\}.$$

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).

Torsion groups over $\mathbb{Q}$

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

Torsion groups over quadratic fields

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

$T(\mathcal{E}(2)) = \{C_n : n = 1, \ldots, 16, 18\} \cup \{C_2 \times C_{2n} : n = 1, \ldots, 6\}$
$\cup \{C_3 \times C_{3n}, n = 1, 2\} \cup \{C_4 \times C_4\}$(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 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).)

For
$n = 22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71$,
all curves with an n-isogeny, with finitely many explicitly stated exception, are in $\mathcal{QC} \backslash \mathcal{IJ}$ (Bruin, N. (2014)).

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)).

Isogeny bounds for $\mathbb{Q}$-curves

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.

$\mathbb{Q}$-classes

As the property of being a $\mathbb{Q}$-curve is twist and isogeny invariant, we see that it is a property of the $\overline{\mathbb{Q}}$-isogeny class.

We introduce the relation on $\overline{\mathbb{Q}}$ of $j_1 \sim j_2$ if elliptic curves E_1 and E_2 with $j(E_1) = j_1$ and $j(E_2) = j_2$ are in the same isogeny class.

This is an equivalence relation, so gives us a partition of $\overline{\mathbb{Q}}$ into isogeny classes.

We say that a class is a $\mathbb{Q}$-class if (all) elliptic curves in it are $\mathbb{Q}$-curves.

We say that a class is *rational* if it contains a $j \in \mathbb{Q}$.

Note that a rational class is automatically a $\mathbb{Q}$-class.

Structure of $\mathbb{Q}$-classes

To a pair of non-CM j_1, j_2 in the same class we define the *degree* $\deg(j_1, j_2)$ to be the degree of a cyclic isogeny between elliptic curves with those j-invariants.

We call an element j of a $\mathbb{Q}$-class a $\mathbb{Q}$-number.

The *degree* of a $\mathbb{Q}$-number j is the LCM of the degrees $\deg(j, g(j))$ for $g \in G_{\mathbb{Q}}$.

A $\mathbb{Q}$-number is *central* if it has square-free degree, in which case its Galois conjugacy class is called a *central (conjugacy) class*.

The existence of a central class in a $\mathbb{Q}$-class has first been proved by Elkies (1994).

Structure of $\mathbb{Q}$-classes

Theorem (Elkies $+\epsilon$)

Let $\mathcal{Q}$ be a non-CM $\mathbb{Q}$-class in $\overline{\mathbb{Q}}$. All central classes C in $\mathcal{Q}$ satisfy:

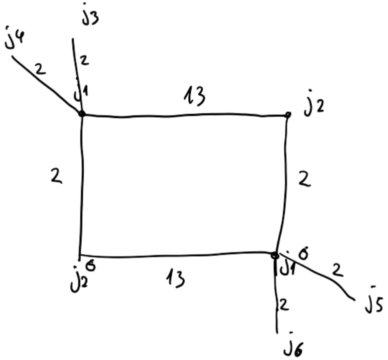
1. $|C| = 2^\rho$ *for some* $\rho \geq 0$;
2. $\mathbb{Q}(C)$ *is a polyquadratic field with* $\mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^\rho$;
3. *the square-free degree* N *of one (and hence all)* $j \in C$ *has* r *prime factors, where* $r \geq \rho$ *and* $r = 0 \iff \rho = 0 \iff \mathcal{Q}$ *is rational.*

The quantities N, r and ρ, and the field $\mathbb{Q}(C)$, are the same for each central class in $\mathcal{Q}$, and we denote them $N(\mathcal{Q})$, $r(\mathcal{Q})$ and $\rho(\mathcal{Q})$ and $L_{\mathcal{Q}}$ respectively.

Open problem : how large can N, r and ρ be? Are they bounded?

Equivalently: when do quotients of $X_0(N)$ by groups of Atkin-Lehner involutions have non-cuspidal $\mathbb{Q}$-points.

Elliptic curves with 26-isogenies over quadratic fields



Here $j_1, j_2 \in K$, where K is a quadratic field, $\sigma \in G_{\mathbb{Q}}$ acts non-trivially on K. j_i for $i = 3, 4, 5, 6$ are defined over a quadratic extension L of K.

There are 2 central classes $C_1 = \{j_1, j_1^\sigma\}$ and $C_2 = \{j_2, j_2^\sigma\}$ and one non-central class $C_3 = \{j_3, j_4, j_5, j_6\}$.

We have $N = 26$, $\rho = 1$, $r = 2$.

Fields of defintion

Lemma

Let E_1/K_1 be isogenous to E_2/K_2. Then E_1 is isogenous to a twist of E_2 over K_1K_2.

Proposition

Let $j \in \mathcal{Q}$, $\mathcal{Q}$ non-CM. Then $L_{\mathcal{Q}} \subseteq \mathbb{Q}(j)$.

So $2^{\rho(\mathcal{Q})} \mid [\mathbb{Q}(j) : \mathbb{Q}]$.

An immediate corollary of the proposition is that any $\mathbb{Q}$-curve E/K is K-isogenous to a central curve, which is itself a base change of an elliptic curve over a polyquadratic field.

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.

Theorem (Cremona, N. (2020))

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

This allows us to prove:

Theorem (The no-quadratic-subfields theorem)

If the non-CM $\mathbb{Q}$-class $\mathcal{Q}$ contains an element j such that $\mathbb{Q}(j)$ has no quadratic subfields, then $\mathcal{Q}$ is rational.

Proving our 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 which for an input of an elliptic curve quickly determines whether it is a $\mathbb{Q}$-curve or not.

The end

Thanks for listening!