Torsion points on elliptic curves over quintic and sextic number fields

Maarten Derickx [1] Andrew Sutherland [2]

[1] Universität Bayreuth

[2] MIT

Arithmetic Aspects of Explicit Moduli Problems
02-06-2017

Let $M, N, d \in \mathbb{N}$ such that $M \mid N$

Question

Does there exist a number field K with $[K : \mathbb{Q}] = d$ and an elliptic curve E/K such that $E(K)_{tors} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$?

Definition/Notation

- *$Y_1(M, N)/\mathbb{Z}[1/N]$ is the curve parametrizing triples (E, P, Q) of elliptic curve, with independent points of order M and N.*
- *$X_1(M, N)/\mathbb{Z}[1/N]$ is its projectivisation.*

Question

Does the curve $Y_1(M, N)_{\mathbb{Q}}$ contain a point of degree d over $\mathbb{Q}$?

Question

Does the curve $Y_1(M, N)_{\mathbb{Q}}$ contain ∞ many points of degree d over $\mathbb{Q}$?

Mazur's torsion theorem (d=1)

Theorem (Mazur)

If $E/\mathbb{Q}$ is an elliptic curve then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

- $\mathbb{Z}/N\mathbb{Z}$ *for* $1 \leq N \leq 10$ *or* $N = 12$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *for* $1 \leq N \leq 4$

And each of these groups occurs for infinitely many non isomorphic elliptic curves.

Uniform Boundedness Conjecture

Definition

A group G is an *elliptic torsion group* of degree d if $G \cong E(K)_{tors}$ for some elliptic curve E/K with $\mathbb{Q} \subseteq K$, $[K : \mathbb{Q}] = d$. The set of all isomorphism classes of such groups is denoted by $\Phi(d)$.

Theorem (Uniform Boundedness Conjecture)

$\Phi(d)$ is finite for all d.

Definition

A prime p is a *torsion prime* of degree d if there exist an $G \in \Phi(d)$ such that $p \mid \#G$.

The set of all torsion primes of degree d is denoted by $S(d)$.

What is known about torsion primes

$$S(d) := \{p \text{ prime} \mid \exists K/\mathbb{Q}\colon [K:\mathbb{Q}] \leq d, \exists E/K\colon p \mid \#E(K)_{tors}\}$$
$$Primes(n) := \{p \text{ prime} \mid p \leq n\}$$

- $\Phi(d)$ is finite $\Leftrightarrow S(d)$ is finite.
- $S(d)$ is finite (Merel)
- $S(d) \subseteq Primes((3^{d/2}+1)^2)$ (Oesterlé) not published
- $S(1) = Primes(7)$ (Mazur)
- $S(2) = Primes(13)$ (Kamienny, Kenku, Momose)
- $S(3) = Primes(13)$ (Parent)
- $S(4) = Primes(17)$ (Kamienny, Stein, Stoll) to be published.
- $S(5) = Primes(19)$ (D., Kamienny, Stein, Stoll) to be published.
- $S(6) = Primes(19) \cup \{37\}$ idem.

Remark For $d \leq 6$ and $p \in S(d)$, $p \neq 37$ there are ∞ many non isomorphic (E, K) such that $E(K)[p] \neq 0$.

What is known for torsion groups

Definition

Let $\Phi^\infty(d)$ denote the set of $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for which $X_1(M, N)$ has infinitely many places of degree d over $\mathbb{Q}$.

- $\Phi^\infty(d) \subseteq \Phi(d)$
- $\Phi^\infty(1) = \Phi(1) = \textit{known}$ (Mazur)
- $\Phi^\infty(2) = \Phi(2) = \textit{known}$ (Kenku,Momose,Kamienny)
- $\Phi^\infty(3), \Phi^\infty(4) = \textit{known}$ (Jeon,Kim,Park,Schweizer)
- $\Phi^\infty(3) \neq \Phi(3)$ (Najman)
- $\Phi(3) = \textit{known}$ (D.,Etropolski, Hoeij, Morrow, Zureick-Brown)
- The cyclic groups in $\Phi^\infty(d)$ are known for $d \leq 8$ (D., Hoeij)

Q2: When has $Y_1(N)$ ∞ many places of degree d

$j \in \mathbb{Q}(X_1(N))$ is a function of degree $[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] \geq \frac{3}{\pi^2}N^2$, hence $Y_1(N)$ has ∞ many places of degree $[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)]$.

Theorem (Abramovich)

$$\mathrm{gon}_{\mathbb{C}}(X_1(N)) \geq \frac{7}{800}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] \qquad (\geq \frac{7}{800}\frac{3}{\pi^2}N^2)$$

Theorem (Frey, (quick corollary of Faltings))

Let K be a number field and C/K be a curve, if C contains ∞ many places of degree d over K then

$$d \geq \mathrm{gon}_K(C)/2$$

Corollary

If $d < \frac{7}{1600}\frac{3}{\pi^2}N^2 \leq \mathrm{gon}_{\mathbb{C}}(X_1(N))/2 \leq \mathrm{gon}_{\mathbb{Q}}(X_1(N))/2$ then $X_1(N)$ contains only finitely many places of deg d.

For $X_1(M,N)$ one has upper and lower bounds quadratic in MN.

Q2: Two reasons for the existence of ∞ many places of degree d on a curve X over a number field K

Consider $u : X^{(d)} \to \mathrm{Pic}^{(d)} X$ and let $D \in X^{(d)}(K)$

1) if $r(D) := \dim |D| \geq 1$ then D occurs in a non constant infinite family of divisors of degree D ($|D| \cong \mathbb{P}^{r(D)}$).
2) if $W_d^0 := u(X^{(d)}) \subseteq \mathrm{Pic}^{(d)} X$ contains a translate of a rank > 0 abelian variety A s.t. $u(D) \in A(K)$, then $u^{-1} A(K)$ is a non constant infinite family of divisors of degree d that contains D.

Theorem (Faltings)

If $\# X^{(d)}(K) = \infty$ then there is a $D \in X^{(d)}(K)$ for which (1) or (2) holds.

Remark: If $\# Pic^{(d)} X(K) < \infty$ then $\mathrm{gon}_K X$ is the smallest degree for which X has infinitely many places of degree d over K. (No need for Faltings)

Some isomorphisms between modular curves

Let $M \mid N$ and d be integers such that $gcd(d, N) = 1$.

Definition

$X_1(M, N)$ is the modular curve parameterizing triples (E, P, Q) of an elliptic curve E, and points P, Q of order M, N such that $\langle P \rangle \cap \langle Q \rangle = 0$. $X_{0,1}(M, N)$ is the modular curve parameterizing triples (E, G, Q) of an elliptic curve E, a cyclic subgroup G of order M and a point Q of order N such that $G \cap \langle Q \rangle = 0$. $X_1(N) := X_1(1, N)$.

- $<d> : X_1(N) \xrightarrow{\sim} X_1(N) \quad (E, Q) \mapsto (E, dQ)$.
- $X_1(M, N) \xrightarrow{\sim} X_{0,1}(M, N) \times \mu'_M \quad (\cong X_{0,1}(M, N)_{\mathbb{Z}[1/N, \zeta_M]})$
  $(E, P, Q) \mapsto (E, \langle P \rangle, Q) \times e_M(P, N/MQ)$
- $X_1(MN)/<N+1> \xrightarrow{\sim} X_{0,1}(M, N)$
  $(E, P) \mapsto (E/(NP),\ E[M]/(NP),\ P \mod NP)$

In particular questions about $X_1(M, N)$ can be answered in terms of $(X_1(MN)/<N+1>)_{\mathbb{Q}(\zeta_M)}$.

Theorem (Kolyvagin,Logachev,Kato)

Let M, N be integers, $\chi : \mathbb{Z}/M\mathbb{Z}^* \to \mathbb{C}$ a character and A be a simple isogeny factor of $J_1(N)$ corresponding to a modular form f. Then the dimension of $(J_1(N)(\mathbb{Q}(\zeta_M)) \otimes_{\mathbb{Z}} \mathbb{C})^\chi$ is zero if $L(f, \chi, 1) \neq 0$.

Theorem (D., Sutherland)

The rank of $J_1(m, mn)$ is zero over $\mathbb{Q}(\zeta_m)$ if any of the following hold:

- $m = 1$ *and* $n \leq 36$;
- $m = 2$ *and* $n \leq 21$;
- $m = 3$ *and* $n \leq 10$;
- $m = 4$ *and* $n \leq 6$;
- $m = 5$ *and* $n \leq 4$;
- $m = 6$ *and* $n \leq 5$.

Proof.

Define $\gamma_\chi := \sum_{a \in (\mathbb{Z}/MZ)^*} \chi(a)\{\infty, a/M\}$ then $\tau(\overline{\chi})L(f, \chi, 1) = \int_{\gamma_{\overline{\chi}}} f$.
We checked computationally that the modular symbol γ_χ was nonzero in the modular symbol space corresponding to f. □

Lower bound for $\mathbb{Q}$-gonality by computing $\mathbb{F}_\ell$ gonality

Proposition

Let $C/\mathbb{Q}$ be a smooth projective curve and ℓ be a prime of good reduction of C then:

$$\text{gon}_{\mathbb{Q}}(C) \geq \text{gon}_{\mathbb{F}_\ell}(C_{\mathbb{F}_\ell})$$

To use this we need to know how compute the $\mathbb{F}_\ell$ gonality of C. Let $\text{div}_d^+ C_{\mathbb{F}_\ell} \subseteq \text{div}^+ C_{\mathbb{F}_\ell}$ be the set of effective divisors of degree d. Then $\#(\text{div}_d^+ C_{\mathbb{F}_\ell}) < \infty$. The following algorithm computes the $\mathbb{F}_\ell$-gonality:

1. set $d = 1$
2. While for all $D \in \text{div}_d^+ C_{\mathbb{F}_\ell}$: $\dim H^0(C, D) = 1$ set $d = d + 1$
3. Output d.

If $f : C_{\mathbb{F}_l} \to \mathbb{P}^1$ then there exists an $x \in \mathbb{P}^1(\mathbb{F}_l)$ with at least $\lceil \#C(\mathbb{F}_l)/(l+1) \rceil$ distinct $\mathbb{F}_l$-rational points in the fiber.
So only need to check effective divisor with at least $\lceil \#C(\mathbb{F}_l)/(l+1) \rceil$ rational points in its support.

Main Theorem

Theorem (D.,Sutherland)

$$\Phi^\infty(5) = \{(1,n) : 1 \leq n \leq 25,\ n \neq 23\} \cup \{(2,2n) : 1 \leq n \leq 8\},$$
$$\Phi^\infty(6) = \{(1,n) : 1 \leq n \leq 30,\ n \neq 23,25,29\} \cup \{(2,2n) : 1 \leq n \leq 10\}$$
$$\cup \{(3,3n) : 1 \leq n \leq 4\} \cup \{(4,4),(4,8),(6,6)\}.$$

Moreover if $(M,N) \in \Phi^\infty(d)$ *for* $d = 5,6$ *then* $X_1(M,N)$ *contains a function of degree* $d/\phi(M)$ *over* $\mathbb{Q}(\zeta_M)$.

Proof.

The hard part is showing that $(M,N) \notin \Phi^\infty$.From Abramovich bound + Frey's bound get that $(M,N) \notin \Phi^\infty(d)$ if $d < \frac{7}{1600}\frac{3}{\pi^2}N^2$ so this leaves finitely many cases.

In the finitely many remaining cases we either proved (by computation) $\mathrm{gon}_{\mathbb{Q}(\zeta_M)} X_1(M,N) > d/\phi(M)$ if rank $J_1(M,N)(\mathbb{Q}(\zeta_M)) = 0$ or $\mathrm{gon}_{\mathbb{Q}(\zeta_M)} X_1(M,N) > 2d/\phi(M)$ if $J_1(M,N)(\mathbb{Q}(\zeta_M)) > 0$. The Theorem follows from Frey's bound on degree d points in terms of gonality. □

Future Work

- More efficient algorithm to compute gonalities over finite fields (Brouwer-Zimmermann for generalized Hamming weight)
- Determine $\Phi^\infty(7)$ and $\Phi^\infty(8)$.
- Study theoretical problems for $\Phi^\infty(9)$, $J_1(37)(\mathbb{Q})$ has positive rank but and $\text{gon}_{\mathbb{Q}}(X_1(37)) = 18 \not> 2 \cdot 9$.

Generalized Hamming weight

Let n be an integer and $n = \sum_{i=0}^{k} \sum_{j=0}^{m_i} b_{i,j}$ be a partition partition of n.

Definition (Generalized Hamming Weight / GHW)

Let $x = (x_{i,j}) \in \mathbb{F}_p^n \cong \bigoplus_{i=0}^{k} \bigoplus_{j=0}^{m_i} \mathbb{F}_p^{b_{i,j}}$, then the GHW of x is

$$h_b(x) = \sum_{i=0}^{k} \sum_{j=0}^{l_i} b_{i,j}$$

where l_i is the largest j for which $x_{i,j} \neq 0$.

- Let b_{triv} be the partition with $k = n$ and both m_i and $b_{i,j}$ constant 1.
- $h_{b_{triv}}$ is the classical Hamming weight
- $h_{b_{triv}}(x) \leq h_b(x)$ for all $x \in \mathbb{F}_p^n$ and all partition partitions b.

Generalized Hamming weight and gonalities

Let $C/\mathbb{F}_p$ be a curve and $D = \sum_{i=0}^{k} m_i D_i$ be an effective divisor of degree n and let b_i denote degree of the field of definition of D_i.

Taking the negative parts of the laurent expansions at the D_i gives a map $H^0(C, D) \to \mathbb{F}_p^n \cong (O_C(D)/O_C)(C)$.

Write $n = \sum_{i=0}^{k} \sum_{j=0}^{m_i} b_i$.

The degree function on $H^0(C, D)$ agrees with the generalized Hamming weight on $\mathbb{F}_p^n$ with respect to the above partition partition.

In conclusion: Adaption of the Brouwer-Zimmermann algorithm for computing minimal weights to the Generalized Hamming weight gives a better than brute force algorithm for gonalities.