Finding all points of degree < gonality on $Y_1(N)$

Maarten Derickx [1] Mark van Hoeij [2]

[1] Algant (Leiden, Bordeaux and Milano)

[2] Florida State University

Harvard Number Theory Seminar
30-10-2013

Slides at: `bit.ly/sporadic-points`

Let $N, d \in \mathbb{N}$

Question

Does there exist a number field K with $[K : \mathbb{Q}] = d$ and an elliptic curve E/K such that $E(K)$ contains a point of exact order N.

Definition/Notation

- *$Y_1(N)/\mathbb{Z}[1/N]$ is the curve parametrizing pairs (E, P) of elliptic curves with a point of exact order N.*
- *$X_1(N)/\mathbb{Z}[1/N]$ is its projectivisation.*

Question

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

Up till now: fix d and find the answer for as many N as possible.
This talk: fix N and find the answer for as many d as possible.

Outline

1. Introduction
2. New results

Outline

1. Introduction

2. New results

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

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 $\leq d$ 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.
- $S(6) = Primes(23) \cup \{37\}$ idem.

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

Some rational points related questions

Fix integers $N, d > 0$ then:

1. does $Y_1(N)$ have a place of degree d over $\mathbb{Q}$?
2. does it have ∞ many places of degree d over $\mathbb{Q}$?
3. if there are finitely many places of deg d, can we find them all?
4. if there are ∞ many places, can we parametrize them all?

Answers to $1, 2$ are known for $d \leq 5$ and N prime (previous slide).

Goal of the 2nd half of this talk:
Answer question $1, 2$ and 3 for N small and all d.

Question 4 is also being worked on for some small N, d in a project by Barry Mazur, Sheldon Kamienny and me. (not the subject of this talk)

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

Let g be the genus of $X_1(N)$.
Then $j \in \mathbb{Q}(X_1(N))$ 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 d.

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 $C/\mathbb{Q}$ be a curve, if C contains ∞ many places of degree d then

$$d \geq \mathrm{gon}_{\mathbb{Q}}(C)/2$$

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.

M. v. Hoeij and I computed the exact $\mathbb{Q}$ gonality for $N \leq 40$.

Q2: Two reasons for the existence of ∞ many places of degree d on $Y_1(N)$

Consider $u : X_1(N)^{(d)} \to \operatorname{Pic}^{(d)} X_1(N)$ and let $D \in X_1(N)^{(d)}(\mathbb{Q})$

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 $W_d^0 := u(X_1(N)^{(d)}) \subseteq \operatorname{Pic}^{(d)} X_1(N)$ contains a translate of a rank > 0 abelian variety A s.t. $u(D) \in A(\mathbb{Q})$ then $u^{-1}A$ is a non constant infinite family of divisors of degree d that contains D.

Definition (Provisional/Just for this talk)

A place D of degree d of $Y_1(N)$ is called:

- **semi-sporadic** if D does not occur in a family as in 1)
- **sporadic** if D does not occur in a family as in 1) or 2)
- **very sporadic** if there are only finitely many places of degree d.

Question: Do there exist places of the above types?

Q1: When has $Y_1(N)$ a place of degree d?

Constructing places of low degree using CM

CM-construction

Let E/K be an elliptic curve with $\mathrm{End}_K\, E = \mathcal{O}_L$ and let $(p) = p_1 p_2 \subset \mathcal{O}_L$ a prime that splits and $P \in E[p_1](\bar{\mathbb{Q}}) \setminus \{0\}$. Then (E, P) gives a point on $Y_1(p)$ of degree $d \leq [K : \mathbb{Q}](p-1)$

Remark: This gives very sporadic points for p big enough since if $d < \frac{7}{1600}\frac{3}{\pi^2}p^2$ then there are only finitely many points of degree d.

Remark: The asymptotic behaviour of the biggest prime p such that there is a place of degree d is not known.

I.e. $d/2 + 1 \leq p$ if p splits in $\mathbb{Z}[i]$ v.s. $p < (3^{d/2} + 1)^2$

Question: Do there exists non CM (very/semi) sporadic points?

$Y_1(N)$ has only finitely many places of degree d if

$$d < \mathrm{gon}_{\mathbb{Q}}\, X_1(N)/2, \text{ or } d < \mathrm{gon}_{\mathbb{Q}} \text{ and } \#J_1(N)(\mathbb{Q}) < \infty.$$

so lets try to find all places of degree < gonality on $Y_1(N)$!

Remark: There is no reason why one couldn't have very sporadic points of degree > gonality.

Outline

1. Introduction
2. New results

Finding all points on degree < gonality on $Y_1(N)$

Two reasons why this rational point problem is easy for many small N

Proposition

Let $N \leq 55$, $N \neq 37, 43, 53$ then the rank of $J_1(N)(\mathbb{Q})$ is 0.

Definition

Let $\mathrm{Cl}^{csp} X_1(N) \subset \operatorname{Pic} X_1(N)(\bar{\mathbb{Q}})$ be the subgroup generated by the cusps, $\mathrm{Cl}^{csp}_{\mathbb{Q}} X_1(N) := \mathrm{Cl}^{csp} X_1(N) \cap \operatorname{Pic} X_1(N)(\mathbb{Q})_{tors}$ and $\mathrm{Cl}^{csp,d}_{\mathbb{Q}} X_1(N)$ its degree d part.

Proposition

Let $N \leq 55$. If $N \neq 24, 32, 33, 40, 48, 54$ then

$$\mathrm{Cl}^{csp,0}_{\mathbb{Q}} X_1(N) = J_1(N)(\mathbb{Q})_{tors}.$$

If $N = 24, 32, 33, 40, 48$ respectively 54 then

$$[J_1(N)(\mathbb{Q})_{tors} : \mathrm{Cl}^{csp,0}_{\mathbb{Q}} X_1(N)]$$

is a divisor of $2, 2, 2, 4, 16$ *respectively* 3.

Determining the rank 0 cases.

Proposition

Let $N \leq 55$, $N \neq 37, 43, 53$ then the rank of $J_1(N)(\mathbb{Q})$ is 0.

Proof.

$L(J_1(N), 1)/\Omega \in \mathbb{Q}$ is non-zero for these N (using Magma's L-ratio computation capabilities).And then use a generalization of a theorem of Kolyvagin and Logachev due to Kato, which states that isogeny factors of $J_1(N)$ have algebraic rank zero if they have analytic rank zero. $\square$

Determining the torsion

What was already known

Conjecture (Conrad,Edixhoven,Stein)

Let N be a prime then

$$\mathrm{Cl}_{\mathbb{Q}}^{csp,0}\, X_1(N) = J_1(N)(\mathbb{Q})_{tors}$$

Theorem (Ohta)

Let N be a prime then the index of $\mathrm{Cl}_{\mathbb{Q}}^{csp,0}\, X_1(N)$ *in* $J_1(N)(\mathbb{Q})_{tors}$ *is a power of* 2.

Remark In fact Conrad, Edixhoven and Stein conjectured and Ohta proved a stronger statement. Namely they proved the statement for the subgroup of $\mathrm{Cl}_{\mathbb{Q}}^{csp,0}\, X_1(N)$ generated by the cusps in $X_1(N)(\mathbb{Q})$.

Question

Does $\mathrm{Cl}_{\mathbb{Q}}^{csp,0}\, X_1(N) = J_1(N)(\mathbb{Q})_{tors}$ *generalize to composite levels?*

Determining the torsion

Proposition

Let $q \nmid 2N$ be a prime then $T_q - q\langle q\rangle - 1$ kills every element in $J_1(N)(\mathbb{Q})_{tors}$.

Proof.

Since $q \neq 2$ we have $J_1(N)(\mathbb{Q})_{tors} \hookrightarrow J_1(N)(\mathbb{F}_q)$. So it suffices to prove the statement for $J_1(N)(\mathbb{F}_q)$.
On $J_1(N)(\mathbb{F}_q)$ on has $1 = \mathrm{Frob}_q$ and $q = \mathrm{Ver}_q$. So the statement follows from $T_q - \mathrm{Ver}\langle q\rangle - \mathrm{Frob} = 0$ (Eichler-Shimura). $\square$

Determining the torsion

Proposition

Let $N \leq 55$. *If* $N \neq 24, 32, 33, 40, 48, 54$ *then*
$$\mathrm{Cl}_{\mathbb{Q}}^{csp,0} X_1(N) = J_1(N)(\mathbb{Q})_{tors}.$$

Proof.

$$J_1(N)(\mathbb{C}) \cong \Omega^1(X_1(N)(\mathbb{C}))^\vee / H_1(X_1(N)(\mathbb{C}), \mathbb{Z}), \text{ and}$$

$$J_1(N)(\bar{\mathbb{Q}})_{tors} \cong H_1(X_1(N)(\mathbb{C}), \mathbb{Q}) / H_1(X_1(N)(\mathbb{C}), \mathbb{Z})$$

this allows one to explicitly compute $T_q - q\langle q \rangle - 1$ on $J_1(N)(\bar{\mathbb{Q}})_{tors}$ in terms of modular symbols using Sage.

Let $M' \subseteq J_1(N)(\bar{\mathbb{Q}})_{tors}$ be the intersection of the kernel of $T_q - q\langle q \rangle - 1$ for several small q, and $M \subseteq M'$ the subgroup invariant under complex conjugation.

We verified using Sage that $M \subseteq \mathrm{Cl}^{csp,0} X_1(N)$ for the above N, so:
$$J_1(N)(\mathbb{Q})_{tors} \subseteq M^{\mathrm{Gal}\,\mathbb{Q}} \subseteq \mathrm{Cl}_{\mathbb{Q}}^{csp,0} X_1(N) \subseteq J_1(N)(\mathbb{Q})_{tors}$$

□

A finite problem

Proposition

Let $N \leq 55$*,* $N \neq 37, 43, 53$ *then the rank of* $J_1(N)(\mathbb{Q})$ *is* 0*.*
Let $N \leq 55$*,* $N \neq 24, 32, 33, 40, 48, 54$ *then*

$$\mathrm{Cl}_{\mathbb{Q}}^{csp,0} X_1(N) = J_1(N)(\mathbb{Q})_{tors}.$$

So for $N \leq 55$, $N \neq 24, 32, 33, 37, 40, 43, 48, 53, 54$ finding all places of degree d (more general finding all g_d^r's since places are g_d^0's) is a finite problem, "just" compute the inverse of $X_1(N)^{(d)}(\mathbb{Q}) \to \mathrm{Pic}^d X_1(N)(\mathbb{Q})$.

Algorithm solving this finite problem

for D in $\mathrm{Pic}^d X_1(N)(\mathbb{Q}) = \mathrm{Cl}_{\mathbb{Q}}^{csp,d} X_1(N)$ do:
  write $D = \sum n_i C_i$ with C_i cusps an $n_i \in \mathbb{Z}$.
  compute $H := H^0(X_1(N), \mathcal{O}(\sum n_i C_i))$
  if $\dim H = 0$ then D is not linearly equivalent to a $D' \geq 0$.
  else $|D| = \mathbb{P}(H)$ is a g_d^r with $r = \dim H - 1$

Finite but huge

$$\#J_1(39)(\mathbb{Q}) = 705125427552 \approx 7 \cdot 10^{11}, \qquad \text{genus} = 33$$
$$\#J_1(41)(\mathbb{Q}) \approx 1.1 \cdot 10^{17}, \qquad \text{genus} = 51$$
$$\#J_1(55)(\mathbb{Q}) \approx 2.5 \cdot 10^{22}, \qquad \text{genus} = 81$$

Computing $7 \cdot 10^{11}$ H^0's over $\mathbb{Q}$ on a genus 33 curve takes too long[1].

Solution If $\#J_1(N)(\mathbb{Q}) < \infty$ and $p \neq 2$ then ρ_2 is injective:

$$\begin{tikzcd} X_1(N)^{(d)}(\mathbb{Q}) \arrow[r, "u_{\mathbb{Q}}"] \arrow[d, "\rho_1"] & \operatorname{Pic}^d X_1(N)(\mathbb{Q}) \arrow[d, hook, "\rho_2"] \\ X_1(N)^{(d)}(\mathbb{F}_p) \arrow[r, "u_{\mathbb{F}_p}"] & \operatorname{Pic}^d X_1(N)(\mathbb{F}_p) \end{tikzcd}$$

So we have to compute $u_{\mathbb{F}_p}$ exactly $\#X_1(N)^{(d)}(\mathbb{F}_p)$ times. And only $\#\operatorname{im} u_{\mathbb{F}_p} \cap \operatorname{im} \rho_2 \quad (\approx \#X_1(N)^{(d)})(\mathbb{Q}))$ times ρ_2^{-1} and an H^0 over $\mathbb{Q}$.[2]

[1] i.e. using one of the world's super computers for more than a month.

[2] even less because if $d < \operatorname{gon}_{\mathbb{Q}} X_1(N)$ we can ignore those known to be in $\rho_2 \circ u_{\mathbb{Q}}$ and $\operatorname{im} u_{\mathbb{Q}}$, e.g. sums of $\operatorname{Gal}(\mathbb{Q})$-orbits of cusps.

How to compute $\rho_2^{-}1$

$$\rho_2 : \operatorname{Pic}^d X_1(N)(\mathbb{Q}) \to \operatorname{Pic}^d X_1(N)(\mathbb{F}_p)$$

If $\mathrm{Cl}_{\mathbb{Q}}^{csp} X_1(N) = J_1(N)(\mathbb{Q})$ then ρ_2^{-1} can be computed by writing $x \in \operatorname{Pic}^d X_1(N)(\mathbb{F}_p)$ as a sum of cusps, and lifting this sum of cusps.

$$\begin{tikzcd} X_1(N)^{(d)}(\mathbb{Q}) \arrow[r, "u_{\mathbb{Q}}"] \arrow[d, "\rho_1"] & \operatorname{Pic}^d X_1(N)(\mathbb{Q}) \arrow[d, hook, "\rho_2"] \\ X_1(N)^{(d)}(\mathbb{F}_p) \arrow[r, "u_{\mathbb{F}_p}"] & \operatorname{Pic}^d X_1(N)(\mathbb{F}_p) \end{tikzcd}$$

If $\mathrm{Cl}_{\mathbb{Q}}^{csp} X_1(N) \neq J_1(N)(\mathbb{Q})$ we might still find all sporadic points of degree d if $\operatorname{im} u_{\mathbb{F}_p} \cap \operatorname{im} \rho_2 \subseteq \rho_2(\mathrm{Cl}_{\mathbb{Q}}^{csp,d} X_1(N))$.

If $[J_1(N)(\mathbb{Q}) : \mathrm{Cl}_{\mathbb{Q}}^{csp} X_1(N)] \mid d$ then $\operatorname{im} u_{\mathbb{F}_p} \cap \operatorname{im} \rho_2 \subseteq \rho_2(\mathrm{Cl}_{\mathbb{Q}}^{csp,d} X_1(N))$ if every $P \in \operatorname{im} u_{\mathbb{F}_p}$ with $dP \in \rho_2(\mathrm{Cl}_{\mathbb{Q}}^{csp,d} X_1(N))$ is in $\rho_2(\mathrm{Cl}_{\mathbb{Q}}^{csp,d} X_1(N))$.

The number of diamond orbits of places on $Y_1(N)$ of degree d

d \ N	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
20	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
19	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
18	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
17	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	12	∞	∞	∞
16	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	11	∞	∞	∞
15	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	3	∞	10	∞
14	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	∞	∞
13	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	4	∞	1	∞	3	26
12	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	3	∞	3	∞
11	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	3	∞	9	∞	1	∞				4
10	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	2	∞	1	∞	∞	∞	2	∞	1	3	1	2
9	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	1	8	1	4		∞			1	1
8	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞		∞		∞	1	3	1	∞			1	1
7	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	∞	∞		∞			1			2				
6	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞		∞	1	∞	∞	∞		∞							1			
5	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞		∞	∞			1		2										
4	∞	∞	∞	∞	∞	∞	∞	∞		∞	∞	∞		∞																
3	∞	∞	∞	∞	∞	∞		∞		∞	1																			
2	∞	∞	∞	∞	∞	∞		∞																						
1		∞																												

correct if $\mathrm{Cl}^{csp}_{\mathbb{Q}} X_1(N) = J_1(N)(\mathbb{Q})_{tors}$

only lower bound

Final remarks:

- The majority of the very sporadic points found have a non integral j-invariant and hence are non-CM.
- The places of degree < 13 on $X_1(37)$ cannot be written as sums of cusps.
- $\operatorname{gon}_{\mathbb{Q}}(X_1(25)) = 5$ but there are no functions of degree 6 or 7 in $\mathbb{Q}(X_1(25))$. Since $\#J_1(25)(\mathbb{Q}) < \infty$ there are only finitely many points of degree 6 and 7, so the points of degree 6 and 7 are very sporadic but of degree > gonality.
- The elliptic curve 37a1 is the only $A \subset J_1(37)$ of positive rank. The lowest degree of an $f : X_1(37) \to 37a1$ is $36 < 40 = g(X_1(37))$ so $f^*(37a1) \subseteq W^0_{36}X_1(37)$. Let d be the smallest integer such that $37a1 \cong E \subseteq W^0_d X_1(37)$ then $E \not\subseteq W^1_d X_1(37)$ hence $\exists L \in E(\mathbb{Q})$ such that $\dim H^0(X_1(37), L) = 1$. So L is a semi-sporadic point that is not sporadic. Is $d < \operatorname{gon}_{\mathbb{Q}} X_1(37) = 18$?
- Is there an N such that $X_1(N)$ contains ∞ many places of degree < gonality? The degree 130 map from $X_1(131)$ to a rank > 0 elliptic curve probably gives rise to an example, but it's hard prove this.

Thank you!

The list of explicit sporadic points can be found at:

`www.math.fsu.edu/~hoeij/files/X1N/LowDegreePlaces`