The rational group structure of modular Jacobians

with applications to torsion points on elliptic curves over number fields

Maarten Derickx

[1] Algant (Leiden, Bordeaux and Milano)

LMFDB Workshop
05-06-2014

Talk will only start after you opened:
`bit.ly/rat-points-mod-jac`

Outline

Definitions and notation

- $N \in \mathbb{N}_{\geq 5}$, $\quad H \subseteq \mathbb{Z}/N\mathbb{Z}^*$
- K a field E/K and E'/K elliptic curves (EC).
- $E(K)[N]$ are the points of order N
- $E(K)[N]'$ are the points of order **exactly** N.
- $Y_1(N)(K) := \{(E, p) \mid E/K \text{ EC}, p \in E(K)[N]'\} / \sim$.
- $n \in \mathbb{Z}/N\mathbb{Z}^*$ acts on $Y_1(N)$ by sending (E, p) to (E, np)
- $Y_H := Y_1(N)/H$, $Y_0(N) = Y_H$ with $H = \mathbb{Z}/N\mathbb{Z}^*$.
- Let $p \in E(K)[N]'$ and $p' \in E'(K)[N]'$ then $(E, p) \sim_H (E', p')$ if there exists $\phi : E \tilde{\to} E'$ and $n \in H$ such that $\phi(p) = np'$.
- $Y_H(\bar{K}) \overset{1:1}{\longleftrightarrow} \{(E, p) \mid E/\bar{K} \text{ EC}, p \in E(\bar{K})[N]'\} / \sim_H$
- $X_H, X_0(N), X_1(N)$ are the compactifications of Y_H, $Y_0(N)$, $Y_1(N)$
- $J_H, J_0(N), J_1(N)$ are the Jacobians of $X_H, X_0(N), X_1(N)$.

Why J_H is awesome

used to prove part of BSD

Theorem (Wiles, Breuil, Conrad, Diamond, Taylor)

Every EC / $\mathbb{Q}$ occurs as an isogeny factor of $J_0(N)$

Conjecture (Weak Birch and Swinnerton-Dyer (Weak BSD))

Let A/K be an abelian variety over a number field then the order of vanishing of $L(A,s)$ at $s = 1$ equals the rank of $A(K)$

Part of Weak BSD has been proven for modular abelian varieties $\mathbb{Q}$:

Theorem ($J_0(N)$: Kolyvagin, Logachev. $J_H(N)$: Kato)

Let $A/\mathbb{Q}$ be an abelian variety isogenous to a sub abelian variety of $J_H(N)$ such that $L(A,1) \neq 0$ then $A(\mathbb{Q})$ has rank 0.

Why J_H is awesome

Studying questions about rational points on modular curves.

The structure of $J_H(\mathbb{Q})$ plays a crucial role in the proof of the following theorems:

Theorem (Mazur)

Let $E \to E'/\mathbb{Q}$ by an isogeny of prime degree p, then $p \leq 19$ or $p = 37, 43, 67, 163$

Theorem (Mazur)

Let $E/\mathbb{Q}$ be an EC then either

- *$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/N\mathbb{Z}$ for $1 \leq N \leq 10$, $N = 12$ or,*
- *$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $1 \leq N \leq 4$*

Theorem (Merel)

Let E/K by an EC over a number field, then $\#E(K) < M_d$ for some constant M_d only depending on $d := [K : \mathbb{Q}]$

Why J_H is awesome

Studying questions about rational points on modular curves.

Let (E, p) be a pair such that it's H equivalence class is defined over $\mathbb{Q}$, then (E, p) gives a rational point on X_H. Let

$$\begin{aligned} \mu_\infty : X_H &\to J_H \\ p &\mapsto p - \infty \end{aligned}$$

Let $\pi : J_H \to A$ be a map of abelian varieties s.t. $\#A(\mathbb{Q}) < \infty$.

$\pi \circ \mu_\infty$ maps $X_H(\mathbb{Q})$ to the finite set $A(\mathbb{Q})$ this gives a lot of restrictions on $X_H(\mathbb{Q})$.

Outline

1. Introduction

2. Determining $J_H(\mathbb{Q})$
   - When has $J_H(\mathbb{Q})$ rank 0
   - Determining $J_H(N)(\mathbb{Q})_{tors}$

3. Application to torsion points on elliptic curves (with Mark van Hoeij)

Theorem (Mazur)

$J_0(N)$ has rank > 0 for $N = 37, 43, 53, 61, 67$ or N a prime ≥ 73.

- Using magma (W. Stein) one can compute $L(J_1(N), 1)/\Omega_{J_1(N)}$
- $L(J_1(N), 1)/\Omega_{J_1(N)} \neq 0$ for all other primes N.
- So the proven part of BSD implies rank $J_1(N)(\mathbb{Q}) = \text{rank } J_H(\mathbb{Q}) = 0$ in the other cases.
- Same method allows everybody with access to magma to proof:

Proposition

If $N \in \mathbb{N}$, $N \neq 37, 43, 53, 57, 58, 61, 63, \ldots$ then rank $J_H(\mathbb{Q}) = 0$.

Remark: there are N such that $J_0(N)$ has rank 0 but $J_1(N)$ not.

Outline

A lot is known for prime level.

Theorem (Mazur)

Let N be prime and $0, \infty$ *the two cusps of* $X_0(N)$ *then* $J_0(N)(\mathbb{Q})_{tors}$ *is cyclic of order numerator* $(\frac{N-1}{12})$ *and generated by* $0 - \infty$*.*

Definition

$\mathrm{Cl}^{\mathbb{Q}-cusp,0}\, X_1(N)(\mathbb{Q}) \subseteq J_1(N)(\mathbb{Q})_{tors}$ is the subgroup generated by the differences of $\mathbb{Q}$-rational cusps in $X_1(N)(\bar{\mathbb{Q}})$.

Conjecture (Conrad,Edixhoven,Stein (CES))

Let N be a prime then $\mathrm{Cl}^{\mathbb{Q}-cusp,0}\, X_1(N)(\mathbb{Q}) = J_1(N)(\mathbb{Q})_{tors}$

Theorem (Ohta)

The index of $\mathrm{Cl}^{\mathbb{Q}-cusp,0}\, X_1(N)(\mathbb{Q})$ *in* $J_1(N)(\mathbb{Q})_{tors}$ *is a power of* 2 *for N prime.*

Three different cuspidal class groups

Definition

- $\mathrm{Cl}^{cusp} X_H \subseteq \mathrm{Pic}\, X_H$ is the group variety of sums of cusps in $X_H(\bar{\mathbb{Q}})$.
- $\mathrm{Cl}^{\mathrm{Gal}(\mathbb{Q})-cusp} X_H \subseteq \mathrm{Cl}^{cusp} X_H$ is the group variety of sums of $\mathrm{Gal}(\mathbb{Q})$-orbits of cusps in $X_H(\bar{\mathbb{Q}})$.
- $\mathrm{Cl}^{\mathbb{Q}-cusp} X_H \subseteq \mathrm{Cl}^{\mathrm{Gal}(\mathbb{Q})-cusp} X_H$ is the group variety of sums of $\mathbb{Q}$-rational cusps in $X_H(\bar{\mathbb{Q}})$.

- in general $\mathrm{Cl}^{\mathrm{Gal}(\mathbb{Q})-cusp} X_H \neq \mathrm{Cl}^{cusp} X_H$
- computations suggest $\mathrm{Cl}^{\mathrm{Gal}(\mathbb{Q})-cusp} X_H(\mathbb{Q}) = \mathrm{Cl}^{cusp} X_H(\mathbb{Q})$
- If N prime then $\mathrm{Cl}^{\mathbb{Q}-cusp} X_H = \mathrm{Cl}^{\mathrm{Gal}(\mathbb{Q})-cusp} X_H$ but for composite N one often has $\mathrm{Cl}^{\mathbb{Q}-cusp} X_H(\mathbb{Q}) \neq \mathrm{Cl}^{\mathrm{Gal}(\mathbb{Q})-cusp} X_H(\mathbb{Q})$

The right generalization of the Conrad Edixhoven Stein conjecture

Definition

- $\mathrm{Cl}^{cusp}\, X_H \subseteq \mathrm{Pic}\, X_H$ is the group variety of sums of cusps in $X_H(\bar{\mathbb{Q}})$.
- $\mathrm{Cl}^{\mathrm{Gal}(\mathbb{Q})-cusp}\, X_H \subseteq \mathrm{Cl}^{cusp}\, X_H$ is the group variety of sums of $\mathrm{Gal}(\mathbb{Q})$-orbits of cusps in $X_H(\bar{\mathbb{Q}})$.
- $\mathrm{Cl}^{\mathbb{Q}-cusp}\, X_H \subseteq \mathrm{Cl}^{\mathrm{Gal}(\mathbb{Q})-cusp}\, X_H$ is the group variety of sums of $\mathbb{Q}$-rational cusps in $X_H(\bar{\mathbb{Q}})$.

Theorem (Manin-Drinfeld)

$$\mathrm{Cl}^{cusp,0}\, X_H(\bar{\mathbb{Q}}) \subseteq J_H(\bar{\mathbb{Q}})_{tors}$$

Conjecture (Generalized CES)

$$\mathrm{Cl}^{cusp,0}\, X_H(\mathbb{Q}) = J_H(\mathbb{Q})_{tors}$$

Proposition

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

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

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

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

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

- The proposition is proved using two different approaches for computing multiplicative upper bounds on $J_1(N)(\mathbb{Q})_{tors}$
- CES: count point on $J_1(N)(\mathbb{F}_p)$ for different values of p.
- Other approach based on finding hecke operators that kill $J_1(N)(\mathbb{Q})_{tors}$.
- Sometimes taking gcd of both multiplicative upper bounds gives a better result.

Killing the torsion

Proposition

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

Proof.

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

Proposition

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

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

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

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

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

Idea behind the proof.

Use that $T_q - q\langle q\rangle - 1$ kills all elements in $J_1(N)(\mathbb{Q})$.
Compute

$$M_q := \ker(T_q - q\langle q\rangle - 1 : J_1(N)(\bar{\mathbb{Q}})_{tors} \to J_1(N)(\bar{\mathbb{Q}})_{tors})$$

for several small $q_1, \ldots, q_n \nmid 2N$.
Compute $M = \cap_i M_{q_i}$ and let $M' \subset M$ be the ones invariant under complex conjugation.
If $M' \subset \mathrm{Cl}^{cusp,0} X_1(\bar{\mathbb{Q}})$ then $\mathrm{Cl}^{cusp,0} X_1(\mathbb{Q}) = J_1(N)(\mathbb{Q})_{tors}$. If $M' \not\subseteq \mathrm{Cl}^{csp,0} X_1(N)$ then one can still get an upper bound on the index. □

Outline

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*

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

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^r_d's since places are g^0_d'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 $\mathrm{Pic}^d X_1(N)(\mathbb{Q}) = \mathrm{Cl}^{cusp,0} X_1(\mathbb{Q})$ 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^r_d with $r = \dim H - 1$

Finite but huge

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

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:

$$\begin{array}{ccc} X_1(N)^{(d)}(\mathbb{Q}) & \xrightarrow{u_{\mathbb{Q}}} & \operatorname{Pic}^d X_1(N)(\mathbb{Q}) \\ \downarrow \rho_1 & & \hookdownarrow \rho_2 \\ X_1(N)^{(d)}(\mathbb{F}_p) & \xrightarrow{u_{\mathbb{F}_p}} & \operatorname{Pic}^d X_1(N)(\mathbb{F}_p) \end{array}$$

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] using the worlds three most powerful 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.

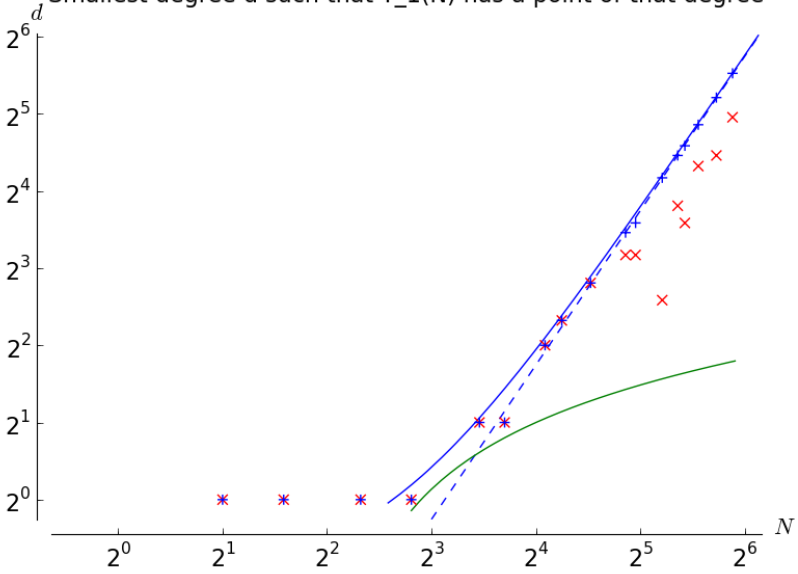
The number of diamond orbits of places on $Y_1(N)$ of degree d

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

Smallest degree d such that Y_1(N) has a point of that degree



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.
- $\text{gon}_{\mathbb{Q}}(X_1(25)) = 5$ 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. Degree > gonality doesn't necessarily imply that there are ∞ points of that degree.
- The same strategy should also work for $X_0(N)$ or more generally X_H and N small we just did not write the code yet.

Thank you!

The list of explicit sporadic points can be found at:

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

The code which is still work in process can be found at:

`https://github.com/koffie/mdsage`

`https://github.com/koffie/mdmagma`