Rational Torsion Subgroups of the Modular Jacobians

William Stein

October 1, 2011

Abstract

The goal (not yet done) of this paper is to show that the group $J_1(p)(\mathbb{Q})_{\mathrm{tor}}$ is cuspidal for all $p \leq 157$. Etc.

1 Introduction

Let J be the Jacobian of a modular curve. We give an approach to computing $J(\mathbb{Q})_{\mathrm{tor}}$ in certain cases.

Acknowledgement: Loic Merel. Michael Stoll. Barry Mazur. John Voight.

2 Annihilating Torsion

Let J be $J_1(N)$, $J_0(N)$, or $J_H(N)$ for any subgroup H of $(\mathbb{Z}/N\mathbb{Z})^*$. For any prime $\ell \nmid N$, let $J(\mathbb{F}_\ell)$ denote the group of points over $\mathbb{F}_\ell$ on the special fiber of the Néron model of J modulo ℓ. Let $S = J(\mathbb{Q})_{\mathrm{tor}}$.

Lemma 2.1. *For any prime $\ell \nmid 2N$, we have $S \hookrightarrow J(\mathbb{F}_\ell)$.*

Proof. See [Kat81, Appendix]. □

Remark 2.2. The above lemma also extends to $\ell \mid N$ if we let $J(\mathbb{F}_\ell)$ denote the group of points on the special fiber of the Néron model.

For any prime $\ell \nmid 2N$, let $\eta_\ell = T_\ell - (1 + \langle \ell \rangle \ell) \in \mathrm{End}(J)$.

Lemma 2.3. *For every $\ell \nmid 2N$, we have $S \subset J(\mathbb{R})[\eta_\ell]$.*

Proof. The Eichler-Shimura relation (see, e.g., [RS01, Thm. 5.16]) asserts that on $J_{\mathbb{F}_\ell}$ we have

$$T_\ell \equiv F + \langle \ell \rangle F^\vee,$$

where F is Frobenius and $F^\vee$ is the dual of Frobenius, so $F^\vee \circ F = F \circ F^\vee = [\ell]$. If $x \in J(\mathbb{F}_\ell)$, then $F(x) = x$, so $\ell x = F^\vee \circ F(x) = F^\vee(x)$. For any $P \in S$, the rational torsion points $T_\ell(P)$ and $P + \langle \ell \rangle \ell P$ both reduce to the same element of $J(\mathbb{F}_\ell)$, so Lemma 2.1 implies that $T_\ell(P) = P + \langle \ell \rangle \ell P$, so $\eta_\ell(P) = 0$. Finally note that $S \subset J(\mathbb{Q}) \subset J(\mathbb{R})$. □

2.1 The Real Eisenstein Ideal

Let I be the ideal generated by η_ℓ for $\ell \nmid 2N$, and let

$$J[I] = \bigcap_{\ell \nmid 2N} J[\eta_\ell].$$

Lemma 2.3 implies that $S \subset J[I](\mathbb{R})$. Let C be the *cuspidal subgroup*, which is the subgroup of $J(\overline{\mathbb{Q}})$ generated by differences of cusps. When $J[I](\mathbb{R}) \subset C$, we thus have $S = C(\mathbb{Q})$, which is useful in practice since $C(\mathbb{Q})$ is computable (see [Ste82]).

Passing from $J[I](\mathbb{C})$ to $J[I](\mathbb{R})$ is crucial to our strategy, because often $J[I]$ is strictly larger than C. For example, consider $J = J_0(p)$, with p prime. Then $C = \langle (0) - (\infty) \rangle$ is cyclic of order the numerator n of $(p-1)/12$. The $\eta_\ell = T_\ell - (1+\ell)$ generate the ideal I, which is contained in (see [**?**, pg. 95]) the Eisenstein ideal $\mathcal{I} = I + (1+w)$, where w is the Atkin-Lehner involution. By [**?**, Prop. 11.1 on pg. 98 and Prop. 11.7 on pg. 100] $J[\mathcal{I}]$ contains both the cuspidal subgroup C, and the Shimura subgroup Σ (also of order n), which is μ-type. We conclude that (usually) $J[I]$ is not equal to C. More concretely, when $p = 11$, we have $J[I] = J[5] \cong (\mathbb{Z}/5\mathbb{Z})^2$, but $C \cong (\mathbb{Z}/5\mathbb{Z})$. Continuing our discussion with $p = 11$ in which J is an elliptic curve, any construction involving Hecke operators (even including bad primes) or Atkin-Lehner operators cannot result in an ideal I' such that $J[I'] = C$, since $\mathrm{End}_{\mathbb{C}}(J) = \mathbb{Z}$, so $J[I'] = (\mathbb{Z}/m\mathbb{Z})^2$ (some m) for all nonzero ideals I'. However, by introducing the $*$-involution, we obtain a bigger ring $\mathbb{T}^* = \mathbb{T}[*]$, which is *not* a subring of $\mathrm{End}(J)$, but for which there is an ideal I^* with $J(\mathbb{C})[I^*] = C$ in this case. The ring $\mathbb{T}^*$ acts via endomorphisms of the abelian group $J(\mathbb{C})$, but not as a ring of endomorphisms of the abelian variety J.

Henceforth we let I^* denote the ideal in $\mathbb{T}^* \subset \mathrm{End}(J(\mathbb{C}))$ generated by I and $* - 1$. We call I^* the *real Eisenstein ideal*, and let

$$E = E(J) = J(\mathbb{C})[I^*] = J[I](\mathbb{R}),$$

which is a finite group that contains $S = J(\mathbb{Q})_{\mathrm{tor}}$.

3 Computing C and Bounding E

Let Γ be a congruence subgroup such as $\Gamma_1(N)$, $\Gamma_0(N)$, or $\Gamma_H(N)$, let $X = X_\Gamma$ be the corresponding modular curve, and $J = \mathrm{Jac}(X)$.

Modular symbols [] provide an explicit realization of $H = \mathrm{H}_1(X, \mathbb{Z})$ in terms of paths between cusps. Let $V = H \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{H}_1(X, \mathbb{Q})$. We represent $J(\overline{\mathbb{Q}})_{\mathrm{tor}}$ as V/H. To any ordered pair $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$ of cusps, we associate the modular symbol $\{\alpha, \beta\} \in V$, which equals the rational homology class corresponding to the functional $\omega \mapsto \int_\alpha^\beta \omega$ on the space $\mathrm{H}^0(X, \Omega^1_X)$ of holomorphic 1-forms. Let $\pi : V \to V/H$ be the natural quotient map.

We can compute the cuspidal subgroup C using modular symbols as follows. Let $r_1, \ldots, r_n$ be right coset representatives for Γ in $\mathrm{SL}_2(\mathbb{Z})$. Then (using Manin's trick as in [] or induction as in [MTT86]), the images in $J(\overline{\mathbb{Q}})_{\mathrm{tor}} = V/H$ of the n elements $\{r_i(0), r_i(\infty)\} \in V$ generates C. We thus represent C explicitly by the lattice $\pi^{-1}(C) \subset V$. We have that $\pi^{-1}(C)/H \cong C$.

The Hecke and diamond bracket operators can also be computed explicitly on modular symbols, hence on V (see []). We can explicitly compute endomorphisms e_ℓ of V that induce η_ℓ on V/H. Viewing $\ker(\eta_\ell)$ as a subgroup of V/H, we have

$$\pi^{-1}(\ker(\eta_\ell)) = e_\ell^{-1}(H) \subset V.$$

Finally, using modular symbols, we can also compute the $*$-involution (see []) explicitly on V and hence on V/H. Just as above, we have

$$\pi^{-1}(J(\mathbb{C})_{\mathrm{tor}}[*-1]) = (*-1)^{-1}(H) \subset V.$$

Taken together the above observations yield an algorithm to compute a nonincreasing sequence of groups that contains $J(\mathbb{C})[I^*]$, using any finite number of η_ℓ.

Remark 3.1. The following is useful for carrying out some of the above computations. Suppose A is an invertible $n \times n$ matrix with integer entries, which we view as an endomorphism of $\mathbb{Z}^n$. Then the rows of A^{-1} form a basis for $A^{-1}(\mathbb{Z}^n) \subset \mathbb{Q}^n$. This is because $A \cdot A^{-1} = I_n$.

4 Examples

Recall that for a modular Jacobian J, we defined the cuspidal subgroup $C \subset J$ and the real Eisenstein subgroup $E \subset J$ in Section 2.1 above.

4.1 $J_0(24)$

The Jacobian associated to $\Gamma = \Gamma_0(24)$ is the elliptic curve $y^2 = x^3 - x^2 - 4x + 4 = (x-2)(x-1)(x+2)$.

Proposition 4.1. *We have* $C = J(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$*, but* $E \approx \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$*.*

Proof. The claim for $J(\mathbb{Q})_{\mathrm{tor}}$ is a standard computation. To compute C, we compute the Galois action on the full cuspidal subgroup, and find that $C(\overline{\mathbb{Q}}) = C(\mathbb{Q})$ and that $C \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Since $C = C(\mathbb{Q}) \subset J(\mathbb{Q})_{\mathrm{tor}}$ and both have order 8, they are equal.

```
sage: J0(24).rational_cuspidal_subgroup()
Finite subgroup with invariants [2, 4] over QQ of Abelian
variety J0(24) of dimension 1
```

For any prime $\ell \nmid 2N$, we have

$$8 = \#J(\mathbb{Q})_{\mathrm{tor}} \mid \#J(\mathbb{F}_\ell) = a_\ell - (\ell+1) = \eta_\ell.$$

For $\ell = 5$, we have $\eta_5 = T_5 - (5+1) = -2 - (5+1) = -8$, so

$$I = (\eta_\ell : \ell \nmid 2N) = (8) \subset \mathbb{T} = \mathbb{Z}.$$

Thus $E = J(\mathbb{R})[8]$. Since J has 2 real components, we have $J(\mathbb{R}) \approx \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{R}/\mathbb{Z})$, so $E = J(\mathbb{R})[8] \approx \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. $\square$

4.2 $J_0(30)$

Let $J = J_0(30)$, which has dimension 3. We have $C = C(\mathbb{Q}) \approx \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$. The subgroup $E' \subset J(\mathbb{R})$ computed using η_ℓ for $\ell = 7, 11, 13$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$, and it stabilizes at this group even if we include all η_ℓ for $\ell < 500$. Similarly, the gcd of $\#J(\mathbb{F}_\ell)$ for $7 \leq \ell < 500$ is equal to $2 \cdot 2 \cdot 8 \cdot 24$. So there are 3 possibilities for the order of $T = J(\mathbb{Q})_{\mathrm{tor}}$.

The abelian variety J is "built" out of 3 elliptic curves (in the notation of [**?**]): $A =$ **15a**?, $B =$ **15a**?, and $C =$ **30a1**, i.e., we have $A, B, C \subset J$, and $A + B + C = J$, and there is an isogeny $A \times B \times C \to J$.

Challenge: Figure out what $J(\mathbb{Q})_{\mathrm{tor}}$ actually is.

5 Application: $J_1(p)$

In [CES03, §6.2.3], the author conjectured that $J_1(p)(\mathbb{Q})_{\mathrm{tor}}$ is cuspidal for all primes p, and computationally verified this for all $p \leq 157$, except $p = 29, 97, 101, 109, 113$.

This is of interest because of [], which classifies the possible prime orders of torsion points on elliptic curves over number fields of degree 4 (and 5?). Some parts of that computation are dramatically simplified by knowing that $J_1(p)(\mathbb{Q})_{\mathrm{tor}}$ is cuspidal for certain small p, e.g., $p = 29$.

The result of [CES03, §6.2.3] is that for the $p \leq 157$, we know that $J_1(p)(\mathbb{Q})_{\mathrm{tor}}(\ell)$ is cuspidal, except possibly for the following pairs (p, ℓ):

$$\{(29, 2), (97, 17), (101, 2), (109, 3), (113, 2), (113, 3)\}.$$

In this section, we deal with the above cases. [[**Not done yet!**]]

Everything after this is old and to be deleted.

6 Application: $J_1(p)$

Proposition 6.1. *The group T is the group generated by $(\alpha) - (\beta)$, where α, β are the rational cusps on $X_1(29)$, i.e., the cusps in the fiber over ∞ of the map $X_1(29) \to X_0(29)$. In particular, T has order $2^6 \cdot 3 \cdot 7 \cdot 43 \cdot 17837$.*

This is wrong: really we have to take det on full homology and get square of good bound. In particular, we obtain a multiple of the order of T:

$$\#T \mid \gcd(\{\det(\eta_\ell) : \ell \neq 2, 29\}),$$

where, e.g., we compute the determinant of η_ℓ acting on the $+1$ quotient of weight 2 cuspidal modular symbols for $\Gamma_1(p)$. Implementing this algorithm, we find that the gcd appears to stabilize at $2^{12} \cdot 3 \cdot 7 \cdot 43 \cdot 17837$:

```
sage: M = ModularSymbols(Gamma1(29), sign=1)
sage: S = M.cuspidal_subspace()
sage: dbd = lambda d: S.diamond_bracket_operator(d).matrix()
sage: eta = lambda ell: (S.hecke_matrix(ell) - (1 + dbd(ell)*ell))
sage: factor(gcd([ZZ(eta(ell).det()) for ell in [3,5,7,11]]))
2^12 * 3 * 7 * 43 * 17837
sage: factor(gcd([ZZ(eta(ell).det()) for ell in [3,5,7,11,13,17,19]]))
2^12 * 3 * 7 * 43 * 17837
```

We know from [CES03, §6.2.3] that $\#T = 2^n \cdot 3 \cdot 7 \cdot 43 \cdot 17837$, where $6 \leq n \leq 12$, where the lower bound of 6 comes because the rational cuspidal subgroup of J has order $2^6 \cdot 3 \cdot 7 \cdot 43 \cdot 17837$, according to a formula of Kubert-Lang.

Proof of Proposition 6.1. Let $H_\mathbb{Z} = \mathrm{H}_1(X_1(29), \mathbb{Z})$ and $H_\mathbb{Q} = \mathrm{H}_1(X_1(29), \mathbb{Q}) = H_\mathbb{Z} \otimes \mathbb{Q}$. Let $M_\ell = \eta_\ell^{-1}(H_\mathbb{Z}) \subset H_\mathbb{Q}$, so we have a canonical isomorphism $J[\eta_\ell] \cong M_\ell / H_\mathbb{Z}$ induced by $J(\mathbb{C})_{\mathrm{tor}} \cong H_\mathbb{Q}/H_\mathbb{Z}$. Let $H_\mathbb{Q}^+$ be the $+1$ eigenspace for the $*$-involution, which is the involution induced by complex conjugation. Let $M = M_3 \cap M_5 \cap M_7$ and $W = M^+/H_\mathbb{Z}$. We have that $W/H_\mathbb{Z} \cong (M/H_\mathbb{Z})^+$, because the real component group of $J_1(p)$ is trivial (new theorem of XXX, plus use a snake lemma to see relevance of this...)

....

□

Question 6.2. Let C be the cuspidal subgroup of $J_1(p)$, and let I be the ideal generated by all η_ℓ for primes $\ell \neq 2, p$. Is $C = J_1(p)[I]$? Do we need to throw in something for $\ell = 2, p$? Is $J_1(p)(\mathbb{Q})_{\mathrm{tor}} = J_1(p)(\mathbb{R})[I]$?

7 Elkies Question

He is interested in rational torsion being cuspidal on $J_0(N)$. See `https://mail.google.com/mail/?shva=1#mbox/12fa91fc242e72f0` in my email.

N = 30, 33, 35, 39, 40, 41, and 48 for genus 3; N = 47 for g=4; N = 46 and 59 for g=5; and N = 71 for g=6.

References

[CES03] B. Conrad, S. Edixhoven, and W. A. Stein, *$J_1(p)$ Has Connected Fibers*, Documenta Mathematica **8** (2003), 331–408, `http://www.wstein.org/papers/j1p/`.

[Kat81] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. MR 82d:14025

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48. MR MR830037 (87e:11076)

[RS01] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, `http://wstein.org/papers/serre/`, pp. 143–232. MR 2002h:11047

[Ste82] G. Stevens, *Arithmetic on modular curves*, Birkhäuser Boston Inc., Boston, Mass., 1982. MR 87b:11050