Nonvanishing Twists and Visible Shafarevich-Tate Groups*

William A. Stein

October 1, 2001

Let E be an elliptic curve over $\mathbb{Q}$. Our long-term goal is to find, for many primes p, rank 0 abelian varieties A such that

$$0 \to A \to J \to E \to 0$$

induces an isomorphism

$$E(\mathbb{Q})/pE(\mathbb{Q}) \cong \mathrm{Vis}_J(Ш(A)[p]) = \ker(Ш(A)[p] \to Ш(J)).$$

Such results are useful in connecting the rank 0 BSD formula to the conjecture that $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rk}(E)$.

1 Terminology

This should be enough to help you guess my notation:

- $\Phi_{E,p}$ denotes the component group of the Néron model of E at p.
- N_E is the conductor of E.
- A prime p is **rigid** for E if

  $$p \nmid 2 \cdot N_E \cdot \prod_{\ell \mid N_E} \#\Phi_{E,\ell}(\overline{\mathbb{F}}_\ell)$$

  and

  $$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$$

  is irreducible.

*These are notes for a Modular Curves Seminar talk.

2 Visibility Theory

Visibility theory has been developed by Barry Mazur, Amod Agashe, and myself, with periodic help from Brian Conrad.

Let $A \hookrightarrow J$ be a closed immersion of abelian varieties. Then

$$\mathrm{Vis}_J(\text{Ш}(A)) = \ker(\text{Ш}(A) \to \text{Ш}(J)).$$

Theorem 2.1. *Suppose $A, B \subset J$, and $(A \cap B)(\overline{\mathbb{Q}})$ is finite. If p is a prime such that $B[p] \subset A$ and*

$$p \nmid 2 \cdot N_J \cdot \#(J/B)(\mathbb{Q})_{\mathrm{tor}} \cdot \#B(\mathbb{Q})_{\mathrm{tor}} \cdot \prod_{\ell \mid N_J} \left(\#\Phi_{A,\ell}(\mathbb{F}_\ell) \cdot \#\Phi_{B,\ell}(\mathbb{F}_\ell)\right),$$

then

$$B(\mathbb{Q})/pB(\mathbb{Q}) \cong \mathrm{Vis}_J(\text{Ш}(A)[p]).$$

For the proof, look at [Agashe-Stein, *Visibility of Shafarevich-Tate Groups of Abelian Varieties*]. It uses the snake lemma, and a careful local analysis at each prime that uses standard arithmetic geometry tools.

3 A Conjecture About Nonvanishing of Twists

Fix E and suppose p is rigid for E. For every $\ell \equiv 1 \pmod{p}$, fix

$$\chi_{p,\ell} : (\mathbb{Z}/\ell\mathbb{Z})^* \twoheadrightarrow \boldsymbol{\mu}_p$$

of order p and conductor ℓ.

Conjecture 3.1 (–). *There exists a prime $\ell \nmid N_E$ such that*

$$L(E, \chi_{p,\ell}, 1) \neq 0$$

and

$$a_\ell(E) \not\equiv \ell + 1 \pmod{p}.$$

Evidence: The conjecture is true for every pair (E, p) I've tried, e.g., for all rigid $p < 50$ for the first 20 rank 1 optimal quotients of $J_0(N)$ and the first two rank 2 quotients.

The following "Density Conjecture" will not be needed for our application:

Conjecture 3.2 (–). *The set of primes $\ell \equiv 1 \pmod{p}$ such that $L(E, \chi_{p,\ell}, 1) = 0$ has Dirichlet density 0 amongst all primes.*

4 p-Torsion

Fix

- elliptic curve E
- rigid prime p
- a prime $\ell \equiv 1 \pmod{p}$ such that $\ell \nmid N_E$.

Let $K/\mathbb{Q}$ be the abelian extension corresponding to a character $\chi_{p,\ell} : (\mathbb{Z}/\ell\mathbb{Z})^* \to \boldsymbol{\mu}_p$ of order p and conductor ℓ.

The diagram we will plug into visibility theory is:

$$\begin{array}{ccccc} E[p] & \longrightarrow & E & & \\ \downarrow & & \downarrow & \overset{[p]}{\searrow} & \\ A & \longrightarrow & J & \xrightarrow{\mathrm{tr}} & E. \end{array}$$

Michael Stoll helped me to prove the following lemma.

Lemma 4.1. *If $a_\ell(E) \not\equiv 2 \pmod{p}$, then the following groups have no nontrivial p-torsion:*

$$E(\mathbb{Q}_\ell), \quad J(\mathbb{Q}_\ell), \quad (J/E)(\mathbb{Q}_\ell), \quad \Phi_{A,\ell}(\mathbb{F}_\ell).$$

Proof.

- We first that prove
$$J(\mathbb{Q}_\ell)[p] = 0.$$
By definition,
$$J(\mathbb{Q}_\ell) = E_K(\mathbb{Q}_\ell \otimes_{\mathbb{Q}} K) \cong E(K_v) \times \cdots \times E(K_v),$$
where K_v is the completion of K at the prime over ℓ. The action of $\mathrm{Frob}_\ell \in \mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell)$ on
$$E[p](\mathbb{Q}_\ell^{\mathrm{ur}}) = E[p](\overline{\mathbb{Q}}_\ell)$$
has characteristic polynomial
$$x^2 - a_\ell(E)x + \ell \in \mathbb{F}_p[x].$$
This polynomial does not have $+1$ as a root, so
$$E[p](\mathbb{Q}_\ell^{\mathrm{ur}}) = 0.$$
If $z \in E[p](K_v)$ then $\mathbb{Q}_\ell(z) \subset K_v$ and K_v is totally ramified, so $\mathbb{Q}_\ell(z) = \mathbb{Q}_\ell$ and $z = 0$. Thus $J(\mathbb{Q}_\ell)[p] = 0$.

- Next,
$$(J/E)(\mathbb{Q}_\ell) \subset (J/E)(K_v) \approx E(K_v) \times \cdots \times E(K_v),$$
so $(J/E)(\mathbb{Q}_\ell)[p] = 0$.

- Finally, consider $\Phi_{A,\ell}$. By Lang's Lemma,
$$\mathcal{A}(\mathbb{F}_\ell) \twoheadrightarrow \Phi_{A,\ell}(\mathbb{F}_\ell).$$
Thus if $\Phi_{A,\ell}(\mathbb{F}_\ell)[p] \neq 0$, then $\mathcal{A}(\mathbb{F}_\ell)[p] \neq 0$. Since $p \neq \ell$, Hensel's lemma (and formal groups) imply that $A(\mathbb{Q}_\ell)[p] \neq 0$, contrary to the fact that $J(\mathbb{Q}_\ell)[p] = 0$.

□

5 Visualizing Mordell-Weil in Rank 0 Sha

Theorem 5.1. *Let E be an elliptic curve over $\mathbb{Q}$. Conjecture 3.1 implies that for every rigid prime p, there is an abelian extension $K/\mathbb{Q}$ of degree p such that*
$$E(\mathbb{Q})/pE(\mathbb{Q}) \cong \mathrm{Vis}_J(\text{Ш}(A/\mathbb{Q})[p]),$$
where $J = \mathrm{Res}_{K/\mathbb{Q}}(E_K)$ and $A \subset J$ has dimension $p-1$ and rank 0.

Proof. Conjecture 3.1 produces a prime $\ell \equiv 1 \pmod{p}$ such that $L(E, \chi_{p,\ell}, 1) \neq 0$ and $a_\ell(E) \not\equiv 2 \pmod{p}$. Since $L(E, \chi_{p,\ell}, 1) \neq 0$ and A is attached to $f \otimes \chi_{p,\ell}$, Kato's work implies that $A(\mathbb{Q})$ is finite. Lemma 4.1 implies that
$$p \nmid \#(J/E)(\mathbb{Q})_{\mathrm{tor}} \cdot \#E(\mathbb{Q})_{\mathrm{tor}} \cdot \#\Phi_{A,\ell}(\mathbb{F}_\ell) \cdot \#\Phi_{E,\ell}(\mathbb{F}_\ell).$$
To apply Theorem 2.1, we just need that $p \nmid \#\Phi_{A,p}(\mathbb{F}_p)$. This is true becaue $\Phi_{A,p}(\overline{\mathbb{F}}_p) = \Phi_{A_K,\wp}(\overline{\mathbb{F}}_p) = 0$, since $K/\mathbb{Q}$ is **unramified** at p, and $A_K = E_K \times \cdots \times E_K$ and E has good reduction at p. Thus
$$E(\mathbb{Q})/pE(\mathbb{Q}) \cong \mathrm{Vis}_J(\text{Ш}(A)[p]),$$
as claimed.

□

BSD Connection: Let E be an elliptic curve. Suppose we don't know anything about $E(\mathbb{Q})$, but *do* know that $L(E,1) = 0$. If we could prove that there is a rigid prime such that
$$\text{Ш}(A/\mathbb{Q})[p] \neq 0 \qquad \text{(as \textit{better be} predicted by the BSD formula)}$$
and
$$\text{Ш}(E/K)[p] = 0,$$
then Theorem 5.1 would imply that $E(\mathbb{Q})$ is infinite.

6 Example

Let E be the rank 2 curve 389A. The prime $p = 3$ is rigid, and $\ell = 7$ satisfies 3.1. We have
$$(\mathbb{Z}/3\mathbb{Z})^2 \cong E(\mathbb{Q})/3E(\mathbb{Q}) \cong \mathrm{Vis}_J(\text{Ш}(A/\mathbb{Q})[3])$$
for $A \subset \mathrm{Res}_{K/\mathbb{Q}}(E_K)$ of rank zero.