Visible Shafarevich-Tate groups of modular abelian varieties*

(Utrecht Arithmetic Geometry Workshop)

William A. Stein

Tuesday, 27 June 2000

*Thanks for inviting me!

Modular abelian varieties

Let $f = \sum a_n q^n \in S_2(\Gamma_0(N); \mathbf{C})$ be a newform.

$f \rightsquigarrow$ optimal quotient A_f of $J_0(N)$

$$\begin{array}{ccc} A_f^\vee & \hookrightarrow & J_0(N) \\ & & \downarrow \\ & & A_f \end{array}$$

Shafarevich-Tate group of A:

$$Ш(A) := \ker\left(H^1(\mathbf{Q}, A) \to \prod_v H^1(\mathbf{Q}_v, A)\right)$$

Conjecture: (Birch, Swinnerton-Dyer, Tate)

1. *Formula:* $Ш(A_f)$ is finite and

$$L(A_f, 1) = \frac{\Omega_{A_f} \cdot \prod_{p|N} c_p}{\#A_f(\mathbf{Q}) \cdot \#A_f^\vee(\mathbf{Q})} \cdot \#Ш(A_f).$$

2. *Rank:* Order of vanishing of $L(A_f, s)$ at 1 equals rank of $A_f(\mathbf{Q})$. (Regulators, etc.)

Mazur: Visualize Ш!

Given $A \hookrightarrow J$, let $B = J/A$. We have:

$$0 \longrightarrow A(\mathbf{Q}) \longrightarrow J(\mathbf{Q}) \longrightarrow B(\mathbf{Q}) \longrightarrow H^1(\mathbf{Q}, A) \longrightarrow H^1(\mathbf{Q}, J) \longrightarrow \cdots$$

The *visible part* of $H^1(\mathbf{Q}, A)$ is the image of $B(\mathbf{Q})$. Points in $B(\mathbf{Q})$ can be "written down." Torsor is fiber over point in $J(\mathbf{Q})$.

Observation: (Greenberg, —) Any $c \in H^q(\mathbf{Q}, A)$, $q \geq 1$, is visible in $J = \mathrm{Res}_{K/\mathbf{Q}}(A_K)$, where K splits c.

Proof: Natural map $\iota : A \hookrightarrow J$ induces

$$H^1(\mathbf{Q}, A) \xrightarrow{\iota_*} H^1(\mathbf{Q}, J) = H^1(K, A)$$

(by Shapiro's Lemma), so $\iota_*(c) = 0$.

Conrad: Abelian varieties over infinite fields embed in Jacobians.

Mazur's query: Is $Ш(A_f^\vee)$ visible in $J_0(N)$?

The data (N prime)

Assume BSD. There are 38 rank zero $A_f^\vee$ of prime level ≤ 2161 with nontrivial odd part of Ш. Of these, 22 have all this Ш visible. E.g.,

A_f	dim	$\sqrt{\#Ш/2^?}$
389E	20	5
433D	16	7
563E	31	13
571D	2	3
709C	30	11
997H	42	9
1061D	46	151
1091C	62	7 (inv)
1171D	53	11
1283C	62	5 (inv)
1429B	53	5 (inv)
1481C	62	13 (inv)
1483D	64	15
1531D	73	73
1559B	90	11 (inv)
1567D	69	$7 \cdot 41$
2111B	112	211 (inv, not eisen)
2333C	101	83341
2593B	109	$67 \cdot 2213$

Criterion for visibility

Theorem 1. (—) *Let $A, B \subset J$ s.t. $(A \cap B)(\mathbf{C})$ and $A(\mathbf{Q})$ finite. Assume B has toric reduction at each $\ell \mid N_J$. Let p be an odd prime (or principle prime ideal) not dividing N_J, the orders of comp. grps. of A and B, $(J/B)(\mathbf{Q})_{\mathrm{tor}}$, $B(\mathbf{Q})_{\mathrm{tor}}$, and $B[p] \subset A$. Then*

$$B(\mathbf{Q})/pB(\mathbf{Q}) \subset Ш(A)^{\mathrm{vis}}.$$

Proof sketch: Since $B[p] \subset A \cap B$, $B \to C$ factors through p:

$$\begin{array}{ccccccccc} & & & & B & \xrightarrow{p} & B & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & J & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

Key diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B(\mathbf{Q}) & \xrightarrow{p} & B(\mathbf{Q}) & \longrightarrow & B(\mathbf{Q})/pB(\mathbf{Q}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \overset{\pi}{\searrow} & \downarrow & & \\ 0 & \longrightarrow & J(\mathbf{Q})/A(\mathbf{Q}) & \longrightarrow & C(\mathbf{Q}) & \longrightarrow & H^1(\mathbf{Q}, A)^{\mathrm{vis}} & \longrightarrow & 0 \end{array}$$

Snake lemma implies $B(\mathbf{Q})/pB(\mathbf{Q})$ injects into $H^1(\mathbf{Q}, A)^{\mathrm{vis}}$. Use subtle exactness properties of Néron models to get into $Ш(A)^{\mathrm{vis}}$.

Visibility at higher level

Theorem 1 can be refined: condition that $p \nmid$ geometric component group of B replaced by

$$p \nmid \prod_{\ell} \#\Phi_{B,\ell}(\mathbf{F}_\ell) \cdot \#H^1(\mathbf{F}_\ell, \Phi_{B,\ell}).$$

A while ago, Cremona and Mazur discovered three elliptic curves, **2849A**, **4343B**, **5389A**, in which BSD predicts odd invisible Ш.

A_f	$\sqrt{\#Ш/2^?}$	becomes visible
2849A	3	$8547 = 3 \cdot 2849 = 3 \cdot 7 \cdot 11 \cdot 37$
5389A	3	$37723 = 7 \cdot 5389 = 7 \cdot 17 \cdot 317$
1429B	5	$2858 = 2 \cdot 1429$ (dim $B = 2$)

Now we know *unconditionally* that there is odd visible Ш!

Conjecture: Let $c \in Ш(A_f^\vee)[p]$. Then there exists an integer M such that $\iota_*(c) = 0$ for $\iota : A_f^\vee \to J_0(NM)$ one of the natural maps. (Require $p \nmid \deg(\iota)$.)

Evidence for the BSD conjecture

In the eventually visible examples above, we have *unconditionally proved* that up to a 2-power $Ш(A_f)$ is as big as BSD predicts.

Vanishing of $L(B, 1)$ usually forces vanishing of $L(A_f, 1)$ modulo p, so we are very unlikely to observe that $Ш(A_f)$ is bigger than BSD predicts.

Query: Constructing points?

Hard open problem: *Suppose* $L(E,1)$ *and* $L'(E,1)$ *vanish. Show* $E(\mathbf{Q})$ *is infinite.*

Formulate visible analogue of BSD conjecture. Deduce the existence of nontrivial visible elements of $Ш(A_f)$ in new way, and conclude that the rank of E is > 0 without computing points on E.

Test question: Prove that the first elliptic curve of rank > 1 has rank > 1 *without* explicitely finding any points. This is the curve E labeled **389A**.

Strategy: Let A be **389E**, so $E[5] \subset A \cap E$. Use "Euler system of Heegner points" to deduce that 5 divides cardinality of *visible part* of $Ш(A)$, then use the key diagram to deduce that $E(\mathbf{Q})/5E(\mathbf{Q})$ is nontrivial (assume $E(\mathbf{Q}) = 0$ and use the snake lemma to derive a contradiction).