Visualizing Mordell-Weil Groups of Elliptic Curves Using Shafarevich-Tate Groups

William A. Stein

February 8, 2002 at University of Arizona

1 Introduction

Today I will tell you about a construction of elements of Shafarevich-Tate groups of abelian varieties A over $\mathbb{Q}$.

A Construction of Elements of $\text{Ш}(A)$

Birch and Swinnerton-Dyer Conjecture

- If $L(A,1) \neq 0$, then

  $$\#\text{Ш}(A) \stackrel{?}{=} \frac{L(A,1)}{\Omega_A} \cdot \frac{\#A(\mathbb{Q})_{\text{tor}} \cdot \#A(\mathbb{Q})^{\vee}_{\text{tor}}}{\prod_{p\mid N} c_{A,p}}$$

  Find A in nature with conjecturally non-trivial $\text{Ш}(A)$, and prove that $\text{Ш}(A)$ is as big as expected.

- Construct A such that $\text{Ш}(A)$ is nontrivial, then check that the BSD conjecture is not obviously false for A.

- Find a method for connecting the rank conjecture about elliptic curves to the rank 0 formula for abelian varieties.

What are the possibilities for $\#\text{Ш}(A)$?

Question (Poonen, 1999 at AWS).
Stoll and Poonen proved that if A is a Jacobian, then $\#\text{Ш}(A)$ is a square or twice a square. If A is not a Jacobian, is $\#\text{Ш}(A)$ always a square or twice a square?

Conjecture (Me, today).
Let G be any finite abelian group (of odd order). Then there is an abelian variety A such that $\text{Ш}(A) \approx G \times H$, where $\gcd(\#G, \#H) = 1$.

2 A Construction of Elements of $\text{Ш}(A)$

Theorem 2.1. *Let E be an elliptic curve over $\mathbb{Q}$, and suppose $\chi : (\mathbb{Z}/\ell\mathbb{Z})^* \to \mathbb{C}^*$ is a Dirichlet character of prime modulus $\ell \nmid N_E$ and order n such that*

- $L(E, \chi^a, 1) \neq 0$ *for* $a = 1, \ldots, n-1$,
- $\gcd\left(n,\ 2N_E \prod_{p \mid N_E} \#\Phi_E(\overline{\mathbb{F}}_p)\right) = 1$, *and*
- $a_\ell \not\equiv \ell + 1 \pmod{p}$ *for all* $p \mid n$.

Let K be the degree n abelian extension of $\mathbb{Q}$ corresponding to χ. Then there exists a K-twist A of $E^{\oplus(n-1)}$ of rank 0 such that $L(A, s) = \prod_{a=1}^{n-1} L(E, \chi^a, s)$ and

$$E(\mathbb{Q})/nE(\mathbb{Q}) \subset \text{Ш}(A/\mathbb{Q}).$$

Remark 2.2. Note that K is contained in the totally real subfield $\mathbb{Q}(\mu_\ell)^+$ of $\mathbb{Q}(\mu_\ell)$ because the order of $\chi(-1)$ divides the odd number n.

Sketch of Proof. Let $R = \mathrm{Res}_{K/\mathbb{Q}}(E_K)$ be the Weil restriction of scalars of E_K down to $\mathbb{Q}$. For any $\mathbb{Q}$-scheme S, we have $R(S) = E_K(S \times_{\mathbb{Q}} K)$, and as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules

$$R(\overline{\mathbb{Q}}) = E(\overline{\mathbb{Q}} \otimes K) \cong E(\overline{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})],$$

where $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\sum P_\sigma \otimes \sigma \in E(\overline{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ by

$$\tau\left(\sum P_\sigma \otimes \sigma\right) = \sum \tau(P_\sigma) \otimes \sigma\tau_{|K}.$$

The L-series of R is $\prod_{a=1}^{n} L(E, \chi^a, s)$, and R has good reduction at all $p \nmid \ell \cdot N$.

Let $\Delta : E \hookrightarrow R$ be the diagonal embedding, which sends P to $\sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} P \otimes \sigma$, and let $\Sigma : R \to E$ be the summation map, which sends $\sum P_\sigma \otimes \sigma$ to $\sum P_\sigma$. Note that both Δ and Σ are defined over $\mathbb{Q}$ and that $\Sigma \circ \Delta = [n]$. If $A = \ker(\Sigma)$ then

$$A_{\overline{\mathbb{Q}}} = \ker\left(+ : E_{\overline{\mathbb{Q}}}^{\oplus n} \to E_{\overline{\mathbb{Q}}}\right) \cong E^{\oplus(n-1)},$$

the isomorphism being the one that sends $(P_1, \ldots, P_{n-1})$ to $(P_1, \ldots, P_{n-1}, -(\sum P_i))$. In particular, A is a twist of $E^{\oplus(n-1)}$. We summarize this information in the following diagram:

$$\begin{array}{ccccc}
E[n] & \longrightarrow & E & \xrightarrow{[n]} & E \\
\downarrow & & \downarrow{\scriptstyle \Delta} & & \| \\
A & \hookrightarrow & R & \xrightarrow{\Sigma} & E.
\end{array} \qquad (1)$$

Now pass to $\mathbb{Q}$-rational points in diagram (1) and rearrange things to obtain the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q}) & \xrightarrow{[n]} & E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow \iota & & \\
0 & \longrightarrow & R(\mathbb{Q})/A(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) & \longrightarrow & \ker(H^1(\mathbb{Q}, A) \to H^1(\mathbb{Q}, R)) & \longrightarrow & 0.
\end{array}$$

Here we have used that $E(\mathbb{Q})[n] = 0$, since $E[p]$ is irreducible for $p \mid n$, and we've included the beginning of the long exact sequence of Galois cohomology associated to $0 \to A \to R \to E \to 0$. Using the snake lemma, we see that ι is surjective and has kernel a subgroup of $R(\mathbb{Q})/(A(\mathbb{Q}) + E(\mathbb{Q}))$. One can use that $a_\ell \not\equiv \ell + 1 \pmod{p}$ for any $p \mid n$ and that $A(\mathbb{Q})$ is finite (which follows from Kato's Euler system work!) to show that $R(\mathbb{Q})/(A(\mathbb{Q}) + E(\mathbb{Q}))$ contains no p-torsion for $p \mid n$, hence $\ker(\iota) = 0$.

To show that the image of ι lies in the subgroup $\text{Ш}(A/\mathbb{Q})$ of $H^1(\mathbb{Q}, A)$, uses that $\gcd(n, 2 \cdot N_E \cdot c) = 1$, where c is the product of all Tamagawa numbers of E and A. These last steps are fairly technical and use some nontrivial machinery. (That n is odd is only used to show that ι maps into $\text{Ш}(A/\mathbb{Q})$.) □

3 Data Collection

Next we collect some data that both gives evidence for the Birch and Swinnerton-Dyer conjecture and for my conjecture that if G is an abelian group then there is an abelian variety A such that $\text{Ш}(A) \approx G \times H$ with $\gcd(\#H, \#G) = 1$. We will always choose E below so that N_E is prime, E is isolated in its isogeny class (hence $\rho_{E,p}$ is surjective for all p), and $c_{E,p} = 1$ for all $p \mid N$.

Let $\#\text{Ш}_{\text{an}}(A)^*$ denote the prime-to-2ℓ part of

$$\frac{L(A,1)}{\Omega_A} \cdot \frac{\#A(\mathbb{Q})_{\text{tor}} \cdot \#A^\vee(\mathbb{Q})_{\text{tor}}}{\prod_{p \mid \ell N_E} c_{A,p}}.$$

Remark 5.4 of Edixhoven's *Néron models and tame ramification* can be used to show that

$$\Phi_{A,\ell}(\overline{\mathbb{F}}_\ell) = E(\overline{\mathbb{F}}_\ell)[n] \approx (\mathbb{Z}/n\mathbb{Z})^2,$$

so $c_{A,\ell} = 1$, since $E(\mathbb{F}_\ell)[p] = 0$ for all $p \mid n$. Since K is only ramified at ℓ and the formation of Néron models commutes with unramified base change, $c_{A,p} = c_{E,p}^{n-1} = 1$ for $p \mid N_E$. Since $A(\mathbb{Q}) \subset A(K) \approx E(K)^{\oplus(n-1)}$, and $E(K)_{\text{tor}} = 0$ (since all $\rho_{E,p}$ are surjective), we have $\#A(\mathbb{Q})_{\text{tor}} = \#A^\vee(\mathbb{Q})_{\text{tor}} = 1$. I think (but have not proven, yet!) that

$$\Omega_{A/\mathbb{Q}} = \left(\frac{1}{\sqrt{\ell}} \cdot \Omega_{E/\mathbb{Q}} \right)^{n-1}.$$

To prove this, it would (mostly) suffice to show that $\Omega_{A/K} = \Omega_{A/\mathbb{Q}}^n \cdot \ell^{\binom{n}{2}}$, where $\binom{n}{2} = n(n-1)/2$. Assume this formula for $\Omega_{A/\mathbb{Q}}$, we can very quickly compute $Ш_{\mathrm{an}}(A)^*$ using modular symbols.

The elliptic curves **61A** of rank 1, **389A** of rank 2, and **5077A** of rank 3 each have prime conductor, trivial torsion subgroup, and Tamagawa number $c_p = 1$. In the table below, p_d denotes a d-digit prime number (where d is written in Roman numerals), and a $-$ means that some hypothesis of Theorem 2.1 is *not* satisfied. (This table took under ten minutes to compute on a Pentium III 933.)

n	ℓ	$\#Ш_{\mathrm{an}}^*$ for **61A**	$\#Ш_{\mathrm{an}}^*$ for **389A**	$\#Ш_{\mathrm{an}}^*$ for **5077A**
3	487	3	3^4	3^3
9	487	$3^2 \cdot 19^2$	3^8	$3^6 \cdot 17^2$
27	487	$3^3 \cdot 19^2 \cdot p_{vi}^2$	$3^{12} \cdot 163^2$	$3^9 \cdot 17^2 \cdot 433^2 \cdot p_{vi}^2$
81	487	$3^4 \cdot 19^2 \cdot p_{iv}^2 \cdot p_{vi}^2 \cdot p_{vii}^2$	$3^{16} \cdot 163^2 \cdot p_{xix}^2$	$3^{12} \cdot 17^2 \cdot 433^2 \cdot p_{iv}^2 \cdot p_v^2 \cdot p_{vi}^2 \cdot p_{vii}^2 \cdot p_{ix}^2$
5	251	5	5^2	$-$
25	251	$5^2 \cdot 151^2 \cdot p_v^2$	$5^4 \cdot 149^2 \cdot p_{iv}^2$	$-$
125	251	$5^3 \cdot 151^2 \cdot p_v^2 \cdot p_{xviii}^2$	$5^6 \cdot 149^2 \cdot p_{iv}^2 \cdot p_v^2 \cdot p_x^2 \cdot p_{xi}^2$	$-$
7	197	$7 \cdot 29^2$	$7^2 \cdot 13^4$	7^3
49	197	$7^2 \cdot 29^2 \cdot p_x^2$	$7^4 \cdot 13^4 \cdot p_{ix}^2$	$7^6 \cdot p_{iv}^2 \cdot p_{iv}^2 \cdot p_v^2$
11	89	$11 \cdot 67^2$	11^2	$11^3 \cdot 67^2$
13	53	13	13^2	$-$
17	103	$17 \cdot 613^2$	$17^2 \cdot 101^2$	$17^3 \cdot 67^2$
19	191	$19 \cdot 37^2$	19^2	$19^5 \cdot 37^2$

The BSD conjecture and this table (and my "conjecture" about Ω_A) imply that for the integers n in the first column of the table, there is an A such that

$$Ш(A) \approx (\mathbb{Z}/n\mathbb{Z}) \times H$$

with $\gcd(n, \#H) = 1$. This is evidence for Conjecture 1, and also gives lots of examples to show that $\#Ш(A)$ is neither a square or twice a square in general.

Challenge: *Let E be one of the curves considered in the table, let r be its rank, and notice that in the table $n^r \mid \#Ш_{\mathrm{an}}^*$. The BSD conjecture predicts that this divisibility should always hold. Prove that it does for infinitely many ℓ.*