Possibilities for Shafarevich-Tate Groups of Modular Abelian Varieties

William Stein
Harvard University
August 22, 2003 for Microsoft Research
Overview of Talk

1. Abelian Varieties
2. Shafarevich-Tate Groups
3. Nonsquare Shafarevich-Tate Groups
Abelian Varieties

**Abelian Variety**: A projective group variety
(group law is automatically abelian).

**Examples:**

1. Elliptic curves
2. Jacobians of curves
3. Modular abelian varieties
4. Weil restriction of scalars
**Jacobians of Curves**

If $X$ is an algebraic curve then

$$\text{Jac}(X) = \{ \text{divisor classes of degree 0 on } X \}.$$ 

**Example:** Let $X_1(N)$ be the modular curve parametrizing pairs

$$(E, \text{embedding of } \mathbb{Z}/N\mathbb{Z} \text{ into } E).$$

The Jacobian of $X_1(N)$ is $J_1(N)$. 
The Modular Jacobian $J_1(N)$

- $J_1(N) = \text{Jacobian of } X_1(N)$
- The Hecke Algebra:
  \[ T = \mathbb{Z}[T_1, T_2, \ldots] \hookrightarrow \text{End}(J_1(N)) \]
- Cuspidal Modular Forms:
  \[ S_2(\Gamma_1(N)) = H^0 \left( X_1(N), \Omega^1_{X_1(N)} \right) \]
Modular Abelian Varieties

A modular abelian variety is any quotient of $J_1(N)$.

Goro Shimura associated an abelian variety $A_f$ to any newform $f$:

$$A_f := J_1(N)/I_f J_1(N)$$

where

$$f = q + \sum_{n \geq 2} a_n q^n \in S_2(\Gamma_1(N))$$

$$I_f = \text{Ker}(T \to \mathbb{Z}[a_1, a_2, a_3, \ldots]), \ T_n \mapsto a_n$$
Extra structure

- $A$ is an abelian variety over $\mathbb{Q}$

- The ring $\mathbb{Z}[a_1,a_2,\ldots]$ is a subring of $\text{End}(A)$

- The dimension of $A$ equals the degree of the field generated by the $a_n$
• **Wiles et al.**: Every elliptic curve over \(\mathbb{Q}\) is modular, i.e., isogenous to an \(A_f\)

**Consequence (Ribet):** Fermat’s Last Theorem

• **Serre’s Conjecture:** Every odd irreducible Galois representation

\[
\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{F}_\ell})
\]

occurs up to twist in the torsion points of some \(A_f\)
Weil Restriction of Scalars

$F/K$: finite extension of number fields
$A/F$: abelian variety over $F$

$R = \text{Res}_{F/K}(A)$ abelian variety over $K$ with

$$\dim(R) = \dim(A) \cdot [F : K]$$

**Functorial characterization:**
For any $K$-scheme $S$,

$$R(S) = A(S \times_K F)$$
Birch and Swinnerton-Dyer
**BSD Conjecture**

\[
\frac{L(r)(A_f, 1)}{r!} \overset{\text{conj}}{=} \frac{(\prod c_p) \cdot \Omega_{A_f} \cdot \text{Reg}_{A_f}}{\# A_f(Q)_{\text{tor}} \cdot \# A_f^\vee(Q)_{\text{tor}}} \cdot \# \text{III}(A_f/Q)
\]

\[
L(A_f, s) = \prod_{\text{galois orbit}} \left( \sum_{n=1}^{\infty} \frac{a_n^{(i)}}{n^s} \right)
\]

\[
r = \text{ord}_{s=1} L(A_f, s) \overset{\text{conj}}{=} \text{rank of } A_f(Q)
\]

\[
c_p = \text{order of component group at } p
\]

\[
\Omega_{A_f} = \text{canonical measure of } A_f(\mathbb{R})
\]
The Shafarevich-Tate Group of $A_f$

Sha is a subgroup of the first Galois cohomology of $A_f$ that measures failure of “local to global”:

$$\Sha(A_f/\mathbb{Q}) = \ker \left( H^1(\mathbb{Q}, A_f) \to \bigoplus_{\text{all } v} H^1(\mathbb{Q}_v, A_f) \right)$$

Example:

$$[3x^3 + 4y^3 + 5z^3 = 0] \in \Sha(x^3 + y^3 + 60z^3 = 0)$$

Conjecture (Shafarevich-Tate):

$$\Sha(A_f/\mathbb{Q}) \text{ is finite.}$$
The Shafarevich-Tate Group $\Sha(A_f / \mathbb{Q})$

$\Sha(A_f / \mathbb{Q})$ (finite?)

$H^1(\mathbb{Q}, A_f)$ (torsion)

$\bigoplus_{\text{all } v} H^1(\mathbb{Q}_v, A_f)$
Finiteness Theorems of Kato, Kolyvagin, Logachev, and Rubin

**Hypothesis:** Suppose \( \dim A = 1 \) and \( \operatorname{ord}_{s=1} L(A, s) \leq 1 \).

**Kolyvagin:** \( \Sha(A/Q) \) is finite.

**Kato:** If \( \chi \) is a Dirichlet character corresponding to an abelian extension \( K/Q \) with \( L(A, \chi, 1) \neq 0 \) then the \( \chi \)-component of \( \Sha(A/K) \) is finite.

**(Rubin:** Similar results first when \( A \) has CM.)
The Dual Abelian Variety

The dual of $A$ is an abelian variety isogenous to $A$ that parametrizes classes of invertible sheaves on $A$ that are algebraically equivalent to zero.

$$A^\vee = \text{Pic}^0(A)$$

The dual is functorial:

If $A \to B$ then $B^\vee \to A^\vee$. 
A polarization of $A$ is an isogeny (homomorphism) from $A$ to its dual that is induced by a divisor on $A$. A polarization of degree 1 is called a principal polarization.

**Theorem.** If $A$ is the Jacobian of a curve, then $A$ is canonically principally polarized. For example, elliptic curves are principally polarized.
Cassels-Tate Pairing

$A/F$: abelian variety over number field

**Theorem.** If $A$ is principally polarized by a polarization arising from an $F$-rational divisor, then there is a nondegenerate alternating pairing on $\text{III}(A/F)/\text{div}$, so for all $p$:

$$\#\text{III}(A/F)[p^\infty]/\text{div} = \square$$

(Same statement away from minimal degree of polarizations.)

**Corollary.** If $\dim A = 1$ and $\text{III}(A/F)$ finite, then

$$\#\text{III}(A/F) = \square$$
What if the abelian variety $A$ is not an elliptic curve?

Assume $\#\text{III}(A/F)$ is finite. Overly optimistic literature:

- Page 306 of [Tate, 1963]: If $A$ is a Jacobian then
  \[\#\text{III}(A/F) = \square.\]

- Page 149 of [Swinnerton-Dyer, 1967]: Tate proved that
  \[\#\text{III}(A/F) = \square.\]
Michael Stoll’s Computation

During a grey winter day in 1996, Michael Stoll sat puzzling over a computation in his study on a majestic embassy-peppered hill near Bonn overlooking the Rhine. He had implemented an algorithm for computing 2-torsion in Shafarevich-Tate groups of Jacobians of hyperelliptic curves. He stared at a curve $X$ for which his computations were in direct contradiction to the previous slide!

$$\#\Sha(Jac(X)/\mathbb{Q})[2] = 2.$$  
What was wrong????
From: Michael Stoll (9 Dec 1996)
Dear Bjorn, Dear Ed:

[...] your results would imply that Sha[2] = Z/2Z
in contradiction to the fact that the order of Sha[2] should
be a square (always assuming, as everybody does, that Sha is finite).
So my question is (of course): What is wrong?

From: Bjorn Poonen (9 Dec 96)
Dear Michael:
Thanks for your e-mails. I'm glad someone is actually taking the time
to think about our paper critically! [...]  
I would really like to resolve the apparent contradiction,
because I am sure it will end with us learning something!
(And I don't think that it will be that Sha[2] can have odd dimension!)

From: Bjorn Poonen (11 hours later)
Dear Michael:
I think I may have resolved the problem. There is nothing wrong with
the paper, or with the calculation. The thing that is wrong is the
claim that Sha must have square order!
Poonen-Stoll Theorem

Theorem (Annals, 1999): Suppose $J$ is the Jacobian of a curve and $J$ has finite Shafarevich-Tate group. Then

$$\#\Sha(J/F) = \Box \text{ or } 2 \cdot \Box$$

Example: The Jacobian of this curve has Sha of order 2

$$y^2 = -3(x^2 + 1)(x^2 - 6x + 1)(x^2 + 6x + 1)$$
Is Sha Always Square or Twice a Square?

Poonen asked at the Arizona Winter School in 2000, “Is there an abelian variety $A$ with Shafarevich-Tate group of order three?”
In 2002 I finally found Sha of order 3 (times a square):

\[ 0 = -x_1^3 - x_1^2 + (-6x_3x_2 + 3x_3^2)x_1 + (-x_2^3 + 3x_3x_2^2 + (-9x_3^2 - 2x_3)x_2 \\
+ (4x_3^3 + x_3^2 + (y_1^2 + y_1 + (2y_3y_2 - y_3^2)))x_2 \\
0 = -3x_2x_1^2 + ((-12x_3 - 2)x_2 + 3x_3^2)x_1 + (-2x_2^3 + 3x_3x_2^2 + \\
-15x_3^2 - 4x_3)x_2 + (5x_3^3 + x_3^2 + (2y_2y_1 + ((4y_3 + 1)y_2 - y_3^2)))x_2 \\
0 = -3x_3x_1^2 + (-3x_2^2 + 6x_3x_2 + (-9x_3^2 - 2x_3))x_1 + (x_2^3 + (-9x_3 - 1)x_2 \\
+ (12x_3^2 + 2x_3)x_2 + (-9x_3^3 - 3x_3^2 + (2y_3y_1 + (y_2^2 - 2y_3y_2 + (3y_3^2 + y_3))))x_2 \\
0 = x_1^2x_2^4 - 8x_1^2x_2^3x_3 + 30x_1^2x_2^2x_3^2 - 44x_1^2x_2x_3^3 + 25x_1^2x_3^4 - 2/3x_1x_2^5 + 26/3x_1x_2^4x_3 + 2/3x_1x_2^4 \\
- 140/3x_1x_2^3x_3^2 - 16/3x_1x_3^3x_3 + 388/3x_1x_2^2x_3^3 + 20x_1x_2^2x_3^2 - 2/3x_1x_2y_2^2 + 8/3x_1x_2y_2^3 \\
- 10/3x_1x_2^2y_3^2 - 490/3x_1x_2x_3^3 - 88/3x_1x_2x_3y_2^2 - 40/3x_1x_2x_3y_2y_3 \\
+ 44/3x_1x_2x_3y_3^2 + 250/3x_1x_3^3 + 50/3x_1x_3^3 - 10/3x_1x_2^2y_2^2 + 44/3x_1x_2y_2y_3 - 50/3x_1x_3^3y_3 \\
+ 1/9x_2^6 - 2x_2^5x_3 - 4x_2^4 + 15x_2^4x_3^2 + 26/9x_2^3x_3 + 1/9x_2^4 - 544/9x_2^3x_3^3 - 140/9x_2^3x_3^3 \\
- 8/9x_2^3x_3^3 + 2x_2^3y_2^2 - 8/9x_2^3y_2y_3 + 10/9x_2^3y_3^2 + 135x_2^4x_3^3 + 388/9x_2^3x_3^4 + 10/3x_2^2x_3^2 \\
- 2x_2^2x_3y_2^2 + 80/9x_2^2x_3y_2y_3 - 94/9x_2^2x_3y_3^2 - 2x_2^2y_2^2 + 8/9x_2y_2y_3 - 10/9x_2y_3^2 \\
- 150x_2x_3^5 - 490/9x_2x_3^4 - 44/9x_2x_3^3 + 50/9x_2x_3^2y_2^2 - 244/9x_2x_3^2y_2y_3 + 30x_2x_3^2y_3^2 \\
+ 8/9x_2x_3y_2^2 - 40/9x_2x_3y_2y_3 + 44/9x_2x_3y_3^2 + 625/9x_3^6 + 250/9x_3^5 + 25/9x_3^4 - 50/9x_3^3y_2^2 \\
+ 220/9x_3^3y_2y_3 - 250/9x_3^3y_3^2 - 10/9x_3^2y_2^2 + 44/9x_3^2y_2y_3 - 50/9x_3^2y_3^2 + 1/9y_2^4 \\
- 8/9y_3^3y_3 + 10/3y_3^2y_3^2 - 44/9y_3^2y_3^2 + 25/9y_3^4}
Plenty of Nonsquare Sha!

- **Theorem (Stein):** *For every prime* $p < 25000$ *there is an abelian variety* $A$ *over* $\mathbb{Q}$ *such that*

$$\#\text{III}(A/\mathbb{Q}) = p \cdot \Box$$

- **Conjecture (Stein):** *Same statement for all* $p$. 
Constructing Nonsquare Sha

While attempting to connect groups of points on elliptic curves of high rank to Shafarevich-Tate groups of abelian varieties of rank 0, I found a construction of nonsquare Shafarevich-Tate groups.
The Main Theorem

Theorem (Stein). Suppose $E$ is an elliptic curve and $p$ an odd prime that satisfies various technical hypothesis. Suppose $\ell$ is a prime congruent to 1 mod $p$ (and not dividing $N_E$) such that

$$L(E, \chi_{p, \ell}, 1) \neq 0 \text{ and } a_\ell(E) \neq \ell + 1 \pmod{p}$$

Here $\chi_{p, \ell} : \mathbb{Z}/\ell^* \to \mu_p$ is a Dirichlet character of order $p$ and conductor $\ell$ corresponding to an abelian extension $K$. Then there is a twist $A$ of a product of $p - 1$ copies of $E$ and an exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \Sha(A/\mathbb{Q})[p^\infty] \to \Sha(E/K)[p^\infty] \to \Sha(E/\mathbb{Q})[p^\infty] \to 0.$$

If $E$ has odd rank and $\Sha(E/\mathbb{Q})[p^\infty]$ is finite then $\Sha(A/\mathbb{Q})[p^\infty]$ has order that is not a perfect square.
What is the Abelian Variety $A$?

Let $R$ be the Weil restriction of scalars of $E$ from $K$ down to $\mathbb{Q}$, so $R$ is an abelian variety over $\mathbb{Q}$ of dimension $p$ (i.e., the degree of $K$). Then $A$ is the kernel of the map induced by trace:

$$0 \to A \to R \to E \to 0$$

Note that

- $A$ has dimension $p - 1$
- $A$ is isomorphic over $K$ to a product of copies of $E$
- Our hypothesis on $\ell$ and Kato’s finiteness theorems imply that $A(\mathbb{Q})$ and $\#\text{III}(A/\mathbb{Q})$ are both finite.
Proof Sketch (1): Exact Sequence of Néron Models

The exact sequence

\[ 0 \to A \to R \to E \to 0 \]

extends to an exact sequence of Néron models (and hence sheaves for the étale topology) over \( \mathbb{Z} \):

\[ 0 \to A \to \mathcal{R} \to \mathcal{E} \to 0. \]

To check this, we use that formation of Néron models commutes with unramified base change and Prop. 7.5.3(a) of [Néron Models, 1990].
Proof (2): Mazur’s Etale Cohomology Sha Theorem

Mazur's *Rational Points of Abelian Varieties with Values in Towers of Number Fields*:

For $F = A, R, E$ let $\mathcal{F} = \text{Néron}(F)$. Then

$$H^1_{\text{ét}}(\mathbb{Z}, \mathcal{F})[p^\infty] \cong \Sha(F/\mathbb{Q})[p^\infty]$$

In general this is not true, but our hypothesis on $p$ and $\ell$ are exactly strong enough to kill the relevant error terms.
Proof (3): Long Exact Sequence

The long exact sequence of étale cohomology begins

\[ 0 \rightarrow A(\mathbb{Q}) \rightarrow R(\mathbb{Q}) \rightarrow E(\mathbb{Q}) \rightarrow \delta \]
\[ H^1_{\text{ét}}(\mathbb{Z}, \mathcal{A}) \rightarrow H^1_{\text{ét}}(\mathbb{Z}, \mathcal{R}) \rightarrow H^1_{\text{ét}}(\mathbb{Z}, \mathcal{E}) \rightarrow H^2_{\text{ét}}(\mathbb{Z}, \mathcal{A}) \]

Take the \( p \)-power torsion in this exact sequence then use Mazur’s theorem. Next analyze the cokernel of \( \delta \)…
Proof (4): Apply Kato’s Finiteness Theorems

We have \( \text{Coker}(\delta) = E(\mathbb{Q})/pE(\mathbb{Q}) \) since

\[
L(E, \chi_p, \ell, 1) \neq 0 \quad \text{and} \quad a_\ell \equiv \ell + 1 \pmod{p}.
\]

(To see this requires chasing some diagrams.)

Also \( H_{\text{ét}}^2(\mathbb{Z}, A)[p^\infty] = 0 \) (proof uses Artin-Mazur duality).

Both of these steps use Kato’s finiteness theorem in an essential way. Putting everything together yields the claimed exact sequence

\[
0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \varPi(A/\mathbb{Q})[p^\infty] \to \varPi(E/K)[p^\infty] \to \varPi(E/\mathbb{Q})[p^\infty] \to 0.
\]
What Next?

• Remove the hypothesis that $p < 25000$, i.e., prove a nonvanishing result about twists of newforms of large degree. (One currently only has results for degrees 2 and in some cases 3.)

• Prove that the Birch and Swinnerton-Dyer conjecture predicts that $\# \text{III}(A/F)$ has order divisible by $p$, in agreement with our construction.

• Replace $E$ by an abelian variety of dimension bigger than 1.
Thank you for coming!

Acknowledgements:

Kevin Buzzard, Cristian Gonzalez, Barry Mazur, Bjorn Poonen, Ken Ribet, and Michael Stoll

For more details including an accepted paper:

http://modular.fas.harvard.edu/papers/nonsquaresha/.