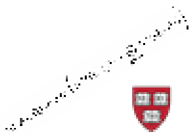
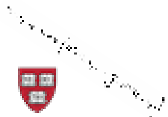
Introduction to Modular Abelian Varieties and Shafarevich-Tate Groups

William Stein
Harvard University

September 15, 2003 for Math 252





$Ш(A_f/\mathbf{Q})$ $Ш(A_f/\mathbf{Q})$

Overview

0. Syllabus
1. Modular Abelian Varieties
2. Shafarevich-Tate Group
3. A Story about Orders of Shafarevich-Tate Groups

Abelian Varieties

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

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

$\mathrm{Jac}(X) = \{$ divisor classes of degree 0 on $X \}$,

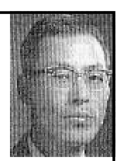
has structure of abelian variety of dimension = genus(X).

Example: Elliptic curves are their own Jacobians.
Example: Let $X_1(N)$ be the **modular curve** that (tries to) parametrize isomorphism classes of pairs

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

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

The Modular Jacobian $J_1(N)$



- $J_1(N)$ = Jacobian of $X_1(N)$
- The **Hecke Algebra**:

$$\mathbf{T} = \mathbf{Z}[T_1, T_2, \ldots] \hookrightarrow \mathrm{End}(J_1(N))$$

- **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 (much of Math 252 will culminate in this construction):

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

where

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

$$I_f = \mathrm{Ker}(\mathbf{T} \to \mathbf{Z}[a_1, a_2, a_3, \ldots]),\ T_n \mapsto a_n$$

$A=A_f$ Has Lots of Structure

- A is an abelian variety defined over $\mathbf{Q}$
- The ring $\mathbf{Z}[a_1,a_2,\ldots]$ is a subring of $\mathrm{End}(A)$
- The dimension of A equals the degree of the field $\mathbf{Q}[a_1,a_2,\ldots]$ generated by the a_n

Modular Abelian Varieties A_f Are Interesting!!!

- **Wiles et al.:** Every elliptic curve over $\mathbf{Q}$ is modular, i.e., isogenous to an A_f
  Consequence (Ribet): Fermat's Last Theorem
  (I will not sketch a proof of either of these statements in 252.)
- **Serre's Conjecture:** Every odd irreducible Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$$

occurs up to twist in the torsion points of some A_f. (I will discuss Serre's conjecture further in 252.)

Birch and Swinnerton-Dyer

The Birch and Swinnerton-Dyer Conjecture

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

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

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

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

$$\Omega_{A_f} = \text{canonical measure of } A_f(\mathbf{R})$$

(We will spend at least 2 weeks on this conjecture in Math 252.)

The Shafarevich-Tate Group of A_f

"Sha" is a subgroup of the first Galois cohomology of A_f; it measures failure of local to global:

$$\text{Ш}(A_f/\mathbf{Q}) = \mathrm{Ker}\left(H^1(\mathbf{Q},A_f) \to \bigoplus_{\text{all } v} H^1(\mathbf{Q}_v,A_f)\right)$$

Example:

$$[3x^3+4y^3+5z^3=0] \in \text{Ш}(x^3+y^3+60z^3=0)$$

Conjecture (Shafarevich-Tate):

$\text{Ш}(A_f/\mathbf{Q})$ *is finite.*

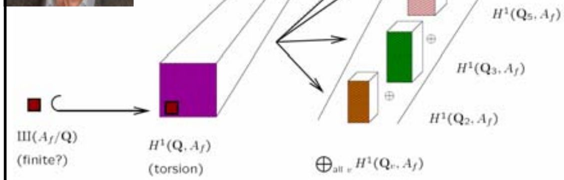
From Birch's paper *Conjectures Concerning Elliptic Curves*

The so-called Tate-Šafarevič conjecture (adopted by Lang, Cassels and Tate, but apparently disowned by Šafarevič) asserts that TS is always a finite group; this is a very natural strengthening of the Selmer conjecture. Unfortunately, the evidence is very weak; in fact, TS has not yet been fully computed for a single curve. It is very difficult to compute more than $(TS)_2$ for a general elliptic curve over Q, and $(TS)_3$ for a curve of shape $y^2=x^3-B$. Cassels' theorem implies that if TS is finite then its order must be a square. In our computations leading to the formula

"$\tau(C_D)=f^2/|TS|$ if $g=0$"

we actually verified that $f^2/\tau(C_D)$ was an integer square, usually 1, and was divisible by the order of $(TS)_n$ when this could be calculated.

The Shafarevich-Tate Group $Ш(A_f/\mathbf{Q})$



Theorems of Kolyvagin, Kato, Rubin, Gross, Zagier, et al.

These are partial results towards the Birch and Swinnerton-Dyer conjecture, which we will discuss at the end of the course.

Now for a motivating story that involves lots of things you shouldn't understand yet, but will when this course is over:

QUESTION: What can we say about the possible sizes of Shafarevich-Tate Groups?

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.

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

The dual is functorial:

$$\text{If } A \to B \text{ then } B^\vee \to A^\vee.$$

Polarized Abelian Varieties

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 $Ш(A/F)_{/\mathrm{div}}$, so for all p:

$$\#Ш(A/F)[p^\infty]_{/\mathrm{div}} = \square$$

(Same statement away from minimal degree of polarizations.)

Corollary. If $\dim A = 1$ and $Ш(A/F)$ finite, then

$$\#Ш(A/F) = \square$$

What if the abelian variety *A* is not an elliptic curve?

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

- Page 306 of [Tate, 1963]: If A is a Jacobian then

$$\#\text{Ш}(A/F) = \square.$$

- Page 149 of [Swinnerton-Dyer, 1967]: Tate proved that

$$\#\text{Ш}(A/F) = \square.$$

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!

$$\#\text{Ш}(\mathrm{Jac}(X)/\mathbf{Q})[2] = 2.$$

What was wrong????

Poonen-Stoll

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 Pooenen (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*

$$\#\text{Ш}(J/F) = \square \text{ or } 2\cdot\square$$

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):

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

Plenty of Non-square Sha!

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

$$\#\text{Ш}(A/\mathbf{Q}) = p \cdot \square$$

- **Conjecture (Stein):** *Same statement for all p.*

How to Construct Non-square 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 non-square 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 ℓ is a prime congruent to 1 mod p (and not dividing N_E) such that*

$$L(E, \chi_{p,\ell}, 1) \neq 0 \text{ and } a_\ell(E) \not\equiv \ell + 1 \pmod{p}$$

Here $\chi_{p,\ell} : (\mathbf{Z}/\ell)^* \twoheadrightarrow \mu_p$ is a Dirichlet character of order p and conductor ℓ 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

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

If E has odd rank and $\text{Ш}(E/\mathbf{Q})[p^\infty]$ is finite then $\text{Ш}(A/\mathbf{Q})[p^\infty]$ has order that is ***not a perfect square****.*

Proof Uses the Weil Restriction of Scalars

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

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

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

Functorial characterization:
For any K-scheme S,

$$R(S) = A(S \times_K F)$$

What is the Abelian Variety *A*?

Let R be the Weil restriction of scalars of E from K down to **Q**, so R is an abelian variety over **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 ℓ and Kato's finiteness theorems imply that $A(\mathbf{Q})$ and $\#\text{Ш}(A/\mathbf{Q})$ are both finite.
- Is isogenous to A_f where f is a twist of newform attached to E.

Proof Sketch (1): Exact Sequence of Neron Models

Neron

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 $\mathbf{Z}$:

$$0 \to \mathcal{A} \to \mathcal{R} \to \mathcal{E} \to 0.$$

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

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

In general this is not true, but our hypothesis on p and ℓ are exactly strong enough to kill the relevant error terms.

Proof (3): Long Exact Sequence

The long exact sequence of étale cohomology begins

$$0 \to A(\mathbf{Q}) \to R(\mathbf{Q}) \to E(\mathbf{Q}) \xrightarrow{\delta} H^1_{\text{ét}}(\mathbf{Z}, \mathcal{A}) \to H^1_{\text{ét}}(\mathbf{Z}, \mathcal{R}) \to H^1_{\text{ét}}(\mathbf{Z}, \mathcal{E}) \to H^2_{\text{ét}}(\mathbf{Z}, \mathcal{A})$$

Take the p-power torsion in this exact sequence then use Mazur's theorem. Next analyze the cokernel of δ…

Proof (4): Apply Kato's Finiteness Theorems

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

$$L(E, \chi_{p,\ell}, 1) \neq 0 \quad \text{and} \quad a_\ell \not\equiv \ell + 1 \pmod{p}.$$

(To see this requires chasing some diagrams.)

Also $H^2_{\text{ét}}(\mathbf{Z}, \mathcal{A})[p^\infty] = 0$ (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

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

Thank you for coming and…
Come Back!!