Possibilities for Shafarevich-Tate Groups of Modular Abelian Varieties

William Stein
Harvard University

March 21, 2003 for Lenstra's Treurfeest

Overview of Tour

1. Review of Abelian Varieties

2. Theorems About Shafarevich-Tate Groups

3. Shafarevich-Tate Groups of Order $p \cdot \square$

Abelian Varieties

Abel

Abelian variety: A projective group variety

Examples:

1. Elliptic curves (i.e., $y^2 = x^3 + ax + b$)

2. Jacobians of curves

3. Modular abelian varieties

4. Weil restriction of scalars

2. Jacobians of Curves

Jacobi

If X is an algebraic curve then

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

Examples (defined over $\mathbf{Q}$):

- $X_1(N) =$ modular curve parameterizing pairs

$$(E,\ \mathbf{Z}/N \hookrightarrow E)$$

- $J_1(N) = \mathrm{Jac}(X_1(N))$

Hecke

The Modular Jacobian $J_1(N)$

- Hecke algebra:

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

- Cuspidal modular forms (cotangent space of $J_1(N)$ at 0):

$$S_2(\Gamma_1(N)) = H^0\left(X_1(N), \Omega^1_{X_1(N)}\right)$$

Shimura

3. Modular Abelian Varieties

A *modular abelian variety* A is any quotient

$$J_1(N) \twoheadrightarrow A$$

Shimura associated abelian varieties to $\mathbf{T}$-eigenforms:

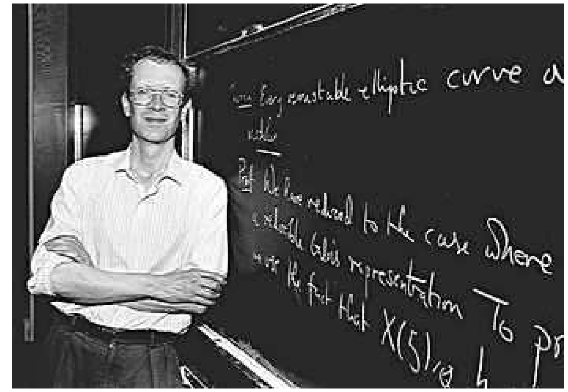
$$f = q + \sum_{n\geq 2} a_n q^n \in S_2(\Gamma_1(N))$$

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

Abelian variety A_f over $\mathbf{Q}$ of $\dim = [\mathbf{Q}(a_1, a_2, \ldots) : \mathbf{Q}]$:

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

The A_f are Interesting



Wiles

- Wiles et al.: Every elliptic curve over $\mathbf{Q}$ is isogenous to an A_f

- Serre's Conjecture: All odd irreducible continuous

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

occur (up to twist) in the torsion points on A_f

- Understand A_f well using modular forms

4. Weil Restriction of Scalars

Weil

Way to construct abelian varieties from others

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:

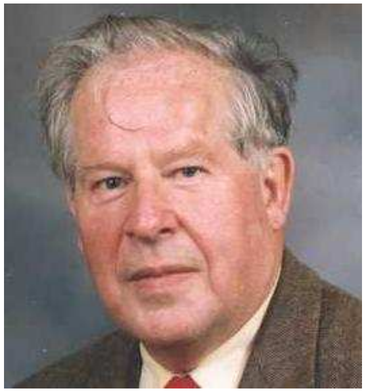
For any K-scheme S,

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

Birch and Swinnerton-Dyer Conjecture

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

BSD Conjecture



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

Here

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

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

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

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

Shafarevich-Tate Group

Shafarevich

A mysterious subgroup of Galois cohomology:

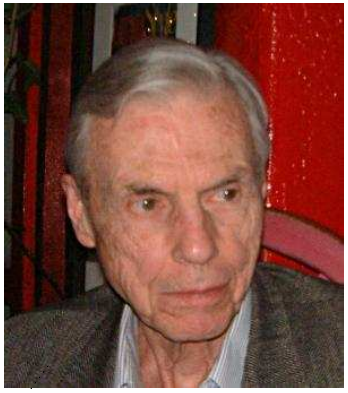
$$Ш(A_f/\mathbf{Q}) = \mathrm{Ker}\left(H^1(\mathbf{Q}, A_f) \to \bigoplus_{\text{all } v} H^1(\mathbf{Q}_v, A_f) \right)$$

Classifies locally trivial torsors for A_f:

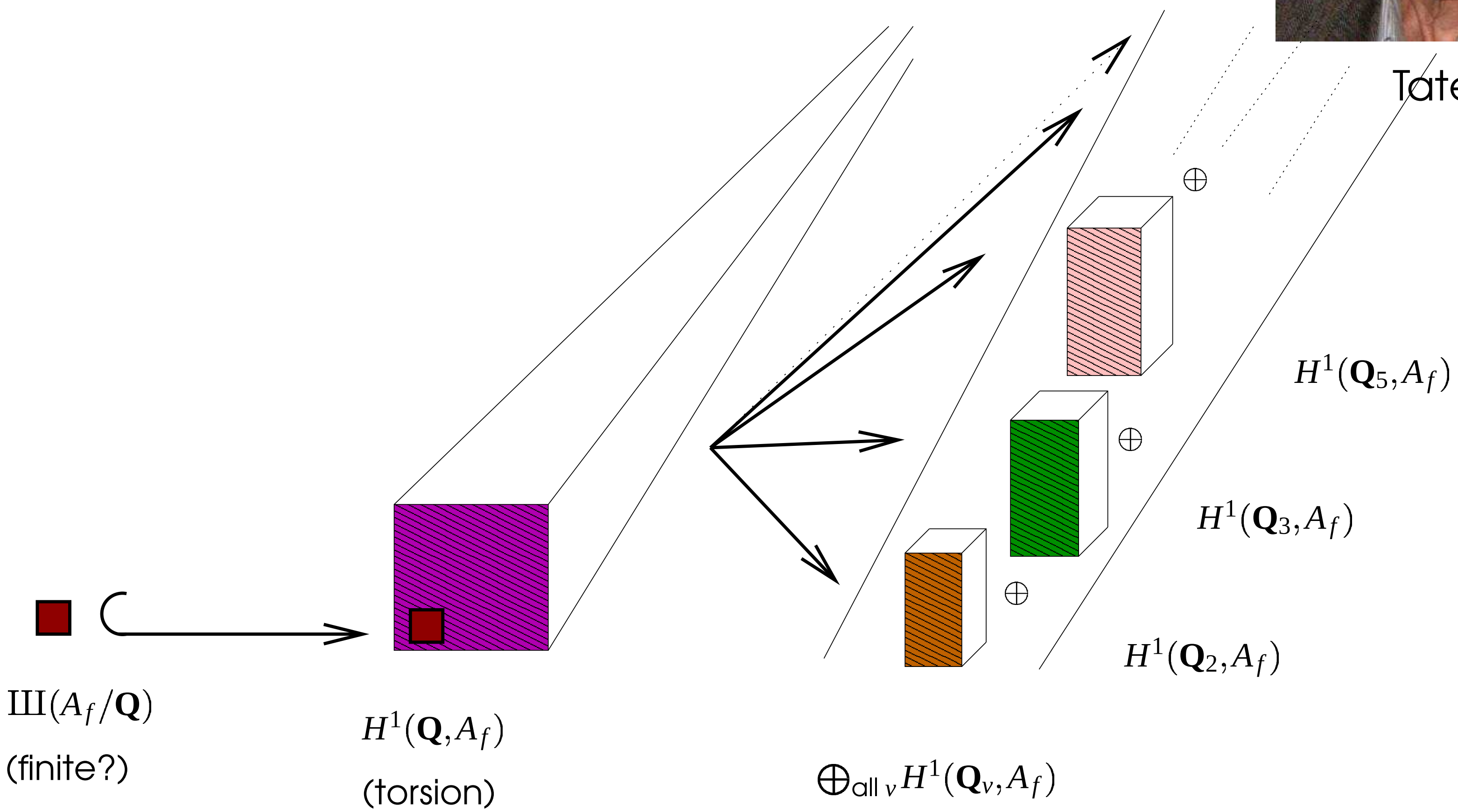
$$[3x^3 + 4y^3 + 5z^3 = 0] \in Ш(x^3 + y^3 + 60z^3 = 0)[3]$$

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

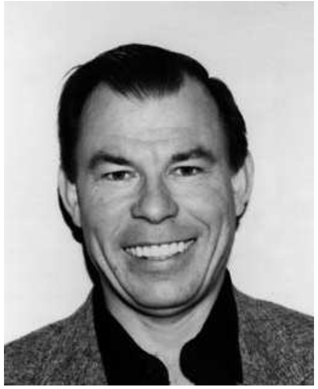
Shafarevich-Tate Group



Tate



Theorems of Kato and Kolyvagin



Kolyvagin

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

Kolyvagin: $Ш(A/\mathbf{Q})$ is finite.

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

(**Rubin:** Similar results first when A has CM.)

Maximal Divisible Subgroup $(\mathbf{Q}_p/\mathbf{Z}_p \subset \text{Ш}(A)?)$

Even if $\text{Ш}(A)$ were not finite, for each prime p the quotient

$$\text{Ш}(A)[p^\infty]_{/\,\mathrm{div}}$$

would be finite. (That we don't know finiteness in general causes much frustration in work toward the BSD conjecture.)

(Here $G_{/\,\mathrm{div}} = G/G_{\mathrm{div}}$ where G_{div} is the subgroup of infinitely divisible elements.)

The Dual of A

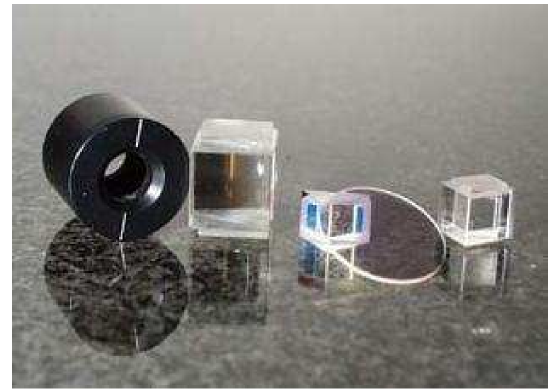
Invertible sheaves on A algebraically equivalent to 0:

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

Functorial:

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

Polarization



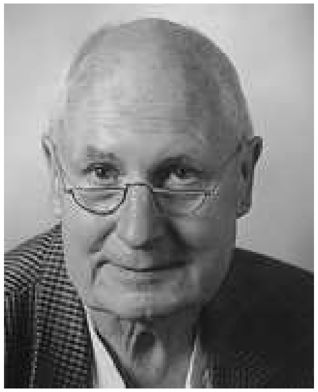
A *polarization* of A is an isogeny

$$\lambda : A \to A^{\vee}$$

induced by divisor class on A. A *principal polarization* is a polarization of degree 1 (an isomorphism).

Example. If $\dim A = 1$, then A is principally polarized since $A \cong A^{\vee}$ by $P \mapsto P - O \in \mathrm{Pic}^0(A)$. Jacobians are also principally polarized.

Theorem of Cassels and Tate



Cassels

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 $\dim A > 1$?

Assume $\#\text{Ш}(A/F)$ 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

$$\#\text{Ш}(A/F) = \square.$$

Stoll's Computation

Stoll

During a grey winter day in 1996, Michael Stoll sat puzzling over a computation in his study on a majestic embassy-peppered hill overlooking the Rhine. He had implemented an algorithm for performing 2-descents on Jacobians of hyperelliptic curves. He stared at a curve X for which his computations implied that

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

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

What was wrong?

Poonen $\longleftrightarrow$ Stoll

Poonen

```
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!
```

Theorem of Poonen-Stoll

Poonen 1988

J a Jacobian over a number field F

Theorem (Annals 1999). If $Ш(J/F)$ finite then

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

Both cases occur and there is a simple criterion to decide.

Example. The Jacobian J of

$$y^2 = -3(x^2+1)(x^2-6x+1)(x^2+6x+1)$$

has $\#Ш(J/\mathbf{Q}) = 2$.

Question

Is $\#Ш(A/F)$ always $\square$ or $2\cdot\square$?

Hendrik Lenstra asked me this once on the bus from MSRI.

Poonen asked at Arizona Winter School 2000: Is there an abelian variety such that

$$\#Ш(A/F) = 3?$$

Answer: YES!

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

Plenty of Nonsquare $Ш[p]$!

Theorem 1 (Stein). For every prime $p < 25000$, there is an abelian variety A over $\mathbf{Q}$ such that

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

Revised Question. Possibilities for $\#Ш(A)$?

Conjecture 1 (Stein). The integers $\pm\#Ш(A)$ for all abelian varieties A represent every element of $\mathbf{Q}^*/\mathbf{Q}^{*2}$.

Constructing Nonsquare Ш

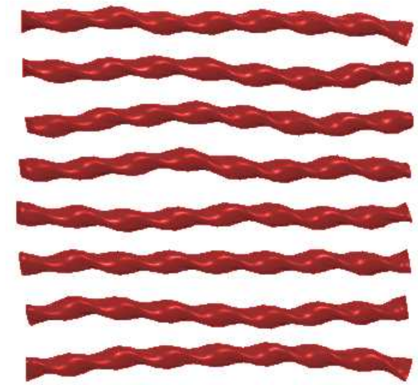
The rest of this talk is about the construction I found to prove Theorem 1.

History. I tried to construct Ш of order 3 directly for a long time, gave up, thought about visibility (in the sense of Mazur) and accidently found Ш of order 3.

Summary. Find visible nonsquare Ш living in

$$\mathrm{Ker}\left(\mathrm{Res}_{K/\mathbf{Q}}(E_K) \xrightarrow{\text{trace}} E\right)$$

Higher Degree Twists



Recall: Quadratic twist of $y^2 = x^3 + ax + b$ by the Dirichlet character χ corresponding to $\mathbf{Q}(\sqrt{D})$:

$$E^{\chi}: \quad Dy^2 = x^3 + ax + b.$$

Generalize:

p a prime and ℓ a prime with $\ell \equiv 1 \pmod{p}$
$\chi : (\mathbf{Z}/\ell)^* \to \mathbf{C}^*$ a Dirichlet character of degree p
$K \subset \mathbf{Q}(\zeta_\ell)$ of degree p
$R = \mathrm{Res}_{K/\mathbf{Q}}(E_K)$ (Note: $R_K \cong E_K^p = E_K \times \cdots \times E_K$)
The *twist of E by χ* is the abelian variety of dimension $p-1$:

$$A = E^{\chi} = \mathrm{Ker}\left(R \xrightarrow{\text{trace}} E\right)$$

Note: A isogenous to A_f where $f = \sum a_n(E)\chi(n)q^n = f_E \otimes \chi$.

Nonvanishing Twist Conjecture

$E/\mathbf{Q}$ an elliptic curve, conductor N
Suppose p is a prime such that

$$p \nmid 2 \cdot \prod_{q|N} c_q \quad \text{and} \quad \rho_{E,p} : G_{\mathbf{Q}} \twoheadrightarrow \mathrm{Aut}(E[p])$$

For any prime $\ell \equiv 1 \pmod{p}$ let

$$\chi_{p,\ell} : (\mathbf{Z}/\ell)^* \twoheadrightarrow \mu_p$$

be the unique (up to conjugacy) character of degree p and conductor ℓ.

Conjecture 2 (Stein). There is a prime $\ell \equiv 1 \pmod{p}$ with $\ell \nmid N$ such that $L(E, \chi_{p,\ell}, 1) \neq 0$ and $a_\ell(E) \not\equiv \ell + 1 \pmod{p}$.

A Visibly Beautiful Exact Sequence

Assume p and ℓ as in above conjecture. Let $\chi = \chi_{p,\ell}$, $A = E^{\chi}$, and $K \subset \mathbf{Q}(\zeta_\ell)$ of degree p.

Theorem 1 (Stein). There is an exact sequence

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

(Remark: The *visible* subgroup of $Ш(A/\mathbf{Q})$ is $E(\mathbf{Q})/pE(\mathbf{Q})$.)

Application. If all $Ш$'s finite and E has odd rank, then

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

Note: By hypothesis $\mathrm{rank}\, E = \dim E(\mathbf{Q})/pE(\mathbf{Q})$.
Remark: Work of Claus Diem on polarizations of A.

Sketch of Proof (1)

Neron

The exact sequence

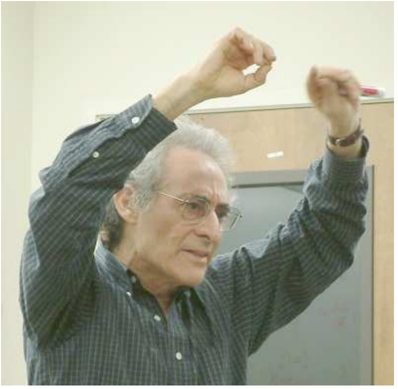
$$0 \to A \to R \to E \to 0$$

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).

Main hypothesis used: $\ell \nmid pN$.



Sketch of Proof (2)

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

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

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

Main hypothesis used:

$$a_\ell(E) \not\equiv \ell + 1 \pmod{p} \qquad \text{and} \qquad p \nmid \prod c_\ell.$$

That $a_\ell(E) \not\equiv \ell + 1 \pmod{p}$ implies Frob_ℓ has no fixed points.

Sketch of Proof (3)

Associated long exact sequence of étale cohomology:

$$
\begin{tikzcd}
0 \arrow[r] & A(\mathbf{Q}) \arrow[r] & R(\mathbf{Q}) \arrow[r] & E(\mathbf{Q}) \arrow[dlll, "\delta"] \\
H^1_{\text{ét}}(\mathbf{Z},\mathcal{A}) \arrow[r] & H^1_{\text{ét}}(\mathbf{Z},\mathcal{R}) \arrow[r] & H^1_{\text{ét}}(\mathbf{Z},\mathcal{E}) \arrow[r] & H^2_{\text{ét}}(\mathbf{Z},\mathcal{A})
\end{tikzcd}
$$

Sketch of Proof (4)

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

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

Also $H^2_{\text{ét}}(\mathbf{Z},\mathcal{A})[p^\infty] = 0$ (proof uses Artin-Mazur duality).

Note: Both of these steps use Kato's finiteness theorem in an essential way.

Putting everything together, yields

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

Application

MECCAH

Let E be $y^2 + y = x^3 - x$ of conductor 37 and rank 1.

Large modular symbols computation to verify Conjecture 2 (nonvanishing twists) for all odd primes $p < 25000$.

For each $p < 25000$, we obtain a twist A of E of dimension $p - 1$ such that $Ш(A/\mathbf{Q})$ is finite and $\#Ш(A/\mathbf{Q})[p^\infty]$ is an odd power of p. Using Cassels-Tate pairing get

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

Some Other Visibly Twisted Ш

Replace p by a prime power. Columns record BSD conjectural order of $Ш(A/\mathbf{Q})$, where p_n denotes an n-digit prime:

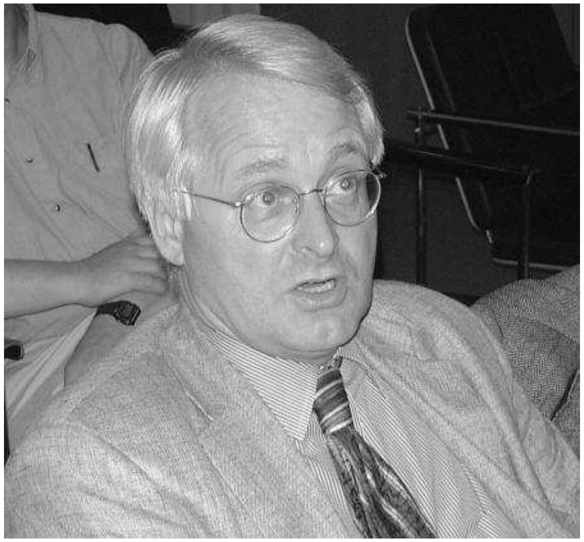
p^r	ℓ	**61A**	**389A**	**5077A**
3	487	3	3^4	3^3
9	487	$3^2 \cdot 19^2$	3^8	$3^6 \cdot 17^2$
27	487	$3^3 \cdot 19^2 \cdot p_6^2$	$3^{12} \cdot 163^2$	$3^9 \cdot 17^2 \cdot 433^2 \cdot p_6^2$
81	487	$3^4 \cdot 19^2 \cdot p_4^2 \cdot p_6^2 \cdot p_7^2$	$3^{16} \cdot 163^2 \cdot p_{19}^2$	$3^{12} \cdot 17^2 \cdot 433^2 \cdot p_4^2 \cdot p_5^2 \cdot p_6^2 \cdot p_7^2 \cdot p_9^2$
5	251	5	5^2	–
25	251	$5^2 \cdot 151^2 \cdot p_5^2$	$5^4 \cdot 149^2 \cdot p_4^2$	–
125	251	$5^3 \cdot 151^2 \cdot p_5^2 \cdot p_{18}^2$	$5^6 \cdot 149^2 \cdot p_4^2 \cdot p_5^2 \cdot p_{10}^2 \cdot p_{11}^2$	–
7	197	$7 \cdot 29^2$	$7^2 \cdot 13^4$	7^3
49	197	$7^2 \cdot 29^2 \cdot p_{10}^2$	$7^4 \cdot 13^4 \cdot p_9^2$	$7^6 \cdot p_4^2 \cdot p_4^2 \cdot p_5^2$
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	$19^5 \cdot 37^2$

Note: **61A** has rank 1, **389A** has rank 2, **5077A** has rank 3.

Thank you for coming!

Acknowledgements: Michael Stoll, Cristian Gonzalez, Barry Mazur, Ken Ribet, Bjorn Poonen

Hendrik, thanks for being my Ph.D. adviser!



For more details:
`http://modular.fas.harvard.edu/papers/nonsquaresha/`.