The Birch & Swinnerton-Dyer conjecture

Karl Rubin

MSRI, January 18 2006

Outline

- Statement of the conjectures
- Definitions
- Results
- Methods

Birch & Swinnerton-Dyer conjecture

Suppose that A is an abelian variety of dimension d over a number field k.

Conjecture (BSD I).

$$\mathrm{ord}_{s=1} L(A/k, s) = \mathrm{rank}(A(k))$$

Conjecture (BSD II). *If* $r = \mathrm{rank}(A(k))$, *then*

$$\lim_{s\to 1} \frac{L(A/k,s)}{(s-1)^r} = \frac{\Omega_{A/k} \cdot R_{A/k} \cdot (\prod_v c_v) \cdot |\text{Ш}(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

The L-function

We will define

$$L(A/k,s) = \prod_v L_v(A/k, q_v^{-s})^{-1}$$

where $L_v(A/k,t) \in \mathbf{Z}[t]$ has degree at most $2d$ and q_v is the cardinality of the residue field of k_v.

If v is a prime of k, let

k_v^{ur} be the maximal unramified extension of k_v,

$I_v = \mathrm{Gal}(\bar{k}_v/k_v^{\mathrm{ur}})$, the inertia group,

$\mathbf{F}_v$ the residue field of k_v, and $q_v = |\mathbf{F}_v|$,

$\mathrm{Frob}_v \in \mathrm{Gal}(k_v^{\mathrm{ur}}/k_v)$ the Frobenius generator (the lift of the automorphism $\alpha \mapsto \alpha^{q_v}$ of $\bar{\mathbf{F}}_v$).

The L-function

If A is an elliptic curve with good reduction at v, then

$$L_v(A/k,t) = 1 - (1 + q_v - |A(\mathbf{F}_v)|)t + q_v t^2 \in \mathbf{Z}[t].$$

For general A and v, and every prime ℓ, define the ℓ-adic Tate module

$$T_\ell(A) = \varprojlim_n A[\ell^n] \cong \varprojlim_n (\mathbf{Z}/\ell^n\mathbf{Z})^{2d} = \mathbf{Z}_\ell^{2d}$$

The L-function

G_k acts $\mathbf{Z}_\ell$-linearly on $T_\ell(A)$.

Suppose ℓ is a prime different from $\mathrm{char}(\mathbf{F}_v)$.

If A has good reduction at v then I_v acts trivially on $T_\ell(A)$, so $\mathrm{Frob}_v \in \mathrm{Gal}(k_v^{\mathrm{ur}}/k_v)$ acts on $T_\ell(A)$

$$L_v(A/k,t) = \det(1 - \mathrm{Frob}_v \cdot t \mid T_\ell(A)) \in \mathbf{Z}_\ell[t].$$

For general v, we define

$$L_v(A/k,t) = \det(1 - \mathrm{Frob}_v^{-1} \cdot t \mid \mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell(A), \mathbf{Z}_\ell)^{I_v})$$

a polynomial in $\mathbf{Z}_\ell[t]$ of degree at most $2d$.

The L-function

A priori $L_v(A/k, t) \in \mathbf{Z}_\ell[t]$, but recall that if A is an elliptic curve with good reduction at v, then

$$L_v(A/k, t) = 1 - (1 + q_v - |A(\mathbf{F}_v)|)t + q_v t^2 \in \mathbf{Z}[t].$$

Theorem. *$L_v(A/k, t) \in \mathbf{Z}[t]$ and is independent of the choice of $\ell \neq \mathrm{char}(\mathbf{F}_v)$.*

The L-function

Definition. $L(A/k,s) = \prod_v L_v(A, q_v^{-s})^{-1}$.

Theorem. *The Euler product for $L(A/k,s)$ converges if $\Re(s) > \frac{3}{2}$.*

Conjecture. *$L(A/k,s)$ has an analytic continuation to all of $\mathbf{C}$, and satisfies a functional equation $s \mapsto 2-s$.*

Conjecture (BSD I).

$$\mathrm{ord}_{s=1} L(A/k,s) = \mathrm{rank}(A(k)).$$

Example

Let A be the elliptic curve $y^2 = x^3 - x$, and $k = \mathbf{Q}$.

$$L(A/k, s) = \prod_{p>2} (1 + (1 + p - |A(\mathbf{F}_p)|)p^{-s} + p^{1-2s})^{-1}.$$

$L(A/k, s)$ has an analytic continuation, and one can compute

$$L(A/k, 1) = .65551538857302995\ldots \neq 0$$

We know that $A(\mathbf{Q})$ has rank zero, so BSD I is true in this case.

BSD II

To define the quantities in BSD II, we need to fix a Néron model $\mathcal{A}$ of A over the ring of integers $\mathcal{O}_k$ of k.

If A is an elliptic curve over $\mathbf{Q}$, then $\mathcal{A}$ is a generalized Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbf{Z}$ are such that the discriminant is minimal among all (generalized Weierstrass) models of A.

The period

$$\lim_{s\to 1} \frac{L(A/k,s)}{(s-1)^r} = \frac{\Omega_{A/k} \cdot R_{A/k} \cdot (\prod_v c_v) \cdot |\text{Ш}(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

If A is an elliptic curve over $\mathbf{Q}$, then

$$\Omega_{A/k} = \int_{E(\mathbf{R})} \frac{dx}{2y + a_1 x + a_3}$$

The period

$$\lim_{s\to 1} \frac{L(A/k,s)}{(s-1)^r} = \frac{\Omega_{A/k} \cdot R_{A/k} \cdot (\prod_v c_v) \cdot |\text{Ш}(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

Suppose for simplicity that the $\mathcal{O}_k$-module of invariant differentials on $\mathcal{A}$ is free $\mathcal{O}_k$-module (for example, this holds if $\mathcal{O}_k$ is a principal ideal domain), and fix an $\mathcal{O}_k$-basis $\{\omega_1, \ldots, \omega_d\}$.

We will define a local period Ω_{A/k_v} for each infinite place v.

The period

$$\lim_{s\to 1}\frac{L(A/k,s)}{(s-1)^r}=\frac{\Omega_{A/k}\cdot R_{A/k}\cdot(\prod_v c_v)\cdot|\text{Ш}(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

Suppose first that $k_v=\mathbf{R}$.

Fix a basis $\{\gamma_1,\ldots,\gamma_d\}$ of $H_1(A(\bar{k}_v),\mathbf{Z})^{\mathrm{Gal}(\bar{k}_v/k_v)}$.

Let m_v be the number of connected components of $A(k_v)$.

Set

$$\Omega_{A/k_v}=m_v|\det(\textstyle\int_{\gamma_i}\omega_j)|.$$

The period

$$\lim_{s\to 1} \frac{L(A/k,s)}{(s-1)^r} = \frac{\Omega_{A/k} \cdot R_{A/k} \cdot (\prod_v c_v) \cdot |Ш(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

Now suppose $k_v = \mathbf{C}$.

Fix a basis $\{\gamma_1, \ldots, \gamma_{2d}\}$ of $H_1(A(\bar{k}_v), \mathbf{Z})$.

Set

$$\Omega_{A/k_v} = |\det(\textstyle\int_{\gamma_i} \omega_j), \overline{\textstyle\int_{\gamma_i} \omega_j})|.$$

Define

$$\Omega_{A/k} = \mathrm{Disc}(k)^{-d/2} \prod_{v|\infty} \Omega_{A/k_v}$$

where $\mathrm{Disc}(k)$ is the discriminant of k.

The regulator

$$\lim_{s\to 1}\frac{L(A/k,s)}{(s-1)^r} = \frac{\Omega_{A/k}\cdot R_{A/k}\cdot(\prod_v c_v)\cdot|\text{Ш}(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

Let $\hat{A}/k$ denote the dual abelian variety.

If A is an elliptic curve, then $\hat{A} = A$, and in general $\hat{A}$ is isogenous to A (there is a surjective morphism $A \to \hat{A}$ with finite kernel).

Let

$$\langle\ ,\ \rangle : A(k)\times\hat{A}(k)\to\mathbf{R}$$

be the canonical height pairing corresponding to the Poincaré divisor on $A\times\hat{A}$.

The regulator

$$\lim_{s\to 1} \frac{L(A/k,s)}{(s-1)^r} = \frac{\Omega_{A/k} \cdot R_{A/k} \cdot (\prod_v c_v) \cdot |Ш(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

Fix $\mathbf{Z}$-bases $\{x_1, \ldots, x_r\}$ of $A(k)/A(k)_{\mathrm{tors}}$ and $\{y_1, \ldots, y_r\}$ of $\hat{A}(k)/\hat{A}(k)_{\mathrm{tors}}$.

Define

$$R_{A/k} = |\det(\langle x_i, y_j \rangle)|.$$

The Tamagawa factors

$$\lim_{s\to 1}\frac{L(A/k,s)}{(s-1)^r} = \frac{\Omega_{A/k}\cdot R_{A/k}\cdot(\prod_v c_v)\cdot|Ш(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

If v is a prime of k let $\mathcal{A}_v = \mathcal{A}\times\mathbf{F}_v$, the fiber of $\mathcal{A}$ over v, and let $\mathcal{A}_v^\circ$ be the connected component of the identity in $\mathcal{A}_v$.

Set

$$c_v = [\mathcal{A}_v(\mathbf{F}_v) : \mathcal{A}_v^\circ(\mathbf{F}_v)].$$

If A has good reduction at v, then $\mathcal{A}_v$ is connected so $c_v = 1$.

Example

Let A be the elliptic curve $y^2 = x^3 - x$, and $k = \mathbf{Q}$.

$$L(A/\mathbf{Q}, 1) = .65551538857302995\ldots$$

$$\Omega_{A/\mathbf{Q}} = 5.24411510858\ldots = 8L(A/\mathbf{Q}, 1)$$

$$R_{A/\mathbf{Q}} = 1$$

$$c_2 = 2$$

$$A(\mathbf{Q})_{\mathrm{tors}} = \hat{A}(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

so BSD II is true if and only if $\text{Ш}(A/\mathbf{Q}) = 0$.

Theorems

Theorem (Wiles, . . .) *Suppose A is an elliptic curve over $\mathbf{Q}$. Then $L(A, s)$ has an analytic continuation and functional equation.*

Theorem (Kolyvagin, Gross & Zagier, . . .). Suppose A is an elliptic curve over $\mathbf{Q}$.

If $\mathrm{ord}_{s=1} L(A/\mathbf{Q}, s) = 0$, *then* $\mathrm{rank}(A(\mathbf{Q})) = 0$ *and* $\text{Ш}(A/\mathbf{Q})$ *is finite.*

If $\mathrm{ord}_{s=1} L(A/\mathbf{Q}, s) = 1$, *then* $\mathrm{rank}(A(\mathbf{Q})) = 1$ *and* $\text{Ш}(A/\mathbf{Q})$ *is finite.*

Theorems

Suppose $L(A/\mathbf{Q}, 1) \neq 0$. To prove $A(\mathbf{Q})$ and $\text{Ш}(A/\mathbf{Q})$ are both finite, one needs to show that $|S_n(A/\mathbf{Q})|$ is bounded as n varies (Kolyvagin).

Suppose $\mathrm{ord}_{s=1}L(A/\mathbf{Q}, s) = 1$. To show that $\mathrm{rank}(A(\mathbf{Q})) = 1$ and $\text{Ш}(A/\mathbf{Q})$ is finite one needs to show

- $A(\mathbf{Q})$ has a point of infinite order (Gross & Zagier),
- $|S_n(A/\mathbf{Q})|/n$ is bounded as n varies (Kolyvagin).

BSD II, rank zero

$$L(A/k,1) \quad \stackrel{?}{=} \quad \frac{\Omega_{A/k}\cdot\left(\prod_v c_v\right)\cdot|\text{Ш}(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

Theorem (Manin, Shimura). *If A is an elliptic curve over $\mathbf{Q}$ then*

$$\frac{L(A/\mathbf{Q},1)}{\Omega_{A/\mathbf{Q}}} \in \mathbf{Q}$$

with an explicit bound on the denominator.

BSD II, rank zero

$$L(A/k,1) \stackrel{?}{=} \frac{\Omega_{A/k}\cdot(\prod_v c_v)\cdot|\text{Ш}(A/k)|}{|A(k)_{\mathrm{tors}}||\hat{A}(k)_{\mathrm{tors}}|}$$

Theorem (Rubin). *Suppose $A/\mathbf{Q}$ is an elliptic curve with complex multiplication by an imaginary quadratic field K. (For example, $y^2 = x^3 - ax$ has CM by $\mathbf{Q}(\sqrt{-1})$, $y^2 = x^3 + b$ has CM by $\mathbf{Q}(\sqrt{-3})$.)*

If $L(A/\mathbf{Q},1) \neq 0$, then BSD II is true for A up to primes dividing the number of roots of unity in K.

Example

Let A be the elliptic curve $y^2 = x^3 - x$, and $k = \mathbf{Q}$. We saw that BSD II is true for A if and only if $\text{Ш}(A/\mathbf{Q}) = 0$.

A has CM by $\mathbf{Q}(\sqrt{-1})$, and $L(A/\mathbf{Q}, 1) \neq 0$, so BSD II is true for A up to a power of 2.

Hence BSD II is true for A if and only if $\text{Ш}(A/\mathbf{Q})[2] = 0$.

We saw yesterday that $\text{Ш}(A/\mathbf{Q})[2] = 0$, so BSD II is true for A.

BSD II, rank zero

$$L(A/k,1) \quad \stackrel{?}{=} \quad \frac{\Omega_{A/k}\cdot(\prod_v c_v)\cdot|\text{Ш}(A/k)|}{|A(k)_{\text{tors}}||\hat{A}(k)_{\text{tors}}|}$$

Theorem (Kato). *Suppose $A/\mathbf{Q}$ is an elliptic curve and A has good reduction at p. If*

$$\mathrm{Gal}(\mathbf{Q}(A[p])/\mathbf{Q}) \to \mathrm{Aut}(A[p]) \xrightarrow{\sim} \mathrm{GL}_2(\mathbf{F}_p)$$

is surjective, then

$$|\text{Ш}(A/\mathbf{Q})[p^\infty]| \quad \text{divides} \quad \frac{L(A/\mathbf{Q},1)}{\Omega_{A/\mathbf{Q}}}.$$

BSD II, rank one

$$L'(A/k,1) \stackrel{?}{=} \frac{\Omega_{A/k} \cdot R_{A/k} \cdot (\prod_v c_v) \cdot |Ш(A/k)|}{|A(k)_{\rm tors}||\hat{A}(k)_{\rm tors}|}$$

Theorem (Gross & Zagier). *If A is an elliptic curve over $\mathbf{Q}$ and $L(A/\mathbf{Q},1) = 0$, then*

$$\frac{L'(A/\mathbf{Q},1)}{\Omega_{A/\mathbf{Q}} R_{A/\mathbf{Q}}} \in \mathbf{Q}.$$

BSD II, rank one

Gross & Zagier showed that for an *explicit* point $x \in A(\mathbf{Q})$ (a Heegner point)

$$\mathrm{h}_{\mathrm{can}}(x) = \alpha \, \frac{L'(A/\mathbf{Q}, 1)}{\Omega_{A/\mathbf{Q}}}$$

with an explicit nonzero rational number α.

Thus if $L'(A/\mathbf{Q}, 1) \neq 0$, then

- x is not a torsion point so $\mathrm{rank}(A(\mathbf{Q})) \geq 1$,
- $\mathrm{h}_{\mathrm{can}}(x)/R_{A/\mathbf{Q}} \in \mathbf{Q}^{\times}$, so $\frac{L'(A/\mathbf{Q},1)}{\Omega_{A/\mathbf{Q}} R_{A/\mathbf{Q}}} \in \mathbf{Q}$.

Abelian varieties

Suppose that $A/\mathbf{Q}$ is a quotient of the jacobian $J_0(N)$ of the modular curve $X_0(N)$ for some N. Then there is a set of Hecke eigenforms $\{f_1, \ldots, f_d\}$ of weight two and level N such that

$$L(A/\mathbf{Q}, s) = \prod_i L(f_i, s).$$

Theorem (Kolyvagin, Gross & Zagier, . . .). *With A as above, suppose $\mathrm{ord}_{s=1} L(f_i, s) \leq 1$ for $1 \leq i \leq d$. Then $\mathrm{ord}_{s=1} L(A/\mathbf{Q}, s) = \mathrm{rank}(A(\mathbf{Q}))$ and $\text{Ш}(A/\mathbf{Q})$ is finite.*

Parity

Suppose A is an elliptic curve over $\mathbf{Q}$, let $N \in \mathbf{Z}^+$ be its conductor, and define

$$\Lambda(A, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(A/\mathbf{Q}, s).$$

Theorem (Wiles, . . .) $\Lambda(A, s) = w_A \Lambda(A, 2 - s)$ with $w_A = \pm 1$.

Conjecturally, $L(A/k, s)$ satisfies a similar functional equation for *every* abelian variety A/k, with "sign" $w_A = \pm 1$.

Parity

Given such a functional equation, we have

$$\mathrm{ord}_{s=1} L(A/k, s) \text{ is } \begin{cases} \text{even} & \text{if } w_A = +1 \\ \text{odd} & \text{if } w_A = -1. \end{cases}$$

Combined with BSD I this leads to:

Parity Conjecture.

$$\mathrm{rank}(A(k)) \text{ is } \begin{cases} \text{even} & \text{if } w_A = +1 \\ \text{odd} & \text{if } w_A = -1. \end{cases}$$

If $\mathrm{rank}(A(k))$ is odd, then $A(k)$ is infinite!

Parity

For squarefree $d \in \mathbf{Z}^+$, let A_d be the elliptic curve $y^2 = x^3 - d^2 x$.

One can compute that

$$w_{A_d} = \begin{cases} +1 & \text{if } d \equiv 1, 2 \text{ or } 3 \pmod 8 \\ -1 & \text{if } d \equiv 5, 6 \text{ or } 7 \pmod 8. \end{cases}$$

So the parity conjecture predicts that if $d \equiv 5, 6$ or $7 \pmod 8$, then $A_d(\mathbf{Q})$ is infinite.

This is known to be true for prime d.

Parity

Theorem (Nekovář). *Suppose $A/\mathbf{Q}$ is an elliptic curve. Then*

$$\mathrm{corank}(S_{p^\infty}(A/\mathbf{Q})) \text{ is } \begin{cases} \text{even} & \text{if } w_A = +1 \\ \text{odd} & \text{if } w_A = -1. \end{cases}$$

Recall that if $Ш(A/\mathbf{Q})$ is finite, then

$$\mathrm{corank}(S_{p^\infty}(A/Q)) = \mathrm{rank}(A(\mathbf{Q})).$$

Parity

Suppose A is an abelian variety over k, p is an odd prime, K/k is a quadratic extension, and L/K is a cyclic p-extension such that L/k is Galois with dihedral Galois group.

Theorem (Mazur & Rubin). *If all primes above p split in K/k and $\mathrm{corank}(S_{p^\infty}(A/K))$ is odd, then*

$$\mathrm{corank}(S_{p^\infty}(A/L)) \geq [L:K].$$

This would follow from the Parity Conjecture.

Parity

If A is an elliptic curve, $k = \mathbf{Q}$ and K is imaginary, then Heegner points account for "most" of the rank in $A(L)$.

For general $L/K/k$, we have no idea where all these points are coming from.

Bounding Selmer groups

Fix an abelian variety A/k, and $n \in \mathbf{Z}^+$.

If v is a prime of k, there is a perfect Tate (cup product) pairing

$$\langle\ ,\ \rangle_v : H^1(k_v, A[n]) \times H^1(k_v, \hat{A}[n]) \longrightarrow \mathbf{Z}/n\mathbf{Z}$$

in which $A(k_v)/nA(k_v)$ and $\hat{A}(k_v)/n\hat{A}(k_v)$ are exact annihilators of each other.

If $c \in S_n(A/k)$, $d \in S_n(\hat{A}/k)$, then $\langle c_v, d_v \rangle_v = 0$.

Bounding Selmer groups

Theorem (Reciprocity Law). *If* $c \in H^1(k, A[n])$, $d \in H^1(k, \hat{A}[n])$ *then* $\sum_v \langle c_v, d_v \rangle_v = 0$.

Suppose Σ is a finite set of primes of k, and

$$S_n^{\Sigma}(\hat{A}/k) := \{d \in H^1(k_v, \hat{A}[n]) : \\ d_v \in \mathrm{image}(\kappa_v) \text{ for every } v \notin \Sigma\}$$

If $d \in S_n^{\Sigma}(\hat{A}/k)$, then for every $c \in S_n(A/k)$

$$\sum_{v \in \Sigma} \langle c_v, d_v \rangle_v = \sum_v \langle c_v, d_v \rangle_v = 0.$$

Bounding Selmer groups

For example, if Σ consists of a single prime v and $d \in S_n^{\Sigma}(\hat{A}/k)$, then for every $c \in S_n(A/k)$

$$\langle c_v, d_v \rangle_v = 0.$$

Since the Tate pairings are nondegenerate, this restricts the image of $S_n(A/k)$ under the localization map

$$S_n(A/k) \hookrightarrow H^1(k, A[n]) \longrightarrow H^1(k_v, A[n]).$$

Bounding Selmer groups

If we can find “enough” d's (as Σ varies), we can show that there are not many c's, i.e., $S_n(A/k)$ is small.

Kolyvagin showed how to use such $d \in S_n^{\Sigma}(\hat{A}/k)$, and how to construct them systematically in some cases. Kato constructed them in other important cases.

Bounding Selmer groups

Every collection of $d \in S_n^{\Sigma}(\hat{A}/k)$ (for varying Σ) gives a bound on the size of the Selmer group $S_n(A/k)$.

This method is not useful if (for example) all the d's one constructs are zero.

In Kolyvagin's and Kato's constructions, the d's are related to the values $L(A/\mathbf{Q}, 1)$ and $L'(A/\mathbf{Q}, 1)$. In this way one obtains a bound on $S_n(A/\mathbf{Q})$ in terms of $L(A/\mathbf{Q}, 1)$, as BSD II predicts.