On the Selmer group associated to a modular form and an algebraic Hecke character.

Yara Elias

McGill University

April 7, 2015

Structure of $E(K)$

Mordell, Weil

Let E be an elliptic curve over a number field K. Then

$$E(K) \simeq \mathbb{Z}^r + E(K)_{tor}$$

where

- $r =$ the algebraic rank of E
- $E(K)_{tors} =$ the finite torsion subgroup of $E(K)$.

Structure of $E(K)$

Mordell, Weil

Let E be an elliptic curve over a number field K. Then

$$E(K) \simeq \mathbb{Z}^r + E(K)_{tor}$$

where

- $r =$ the algebraic rank of E
- $E(K)_{tors} =$ the finite torsion subgroup of $E(K)$.

Questions arising

- Is $E(K)$ finite?
- How do we compute r?
- Could we produce a set of generators for $E(K)/E(K)_{tors}$?

Main insight in the field

Wiles, Breuil, Conrad, Diamond, Taylor

For $K = \mathbb{Q}$, $L(E/K, s)$ has analytic continuation to all of $\mathbb{C}$ and satisfies

$$L^*(E/K, 2-s) = w(E/K)L^*(E/K, s).$$

Main insight in the field

Wiles, Breuil, Conrad, Diamond, Taylor

For $K = \mathbb{Q}$, $L(E/K, s)$ has analytic continuation to all of $\mathbb{C}$ and satisfies

$$L^*(E/K, 2-s) = w(E/K)L^*(E/K, s).$$

Birch, Swinnerton-Dyer's conjecture

The analytic rank of E/K is defined as

$$r_{an} = ord_{s=1}L(E/K, s).$$

Conjecturally,

$$r = r_{an}.$$

Kummer sequence

Exact sequence of G_K modules

Let $K =$ imaginary quadratic field. Consider the short exact sequence of modules

$$0 \longrightarrow E_p \longrightarrow E \xrightarrow{p} E \longrightarrow 0.$$

Kummer sequence

Exact sequence of G_K modules

Let $K =$ imaginary quadratic field. Consider the short exact sequence of modules

$$0 \longrightarrow E_p \longrightarrow E \xrightarrow{p} E \longrightarrow 0.$$

Descent exact sequence

Taking Galois cohomology in G_K, we obtain

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} H^1(K, E_p) \longrightarrow H^1(K, E)_p \longrightarrow 0.$$

Selmer group and Shafarevich-Tate group

Local cohomology

For a place v of K, $K \hookrightarrow K_v$ induces $Gal(\overline{K_v}/K_v) \longrightarrow Gal(\overline{K}/K)$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \longrightarrow & H^1(K, E)_p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \overset{\rho}{\searrow} & \downarrow r & & \\
0 & \rightarrow & \prod_v E(K_v)/pE(K_v) & \xrightarrow{\delta} & \prod_v H^1(K_v, E_p) & \rightarrow & \prod_v H^1(K_v, E)_p & \rightarrow & 0
\end{array}$$

Selmer group and Shafarevich-Tate group

Local cohomology

For a place v of K, $K \hookrightarrow K_v$ induces $Gal(\overline{K_v}/K_v) \longrightarrow Gal(\overline{K}/K)$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \longrightarrow & H^1(K,E)_p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \searrow^{\rho} & \downarrow r & & \\
0 & \rightarrow & \prod_v E(K_v)/pE(K_v) & \xrightarrow{\delta} & \prod_v H^1(K_v, E_p) & \rightarrow & \prod_v H^1(K_v,E)_p & \rightarrow & 0
\end{array}$$

Definition

- $Sel_p(E/K) = ker(\rho)$
- $Ш(E/K)_p = ker(r)$

Importance of the Selmer group

Information on the algebraic rank r

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} Sel_p(E/K) \longrightarrow Ш(E/K)_p \longrightarrow 0$$

relates r to the size of $Sel_p(E/K)$.

Importance of the Selmer group

Information on the algebraic rank r

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} Sel_p(E/K) \longrightarrow Ш(E/K)_p \longrightarrow 0$$

relates r to the size of $Sel_p(E/K)$.

Shafarevich-Tate conjecture

The Shafarevich group $Ш(E/K)$ is conjecturally finite

$$\Longrightarrow Sel_p(E/K) = \delta(E(K)/pE(K))$$

for all but finitely many p.

From analytic to algebraic rank

Gross, Zagier

$$L'(E/K,1) = * \; height(y_K),$$

where $y_K \in E(K) \rightsquigarrow$ Heegner point of conductor 1. Hence,

$$r_{an} = 1 \implies r \geq 1.$$

From analytic to algebraic rank

Gross, Zagier

$$L'(E/K,1) = *\ height(y_K),$$

where $y_K \in E(K) \rightsquigarrow$ Heegner point of conductor 1. Hence,

$$r_{an} = 1 \implies r \geq 1.$$

Kolyvagin

If y_K is of infinite order in $E(K)$ then $Sel_p(E/K)$ has rank 1 and so does $E(K)$. Hence,

$$r_{an} = 1 \implies r = 1 \ \ \& \ \ r_{an} = 0 \implies r = 0.$$

From analytic to algebraic rank

Gross, Zagier

$$L'(E/K,1) = *\ height(y_K),$$

where $y_K \in E(K) \rightsquigarrow$ Heegner point of conductor 1. Hence,

$$r_{an} = 1 \implies r \geq 1.$$

Kolyvagin

If y_K is of infinite order in $E(K)$ then $Sel_p(E/K)$ has rank 1 and so does $E(K)$. Hence,

$$r_{an} = 1 \implies r = 1 \ \ \&\ \ r_{an} = 0 \implies r = 0.$$

Remark

Both of these theorems require the modularity of elliptic curves proved by Wiles, Breuil, Diamond, Conrad and Taylor.

From algebraic to analytic rank

Skinner, Urban

Let $r_p = rk(Hom_{\mathbb{Z}_p}(Sel_{p^\infty}(E/K), \mathbb{Q}/\mathbb{Z}))$,

$$r_p = 0 \implies r_{an} = 0.$$

From algebraic to analytic rank

Skinner, Urban

Let $r_p = rk(Hom_{\mathbb{Z}_p}(Sel_{p^\infty}(E/K), \mathbb{Q}/\mathbb{Z}))$,

$$r_p = 0 \implies r_{an} = 0.$$

Skinner

For certain elliptic curves,

$$r = 1 \ \& \ Ш < \infty \implies r_{an} = 1.$$

From algebraic to analytic rank

Skinner, Urban

Let $r_p = rk(Hom_{\mathbb{Z}_p}(Sel_{p^\infty}(E/K), \mathbb{Q}/\mathbb{Z}))$,

$$r_p = 0 \implies r_{an} = 0.$$

Skinner

For certain elliptic curves,

$$r = 1 \ \& \ Ш < \infty \implies r_{an} = 1.$$

Wei Zhang

For large classes of elliptic curves,

$$r_p = 1 \implies r_{an} = 1.$$

Probabilistic result

Bhargava, Shankar

$$Av\ Sel_5(E(\mathbb{Q})) = 6.$$

$\Longrightarrow$ average rank of E.C over $\mathbb{Q}$ ordered by height ≤ 1

$\Longrightarrow$ at least $4/5$ of E.C over $\mathbb{Q}$ have rank 0 or 1 and at least $1/5$ of of E.C over $\mathbb{Q}$ have rank 0

Probabilistic result

Bhargava, Shankar

$$Av\ Sel_5(E(\mathbb{Q})) = 6.$$

$\implies$ average rank of E.C over $\mathbb{Q}$ ordered by height ≤ 1

$\implies$ at least $4/5$ of E.C over $\mathbb{Q}$ have rank 0 or 1 and at least $1/5$ of of E.C over $\mathbb{Q}$ have rank 0

Bhargava, Skinner, Wei Zhang

At least 66% of E.C over $\mathbb{Q}$ satisfy BSD and have finite Shafarevich group.

From elliptic curve to modular form

Generalization

$$E \rightsquigarrow f, \quad T_p(E) \rightsquigarrow A$$

- $f =$ newform of even weight
- $A = p$-adic Galois representation associated to f, higher-weight analog of the Tate module $T_p(E)$

From elliptic curve to modular form

Generalization

$$E \rightsquigarrow f, \quad T_p(E) \rightsquigarrow A$$

- $f =$ newform of even weight
- $A = p$-adic Galois representation associated to f, higher-weight analog of the Tate module $T_p(E)$

Notation

- f normalized newform of level $N \geq 5$ and even weight $r+2 \geq 2$.
- $K = \mathbb{Q}(\sqrt{-D})$ imaginary quadratic field with odd discriminant satisfying the Heegner hypothesis with $|\mathcal{O}_K^\times| = 2$.

Set up

Algebraic Hecke character

$\psi : \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ Hecke character of K of infinity type $(r, 0)$

$\Longrightarrow$ there is an E.C A defined over the Hilbert class field K_1 of K with CM by $\mathscr{O}_K$.

Set up

Algebraic Hecke character

$\psi : \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ Hecke character of K of infinity type $(r, 0)$

$\Longrightarrow$ there is an E.C A defined over the Hilbert class field K_1 of K with CM by $\mathscr{O}_K$.

Ring of coefficients and prime p

Let $\mathscr{O}_F$ be the ring of integers of

$$F = \mathbb{Q}(a_1, a_2, \cdots, b_1, b_2, \cdots),$$

where the a_i's are the coefficients of f and the b_i's are the coefficients of θ_ψ. Let p be a prime with

$$(p, ND\phi(N)N_A r!) = 1,$$

where N_A is the conductor of A.

Motive associated to f and ψ.

Galois representations associated to f and A

- $f \rightsquigarrow V_f$, the f-isotypic part of the p-adic étale realization of the motive associated to f by Deligne.
- $A \rightsquigarrow V_A$, the p-adic étale realization of the motive associated to A.

V_f and V_A give rise (by extending scalars appropriately) to free $\mathscr{O}_F \otimes \mathbb{Z}_p$-modules of rank 2.

Motive associated to f and ψ.

Galois representations associated to f and A

- $f \rightsquigarrow V_f$, the f-isotypic part of the p-adic étale realization of the motive associated to f by Deligne.
- $A \rightsquigarrow V_A$, the p-adic étale realization of the motive associated to A.

V_f and V_A give rise (by extending scalars appropriately) to free $\mathcal{O}_F \otimes \mathbb{Z}_p$-modules of rank 2.

Galois representation associated to f and A

$$V = V_f \otimes_{\mathcal{O}_F \otimes \mathbb{Z}_p} V_A(r+1)$$

$V_{\wp_1}$ its localization at a prime $\wp_1$ in F dividing p, is a four dimensional representation of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Generalized Heegner cycles (Bertolini, Darmon, Prasana)

Level N structure

Heegner hypothesis

$\implies$ there is an ideal $\mathcal{N}$ of $\mathcal{O}_K$ satisfying $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$

$\implies$ level N structure on A, that is a point of exact order N defined over the ray class field L_1 of K of conductor $\mathcal{N}$.

Generalized Heegner cycles (Bertolini, Darmon, Prasana)

Level N structure

Heegner hypothesis
$\implies$ there is an ideal $\mathcal{N}$ of $\mathcal{O}_K$ satisfying $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$
$\implies$ level N structure on A, that is a point of exact order N defined over the ray class field L_1 of K of conductor $\mathcal{N}$.

GHC of conductor i

Consider (φ_i, A_i) where A_i is an E.C defined over K_1 with level N structure and $\varphi_i : A \longrightarrow A_i$ is an isogeny over $\overline{K}$.
$\rightsquigarrow$ codimension $r+1$ cycle on V

$$\Upsilon_{\varphi_i} = Graph(\varphi_i)^r \subset (A \times A_i)^r \simeq (A_i)^r \times A^r$$

$\rightsquigarrow$ GHC $\Delta_{\varphi_i} = e_r \Upsilon_{\varphi_i}$ of conductor i defined over $L_i = L_1 K_i$, where $K_i =$ ring class field of K of conductor i.

Selmer group

Definition

The Selmer group

$$S \subseteq H^1(L_1, V_{\wp_1}/p)$$

consists of the cohomology classes whose localizations at a prime v of L_1 lie in

$$\begin{cases} H^1(L_{1,v}^{ur}/L_{1,v}, V_{\wp_1}/p) \text{ for } v \text{ not dividing } NN_A p \\ H^1_f(L_{1,v}, V_{\wp_1}/p) \text{ for } v \text{ dividing } p \end{cases}$$

where $L_{1,v}$ is the completion of L_1 at v, and

$$H^1_f(L_{1,v}, V_{\wp_1}/p)$$

is the *finite part* of $H^1(L_{1,v}, V_{\wp_1}/p)$.

Analog of the transition map

Kuga-Sato like variety

$W_r = (\mathscr{E} \times_{X_N} \cdots \times_{X_N} \mathscr{E})^{c,s} =$ Kuga-Sato variety of dimension $r+1$.

$$X = W_r \times_{X_N} A^r.$$

Analog of the transition map

Kuga-Sato like variety

$W_r = (\mathscr{E} \times_{X_N} \cdots \times_{X_N} \mathscr{E})^{c,s}$ = Kuga-Sato variety of dimension $r+1$.

$$X = W_r \times_{X_N} A^r.$$

Chow group

$CH^r(X/L_1)_0$ = r-th Chow group of X over L_1 = group of homologically trivial cycles on X of codimension r modulo rational equivalence.

Analog of the transition map

Kuga-Sato like variety

$W_r = (\mathscr{E} \times_{X_N} \cdots \times_{X_N} \mathscr{E})^{c,s}$ = Kuga-Sato variety of dimension $r+1$.

$$X = W_r \times_{X_N} A^r.$$

Chow group

$CH^r(X/L_1)_0$ = r-th Chow group of X over L_1 = group of homologically trivial cycles on X of codimension r modulo rational equivalence.

p-adic Abel-Jacobi map

$$\phi : CH^r(X/L_1)_0 \longrightarrow H^1(L_1, V)$$

Analog of the BSD conjecture

Beilinson-Bloch's conjecture

$$rank(Im(\phi)) = ord_{s=r+1} L(f \otimes \theta_\psi, s).$$

Analog of the BSD conjecture

Beilinson-Bloch's conjecture

$$rank(Im(\phi)) = ord_{s=r+1} L(f \otimes \theta_\psi, s).$$

Conjectures on Φ

- $Ker(\Phi) = 0$
- $Im(\Phi) = S$.

Analog of the BSD conjecture

Beilinson-Bloch's conjecture

$$rank(Im(\phi)) = ord_{s=r+1} L(f \otimes \theta_\psi, s).$$

Conjectures on Φ

- $Ker(\Phi) = 0$
- $Im(\Phi) = S$.

Nekovar (ψ of infinity type $(0,0)$)

Assuming Φ(*Heegner cycle*) is not torsion,

$$rank(Im(\Phi)) = 1.$$

Results of Brylinski and Gross-Zagier $\rightsquigarrow$ p-adic analog of Beilinson-Bloch (Perrin-Riou).

Main theorem

Assumptions

- $(p, ND\phi(N)N_A r!) = 1$
- $G = Gal\left(L_1(V_{\wp_1}/p)/L_1\right) \simeq Aut(V_{\wp_1}/p)$
- $V_{\wp_1}/p$ is a simple $Aut(V_{\wp_1}/p)$-module
- the eigenvalues of the generator $Fr(v)$ of $Gal(L_{1,v}^{ur}/L_{1,v})$ acting on $V_{\wp_1}$ are not equal to 1 modulo p for v dividing NN_A

Main theorem

Assumptions

- $(p, ND\phi(N)N_A r!) = 1$
- $G = Gal\left(L_1(V_{\wp_1}/p)/L_1\right) \simeq Aut(V_{\wp_1}/p)$
- $V_{\wp_1}/p$ is a simple $Aut(V_{\wp_1}/p)$-module
- the eigenvalues of the generator $Fr(v)$ of $Gal(L_{1,v}^{ur}/L_{1,v})$ acting on $V_{\wp_1}$ are not equal to 1 modulo p for v dividing NN_A

Statement

If $\Phi(\Delta_{\varphi_1}) \neq 0$, then the Selmer group S has dimension 1 over $\mathscr{O}_{F,\wp_1}/p$, the localization of $\mathscr{O}_F$ at $\wp_1$ mod p.

Kolyvagin prime

Kolyvagin prime

A rational prime ℓ is a Kolyvagin prime if

$$\left(\frac{-D}{\ell}\right) = -1, \; a_\ell \equiv b_\ell \equiv \ell + 1 \equiv 0 \mod p.$$

Kolyvagin prime

Kolyvagin prime

A rational prime ℓ is a Kolyvagin prime if

$$\left(\frac{-D}{\ell}\right) = -1, \; a_\ell \equiv b_\ell \equiv \ell + 1 \equiv 0 \mod p.$$

Conductors of GHC

Let $n = \prod \ell$ be a squarefree integer where the ℓ's are Kolyvagin primes. Then

$$G_n = Gal(L_n/L_1) \simeq Gal(K_n/K_1) \simeq \prod_\ell Gal(K_\ell/K_1).$$

Let σ_ℓ be a generator of the cyclic group $Gal(K_\ell/K_1)$ of order $\ell + 1$.

Euler system properties

Set up

Consider isogenous pairs (A_n, φ_n), (A_m, φ_m) where $n = \ell m$ for an odd prime ℓ.

Euler system properties

Set up

Consider isogenous pairs (A_n, φ_n), (A_m, φ_m) where $n = \ell m$ for an odd prime ℓ.

Global compatibilies

$$T_\ell \Phi(\Delta_{\varphi_m}) = cor_{L_n, L_m} \Phi(\Delta_{\varphi_n}) = a_\ell b_\ell \Phi(\Delta_{\varphi_m}).$$

Euler system properties

Set up

Consider isogenous pairs (A_n, φ_n), (A_m, φ_m) where $n = \ell m$ for an odd prime ℓ.

Global compatibilies

$$T_\ell \Phi(\Delta_{\varphi_m}) = cor_{L_n,L_m} \Phi(\Delta_{\varphi_n}) = a_\ell b_\ell \Phi(\Delta_{\varphi_m}).$$

Local compatibilities

$$res_{\lambda_n} \Phi(\Delta_{\varphi_n}) = Frob_\ell(L_n/L_m)\ res_{\lambda_m} \Phi(\Delta_{\varphi_m}).$$

Euler system properties

Set up

Consider isogenous pairs (A_n, φ_n), (A_m, φ_m) where $n = \ell m$ for an odd prime ℓ.

Global compatibilies

$$T_\ell \Phi(\Delta_{\varphi_m}) = cor_{L_n, L_m} \Phi(\Delta_{\varphi_n}) = a_\ell b_\ell \Phi(\Delta_{\varphi_m}).$$

Local compatibilities

$$res_{\lambda_n} \Phi(\Delta_{\varphi_n}) = Frob_\ell(L_n/L_m)\ res_{\lambda_m} \Phi(\Delta_{\varphi_m}).$$

We denote by y_n the image of $\Phi(\Delta_{\varphi_n}) \in H^1(L_n, V)$ in $H^1(L_n, V_p)$.

Lifting the cohomology classes

Proposition

The restriction map

$$res_{L_1,L_n} : H^1(L_1, V_p) \longrightarrow H^1(L_n, V_p)^{G_n}$$

is an isomorphism.

Lifting the cohomology classes

Proposition

The restriction map

$$res_{L_1,L_n} : H^1(L_1, V_p) \longrightarrow H^1(L_n, V_p)^{G_n}$$

is an isomorphism.

Operators

Let

$$Tr_\ell = \sum_{i=0}^{\ell} \sigma_\ell^i, \quad D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i.$$

Define

$$D_n = \prod_{\ell|n} D_\ell \in \mathbb{Z}[G_n].$$

Kolyvagin cohomology classes

Proposition

$$D_n y_n \in H^1(L_n, V_p)^{G_n}.$$

$\implies D_n y_n$ can be lifted to $P(n) \in H^1(L_1, V_p)$.

Kolyvagin cohomology classes

Proposition

$$D_n y_n \in H^1(L_n, V_p)^{G_n}.$$

$\Longrightarrow$ $D_n y_n$ can be lifted to $P(n) \in H^1(L_1, V_p)$.

Local properties of $P(n)$

Let v be a prime of L_1.

- If $v | N_A N$, then $res_v(P(n))$ is trivial.
- If $v \nmid N_A Nnp$, then $res_v(P(n))$ lies in $H^1(L_{1,v}^{ur}/L_{1,v}, V_p)$.

Extension by Kolyvagin classes

Global pairing

The restriction map where $L = L_1(V_p)$

$$r : H^1(L_1, V_p) \longrightarrow H^1(L, V_p)^G = Hom_G(Gal(\overline{\mathbb{Q}}/L), V_p)$$

is injective and induces the evaluation pairing

$$[\ ,\ ]\ r(S) \times Gal(\overline{\mathbb{Q}}/L) \longrightarrow V_p.$$

Extension by Kolyvagin classes

Global pairing

The restriction map where $L = L_1(V_p)$

$$r : H^1(L_1, V_p) \longrightarrow H^1(L, V_p)^G = Hom_G(Gal(\overline{\mathbb{Q}}/L), V_p)$$

is injective and induces the evaluation pairing

$$[\ ,\ ]\ r(S) \times Gal(\overline{\mathbb{Q}}/L) \longrightarrow V_p.$$

Notation

- $Gal_S(\overline{\mathbb{Q}}/L) =$ annihilator of $r(S)$
- $L^S =$ extension of L fixed by $Gal_S(\overline{\mathbb{Q}}/L)$
- $G_S = Gal(L^S/L)$
- $I = Gal(L^S/L(y_1))$

Choice of a pertinent Kolyvagin class

Proposition

There is a Kolyvagin prime q such that

$$Frob_q(L^S/\mathbb{Q}) = \tau h, \quad h \in Gal(L^S/L), \quad h^{\tau+1} \notin I \quad \text{and} \quad res_\beta y_1 \neq 0$$

for some prime β in L_1 above q.

Choice of a pertinent Kolyvagin class

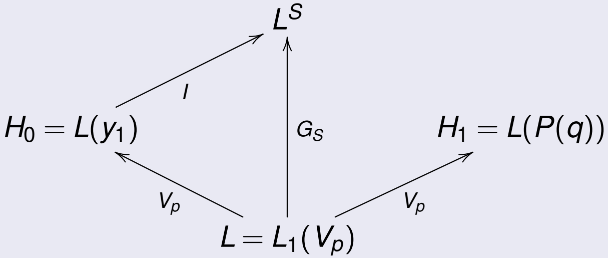
Proposition

There is a Kolyvagin prime q such that

$$Frob_q(L^S/\mathbb{Q}) = \tau h, \quad h \in Gal(L^S/L), \quad h^{\tau+1} \notin I \quad \text{and} \quad res_\beta y_1 \neq 0$$

for some prime β in L_1 above q.

Scheme



Local Tate duality

Proposition

$P(n)$ belongs to the $(-1)^{\omega(n)}\varepsilon$-eigenspace where $\omega(n)$ is the number of distinct prime factors of n.

Local Tate duality

Proposition

$P(n)$ belongs to the $(-1)^{\omega(n)}\varepsilon$-eigenspace where $\omega(n)$ is the number of distinct prime factors of n.

Local pairing

Using local Tate duality, we have a perfect local pairing

$$\langle\ .\ ,\ .\ \rangle_{\lambda'} : H^1(L_{1,\lambda'}^{ur}/L_{1,\lambda'}, V_p) \times H^1(L_{1,\lambda'}^{ur}, V_p) \longrightarrow \mathbb{Z}/p.$$

The action of complex conjugation induces non-degenerate pairings of eigenspaces.

From local to global information

Reciprocity law

We have

$$\sum_{\lambda'|\ell|n} \langle s_{\lambda'}, res_{\lambda'} P(n) \rangle_{\lambda'} = 0.$$

From local to global information

Reciprocity law

We have

$$\sum_{\lambda'|\ell|n} \langle s_{\lambda'}, res_{\lambda'} P(n) \rangle_{\lambda'} = 0.$$

Proposition 1

We have $S^{-\varepsilon}$ is of dimension 0 over $\mathcal{O}_{F,\wp_1}/p$.

From local to global information

Reciprocity law

We have

$$\sum_{\lambda'|\ell|n} \langle s_{\lambda'}, res_{\lambda'} P(n) \rangle_{\lambda'} = 0.$$

Proposition 1

We have $S^{-\varepsilon}$ is of dimension 0 over $\mathcal{O}_{F,\wp_1}/p$.

Proposition 2

We have $S^{+\varepsilon}$ is of dimension 1 over $\mathcal{O}_{F,\wp_1}/p$.

Sketch of proof 1

Consider $P(\ell)$ where ℓ is a Kolyvagin prime satisfying

$$Frob_\ell(L^S/\mathbb{Q}) = \tau h, \quad h \in G_S, \quad h \notin Gal(L^S/L(y_1)).$$

$P(\ell)$ belongs to the $-\varepsilon$-eigenspace. Let $s \in S^{-\varepsilon}$. Then

$$\sum_{\lambda'|\ell} \langle res_{\lambda'} s, res_{\lambda'} P(\ell) \rangle_{\lambda'}^{-\varepsilon} = 0$$

$\implies res_{\lambda'} s = 0$
$\implies s(G_S^+) = 0$ by Cebotarev's density theorem
$\implies s : G_S^- \longrightarrow V_p^\pm$
$\implies s(G_S^-) = s = 0$ since $V_p^\pm$ are of rank 2 over $\mathscr{O}_{F,\wp_1}/p$ and V_p has no non-trivial G-submodules.

Consider $P(\ell q)$ where ℓ be a Kolyvagin prime such that

- $Frob_\ell(L^S/\mathbb{Q}) = \tau i, \;\; i \in Gal(L^S/L(y_1))$
- $Frob_\ell(L(P(q))/\mathbb{Q}) = \tau j, \;\; j \in Gal(L(P(q))/L), \;\; j^{\tau+1} \neq 1.$

$P(\ell q)$ belongs to the ε-eigenspace. Let $s \in S^{+\varepsilon}$. Then

$$\sum_{\lambda'|\lambda} \langle res_{\lambda'} s, res_{\lambda'} P(\ell q)\rangle_{\lambda'}^{+\varepsilon} + \sum_{\beta'|\beta} \langle res_{\beta'} s, res_{\beta'} P(\ell q)\rangle_{\beta'}^{+\varepsilon} = 0$$

$\implies res_{\lambda'} s = 0$
$\implies s(I^+) = 0$ by Cebotarev's density theorem
$\implies s : I^- \longrightarrow V_p^{\pm}$
$\implies s(I^-) = s(I) = 0$
$\implies s \in Hom_G(Gal(L^S/L)/I, V_p) \simeq Hom_G(V_p, V_p) \simeq \mathcal{O}_{F,\wp_1}/p.$

Thank You!