Cup products
and Selmer groups of reducible representations

Romyar Sharifi

McMaster University

July 18, 2008

Introduction

At CNTA IX, we discussed an explicit conjectural correspondence of the following form, for an odd prime p.

cup products of cyclotomic p-units in étale cohomology of p-integers	$\leftrightarrow$	reductions of p-adic L-values of newforms congruent to Eisenstein series at p

In this talk, we will

- explain the conjecture in a special yet fundamental case
- discuss evidence for it arising from Selmer groups

The cup product

p odd prime, μ_p pth roots of unity in $\overline{\mathbf{Q}}$
$F = \mathbf{Q}(\mu_p)$ pth cyclotomic field

$\mathfrak{G}_F$ Galois group of maximal extension of F in which only the prime above p ramifies

Consider the following cup product in Galois cohomology:

$$H^1(\mathfrak{G}_F, \mu_p) \otimes H^1(\mathfrak{G}_F, \mu_p) \xrightarrow{\cup} H^2(\mathfrak{G}_F, \mu_p^{\otimes 2})$$

The cup product

p odd prime, μ_p pth roots of unity in $\overline{\mathbf{Q}}$
$F = \mathbf{Q}(\mu_p)$ pth cyclotomic field

$\mathfrak{G}_F$ Galois group of maximal extension of F in which only the prime above p ramifies

Consider the following cup product in Galois cohomology:

$$H^1(\mathfrak{G}_F, \mu_p) \otimes H^1(\mathfrak{G}_F, \mu_p) \xrightarrow{\cup} H^2(\mathfrak{G}_F, \mu_p^{\otimes 2})$$

The cup product tells us about the commutators appearing in relations among generators in a presentation of the Galois group of the maximal pro-p quotient of $\mathfrak{G}_F$.

Applications of the cup product

This cup product has quite a few other applications to the structure of Galois groups and related modules, including:

- Hilbert p-class field tower of F – when is it just one step?
- p-parts of class groups of Kummer extensions of F that are unramified outside p – describes 2nd graded piece in their augmentation filtration
- Galois group of the maximal abelian pro-p extension of the compositum of all $\mathbf{Z}_p$-extensions of F – yields information on its size
- Selmer groups of residually reducible representations – will discuss later in this talk

Objects attached to the pth cyclotomic field

$\Delta = \mathrm{Gal}(F/\mathbf{Q})$
ζ fixed primitive pth root of unity in F

Teichmüller character $\omega\colon \Delta \xrightarrow{\sim} \mu_{p-1}(\mathbf{Z}_p) \subset \mathbf{Z}_p^\times$, $\delta(\zeta) = \zeta^{\omega(\delta)}$.

Objects attached to the pth cyclotomic field

$\Delta = \mathrm{Gal}(F/\mathbf{Q})$
ζ fixed primitive pth root of unity in F

Teichmüller character $\omega\colon \Delta \xrightarrow{\sim} \mu_{p-1}(\mathbf{Z}_p) \subset \mathbf{Z}_p^\times$, $\delta(\zeta) = \zeta^{\omega(\delta)}$.

Fundamental $\mathbf{Z}_p[\Delta]$-modules:

- p-completion $\mathcal{E}_F$ of p-units $\mathbf{Z}[\zeta, 1/p]^\times$ in F
- p-completion $\mathcal{C}_F$ of the cyclotomic p-units of F, generated by $1-\zeta$ as a $\mathbf{Z}_p[\Delta]$-module
- p-part A_F of the ideal class group of F (p-power torsion)

Objects attached to the pth cyclotomic field

$\Delta = \mathrm{Gal}(F/\mathbf{Q})$
ζ fixed primitive pth root of unity in F

Teichmüller character $\omega\colon \Delta \xrightarrow{\sim} \mu_{p-1}(\mathbf{Z}_p) \subset \mathbf{Z}_p^\times$, $\delta(\zeta) = \zeta^{\omega(\delta)}$.

Fundamental $\mathbf{Z}_p[\Delta]$-modules:

- p-completion $\mathcal{E}_F$ of p-units $\mathbf{Z}[\zeta, 1/p]^\times$ in F
- p-completion $\mathcal{C}_F$ of the cyclotomic p-units of F, generated by $1-\zeta$ as a $\mathbf{Z}_p[\Delta]$-module
- p-part A_F of the ideal class group of F (p-power torsion)

Kummer theory yields

$$\mathcal{E}_F/p\mathcal{E}_F \hookrightarrow H^1(\mathfrak{G}_F, \mu_p) \quad \text{and} \quad A_F/pA_F \cong H^2(\mathfrak{G}_F, \mu_p).$$

Thus, our cup product sets up a Galois-equivariant pairing

$$(\,\cdot\,,\,\cdot\,)\colon \mathcal{C}_F \times \mathcal{C}_F \to A_F \otimes \mu_p.$$

Eigenspaces

Given a $\mathbf{Z}_p[\Delta]$-module A, we have a decomposition

$$A = \bigoplus_{i=0}^{p-2} A^{(i)}, \qquad A^{(i)} = \{a \in A \mid \delta a = \omega(\delta)^i a, \text{ for all } \delta \in \Delta\}.$$

Eigenspaces

Given a $\mathbf{Z}_p[\Delta]$-module A, we have a decomposition

$$A = \bigoplus_{i=0}^{p-2} A^{(i)}, \qquad A^{(i)} = \{a \in A \mid \delta a = \omega(\delta)^i a, \text{ for all } \delta \in \Delta\}.$$

We also have (± 1)-eigenspaces $A^{\pm}$ for the element of order 2, which results in a decomposition $A = A^+ \oplus A^-$. Note that

$$A^+ = \bigoplus_{\substack{i=0 \\ i \text{ even}}}^{p-3} A^{(i)} \quad \text{and} \quad A^- = \bigoplus_{\substack{i=1 \\ i \text{ odd}}}^{p-2} A^{(i)}.$$

Eigenspaces

Given a $\mathbf{Z}_p[\Delta]$-module A, we have a decomposition

$$A = \bigoplus_{i=0}^{p-2} A^{(i)}, \qquad A^{(i)} = \{a \in A \mid \delta a = \omega(\delta)^i a, \text{ for all } \delta \in \Delta\}.$$

We also have (± 1)-eigenspaces $A^{\pm}$ for the element of order 2, which results in a decomposition $A = A^+ \oplus A^-$. Note that

$$A^+ = \bigoplus_{\substack{i=0 \\ i \text{ even}}}^{p-3} A^{(i)} \quad \text{and} \quad A^- = \bigoplus_{\substack{i=1 \\ i \text{ odd}}}^{p-2} A^{(i)}.$$

We have idempotents ϵ_i yielding the projections $A \to A^{(i)}$:

$$\epsilon_i \in \mathbf{Z}_p[\Delta], \qquad \epsilon_i = \frac{1}{p-1} \sum_{\delta \in \Delta} \omega(\delta)^{-i} \delta.$$

Eigenspaces of p-units and class groups

Facts: $\mathcal{E}_F = \mathcal{E}_F^+ \oplus \mu_p$ and $[\mathcal{E}_F : \mathcal{C}_F] = |A_F^+|$.

Eigenspaces of p-units and class groups

Facts: $\mathcal{E}_F = \mathcal{E}_F^+ \oplus \mu_p$ and $[\mathcal{E}_F : \mathcal{C}_F] = |A_F^+|$.
Vandiver's Conjecture: $A_F^+ = 0$ (known for $p <$ 12,000,000).

Eigenspaces of p-units and class groups

Facts: $\mathcal{E}_F = \mathcal{E}_F^+ \oplus \mu_p$ and $[\mathcal{E}_F : \mathcal{C}_F] = |A_F^+|$.
Vandiver's Conjecture: $A_F^+ = 0$ (known for $p <$ 12,000,000).

For odd i, set $\eta_i = (1-\zeta)^{\epsilon_{1-i}}$. Then $\mathcal{C}_F^{(1-i)} = \langle \eta_i \rangle$.

Eigenspaces of p-units and class groups

Facts: $\mathcal{E}_F = \mathcal{E}_F^+ \oplus \mu_p$ and $[\mathcal{E}_F : \mathcal{C}_F] = |A_F^+|$.
Vandiver's Conjecture: $A_F^+ = 0$ (known for $p <$ 12,000,000).

For odd i, set $\eta_i = (1-\zeta)^{\epsilon_{1-i}}$. Then $\mathcal{C}_F^{(1-i)} = \langle \eta_i \rangle$.

B_k kth Bernoulli number

Theorem (Herbrand-Ribet)

For $k \geq 2$ even,

$$A_F^{(1-k)} \neq 0 \Leftrightarrow p \mid \frac{B_k}{k}.$$

We say (p, k) is irregular if $p \mid B_k$ and $2 \leq k \leq p-3$.

Eigenspaces of p-units and class groups

Facts: $\mathcal{E}_F = \mathcal{E}_F^+ \oplus \mu_p$ and $[\mathcal{E}_F : \mathcal{C}_F] = |A_F^+|$.
Vandiver's Conjecture: $A_F^+ = 0$ (known for $p <$ 12,000,000).

For odd i, set $\eta_i = (1-\zeta)^{\epsilon_{1-i}}$. Then $\mathcal{C}_F^{(1-i)} = \langle \eta_i \rangle$.

B_k kth Bernoulli number

Theorem (Herbrand-Ribet)

For $k \geq 2$ even,

$$A_F^{(1-k)} \neq 0 \Leftrightarrow p \mid \frac{B_k}{k}.$$

We say (p,k) is irregular if $p \mid B_k$ and $2 \leq k \leq p-3$.

Reflection principle: for k even,

$$A_F^{(k)} = 0 \Rightarrow A_F^{(1-k)} \text{ cyclic.}$$

A pairing arising from the cup product

For i odd and k even, set

$$e_{i,k} = (\eta_i, \eta_{k-i}) \in A_F^{(1-k)} \otimes \mu_p.$$

A pairing arising from the cup product

For i odd and k even, set

$$e_{i,k} = (\eta_i, \eta_{k-i}) \in A_F^{(1-k)} \otimes \mu_p.$$

Conjecture (McCallum-S.)

The $e_{i,k}$ generate $A_F^{(1-k)} \otimes \mu_p$.

Under Vandiver, $A_F^{(1-k)} \otimes \mu_p$ is a 1-dimensional $\mathbf{F}_p$-vector space.

For irregular (p, k) with $p < 25{,}000$, we computed of a unique possibility for $(e_{1,k} \; e_{3,k} \; \dots \; e_{p-2,k}) \in \mathbf{P}^{(p-3)/2}(\mathbf{F}_p)$, should the conjecture hold.

A pairing arising from the cup product

For i odd and k even, set

$$e_{i,k} = (\eta_i, \eta_{k-i}) \in A_F^{(1-k)} \otimes \mu_p.$$

Conjecture (McCallum-S.)

The $e_{i,k}$ generate $A_F^{(1-k)} \otimes \mu_p$.

Under Vandiver, $A_F^{(1-k)} \otimes \mu_p$ is a 1-dimensional $\mathbf{F}_p$-vector space.

For irregular (p, k) with $p < 25{,}000$, we computed of a unique possibility for $(e_{1,k} \; e_{3,k} \; \dots \; e_{p-2,k}) \in \mathbf{P}^{(p-3)/2}(\mathbf{F}_p)$, should the conjecture hold.

Theorem (S.)

The conjecture holds for $p < 1000$.

Examples of the $(e_{1,k}\ e_{3,k}\ \dots\ e_{p-2,k})$

- $p = 37,\ k = 32$
  (1 26 0 36 1 35 31 34 3 6 2 36 1 0 11 36 11 26)
- $p = 59,\ k = 44$
  (1 45 21 30 14 35 5 0 48 57 7 52 2 11 0 54 24 45 29 38 14 58 27 32 15 0 44 27 32)
- $p = 67,\ k = 58$
  (1 45 38 56 0 47 62 9 29 15 65 26 45 57 0 10 22 41 2 52 38 58 5 20 0 11 29 22 66 2 24 43 65)
- $p = 101,\ k = 68$
  (1 56 40 96 26 63 0 61 81 71 35 92 73 64 6 88 0 0 13 95 37 28 9 66 30 20 40 0 38 75 5 61 45 100 17 17 12 66 72 53 86 31 70 15 48 29 35 89 84 84)

Examples of the $(e_{1,k}\ e_{3,k}\ \ldots\ e_{p-2,k})$

- $p = 37,\ k = 32$
  (1 26 0 36 1 35 31 34 3 6 2 36 1 0 11 36 11 26)
- $p = 59,\ k = 44$
  (1 45 21 30 14 35 5 0 48 57 7 52 2 11 0 54 24 45 29 38 14 58 27 32 15 0 44 27 32)
- $p = 67,\ k = 58$
  (1 45 38 56 0 47 62 9 29 15 65 26 45 57 0 10 22 41 2 52 38 58 5 20 0 11 29 22 66 2 24 43 65)
- $p = 101,\ k = 68$
  (1 56 40 96 26 63 0 61 81 71 35 92 73 64 6 88 0 0 13 95 37 28 9 66 30 20 40 0 38 75 5 61 45 100 17 17 12 66 72 53 86 31 70 15 48 29 35 89 84 84)

Question

What is the arithmetic meaning of these values?

Congruences of newforms with Eisenstein series

Eisenstein series of weight 2, level p, character ω^{k-2}

$$G_{2,\omega^{k-2}} = -\frac{B_{2,\omega^{k-2}}}{2} + \sum_{n=1}^{\infty} \left(\sum_{1 \leq t | n} \omega^{k-2}(t) t \right) q^n.$$

Congruences of newforms with Eisenstein series

Eisenstein series of weight 2, level p, character ω^{k-2}

$$G_{2,\omega^{k-2}} = -\frac{B_{2,\omega^{k-2}}}{2} + \sum_{n=1}^{\infty} \left(\sum_{1 \le t \mid n} \omega^{k-2}(t) t \right) q^n.$$

(p, k) irregular $\Rightarrow p \mid B_{2,\omega^{k-2}}$.

Eisenstein series of weight 2, level p, character ω^{k-2}

$$G_{2,\omega^{k-2}} = -\frac{B_{2,\omega^{k-2}}}{2} + \sum_{n=1}^{\infty} \left(\sum_{1 \le t | n} \omega^{k-2}(t) t \right) q^n.$$

(p, k) irregular $\Rightarrow p \mid B_{2,\omega^{k-2}}$.

In this case, there exists a newform f of the same weight, level, and character and a congruence

$$f \equiv G_{2,\omega^{k-2}} \bmod \mathfrak{p}_f,$$

where $f = \sum_{n=1}^{\infty} a_n q^n$, $\mathcal{O}_f = \mathbf{Z}_p[a_2, a_3, \ldots]$, and $\mathfrak{p}_f \subset \mathcal{O}_f$ is generated by p and $a_\ell - 1 - \ell\omega^{k-2}(\ell)$ for all primes ℓ.

A comparison map

The p-adic L-functions of newforms (Mazur-Tate-Teitelbaum) interpolate the special values of classical L-functions for f and its twists, up to certain factors.

Let H_f be the $\mathcal{O}_f$-lattice in $\mathbf{C}_p$ spanned by all $L_p(f, \omega^j, 1)$.

$H_f = H_f^+ \oplus H_f^-$, where $H_f^\pm$ is spanned by the $L_p(f, \omega^j, 1)$ with j even/odd, resp.

A comparison map

The p-adic L-functions of newforms (Mazur-Tate-Teitelbaum) interpolate the special values of classical L-functions for f and its twists, up to certain factors.

Let H_f be the $\mathcal{O}_f$-lattice in $\mathbf{C}_p$ spanned by all $L_p(f, \omega^j, 1)$.

$H_f = H_f^+ \oplus H_f^-$, where $H_f^\pm$ is spanned by the $L_p(f, \omega^j, 1)$ with j even/odd, resp.

We derive the following using the work of Ohta (following Ribet, Mazur-Wiles, Wiles, Kurihara, and Harder-Pink).

Proposition

There exists an (almost canonical) homomorphism

$$\phi_f \colon A_F^{(1-k)} \otimes \mu_p \to H_f^+/\mathfrak{p}_f H_f^+,$$

that is surjective if $(p, p+1-k)$ is regular.

The conjecture

For i odd, let $g_{i,f}$ be the image of $L_p(f, \omega^{i-1}, 1)$ in $H_f^+/\mathfrak{p}_f H_f^+$.

Conjecture (S.)

For each irregular pair (p, k) and f as above, there exists a canonical $c_f \in (\mathbf{Z}/p\mathbf{Z})^\times$ such that

$$\phi_f(e_{i,k}) = c_f g_{i,f}$$

for all odd i.

The conjecture

For i odd, let $g_{i,f}$ be the image of $L_p(f, \omega^{i-1}, 1)$ in $H_f^+/\mathfrak{p}_f H_f^+$.

Conjecture (S.)

For each irregular pair (p, k) and f as above, there exists a canonical $c_f \in (\mathbf{Z}/p\mathbf{Z})^\times$ such that

$$\phi_f(e_{i,k}) = c_f g_{i,f}$$

for all odd i.

Theorem (S.)

If $(p, p+1-k)$ is regular, then $\phi_f(e_{1,k}) = c_f g_{1,f}$ for some $c_f \in (\mathbf{Z}/p\mathbf{Z})^\times$.

The conjecture

For i odd, let $g_{i,f}$ be the image of $L_p(f, \omega^{i-1}, 1)$ in $H_f^+/\mathfrak{p}_f H_f^+$.

Conjecture (S.)

For each irregular pair (p, k) and f as above, there exists a canonical $c_f \in (\mathbf{Z}/p\mathbf{Z})^\times$ such that

$$\phi_f(e_{i,k}) = c_f g_{i,f}$$

for all odd i.

Theorem (S.)

If $(p, p+1-k)$ is regular, then $\phi_f(e_{1,k}) = c_f g_{1,f}$ for some $c_f \in (\mathbf{Z}/p\mathbf{Z})^\times$.

Corollary

The conjecture is true for $p < 1000$.

The Galois modules

We may consider H_f as a lattice in the Galois representation attached to f, so it has a $G_{\mathbf{Q}}$-action unramified outside p, ∞.

The Galois modules

We may consider H_f as a lattice in the Galois representation attached to f, so it has a $G_{\mathbf{Q}}$-action unramified outside p, ∞.

Let

$$W_f = H_f \otimes_{\mathcal{O}_f} \mathrm{Hom}(\mathcal{O}_f, \mathbf{Q}_p/\mathbf{Z}_p).$$

As $G_{\mathbf{Q}_p}$-modules, we have

$$0 \to W_f^- \to W_f \to W_f/W_f^- \to 0.$$

The Galois modules

We may consider H_f as a lattice in the Galois representation attached to f, so it has a $G_{\mathbf{Q}}$-action unramified outside p, ∞.

Let

$$W_f = H_f \otimes_{\mathcal{O}_f} \mathrm{Hom}(\mathcal{O}_f, \mathbf{Q}_p/\mathbf{Z}_p).$$

As $G_{\mathbf{Q}_p}$-modules, we have

$$0 \to W_f^- \to W_f \to W_f/W_f^- \to 0.$$

Let $T_f = W_f[\mathfrak{p}_f]$ be the submodule of W_f killed by all elements of $\mathfrak{p}_f$. Then

$$T_f \cong H_f/\mathfrak{p}_f H_f,$$

and it fits into an exact sequence of $G_{\mathbf{Q}}$-modules

$$0 \to T_f^+ \to T_f \to T_f/T_f^+ \to 0$$

that is locally split at p .

Selmer groups

Let us now fix an odd integer i.
We consider the twist of W_f by ω^{i-1}:

$$W_{i,f} = W_f \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[\Delta]^{(i-1)}.$$

Its Selmer group may be defined as

$$\mathrm{Sel}(\mathbf{Q}, W_{i,f}) = \ker(H^1(\mathfrak{G}_{\mathbf{Q}}, W_{i,f}) \to H^1(I_p, W_{i,f}/W_{i,f}^-)),$$

where $\mathfrak{G}_{\mathbf{Q}}$ is the Galois group of the maximal extension of $\mathbf{Q}$ unramified outside $\{p, \infty\}$ and I_p is an inertia group at p.

Let us now fix an odd integer i.
We consider the twist of W_f by ω^{i-1}:

$$W_{i,f} = W_f \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[\Delta]^{(i-1)}.$$

Its Selmer group may be defined as

$$\mathrm{Sel}(\mathbf{Q}, W_{i,f}) = \ker(H^1(\mathfrak{G}_{\mathbf{Q}}, W_{i,f}) \to H^1(I_p, W_{i,f}/W_{i,f}^{-})),$$

where $\mathfrak{G}_{\mathbf{Q}}$ is the Galois group of the maximal extension of $\mathbf{Q}$ unramified outside $\{p, \infty\}$ and I_p is an inertia group at p.

We take

$$T_{i,f} = W_{i,f}[\mathfrak{p}_f] \cong H_f/\mathfrak{p}_f H_f \otimes \mu_p^{\otimes(i-1)},$$

and define $\mathrm{Sel}(\mathbf{Q}, T_{i,f})$ in the same way.

Selmer groups of the residual representations

Simplifying assumptions: $i \not\equiv \pm(1-k) \bmod p-1$,

$$A_F^{(k)} = A_F^{(k-i)} = 0.$$

Selmer groups of the residual representations

Simplifying assumptions: $i \not\equiv \pm(1-k) \bmod p-1$,

$$A_F^{(k)} = A_F^{(k-i)} = 0.$$

Then

$$0 \to \mu_p^{\otimes(i+1-k)} \to T_{i,f} \to \mu_p^{\otimes i} \to 0.$$

Selmer groups of the residual representations

Simplifying assumptions: $i \not\equiv \pm(1-k) \bmod p-1$,

$$A_F^{(k)} = A_F^{(k-i)} = 0.$$

Then

$$0 \to \mu_p^{\otimes(i+1-k)} \to T_{i,f} \to \mu_p^{\otimes i} \to 0.$$

One can derive the following using the relationship between cup product values and class groups of Kummer extensions of F:

Theorem (S.)

Under our assumptions,

$$\mathrm{Sel}(\mathbf{Q}, T_{i,f}) \cong \begin{cases} \mathbf{Z}/p\mathbf{Z} & e_{i,k} = 0 \\ 0 & e_{i,k} \neq 0. \end{cases}$$

The main conjecture for modular forms

Let $\mathbf{Q}_\infty$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Then $\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f})$ is defined in the same manner as for $\mathbf{Q}$.

The main conjecture of Iwasawa theory for f (Mazur, Greenberg) tells us that the structure of $\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f})$ is largely governed by $L_p(f, \omega^{i-1}, s)$.

The main conjecture for modular forms

Let $\mathbf{Q}_\infty$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$.
Then $\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f})$ is defined in the same manner as for $\mathbf{Q}$.

The main conjecture of Iwasawa theory for f (Mazur, Greenberg) tells us that the structure of $\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f})$ is largely governed by $L_p(f, \omega^{i-1}, s)$.

More precisely, the p-adic L-function $L_p(f, \omega^{i-1}, s)$ determines a power series $F_{i,f} \in \mathcal{O}_f[[T]]$ with

$$F_{i,f}((1+p)^s - 1) = L_p(f, \omega^{i-1}, s)$$

for all $s \in \mathbf{Z}_p$. The main conjecture asserts that $F_{i,f}$ generates the "characteristic ideal" of $\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f})^\vee$ over $\mathcal{O}_f[[T]]$.

The main conjecture for modular forms

Let $\mathbf{Q}_\infty$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$.
Then $\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f})$ is defined in the same manner as for $\mathbf{Q}$.

The main conjecture of Iwasawa theory for f (Mazur, Greenberg) tells us that the structure of $\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f})$ is largely governed by $L_p(f, \omega^{i-1}, s)$.

More precisely, the p-adic L-function $L_p(f, \omega^{i-1}, s)$ determines a power series $F_{i,f} \in \mathcal{O}_f[[T]]$ with

$$F_{i,f}((1+p)^s - 1) = L_p(f, \omega^{i-1}, s)$$

for all $s \in \mathbf{Z}_p$. The main conjecture asserts that $F_{i,f}$ generates the "characteristic ideal" of $\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f})^\vee$ over $\mathcal{O}_f[[T]]$.

Remark

We have chosen the lattice H_f such that we expect the Selmer group to be finitely generated over $\mathbf{Z}_p$.

Relationship with our conjecture

We have the following corollary of our result on $\mathrm{Sel}(\mathbf{Q}, T_{i,f})$:

Corollary

$$\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f}) = 0 \Leftrightarrow e_{i,k} \neq 0.$$

Relationship with our conjecture

We have the following corollary of our result on $\mathrm{Sel}(\mathbf{Q}, T_{i,f})$:

Corollary

$$\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f}) = 0 \Leftrightarrow e_{i,k} \neq 0.$$

Recall that $g_{i,f}$ is the image of $L_p(f, \omega^{i-1}, 1)$ in $H_f^+/\mathfrak{p}_f H_f^+$. The main conjecture then implies:

Conjecture

$$\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f}) = 0 \Rightarrow g_{i,f} \neq 0.$$

Relationship with our conjecture

We have the following corollary of our result on $\mathrm{Sel}(\mathbf{Q}, T_{i,f})$:

Corollary

$$\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f}) = 0 \Leftrightarrow e_{i,k} \neq 0.$$

Recall that $g_{i,f}$ is the image of $L_p(f, \omega^{i-1}, 1)$ in $H_f^+/\mathfrak{p}_f H_f^+$.
The main conjecture then implies:

Conjecture

$$\mathrm{Sel}(\mathbf{Q}_\infty, W_{i,f}) = 0 \Rightarrow g_{i,f} \neq 0.$$

Putting these together, we conclude:

Theorem

Assuming the main conjecture for f and with our earlier assumptions, we have that

$$e_{i,k} \neq 0 \Rightarrow g_{i,f} \neq 0.$$