CRITICAL VALUES, CONGRUENCES AND MOVING BETWEEN SELMER GROUPS

NEIL DUMMIGAN

Abstract. We look at various related constructions of elements in Selmer groups, which confirm predictions of the Bloch-Kato conjecture, or which, in conjunction with the Bloch-Kato conjecture, yield predictions that can be verified. We begin with a particular critical value for the tensor product $L$-function associated to a pair of cusp forms of different weights.

1. A critical value of the tensor product $L$-function

In this section we review parts of [Du1], in particular Theorem 14.2. Let $f \in S_{k'} := S_k^*(\text{SL}_2(\mathbb{Z}))$, $g \in S_k$, with $k' > k$, be normalised eigenforms. If $f = \sum_{n=1}^{\infty} a_n q^n$ then

$$L_f(s) = \sum_{n=1}^{\infty} a_n n^{-s} = \prod_{p \text{ prime}} L_{f,p}(s),$$

where $L_{f,p}(s) = (1 - a_p p^{-s} + p^{k'-1-2s})^{-1}$. The series converges for $\Re s$ sufficiently large, but there is an analytic continuation to the whole of $\mathbb{C}$.

Let $K$ be any number field containing $\mathbb{Q}(\{a_n\})$, and $\lambda$ any prime of $\mathcal{O}_K$, say $\lambda | \ell$. By a theorem of Deligne, there exists a continuous linear representation $\rho_f : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(V'_\lambda)$ (where $V'_\lambda$ is a 2-dimensional $\mathbb{K}'_\lambda$-vector space) such that, for any prime $p$, and any $\lambda$ such that $\ell \neq p$,

$$L_{f,p}(s) = \det(1 - \rho_f(\text{Frob}_p^{-1})p^{-s})^{-1}.$$

Here $\text{Frob}_p$ is an element of $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \text{Gal}(\bar{\mathcal{O}}/\mathbb{Q})$ lifting the automorphism $x \mapsto x^p$ of $\text{Gal}^{\text{alg}}(\bar{\mathbb{F}}/\mathbb{F}_p)$.

Let $K = \mathbb{Q}(\{a_n, b_n\})$, where $g = \sum_{n=1}^{\infty} b_n q^n$. We also have $\rho_g : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(V_\lambda)$, and define in the natural way $\rho_{f \otimes g} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(V'_\lambda \otimes V_\lambda)$. Substituting $\rho_{f \otimes g}$ for $\rho_f$ in (1), we obtain

$$L(s) := L_{f \otimes g}(s) := \prod_{p} L_{f \otimes g,p}(s).$$

This, like $L_f(s)$, is an example of a motivic $L$-function, and its critical values are $L(t)$ for $k \leq t \leq k' - 1$. It is easy to show that

$$L_{f \otimes g}(s) = \zeta(2s+2-k-k')D(s, f, g),$$

Date: June 23rd, 2009.
1991 Mathematics Subject Classification. 11F67, 11F80, 11F33, 11G40.
with \(D(s,f,g) := \sum_{n=1}^{\infty} a_n b_n n^{-s}\). Shimura [Sh] proved the following formula for the critical values:

\[
D(k' - 1 - r, f, g) = c\pi^{k'-1} (f, g\delta^{(r)}_{k'-k-2r}, E_{k'-k-2r})
\]

(Petersson inner product), where \(c = \frac{(k'-k-2r-1)!}{[(k'-2r-1)!(k-k-r-1)]](-1)^r 4^{k'-1}\).

Hence it suffices to show that \(\text{ord}_{\ell} \lambda\) lies in the critical range.

The condition \(k' > 2k\) guarantees that \((k'/2) + k - 1\) lies in the critical range.

**Proof.** Note that \(r = (k'/2) - k\) is odd, \(k' - k - 2r = k\) and \(2s + 2 - k - k' = k\). By (2) and (3),

\[
L((k'/2) + k - 1) = \zeta(k)c.\pi^{k'-1} (f, g\delta^{(r)}_{k} E_k).
\]

Hence it suffices to show that \(\text{ord}_{\lambda} \left(\frac{L((k'/2) + k - 1)}{\pi^{k'+k-1}(f,f)}\right) > 0\). Note that \((f, g\delta^{(r)}_{k} E_k) = (f, \text{Hol}(g\delta^{(r)}_{k} E_k))\), where the holomorphic projection operator is such that, term-by-term, the constant term disappears, and for \(m > 0\),

\[
\text{Hol} : y^{-1} q^m \mapsto \frac{(k' - 2 - j)!}{(k' - 2)!} (4\pi m)^{q^m}.
\]

(See [St] or pp. 288–290 of [GZ].) A lemma of Hida (Lemma 5.3 of [Hi]) says that \(\text{Hol}(g\delta^{(r)}_{k} g') = (-1)^r \text{Hol}(g' \delta^{(r)}_{k} g)\), for any \(g' \in \mathcal{M}_k\). Letting \(g' = g\), and recalling that \(r\) is odd, we find that \(\text{Hol}(g\delta^{(r)}_{k} g) = 0\). Letting \(h = g + \frac{B_k}{2k} E_k\), it then suffices to show that \(\text{ord}_{\lambda} \left(\frac{(f, g\delta^{(r)}_{k} h)}{(f,f)}\right) > 0\). The congruence (4) implies that \(\lambda\) divides all the Fourier coefficients of \(h\). Then the fact that \(\ell\) is too large to divide the denominator in (5) implies that \(\lambda\) also divides all the Fourier coefficients of \(h' := \text{Hol}(g\delta^{(r)}_{k} h)\). Let \(\{f_1, \ldots, f_d\}\) be a basis of eigenforms for \(S_k\), with \(f_1 = f\). If \(h' = \sum \alpha_i f_i\), then we need \(\lambda \mid \alpha_1\). But this follows easily from \(\lambda \mid h'\) and the fact that \(\lambda\) is not a congruence prime for \(f\).}

There is a “natural” way to choose \(\text{Gal} (\overline{\mathbb{Q}}/\mathbb{Q})\)-invariant \(\mathcal{O}_\lambda\)-lattices \(T'_\lambda\) in \(V'_\lambda\) and \(T_\lambda\) in \(V_\lambda\), as in 1.6 of [DFG]. Let \(W'_\lambda := V'_\lambda / T'_\lambda, W'[\lambda] = W'_\lambda[\lambda], \) etc. Let \(V''_\lambda := V'_\lambda \otimes V_\lambda\). Note that \(T'_\lambda(k'/2)\) is analogous to the \(\ell\)-adic Tate module of an elliptic curve.
One can show that, given Theorem 1.1, a special case of the general Bloch-Kato conjecture on special values of L-functions [BK, Fo] demands the existence of a non-zero element of the Selmer group \( H_1^f(Q, W'_\ell(k'/2) + k - 1) \). This is a subgroup of \( H_1^f \) defined by conditions on the local restrictions. (A Tate twist has been applied to the coefficient module, corresponding to the point at which the L-function is evaluated.) It is analogous to the Shafarevich-Tate group appearing in the rank-zero case of the Birch and Swinnerton-Dyer leading-term conjecture. We can support the Bloch-Kato conjecture by constructing such an element as follows.

Since \( k'/2 \) is odd and the sign in the functional equation of \( L_f(s) \) is \((-1)^{k'/2} \), \( L_f(k'/2) = 0 \). (Note that \( s = k'/2 \) is the centre of symmetry of the functional equation.) An analogue of the Birch and Swinnerton-Dyer conjecture predicts that the dimension of \( H_1^f(Q, V_f'((k'/2)/2)) \) equals the order of vanishing of \( L_f(s) \) at \( s = k'/2 \).

If we assume that \( \lambda \neq \alpha_{f^*} \) (i.e. that \( f \) is “ordinary” at \( \lambda \)), then, given the oddness of the order of vanishing, theorems of Skinner-Urban\([SU]\) or Nekovár\([N]\) (either will do) give us that \( H_1^f(Q, V_f'((k'/2)/2)) \neq 0 \). Scaling to land in \( H_1^f(Q, V_h'((k'/2)/2)) \), then reducing \((\bmod \lambda)\), yields a non-zero element of \( H^1(Q, W'_{\lambda}[k'/2]) \).

By (4) we have, for all primes \( p \), \( b_p \equiv 1 + p^{k-1} \pmod{\lambda} \). Using the fact that \( b_p = \text{Tr}(\rho_{p^{*}}(\text{Frob}_{p^{-1}})) \), this implies that the composition factors of \( W_{\lambda} \) (i.e. of \( \overline{\rho}_p \)) are \( F_{\lambda} \) and \( F_\lambda(1 - k) \). With our natural choices of lattices, it is possible to show that \( F_\lambda(1 - k) \) is a submodule (Theorem 7.3 of \([Du3]\)). Hence \( W_{\lambda}(k - 1) \) has a trivial submodule \( F_{\lambda} \), so \( W_{\lambda} \bigotimes W_{\lambda}(k - 1 + (k'/2)) \) has a submodule isomorphic to \( W'_{\lambda}(k'/2) \).

Hence our non-zero element of \( H^1(Q, W'_{\lambda}[k'/2]) \) produces elements of \( H^1(Q, W'_{\lambda}[((k'/2) + k - 1)]) \), then of \( H^1(Q, W'_{\lambda}[((k'/2) + k - 1)]) \). It is possible to show that this latter element is non-zero, and satisfies the Bloch-Kato local conditions.

### 2. Applications of related constructions

1. Essentially the same construction produces a non-zero element of \( \lambda \)-torsion in a Selmer group attached to \( L(\text{Sym}^2 g, (k/2) + k - 1) \), when \( (k/2) \) is odd, where \( \lambda \) is the modulus of (4). Then, working backwards, the Bloch-Kato conjecture predicts (in the case that \( \lambda \) is not a congruence prime for \( g \) in \( S_k \)) that \( \lambda \) divides \( L(\text{Sym}^2 g, (k/2) + k - 1) \). This divisibility may be observed experimentally \([Du1]\), but it appears to be an open problem to prove it in general, in contrast to the tensor-product case. For some experimental evidence in the Hilbert modular case, see also \([Du2]\).

2. The best understood critical value of \( L(\text{Sym}^2 g, s) \) is at \( s = k \), where one gets a simple multiple of \( (g, g) \) \((s = 2)\), see also (2.5) of \([Sh]\). Only in the case \( k = 2 \) is \( (k/2) + k - 1 = k \). The above construction may be applied in the case of \( g \in S_2(\Gamma_0(N)) \) attached to an elliptic curve \( E/Q \). We must have \( E(Q) \) of positive rank (to get the analogue of \( H_1^f(Q, V_h'((k'/2)/2)) \neq 0 \)), and also a rational point of order \( \ell \) (to get factors \( F_{\ell} \) and \( F_{\ell}(-1) \) for \( \overline{\rho}_\ell \simeq E[\ell](-1) \)). The ratio of \( (g, g) \) to the canonical Deligne period is essentially the degree of the modular parametrisation \( \Phi : X_0(N) \to E \). (Let’s suppose that \( E \) is chosen to be optimal in its isogeny class, i.e. \( \Phi \) has minimal degree.) This leads to predictions about the modular degree, which can be proved. Specifically, the following is Theorem 1.3 of \([Du3]\).
Theorem 2.1. Let $E/\mathbb{Q}$ be an optimal elliptic curve of conductor $N$. Suppose that $E$ has a rational point of prime order $\ell = 5$ or $7$. Suppose also that $E$ has a prime $p$ of split multiplicative reduction such that $p \not\equiv 1 \pmod{\ell}$. If $L(E, 1) = 0$ then $\ell | \deg(\phi)$.

This work has been refined and generalised to modular abelian varieties of higher dimension, by my student Ian Young.

(3) The construction used above depends on having a map from one Galois module to another, which can be used to carry an element from the cohomology of one to the cohomology of the other, providing a candidate for an element of a Selmer group. For example, in the above case, multiplication by the rational point of order $\ell$ gives a map from $E[\ell]$ to $\text{Sym}^2E[\ell]$. This is used to get from $\text{Sym}^2E[7]$ to $\text{Sym}^6E[7]$.

In [DIK] a different map is used, namely the cubing map from $E[2]$ to $\text{Sym}^3E[2]$, to try to explain Watkins’ conjecture that $2^k$ divides $\deg(\phi)$, where $R$ is the rank of $E(\mathbb{Q})$. 7.2(2) of [DW] is a numerical example in which multiplication by a rational point of order 7 is likewise used to get from $\text{Sym}^5E[7]$ to $\text{Sym}^6E[7]$.

In [Du4] a different map is used, namely the cubing map from $E[2]$ to $\text{Sym}^3E[2]$.

(4) In [CM], the two Galois modules are isomorphic: $E[\ell] \simeq E'[\ell]$, and the cohomology class coming from a rational point of infinite order on $E$ is used to produce an element of order $\ell$ in the Shafranovich-Tate group of $E'$, in examples where the Birch and Swinnerton-Dyer conjecture predicts the latter. In fact, the same congruence of modular forms resulting from $E[\ell] \simeq E'[\ell]$ also shows how vanishing of $L(E, 1)$ leads to divisibility by $\ell$ of $L_{\text{alg}}(E', 1)$, as explained in [DSW], which contains a generalisation to higher weight cusp forms.

(5) In [DIK], we have a cuspidal Hecke eigenform $f$ of weight $j + 2k - 2$, a cuspidal Hecke eigenform $F$ of genus 2 and type $\text{Sym}^1 \otimes \text{det}^k$ (vector valued when $j > 0$), and a congruence of Hecke eigenvalues (for all $p$) $\mu_f(p) \equiv \mu_F(f) + p^{k-2} + p^{j+k-1} \pmod{\lambda}$, where $\lambda$ is a large prime divisor of $L_{\text{alg}}(f, j + k)$ and $\mu_F(p)$ is the eigenvalue of a genus-2 Hecke operator $T(p)$ acting on $F$. In the case $j = 0$, $F$ is a non-lift congruent to the Saito-Kurokawa lift of $f$, while in the case $j > 0$ the congruence is predicted by Harder’s conjecture [Ha, vdG]. If $p_f$ is a $\ell$-adic representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to $F$, then the congruence implies that the composition factors of $p_F$ are $p_{\ell F}$, $F_{\ell}(2-k)$ and $F_{\ell}(1-j-k)$ to be a submodule, $F_{\ell}(1-j-k)$ to be a quotient, with $p_{\ell F}$ in the middle. Then $p_{\ell F}(2-k)$ is a submodule of $\Lambda^2 p_{\ell F}$. This can be used to move an element of order $\lambda$ in a Selmer group associated to $\lambda L_{\text{alg}}(f, j + k)$ [Br], to one in a Selmer group associated to a certain critical value of the standard $L$-function of $F$. Bloch-Kato then predicts the divisibility by $\lambda$ of a certain ratio of standard $L$-values for $F$. This divisibility may be proved in the case $j = 0$, and confirmed by computation in examples for which $j > 0$.

References


CRITICAL VALUES, CONGRUENCES AND MOVING BETWEEN SELMER GROUPS


University of Sheffield, Department of Pure Mathematics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.

E-mail address: n.p.dummigan@shef.ac.uk