ASIAN J. MATH.
Vol. 4, No. 2, pp. 437–498, June 2000

011

ON THE PARITY OF RANKS OF SELMER GROUPS*

JAN NEKOVÁŘ† AND ANDREW PLATER‡

0. Introduction. Let $f = \sum_{n\geq 1} a_n(f)q^n \in S_{k_0}(\Gamma_0(N))$ be a normalized newform of even weight $k_0 \geq 2$. Let F be the number field generated by the coefficients of f and $\mathfrak{p}$ a prime of F lying above a rational prime p. There is a two-dimensional representation $V(f)$ of $G_{\mathbb{Q}} = \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ over $F_{\mathfrak{p}}$ associated to f, characterized by the conditions

$$\mathrm{Tr}\left(\mathrm{Fr}(\ell)_{\mathrm{geom}}|V(f)\right) = a_\ell(f)$$
$$\det\left(\mathrm{Fr}(\ell)_{\mathrm{geom}}|V(f)\right) = \ell^{k_0-1}$$

for all primes $\ell \nmid pN$. The Tate twist $V_{k_0} = V(f)(k_0/2)$ is self dual: there is a skew-symmetric bilinear form

$$V_{k_0} \times V_{k_0} \longrightarrow F_{\mathfrak{p}}(1)$$

inducing an isomorphism $V_{k_0} \xrightarrow{\sim} V_{k_0}^*(1) = \mathrm{Hom}_{F_{\mathfrak{p}}}\left(V_{k_0}, F_{\mathfrak{p}}(1)\right)$.

The complex L-function $L_\infty(f,s) = \sum_{n\geq 1} a_n(f)n^{-s}$ satisfies the functional equation

$$\Lambda_\infty(f,s) := \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L_\infty(f,s) = w_\infty(f)\Lambda_\infty(f,k_0-s),$$

where $w_\infty(f) = \pm 1 = (-1)^{e_\infty}$ for $e_\infty = 0$ or 1. Bloch and Kato [Bl-Ka] defined a generalized "Selmer group" $H^1_f(\mathbb{Q}, V_{k_0}) \subseteq H^1(\mathbb{Q}, V_{k_0})$ and conjectured that

$$\mathrm{ord}_{s=k_0/2} L_\infty(f,s) \stackrel{?}{=} \dim_{F_{\mathfrak{p}}} H^1_f(\mathbb{Q}, V_{k_0}).$$

We are interested in a (mod 2) version of this conjecture:

The Parity Conjecture for ranks of Selmer groups

$$\mathrm{ord}_{s=k_0/2} L_\infty(f,s) \stackrel{?}{\equiv} \dim_{F_{\mathfrak{p}}} H^1_f(\mathbb{Q}, V_{k_0}) \pmod 2.$$

Assume that $p > 3$ and that f is ordinary at p, i.e. that $a_p(f) \in F_{\mathfrak{p}}$ is a $\mathfrak{p}$-adic unit. According to Hida's theory, there is a p-adic family of ordinary modular forms of varying weights containing f (we ignore the phenomenon of "p-stabilization" in this Introduction). In concrete terms, this means that there is an integer $c \geq 0$ such that for every integer $k \geq 2$ satisfying $k \equiv k_0 \pmod{(p-1)p^c}$, there is an ordinary newform f_k of weight k on $\Gamma_0(N)$ such that $f_{k_0} = f$ and

$$k \equiv k' \pmod{(p-1)p^{n+c}} \quad \text{implies} \quad f_k \equiv f_{k'} \pmod{p^n}.$$

Let

$$\varepsilon_k = \begin{cases} 1 & \textit{if } p \,\|\, N,\ k=2,\ a_p(f)=1, \\ 0 & \textit{otherwise.} \end{cases}$$

* Received December 11, 1998; accepted for publication April 19, 1999.
† Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK (nekovar@dpmms.cam.ac.uk).
‡ Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK (ajp@dpmms.cam.ac.uk).
The author was supported by an EPSRC grant.