CONGRUENCE PROPERTIES OF VALUES OF L-FUNCTIONS AND APPLICATIONS

J. H. Bruinier, K. James, W. Kohnen,
K. Ono, C. Skinner and V. Vatsal

Dedicated to the memory of S. Chowla

1. Introduction

Ever since Dirichlet's introduction of the analytic class number formula, special values of L-functions have been the subject of much study and speculation. In this paper we survey some recent results about such values that were presented at this conference. Our attention is essentially restricted to the central values of L-functions associated to certain (holomorphic) newforms. These results have many applications to class numbers of imaginary quadratic fields, Selmer groups of elliptic curves, and K-groups of real quadratic fields, a few of which are included.

To describe the problem we will address, we need to introduce some notation. Let $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}(M)$ ($q = e^{2\pi iz}$ as usual) be a newform of weight $2k$ on $\Gamma_0(M)$ with trivial Nebentypus character, and for $\mathrm{Re}(s) \gg 0$ let $L(F,s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ be

1991 *Mathematics Subject Classification.* Primary 11F67 ; Secondary 11F37.
Key words and phrases. modular forms, critical values of $L-$functions.
The fourth author is supported by NSF grant DMS-9508976 and NSA grant MSPR-97Y012 and the fifth author is supported by NSF grant DMS-9304580 and by an Ostrowski Fellowship.

its L-function. Let D denote a fundamental discriminant of a quadratic field that is coprime to M; then χ_D shall denote the Kronecker character for the field $\mathbb{Q}(\sqrt{D})$.

The D-quadratic twist of F, denoted F_D, is given by $F_D(z) = \sum_{n=1}^{\infty} \chi_D(n)a(n)q^n$, and for $\mathrm{Re}(s) \gg 0$ its L-function is given by $L(F_D, s) = \sum_{n=1}^{\infty} \chi_D(n)a(n)n^{-s}$. These L-functions have analytic continuations to $\mathbb{C}$ and satisfy well known functional equations. If $\Lambda(F, s) = (2\pi)^{-s}\Gamma(s)M^{s/2}L(F, s)$, then

$$\Lambda(F, s) = \epsilon \cdot \Lambda(F, 2k - s),$$

where $\epsilon = \pm 1$ is the so-called sign of the functional equation, and the quadratic twists satisfy

$$\Lambda(F_D, s) = \epsilon \cdot \chi_D(-M)\Lambda(F_D, 2k - s).$$

The value $L(F_D, k)$ is the *central value* of $L(F_D, s)$. Our motivating problem is to describe the behaviour of the family of values $L(F_D, k)$, as a function of D. Notice that if $\chi_D(-M)\epsilon = -1$, then $L(F_D, k) = 0$. Therefore at least 'half' of the $L(F_D, k)$ are trivially zero. As we shall see, the 'nontrivial zeros' (as one varies D) are quite mysterious. If F is a weight 2 newform associated to an elliptic curve E, then there are infinitely many non-trivial zeros, but in the case of Ramanujan's Delta-function $F = \Delta(z) \in S_{12}(1)$ there are no known non-trivial zeros.

For $X > 0$ let

$$N_F(X) = \#\{D \ \mid \mid D \mid < X \text{ and } L(F_D, k) \neq 0\}.$$

It is widely believed that

$$N_F(X) \gg_F X. \tag{1}$$

The following conjecture, due to Goldfeld, is more precise.

Goldfeld's Conjecture [G]. *If $F(z) \in S_{2k}(M)$ is a newform, then*

$$\sum_{|D|<X \text{ and } (D,M)=1} \text{ord}_{s=k} L(F_D, s)$$

$$\sim \frac{1}{2}\#\{D \mid |D| < X \text{ and } (D, M) = 1\}. \tag{2}$$

(Note: This conjecture was posed for weight 2 newforms associated to modular elliptic curves.)

Goldfeld's Conjecture is an analytic assertion, and it has been extensively studied as such, often with the help of sophisticated analytic techniques. Thanks to the work of Katz, Sarnak, Iwaniec, Kowalski, Michel, R. Murty and K. Murty, and others, much is known about the general phenomenon of the nonvanishing of values of L-functions and their derivatives. The results described in this paper follow from an essentially *algebraic* approach, based on the fact that the central value is a *critical* value (in the sense of Deligne). More concretely, this means that there exist nonzero complex numbers $\Omega_F^{\pm}$ known as *periods* for F, such that the quotient $L(F_D, k)/\Omega_F^{\text{sign}(D)}$ is an algebraic integer, loosely referred to as the *algebraic part* of $L(F_D, k)$. Non-vanishing of $L(F_D, k)$ is equivalent to non-vanishing of the algebraic part, and the latter may be studied by using algebraic techniques. The key to the results in this paper is the observation that, to show nonvanishing of the central value, it suffices to show that the algebraic part is nonzero modulo p, for some prime p.

2. Statement of Results

The first result we wish to describe gives a strong estimate for the number of quadratic twists of F whose L-functions do not vanish at $s = k$. This result was proven by two of the present authors (see [O-S1]) by using the theory of 2-adic Galois representations and a congruence modulo the prime 2.

Theorem 1. [O-S1, Cor. 3]. *If $F(z) \in S_{2k}(M)$ is a newform, then*

$$N_F(X) \gg_F \frac{X}{\log X}.$$

Recall that if $E/\mathbb{Q}$ is an elliptic curve given by

$$E: \quad y^2 = x^3 + Ax + B,$$

then E_D, its D-quadratic twist, is the curve given by

$$E_D: \quad y^2 = x^3 + AD^2x + BD^3.$$

Let $L(E_D, s)$ be the Hasse-Weil L-function for E_D. For modular E, Kolyvagin [Ko] proved that if $L(E_D, 1) \neq 0$, then E_D has rank zero. Theorem 1 together with Kolyvagin's theorem implies:

Corollary 1. *If $E/\mathbb{Q}$ is a modular elliptic curve, then the number of $|D| \leq X$ for which E_D has rank zero is $\gg_E X/\log X$.*

While Theorem 1 is very strong in that it applies to a general F, it falls short of the 'positive proportion' estimates predicted by Goldfeld. However, we will now describe a series of results showing that it is possible to do better in a class of special cases, namely the class of forms F for which there exist special congruence relations between $L(F_D, k)$ and class numbers of quadratic fields. When such relations exist modulo 3, results of Davenport and Heilbronn [D-H], suitably modified by Horie and Nakagawa [N-H], may be employed to prove the estimate (1). This approach was first carried out by James [Ja] for several weight 2 newforms associated to modular elliptic curves.

Using the same ideas, Kohnen [K] proved the following theorem for eigenforms with respect to the full modular group $SL_2(\mathbb{Z})$.

Theorem 2 [K, Cor. 1]. *Let $k \geq 6$ be even. If $\epsilon > 0$ and $X \gg_\epsilon 0$, then there exists a Hecke eigenform $F(z) \in S_{2k}(1)$ for which*

$$N_F(X) \geq \left(\frac{9-\epsilon}{16 g_k \pi^2}\right) X$$

where $g_k = \dim(S_{2k}(1))$.

Corollary 2. *Let $\Delta(z) \in S_{12}(1)$ be Ramanujan's Delta-function. If $\epsilon > 0$ and $X \gg_\epsilon 0$, then*

$$N_\Delta(X) \geq \left(\frac{9-\epsilon}{16\pi^2}\right) X.$$

This technique can also be exploited in the context of certain elliptic curves with rational torsion points. But before stating the general theorem, we need to introduce some notation. Let E be a modular elliptic curve over $\mathbb{Q}$. Assume that E has a rational point of odd prime order p (so $p = 3$, 5, or 7), that the level M of E is squarefree, and that E has good reduction at p. Let q be any prime with $(q, M) = 1$ and $q \equiv 1 \pmod 9$ if $p = 3$ and $q \equiv 1 \pmod p$ if $p = 5$ or 7. Let M_1 denote the product of primes $\ell | M$ such that E has nonsplit multiplicative reduction, and let $M_2 = qM/M_1$.

Theorem 3 [V, Th. 0.3]. *Let the elliptic curve E be as above. Then there exists a period Ω^- for E such that we have*

$$\begin{aligned}(1 - \chi_D(q)/q) \cdot \tau(\chi_D) &\frac{L(E_D, 1)}{(-2\pi i)\Omega^-} \\ &\equiv \frac{1}{2} \prod_{\ell | M_1} (1 - \chi_D(\ell)/\ell) \prod_{\ell | M_2} (1 - \chi_D(\ell)) \cdot L(\chi_D, 0)^2 \pmod p,\end{aligned}$$

for any $D < 0$ prime to Mq. Here $\tau(\chi_D)$ denotes the usual Gauss sum associated to χ_D.

Observe now that $L(\chi_D, 0)$ is essentially the class number $h(D)$ of $\mathbb{Q}(\sqrt{D})$. Thus if D is such that $h(D)$ and the various Euler factors are nonzero modulo p, then we may conclude that the value $L(E_D, 1)$ is nonzero. The aforementioned results of Davenport-Heilbronn and Horie-Nakagawa then yield the following result:

Corollary 3. *If E is as in Theorem 3 and $p = 3$, then*

$$\#\{-X < D < 0 \mid L(E_D, 1) \neq 0)\} \gg_E X.$$

Theorem 3 was already predicted by the work of Frey [F], who shows that the order of p-Selmer groups of certain curves E_D are trivial whenever $h(D)$ is prime to p. Thus our theorem may be viewed as an analytic counterpart to Frey's theorem, hence as verification of a weak form of the Birch and Swinnerton-Dyer Conjecture 'mod p' for rank zero quadratic twists E_D.

Work of Waldspurger [W1, W2] shows that the values $L(F_D, k)$ are essentially Fourier coefficients of modular forms of half-integral weight $k + \frac{1}{2}$. Theorems 1 and 2 are proved by studying the Fourier coefficients of such half-integral weight modular forms modulo p. There have been a number of investigations into the indivisibility of such coefficients in the works of Jochnowitz [J], Ono and Skinner [O-S2], and most recently Bruinier [B]. Our final theorem is a statement of the main result in [B]. First let us introduce some notation. Let k be an integer as before, M a positive integer divisible by 4 and χ a Dirichlet character modulo M. For convenience put $\chi^* = (\frac{-1}{\cdot})^k \chi$. If p is a prime, then let v_p denote a continuation of the usual p-adic valuation on $\mathbb{Q}$ to a fixed algebraic closure. Write $M_{k+1/2}(M, \chi)$ for the space of modular forms of weight $k + 1/2$ with respect to $\Gamma_0(M)$ and Nebentypus character χ (in the sense of [Sh]).

Theorem 4 [B, Th. 2]. *Let $f(z) = \sum_{n=0}^{\infty} a(n) q^n \in M_{k+\frac{1}{2}}(M, \chi)$ be an eigenform of all the Hecke operators $T(\ell^2)$ with corresponding eigenvalues λ_ℓ. If the coefficients $a(n)$ are algebraic integers, $p \nmid M$ is prime, and there is a positive integer m^* with $v_p(a(m^*)) = 0$, then define $w(f; p, m^*)$ by*

$$w(f; p, m^*) := \min_{\ell} v_p \left(\lambda_\ell - \left(\frac{m^*}{\ell} \right) \chi^*(\ell)(\ell^k + \ell^{k-1}) \right),$$

Here the minimum is taken over all primes ℓ with $(\ell, Npm^*) = 1$ and $\ell \not\equiv 1 \pmod{p}$. Then there exist infinitely many square-free integers d with $v_p(a(d)) \leq w(f; p, m^*)$.

There are many immediate consequences of results like Theorem 4. Here we list a few exceptional examples. The deduction of these corollaries employs the aforementioned results of Waldspurger, which

relate the algebraic parts of the values $L(F_D, k)$ to the Fourier coefficients at square-free integers of certain half-integral weight modular forms.

Corollary 4. *If $E/\mathbb{Q}$ has complex multiplication, then for every prime $p \gg_E 0$ there are infinitely many D for which*

$$rk(E_D) = 0 \quad \text{and} \quad p \nmid \#Ш(E_D).$$

Corollary 5. *Let $E/\mathbb{Q}$ be a modular elliptic curve for which $L(E, s)$ has a simple zero at $s = 1$. For all primes p outside a finite set which is effectively determinable* (see [O-S2])

$$ord_p(|Ш(E)|) \leq ord_p(\text{Sha}(E)),$$

where $\text{Sha}(E)$ *denotes the order of* $Ш(E)$ *as predicted by the Birch and Swinnerton-Dyer Conjecture.*

We also obtain a generalization of results due to Horie on the existence of certain infinite families of imaginary quadratic fields [Ho].

Corollary 6 [B, Theorem 7]. *Let $p_1, \ldots, p_r$ be distinct odd primes and $\varepsilon_1, \ldots, \varepsilon_r \in \{-1, 0, +1\}$. Let p be a prime ≥ 5 such that p does not divide $p_j(p_j - 1)(p_j + 1)$ for $j = 1, \ldots, r$. Then there are infinitely many fundamental discriminants $D < 0$ for which $h(D)$ is not divisible by p and $(\frac{D}{p_j}) = \varepsilon_j$ for $j = 1, \ldots, r$.*

Applying Theorem 4 to the Cohen-Eisenstein series, we obtain indivisibility results for certain values of Dirichlet L-series.

Corollary 7 [B, Theorem 6]. *Let k be a positive even integer and p a prime for which $p - 1 \nmid 2k$ and $v_p(\zeta(1 - k)) = 0$. Then there exist infinitely many fundamental discriminants $D > 0$ with $v_p(L(1 - k, \chi_D)) = 0$.*

Using the work of Mazur and Wiles [M-W] one immediately obtains the following from Corollary 7.

Corollary 8 [B, Cor. 2]. *Let p be a prime ≥ 7. Then there exist infinitely many real quadratic fields F such that the K-group K_2A_F of the ring of integers A_F of F contains no element of order p.*

In the remainder of this paper, we will briefly describe the proofs of the theorems stated above.

3. Discussion of Theorem 1

The proof of Theorem 1 (see [O-S1] for details) is based on the simple observation that if $\theta(z) = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$ is the standard theta function, then $1 \equiv \theta(Nz) \pmod 2$ for any positive integer N. This is exploited as follows. The main results of [W1, W2] ensure the existence of a weight $k + \frac{1}{2}$ cusp form $f(z) = \sum_{n=1}^{\infty} c(n)q^n$ of some level $4M'$ and $\delta_F \in \{\pm\}$ such that if $(D, 4MM') = 1$ and if $\delta_F D > 0$, then $c(|D|)^2$ is essentially the algebraic part of $L(F_D, k)$. More precisely, let $P(F)$ denote the set of D's just described. Then for all $D \in P(F)$

$$c(|D|) \neq 0 \Rightarrow L(F_D, k) \neq 0.$$

The form $G(z) = f(z) \cdot \theta(Nz) = \sum_{n=1}^{\infty} b(n)q^n$ has integral weight $k+1$ and satisfies $b(n) \equiv c(n) \pmod 2$. Thus to show that $L(F_D, k) \neq 0$ for some $D \in P(F)$, it sufficies to show that $b(|D|) \not\equiv 0 \pmod 2$. For simplicity, suppose that $c(n) \in \mathbb{Z}$ for all n and that $G(z)$ is a newform. Suppose also that $2 \nmid c(|D_0|)$ for some $D_0 \in P(F)$. Write $D_0 = p_1 \cdots p_r$. Applying the Chebotarev Density Theorem to the mod 2 Galois representation associated to G, one finds that there are $\gg X/\log X$ sets of primes $\{q_1, ..., q_r\}$ such that $b(q_i) \equiv b(p_i) \pmod 2$, $q_1 \cdots q_r < X$, $\delta_F q_1 \cdots q_r \in P(F)$. As

$$\begin{aligned} b(q_1 \cdots q_r) &\equiv b(q_1) \cdots b(q_r) \\ &\equiv b(p_1) \cdots b(p_r) \equiv b(|D_0|) \pmod 2, \end{aligned}$$

the desired result follows. The proof in the general case is similar, but made more complicated by having to work in a general number field and by the fact that G is not usually a newform.

4. Discussion of Theorem 2

In this section we briefly sketch the proof of Theorem 2 (see [K] for details). Essentially, one uses a sufficiently explicit form of the Shimura correspondence and Waldspurger's theorem, due to Kohnen-Zagier, to find explicit relations between the twisted L-values and clas numbers of quadratic fields. One concludes the proof by using the Davenport-Heilbronn theorem, as mentioned previously.

Sketch of Proof of Theorem 2: Let k be even and $S^+_{k+1/2}$ be the space of cusp forms of weight $k+1/2$ w.r.t. $\Gamma_0(4)$ having a Fourier expansion of the form $\sum_{n\geq 1} c(n)q^n$ with $c(n) = 0$ unless $n \equiv 0, 1 \pmod 4$. The spaces $S^+_{k+1/2}$ and $S_{2k} = S_{2k}(1)$ are isomorphic as modules over the Hecke algebra. If $f(z) = \sum_{n\geq 1} a(n)q^n$ is a normalized Hecke eigenform in S_{2k} and $g = \sum_{n\geq 1} c(n)q^n$ is a Hecke eigenform in $S^+_{k+1/2}$ corresponding to it, then for every fundamental discriminant $D > 0$ one has

$$\frac{|\, c(D)\,|^2}{\langle g, g\rangle} = \frac{(k-1)!}{\pi^k} D^{k-1/2} \frac{L(f, D, k)}{\langle f, f\rangle},$$

where $\langle g, g\rangle$ and $\langle f, f\rangle$ are appropriately normalized Petersson scalar products (cf. [K-Z]; the above identity is a more precise version of Waldspurger's formula [W1] in the special case of the full modular group). For $k \geq 4$ let

$$G_k(z) = \frac{1}{2}\zeta(1-k) + \sum_{n\geq 1} \sigma_{k-1}(n)q^n$$

($\sigma_\nu(n) := \sum_{d|n} d^\nu$) be the Eisenstein series of weight k and level 1, and let $\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2}$ be the standard theta series of weight $1/2$.

We put

$$\delta_k(z) := \frac{1}{4\pi i}\big((\frac{k}{2} - 1)G_{k-2}(4z)\theta'(z) - G'_{k-2}(4z)\theta(z)\big)$$

and write $\alpha_k(n)$ for the Fourier coefficients of δ_k (cf. [K-Z], p. 187). One has $\delta_k \in S^+_{k+1/2}$; in fact, up to normalization δ_k is the first Rankin-Cohen bracket of $G_{k-2}(4z)$ and $\theta(z)$.

For simplicity let's suppose that k is not congruent to 1 modulo 3. It is easy to see that it is sufficient to prove that

$$\#\{0 < D < X, D \equiv -1 \pmod 3, \alpha_k(D) \neq 0\} \geq \left(\frac{9-\epsilon}{16\pi^2}\right) X.$$

To do this one first shows the congruence

$$\alpha_k(D) \equiv u_k h(-3D) \pmod 3 \qquad (D \equiv -1 \pmod 3)$$

where $u_k = -1$ resp 1 for $k \equiv 0 \pmod 3$ resp. $k \equiv 2 \pmod 3$.

Except for some elementary calculations modulo 3, the above congruence follows from an identity of Siegel which relates a certain finite sum involving σ_1 to the second generalized Bernoulli number of χ_D, and a classical formula of Lerch relating this Bernoulli number to the class number $h(-3D)$ modulo 3.

The proof then is finished using the results of [D-H] and [N-H], in a similar way as in [Ja]. Let m and N be positive integers, N odd and such that if p is an odd prime dividing (m, N), then $p^2 \mid N$ and p^2 does not divide m. Denote by $N_2^-(X, m, N)\,(X > 0)$ the number of fundamental discriminants D with $-X < D < 0$ and $D \equiv m \pmod N$.

The main result of [D-H, N-H] implies that

$$\sum_{-x<D<0, D\equiv m \pmod N, (h(D),3)=1} 1 \geq (\frac{1}{2} - \epsilon) N_2^-(X, m, N) \quad (X \gg_\epsilon 0).$$

Applying the latter formula with $m = 3$ and $N = 9$ and observing that $N_2^-(3X, 3, 9) \sim \frac{9}{8\pi^2} X$ for $X \to \infty$ (cf. e.g. [N-H], Prop. 2), the assertion of Theorem 2 easily follows.

Q.E.D.

5. Discussion of Theorem 3.

We now sketch the proof of Theorem 3 (see [V] for details). The idea of the proof is simple: we will show that there exists a congruence modulo p between E and a suitable Eisenstein series G, and then relate the L-values of E to those of G. The latter are products of Dirichlet L-functions, and the special values are Bernoulli numbers whose relationship to class numbers is well-documented.

Proof of Theorem 3: Let ρ_0 denote the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-division points $E[p]$ of E. Our hypotheses imply that there is an exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0.$$

Let $f(z) = \sum a_n(f)q^n$ be the newform associated to E; then the exact sequence above implies that $a_q(f) \equiv q+1 \pmod{p}$, for each prime q not dividing pM. Now let G be the non-holomorphic Eisenstein series of weight 2 and level 1. Thus we have

$$G(z) - \frac{1}{8\pi y} = \frac{-1}{24} + \sum \sigma(n)q^n,$$

where $\sigma(n) = \sum_{d|n} d$. Therefore $\sigma(n) \equiv a_n(f) \pmod{p}$ for all n with $(n, pM) = 1$. Observe also that we have the equality

$$\tau(\chi_D)\frac{L(1, G_D)}{(-2\pi i)} = \frac{1}{2}L(\chi_D, 0)^2.$$

Now theorem (3.3) of [V] shows how to modify f and G to obtain forms $f^* = \sum a_n(f)^* q^n$ and $G^* = \sum a_n(g)^* q^n$ of level Mq such that the congruence $a_n(f)^* \equiv a_n(g)^* \pmod{p}$ is valid at *all* integers n. Furthermore the Eisenstein series G^* has the property that the constant term in the Fourier expansion at every cusp is a rational integer divisible by p.

Put $\Gamma = \Gamma_1(Mq)$ and let $\delta \in H^1(\Gamma, \mathbb{Z})$ be the cocycle obtained by integrating G^*. Then δ vanishes modulo p on parabolic elements

and we obtain a parabolic cocycle $\overline{\delta} \in H^1(\Gamma, \mathbb{Z}/p)$. Furthermore, it may be shown that δ lies in the minus eigenspace $H^1(\Gamma, \mathbb{Z})^-$ for the action of complex conjugation.

Let $\mathbb{T}$ be the Hecke ring generated over $\mathbb{Z}_p$ in the space of cusp-forms for $\Gamma = \Gamma_1(Mq)$. Let m be the the maximal ideal determined by f^*. It can be shown that there is an isomorphism $\theta : S_2(\Gamma, \mathbb{Z}_p)_m \cong H^1(\Gamma, \mathbb{Z}_p)^-_m$ (see Theorem 2.7 in [V]). Thus we may define a canonical cocycle $\delta^* = \theta(f^*) \in H^1(\Gamma, \mathbb{Z}_p)^-$. One checks that there is a period Ω^- such that $\Omega^- \delta^* = (\omega)^-$, where ω is the differential form on $X_1(Nq)$ associated to f^*. It is a consequence of a theorem of Washington that the image of δ^* in $H^1(\Gamma, \mathbb{Z}/p)$ coincides up to unit with the Eisenstein cocycle $\overline{\delta}$ defined previously. Our Theorem 3 now follows upon computing the twisted L-values of δ^* and $\overline{\delta}$, using the definition for the former, and the theory of Dedekind sums for the latter (see [St], Lemma 2.2).

Q.E.D.

Applying Theorem 3 along with the techniques developed in [Ja] to all elliptic curves having a torsion point of order 3 and whose conductor is less than or equal to 50, we have compiled the following table. For each curve E, we list a Weierstrass equation for E, the conductor N_E of E, and a lower bound δ_E for

$$\liminf_{x \to \infty} \left[\frac{\#\{D \ \mid \mid D \mid < X \text{ and } L(E_D, 1) \neq 0\}}{2X} \right].$$

E	N_E	δ_E
$y^2 = x^3 + x^2 + 72x - 368$	14	$21/64\pi^2$
$y^2 = x^3 + 4x^2 - 144x - 944$	19	$19/80\pi^2$
$y^2 = x^3 + x^2 + 4x + 4$	20	$15/72\pi^2$
$y^2 = x^3 + x^2 - 72x - 496$	26	$39/112\pi^2$
$y^2 = x^3 - 432$	27	$3/8\pi^2$
$y^2 = x^3 + x^2 + 24x + 144$	30	$15/128\pi^2$
$y^2 = x^3 + x^2 - 48x + 64$	34	$17/48\pi^2$
$y^2 = x^3 + 4x^2 + 144x + 80$	35	$35/192\pi^2$
$y^2 = x^3 + 1$	36	$3/4\pi^2$
$y^2 = x^3 + 4x^2 - 368x - 3184$	37	$37/114\pi^2$
$y^2 = x^3 + x^2 + 152x + 5776$	38	$19/160\pi^2$
$y^2 = x^3 + x^2 + 3x - 1$	44	$11/48\pi^2$
$y^2 = x^3 + 5x^2 - 200x - 14000$	50	$5/8\pi^2$

5. Discussion of Theorem 4

Here we describe the main ideas of the proof of Theorem 4 (see [B] for details). A related result and some more applications to elliptic curves are obtained in [O-S2] via the theory of p-adic Galois representations.

Here f denotes an element of $M_{k+1/2}(M, \chi)$ with algebraic integer Fourier coefficients $a(n)$. Define $v_p(f) = \inf_n(v_p(a(n))$ and denote the usual Fricke involution by W_M. Using the q-expansion principle one may deduce that $f \,|\, W_M$ also has algebraic Fourier coefficients and moreover that $v_p(f) = v_p(f \,|\, W_M)$ for every prime p not dividing M ([B], Lemma 1).

Now let ℓ be a prime not dividing M and suppose that f is an eigenform of the Hecke operator $T(\ell^2)$. Then taking into account the lemma above and the properties of various operators defined on modular forms (in particular the commutation relation of a quadratic twist and W_M), it can be shown that a certain set of congruences modulo p for the Fourier coefficients implies a congruence for the Hecke eigenvalue λ_ℓ. Since this result might be of independent interest, let us state part of it in a more precise form.

Theorem 4′ [B, Theorem 1]. *Let ℓ be a prime not dividing M, $\varepsilon \in \{\pm 1\}$, and $\nu > 0$. Further let p be a prime with $(p, N\ell(\ell-1)) = 1$ and $v_p(f) = 0$. Suppose that f is an eigenform of $T(\ell^2)$ with corresponding eigenvalue λ_ℓ. If $v_p(a(n)) \geq \nu$ for all n with $(\frac{n}{\ell}) = -\varepsilon$, then the congruence $v_p\left(\lambda_\ell - \varepsilon\chi^*(\ell)(\ell^k + \ell^{k-1})\right) \geq \nu$ holds.*

As a *corollary* to Theorem 4' one infers that there always is an integer m_ε with $(\frac{m_\varepsilon}{\ell}) = -\varepsilon$ and $v_p(a(m_\varepsilon)) \leq v_p\left(\lambda_\ell - \varepsilon\chi^*(\ell)(\ell^k + \ell^{k-1})\right)$.

Proof of Theorem 4: We may choose a prime ℓ with $(\ell, Mpm^*) = 1$, $\ell \not\equiv 1 \pmod{p}$ and

$$v_p\left(\lambda_\ell - \left(\frac{m^*}{\ell}\right)\chi^*(\ell)(\ell^k + \ell^{k-1})\right) = w(f; p, m^*).$$

Then according to the above corollary there is an m with $(\frac{m}{\ell}) = -(\frac{m^*}{\ell})$ and $v_p(a(m)) \leq w(f; p, m^*)$. In fact, by an inductive argument ([B], Lemma 3) it can be seen that there are infinitely many such m with mutually distinct square-free part. Now, using the multiplicative properties of the Fourier coefficients the assertion can be deduced.

Q.E.D.

References

[B] J. H. Bruinier, *Non-vanishing modulo p of Fourier coefficients of half-integral weight modular forms*, (preprint).

[D–H] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields.II*, Proc. Roy. Soc. London **ser. A 322** (1971), 405-420.

[F–H] S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automophic L-functions on GL*(2), Ann. Math. **142** (1995), 385-423.

[F] G. Frey, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Can. J. Math. **XL** (1988), 649-665.

[G] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory, Carbondale, Springer Lect. Notes **751** (1979), 108-118.

[Ho] K. Horie, *Trace formulae and imaginary quadratic fields*, Math. Ann. **288** (1990), 605-612.

[Ja] K. James, *L-series with non-zero central critical value*, J. Amer. Math. Soc. **11** (1998), 635-641.

[J] N. Jochnowitz, *Congruences between modular forms of half-integral weights and implications for class numbers and elliptic curves*, (preprint).

[K] W. Kohnen, *On the proportion of quadratic character twists of L-functions attached to cusp forms not vanishing at the central point*, J. reine angew. math. (to appear).

[K–Z] W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), 173-198.

[M–W] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), 179-330.

[N–H] J. Nakagawa and K. Horie, *Elliptic curves with no rational points*, Proc. AMS **104, no.1** (1988), 20-24.

[O–S1] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular L-functions*, Invent. Math., (to appear).

[O–S2] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo* ℓ, Annals of Math. **147** (1998), 451-468.

[Sh] G. Shimura, *On modular forms of half integral weight*, Annals of Math. **97**, 440-481.

[St] G. Stevens, *The cuspidal group and special values of L-functions*, Trans. A.M.S. **291**, 519-550.

[V] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. (to appear).

[V2] V. Vatsal, *Rank-one twists of a cetain elliptic curve*, Math. Annalen (to appear).

[W1] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.

[W2] J.-L. Waldspurger, *Correspondances de Shimura et quaternions*, Forum Math. **3** (1991), 219-307.

Mathematisches Institut, Universität Heidelberg, INF 288, D-69120 Heidelberg, Germany

E-mail address: bruinier@mathi.uni-heidelberg.de

Department of Mathematics, The Pennsylvania State University, University Park, Pa. 16802

E-mail address: klj@math.psu.edu

Mathematisches Institut, Universität Heidelberg, INF 288, D-69120 Heidelberg, Germany

E-mail address: winfried@mathi.uni-heidelberg.de

Department of Mathematics, The Pennsylvania State University, University Park, Pa. 16802

E-mail address: ono@math.psu.edu

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540
E-mail address: cskinner@math.ias.edu

Department of Mathematics, University of Toronto, Toronto, Canada M5S 1A1
E-mail address: vatsal@math.toronto.edu