CONGRUENCES FOR FOURIER COEFFICIENTS OF HALF-INTEGRAL WEIGHT MODULAR FORMS AND SPECIAL VALUES OF $L-$FUNCTIONS

Antal Balog, Henri Darmon and Ken Ono

Proceedings for a conference in honor of Heini Halberstam, 1, 1996, pages 105-128.

Abstract. Congruences for Fourier coefficients of integer weight modular forms have been the focal point of a number of investigations. In this note we shall exhibit congruences for Fourier coefficients of a slightly different type. Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ be a holomorphic half integer weight modular form with integer coefficients. If ℓ is prime, then we shall be interested in congruences of the form

$$a(\ell N) \equiv 0 \mod \ell$$

where N is any quadratic residue (resp. non-residue) modulo ℓ. For every prime $\ell > 3$ we exhibit a natural holomorphic weight $\frac{\ell}{2}+1$ modular form whose coefficients satisfy the congruence $a(\ell N) \equiv 0 \mod \ell$ for every N satisfying $\left(\frac{-N}{\ell}\right) = 1$. This is proved by using the fact that the Fourier coefficients of these forms are *essentially* the special values of real Dirichlet $L-$series evaluated at $s = \frac{1-\ell}{2}$ which are expressed as generalized Bernoulli numbers whose numerators we show are multiples of ℓ. From the works of Carlitz and Leopoldt, one can deduce that the Fourier coefficients of these forms are almost always a multiple of the denominator of suitable Bernoulli numbers. Using these examples as a template, we establish sufficient conditions for which the Fourier coefficients of a half integer weight modular form are almost always divisible by a given positive integer M.

We also present two more examples of half-integer weight forms with such congruence properties, whose coefficients are determined by the special values at the center of the critical strip for the quadratic twists of the modular L-functions associated to the modular form Δ of weight 12 and level 1, and to the unique form $\eta^8(z)\eta^8(2z)$ of weight 8 and level 2. We suggest a conceptual explanation for these congruences by remarking that the twists of the mod p Galois representations ($p = 11$ and 7 respectively) associated to these two forms are isomorphic to the Galois representations associated to certain elliptic curves of odd analytic rank.

Key words and phrases. congruences, modular forms, special values of $L-$functions.

The second author wishes to acknowledge CICMA for providing a stimulating intellectual environment while this paper was written. His research was supported by a grant from NSERC and by a nouveaux chercheurs grant from FCAR. The third author is supported by grants DMS-9304580 and DMS-9508976.

1. Congruences for Fourier coefficients

First we shall fix the following notation. If $D \equiv 0, 1 \mod 4$ is the fundamental discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$, then let χ_D denote the Kronecker character with conductor $|D|$. In particular, if p is a prime that splits (resp. is inert) in $\mathbb{Q}(\sqrt{D})$, then $\chi_D(p) = 1$ (resp. $\chi_D(p) = -1$). It turns out that χ_D, in terms of Jacobi symbols, is given by:

$$(0) \qquad \chi_D(n) := \begin{cases} \left(\frac{n}{|D|}\right) & \text{if } D \equiv 1 \mod 4 \\ \left(\frac{-1}{n}\right)\left(\frac{n}{|D|}\right) & \text{if } D = 4D_1,\ D_1 \equiv 3 \mod 4 \\ \left(\frac{2}{n}\right)\chi_{D_1}(n) & \text{if } D = 2D_1,\ D_1 \equiv 1 \mod 4 \\ \left(\frac{2}{n}\right)\chi_{4D_1}(n) & \text{if } D = 2D_1,\ D_1 \equiv 3 \mod 4. \end{cases}$$

Here $\left(\dfrac{-1}{n}\right) := (-1)^{\frac{n-1}{2}}$ if n is odd and is zero otherwise, and $\left(\dfrac{2}{n}\right) := (-1)^{\frac{n^2-1}{8}}$ if n is odd and is zero otherwise. By χ_0 we shall mean the identity character.

If χ is a Dirichlet character modulo N and k is a positive integer or $k \in \mathbb{Z}_{\geq 0} + \frac{1}{2}$, then let $M_k(N, \chi)$ (resp. $S_k(N, \chi)$) denote the finite dimensional complex vector space of holomorphic modular forms (resp. cusp forms) with respect to $\Gamma_0(N)$. Similarly let $M_k(N)$ (resp. $S_k(N)$) denote the space of holomorphic modular forms (resp. cusp forms) with respect to $\Gamma_1(N)$. If $f(z)$ is such a modular form, then it has a Fourier expansion in $q := e^{2\pi i z}$ of the form

$$f(z) = \sum_{n=0}^{\infty} a(n) q^n.$$

For more on the theory of modular forms see [12,13,23].

The congruence properties of Fourier coefficients have been investigated by a number of authors (see [21,22,25,26]). For example, if $\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n$ is the unique normalized cusp form of weight 12 with respect to $SL_2(\mathbb{Z})$, then it is well known that

$$\tau(n) \equiv \sigma_{11}(n) \mod 691$$

and

$$(1) \qquad \tau(n) \equiv 0 \mod 23 \text{ if } \left(\frac{n}{23}\right) = -1$$

where $\sigma_{11}(n) := \sum_{0<d|n} d^{11}$. These congruences are explained by the theory of modular ℓ−adic Galois representations as developed by Deligne, Serre, and Swinnerton Dyer.

Still there are other examples of congruences for Fourier coefficients which have been the focus of some attention. For example, if $p(n)$ denotes the number of partitions of n, then it is well known that

$$p(5n+4) \equiv 0 \mod 5,$$

$$(2) \qquad p(7n+5) \equiv 0 \mod 7,$$

and

$$p(11n+6) \equiv 0 \mod 11$$

for every non-negative integer n. These congruences may be viewed as consequences of the action of certain Hecke operators. Here we illustrate this fact for (2). To see this we construct a holomorphic integer weight modular form whose coefficients inherit these congruence properties. Recall that Euler's generating function for $p(n)$ is given by the infinite product

$$\prod_{n=1}^{\infty} \frac{1}{1-q^n}.$$

Also recall that $\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n)$, the Dedekind eta-function, is a weight $\frac{1}{2}$ cusp form. If we define $F_7(z)$ and $a(n)$ by

$$F_7(z) = \frac{\eta^7(7z)}{\eta(z)} = q^2 \prod_{n=1}^{\infty} \frac{(1-q^{7n})^7}{(1-q^n)} = \sum_{n=2}^{\infty} a(n)q^n,$$

then (2) holds if and only if

$$a(7n) \equiv 0 \mod 7$$

for every positive integer n. However $F_7(z)$ is a holomorphic modular form in $M_3(7, \chi_{-7})$ and may be rewritten as

$$F_7(z) = \frac{1}{8}E_3(z) - \frac{1}{8}\eta^3(z)\eta^3(7z)$$

where $E_3(z) = \sum_{n=1}^{\infty} \sigma_{3,\chi_{-7}}(n)q^n$ and $\sigma_{3,\chi_{-7}}(n) = \sum_{0<d|n} \chi_{-7}(d)\frac{n^2}{d^2}$.

It is easy to verify that

$$F_7(z) \mid T_7 = \sum_{n=1}^{\infty} a(7n)q^n = \frac{49}{8}E_3(z) + \frac{7}{8}\eta^3(z)\eta^3(7z);$$

this implies that $a(7n) \equiv 0 \mod 7$ for all n which implies (2).

However there are other congruences that the partition function satisfies. For example it is known that

$$p(49n+19) \equiv p(49n+33) \equiv p(49n+40) \equiv 0 \mod 49$$

for every non-negative integer n (see [17]). In a more convenient form, $p(49n + 7\delta - 2) \equiv 0 \mod 49$ for all n if δ is a quadratic non-residue modulo 7. Following an argument similar to the one above, this means that the Fourier coefficients of the holomorphic integer weight modular form

$$\frac{\eta^{49}(49z)}{\eta(z)} = q^{100} \prod_{n=1}^{\infty} \frac{(1-q^{49n})^{49}}{1-q^n} = \sum_{n=0}^{\infty} a(n)q^n$$

satisfies the congruence

$$a(49n+7\delta) \equiv 0 \mod 49$$

for all n where δ is a quadratic non-residue modulo 7.

We shall be interested in the arithmetic implications of other congruences of this type.

Definition 1. *Let $F(n)$ be an integer valued arithmetic function, M a positive integer, and ℓ a prime. If*

$$F(\ell N) \equiv 0 \mod M$$

for every positive integer N that is a quadratic residue (resp. non-residue) modulo ℓ, then we say that F has a quadratic congruence modulo M of type $(\ell, +1)$ (resp. $(\ell, -1)$).

Therefore if $F(n) = p(n-2)$, then F has a quadratic congruence modulo 49 of type $(7, -1)$. Moreover by (1) we see that the Fourier coefficients of $\Delta(23z)$ satisfy the quadratic congruence modulo 23 of type $(23, -1)$.

In the following proposition we will give an explicit criterion for determining the truth of certain congruences of this type that will be used in the sequel.

Proposition 2. *Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(N, \chi_0)$ be a holomorphic integer weight modular form with rational integer coefficients. If ℓ is a prime dividing N, then the coefficients possess a quadratic congruence of type $(\ell, +1)$ (resp. $(\ell, -1)$) if and only if*

$$a(\ell n) \equiv 0 \mod \ell$$

for every positive integer $n \leq C$ satisfying $\left(\frac{n}{\ell}\right) = 1$ (resp. $\left(\frac{n}{\ell}\right) = -1$) where

$$C := \frac{kN\ell^3}{12} \prod_{p \mid N} \left(1 + \frac{1}{p}\right). \tag{3}$$

Proof of Proposition 2. If $f(z) = \sum_{n=0}^{\infty} a(n)q^n$, and $g(z) = \sum_{n=0}^{\infty} b(n)q^n \in M_k(N, \chi_0)$ have algebraic integer Fourier coefficients, then by a theorem of Sturm [25], $f(z) \equiv g(z) \mod M$ if $a(n) \equiv b(n)$ for every $n \leq \frac{kN}{12} \prod_{p \mid N}(1 + \frac{1}{p})$.

Define $f_1(z)$ and $f_2(z)$ by

$$f_1(z) := f(z)|T_\ell \equiv \sum_{n=0}^{\infty} a(\ell n)q^n \mod \ell$$

and

$$f_2(z) := f(z)|T_{\ell^2} \equiv \sum_{n=0}^{\infty} a(\ell^2 n)q^n \mod \ell.$$

Since the Hecke operators preserve spaces of modular forms, we find that $f_1(z), f_2(z) \in M_k(N, \chi_0)$. If $f_3(z) = f_2(\ell z) \in M_k(N\ell, \chi_0)$, then $f_4(z) := f_1(z) - f_3(z) \in M_k(N\ell, \chi_0)$ and

$$f_4(z) \equiv \sum_{\substack{n=0 \\ (n,\ell)=1}}^{\infty} a(\ell n)q^n \mod \ell.$$

Now let $f_5(z)$ denote the modular form that is the *quadratic twist* of $f_4(z)$ by $\left(\frac{n}{\ell}\right)$; therefore we find that

$$f_5(z) \equiv \sum_{\substack{n=0 \\ (n,\ell)=1}}^{\infty} \left(\frac{n}{\ell}\right) a(\ell n)q^n \mod \ell.$$

It turns out that $f_5(z) \in M_k\left(N\ell^3, \chi_0\right)$. Therefore if we define the modular forms $f_+(z)$ and $f_-(z)$ by

$$f_+(z) := \frac{1}{2}\left(f_4(z) + f_5(z)\right)$$

and

$$f_-(z) := \frac{1}{2}\left(f_4(z) - f_5(z)\right),$$

then we will find that $f_+(z) \equiv 0 \mod \ell$ (resp. $f_-(z) \equiv 0 \mod \ell$) if and only if the Fourier coefficients of $f(z)$ satisfy a quadratic congruence modulo ℓ of type $(\ell, +1)$ (resp. $(\ell, -1)$).

The claim then follows from Sturm's theorem if we let $g(z) = 0$. □

2. Special values of $L(s, \chi_D)$

In this section we present a number of examples of such congruences which involve special values of real Dirichlet $L-$functions at negative integers.

If χ is a Dirichlet character with conductor f and n is any positive integer, then it is well known that $L(1-n, \chi) = -\frac{B_{n,\chi}}{n}$ where $B_{n,\chi}$ is the n^{th} generalized Bernoulli number with character χ defined by

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}.$$

The properties of these numbers are important in the construction of $p-$adic L-functions (see [11,28]). These numbers also occur in congruences involving the special values of $L-$functions of elliptic curves with complex multiplication and also the class numbers of real quadratic fields (see [18]).

In [5] H. Cohen explicitly constructed holomorphic modular forms of half integer weight whose Fourier coefficients are explicit expressions involving the special values at negative integers of Dirichlet $L-$functions of quadratic characters.

Fix a positive integer r. If $N = 0$, then let $H(r, 0) := \zeta(1-2r)$. If N is a positive integer and $Dn^2 = (-1)^r N$ where D is the fundamental discriminant of a quadratic number field, then define $H(r, N)$ by

$$H(r, N) := L(1-r, \chi_D) \sum_{d|n} \mu(d)\chi_D(d)d^{r-1}\sigma_{2r-1}\left(\frac{n}{d}\right). \tag{4}$$

In particular, if $D = (-1)^r N$ is the discriminant of a quadratic field, then

$$H(r, N) = L(1-r, \chi_D) = -\frac{B_{r,\chi_D}}{r}. \tag{5}$$

In all other cases let $H(r, N) := 0$.

If $r \geq 2$ and $F_r(z) := \sum_{n=0}^{\infty} H(r, n)q^n$, then $F_r(z) \in M_{r+\frac{1}{2}}(4, \chi_0)$ (see [Th. 3.1,5]). We shall show that lots of these modular forms have the desired congruence properties. First we need the following lemma:

Lemma 3. *Let $p>3$ be a prime and suppose that D is a fundamental discriminant of $\mathbb{Q}(\sqrt{D})$ of the form $D=(-1)^{\frac{p+1}{2}}pN$ where N is a positive integer satisfying $\left(\frac{-N}{p}\right)=1$. Then*

$$\sum_{a=1}^{|D|}\chi_D(a)a^{\frac{p+1}{2}}\equiv 0 \mod p|D|.$$

Proof of Lemma 3. From (0) and the law of quadratic reciprocity, we may factor $\chi_D(n)$ as

$$\chi_D(n)=\left(\frac{n}{p}\right)\chi(n)$$

where χ is a non-trivial real character modulo N satisfying $\chi(p)=\left(\frac{-N}{p}\right)$. Therefore the sum, which we denote T, may be rewritten as

$$T:=\sum_{a=1}^{|D|}\chi_D(a)a^{\frac{p+1}{2}}=\sum_{a=1}^{pN}\left(\frac{a}{p}\right)\chi(a)a^{\frac{p+1}{2}}.$$

We first show that $T\equiv 0 \mod N$, a fact which does not depend on the condition that $\left(\frac{-N}{p}\right)=1$. We split T into residue classes modulo N, and by the Binomial Theorem deduce that

$$T=\sum_{b=0}^{p-1}\sum_{r=1}^{N}\left(\frac{bN+r}{p}\right)\chi(r)(bN+r)^{\frac{p+1}{2}}\equiv$$
$$\equiv\sum_{r=1}^{N}\chi(r)r^{\frac{p+1}{2}}\sum_{b=0}^{p-1}\left(\frac{bN+r}{p}\right) \mod N.$$

Since $\left(\frac{n}{p}\right)$ is a non-trivial Dirichlet character with conductor p and since $\gcd(N,p)=1$, we find that

$$\sum_{b=0}^{p-1}\left(\frac{bN+r}{p}\right)=\sum_{d=0}^{p-1}\left(\frac{d}{p}\right)=0.$$

Therefore it is easy to see that $T\equiv 0 \mod N$. Using the same argument, it is also easy to deduce that $T\equiv 0 \mod p$. However to complete the proof we need to establish that $T\equiv 0 \mod p^2$ since $p||D|$.

To establish this claim, we split the sum T into residue classes modulo p and from the Binomial Theorem we find that

$$T=\sum_{c=0}^{N-1}\sum_{s=1}^{p}\left(\frac{cp+s}{p}\right)\chi(cp+s)(cp+s)^{\frac{p+1}{2}}\equiv$$
$$\equiv\sum_{c=0}^{N-1}\sum_{s=1}^{p}\left(\frac{s}{p}\right)\chi(cp+s)\left(s^{\frac{p+1}{2}}+\frac{p+1}{2}\cdot cps^{\frac{p-1}{2}}\right) \mod p^2.$$

Since $\chi(n)$ is a non-trivial Dirichlet character with conductor N, and $\gcd(N,p)=1$, we find that for every integer s

$$\sum_{c=0}^{N-1}\chi(cp+s)=\sum_{d=0}^{N-1}\chi(D)=0. \tag{6}$$

Therefore we find that

$$2T \equiv 2\sum_{s=1}^{p}\left(\frac{s}{p}\right)s^{\frac{p+1}{2}}\sum_{c=0}^{N-1}\chi(cp+s) + \sum_{c=0}^{N-1}\sum_{s=1}^{p}\left(\frac{s}{p}\right)\chi(cp+s)(p+1)cps^{\frac{p-1}{2}} \mod p^2$$
$$\equiv (p+1)\sum_{c=0}^{N-1}\sum_{s=1}^{p}\left(\frac{s}{p}\right)\chi(cp+s)cps^{\frac{p-1}{2}} \mod p^2.$$

Since $\left(\frac{s}{p}\right)s^{\frac{p-1}{2}} \equiv 1 \mod p$, for every integer $s \not\equiv 0 \mod p$ then

$$2T \equiv (p+1)\sum_{c=0}^{N-1}\sum_{s=1}^{p-1}\chi(cp+s)cp \mod p^2.$$

Finally we show that

$$S := \sum_{c=0}^{N-1}\sum_{s=1}^{p-1}\chi(cp+s)c = (1-\chi(p))\sum_{r=1}^{N}\chi(r)r.$$

This implies that $2T \equiv pS \equiv 0 \mod p^2$ since $\chi(p) = \left(\frac{-N}{p}\right) = 1$ which would complete the proof.

Note that this identity holds for arbitrary Dirichlet characters. By (6) we have

$$S = \frac{1}{p}\sum_{c=0}^{N-1}\sum_{s=1}^{p-1}\chi(cp+s)cp + \frac{1}{p}\sum_{s=1}^{p-1}s\sum_{c=0}^{N-1}\chi(cp+s) =$$
$$= \frac{1}{p}\sum_{c=0}^{N-1}\sum_{s=1}^{p-1}\chi(cp+s)(cp+s) =$$
$$= \frac{1}{p}\sum_{c=0}^{N-1}\sum_{s=1}^{p}\chi(cp+s)(cp+s) - \frac{1}{p}\sum_{c=0}^{N-1}\chi(cp+p)(cp+p)$$
$$= \frac{1}{p}\sum_{a=1}^{pN}\chi(a)a - \chi(p)\sum_{r=1}^{N}\chi(r)r.$$

We split the first sum again into residue classes modulo N and obtain

$$\frac{1}{p}\sum_{a=1}^{pN}\chi(a)a = \frac{1}{p}\sum_{b=0}^{p-1}\sum_{r=1}^{N}\chi(r)\,(bN+r) =$$
$$= \frac{1}{p}\sum_{b=0}^{p-1}\sum_{r=1}^{N}\chi(r)r = \sum_{r=1}^{N}\chi(r)r.$$

Therefore we find that $2T \equiv pS = 0 \mod p^2$; this completes the proof.

□

Although the congruence properties of the denominator of ordinary and generalized Bernoulli numbers are well known by the Von Staudt-Clausen type theorems (see [4,10,28]), the nature of the prime divisors of the numerators seems to be quite elusive although some results in this direction are known. In the next theorem we present elementary circumstances for which a given prime $p > 3$ must divide the numerator of the generalized Bernoulli number $B_{\frac{p+1}{2},\chi_D}$.

Theorem 4. *If $p > 3$ is prime and D is a fundamental discriminant of $\mathbb{Q}(\sqrt{D})$ of the form $D = (-1)^{\frac{p+1}{2}} pN$ where N is a positive integer satisfying $\left(\frac{-N}{p}\right) = 1$, then*

$$B_{\frac{p+1}{2},\chi_D} \equiv 0 \mod p.$$

Moreover the special value $L(\frac{1-p}{2}, \chi_D) \equiv 0 \mod p$.

Proof Theorem 4. It is well known that

$$B_{\frac{p+1}{2},\chi_D} = |D|^{\frac{p-1}{2}} \sum_{a=1}^{|D|} \chi_D(a) B_{\frac{p+1}{2}}\left(\frac{a}{|D|}\right)$$

where $B_{\frac{p+1}{2}}(x)$ is the $\frac{p+1}{2}^{\text{st}}$ Bernoulli polynomial defined by

$$B_{\frac{p+1}{2}}(x) = \sum_{i=0}^{\frac{p+1}{2}} \binom{\frac{p+1}{2}}{i} B_i x^{\frac{p+1}{2}-i}.$$

Therefore one finds that

$$B_{\frac{p+1}{2},\chi_D} = \sum_{a=1}^{|D|} \chi_D(a) \sum_{i=0}^{\frac{p+1}{2}} \binom{\frac{p+1}{2}}{i} B_i |D|^{i-1} a^{\frac{p+1}{2}-i}.$$

Since $p > 3$ and $i \leq \frac{p+1}{2}$, by Von Staudt-Clausen it follows that all of the B_i in the above sum are $p-$integral (i.e. denominators are prime to p). Therefore since $|D| \equiv 0 \mod p$ we find that

$$B_{\frac{p+1}{2},\chi_D} \equiv \sum_{a=1}^{|D|} \chi_D(a) \left(B_0 |D|^{-1} a^{\frac{p+1}{2}} + \frac{p+1}{2} \cdot a^{\frac{p-1}{2}} B_1 \right) \mod p.$$

This reduces to

$$B_{\frac{p+1}{2},\chi_D} \equiv B_0 |D|^{-1} \sum_{a=1}^{|D|} \chi_D(a) a^{\frac{p+1}{2}} + \frac{p+1}{2} \cdot B_1 \sum_{a=1}^{|D|} \chi_D(a) \left(\frac{a}{p}\right) \mod p.$$

Since $\chi_D(n)\left(\frac{n}{p}\right)$ is a character modulo $|D|$, the second sum is identically zero and hence we find that

$$B_{\frac{p+1}{2},\chi_D} \equiv |D|^{-1} B_0 \sum_{a=1}^{|D|} \chi_D(a) a^{\frac{p+1}{2}} \mod p.$$

The result now follows as a consequence of (5) and Lemma 3.

□

Corollary 5. *Let $\ell > 3$ be prime. Then the Fourier coefficients $H(\frac{\ell+1}{2}, n)$ of the weight $\frac{\ell}{2}+1$ modular form $F_{\frac{\ell+1}{2}}(z)$ satisfy a quadratic congruence modulo ℓ of type $(\ell, (\frac{-1}{\ell}))$.*

Proof Corollary 5. By (5) and Theorem 4 we see that if D is a fundamental discriminant of the form $D = (-1)^{\frac{\ell+1}{2}}\ell N$ where N is a positive integer satisfying $\left(\frac{-N}{\ell}\right) = 1$, then

$$H\left(\frac{\ell+1}{2}, \ell N\right) = -\frac{2B_{\frac{\ell+1}{2},\chi_D}}{\ell+1} \equiv 0 \mod \ell.$$

Then by (4) it is easy to deduce that for every integer n that

$$H\left(\frac{\ell+1}{2}, \ell N n^2\right) \equiv 0 \mod \ell.$$

Therefore it follows that

$$H\left(\frac{\ell+1}{2}, M\right) \equiv 0 \mod \ell$$

for every positive integer $M = \ell m$ where $\left(\frac{-m}{\ell}\right) = 1$. However this is precisely the condition that $\left(\frac{m}{\ell}\right) = \left(\frac{-1}{\ell}\right)$. Therefore the modular form $F_{\frac{\ell+1}{2}}(z)$ satisfies a quadratic congruence modulo ℓ of type $(\ell, (\frac{-1}{\ell}))$.

□

There are various other congruences for $H(r, N)$ which are not of this type which are also of interest. To illustrate this we now prove the following theorem.

Theorem 6. *For every positive integer $N \equiv 1 \mod 5$ the function $H(5, N)$ satisfies the congruence*

$$H(5, N) \equiv 0 \mod 5.$$

Proof of Theorem 6. Let $f_1(z) := F_5(z)\Theta(5z) \in M_6(20, \chi_5)$, its Fourier expansion is given by

$$f_1(z) = \sum_{n=0}^{\infty} b(n)q^n = -\frac{1}{132}\left(\Theta^{11}(z) - \frac{22\Theta^7(z)\eta^8(4z)}{\eta^4(2z)} + \frac{88\Theta^3(z)\eta^{16}(4z)}{\eta^8(2z)}\right)\Theta(5z).$$

Since $\Theta(5z) = 1 + 2\sum_{n=1}^{\infty} q^{5n^2}$, it is clear that it suffices to check that

$$b(n) \equiv 0 \mod 5$$

for every positive integer $n \equiv 1 \mod 5$. Now it is known that

$$f_3(z) = \sum_{n \equiv 1 \mod 5}^{\infty} b(n)q^n$$

is a weight 6 modular form with respect to $\Gamma_1(500)$. Therefore by Sturm's theorem it suffices to check that $b(n) \equiv 0 \mod 5$ for every $n \equiv 1 \mod 5$ up to 90000. The congruence has been verified with machine computation.

□

In [Th. 4, 4] Carlitz proved that if χ is a primitive Dirichlet character with conductor f and p is a prime for which $p \nmid f$ and n is a positive integer for which $p^e \mid n$, then p^e divides the numerator of $B_{n,\chi}$. For example if $D = -N$ is the fundamental discriminant of the quadratic number field $\mathbb{Q}(\sqrt{D})$ where $N \equiv 1 \mod 5$, then this result implies that the numerator of B_{5,χ_D} is a multiple of 5. However by Theorem 6 we find that even more is true. We obtain:

Corollary 7. *Let $D = -N$ be the fundamental discriminant of $\mathbb{Q}(\sqrt{D})$ where $N \equiv 1 \mod 5$ is a positive integer. Then the numerator of B_{5,χ_D} is a multiple of* 25.

Proof Corollary 7. By (5) and Theorem 6 it follows that

$$H(5, N) = L(-4, \chi_D) = -\frac{B_{5,\chi_D}}{5} \equiv 0 \mod 5.$$

This immediately implies that the numerator of B_{5,χ_D} is a multiple of 25.

□

Now we make some observations regarding the divisibility of the Fourier coefficients of half-integer weight modular forms. In [22] Serre proved a remarkable theorem regarding the divisibility of the Fourier coefficients of holomorphic integer weight modular forms. Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ be the Fourier expansion of a holomorphic integer weight modular form with respect to some congruence subgroup of $SL_2(\mathbb{Z})$ whose coefficients $a(n)$ are algebraic integers in a fixed number field. Then he proved that given a positive integer M, the set of non-negative integers n for which $a(n) \equiv 0 \mod M$ has arithmetic density one.

Unfortunately much less is known regarding the divisibility properties of the coefficients of holomorphic half-integer weight forms. Let r be a non-negative integer and let $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_{r+\frac{1}{2}}(N, \chi)$ with rational integer coefficients. If $r = 0$, then by the Serre-Stark basis theorem (see [19]), it is known that $f(z)$ is a finite linear combination of theta functions. Moreover these functions are of the form $\Theta_{a,M}(dz)$ where d is a positive integer and

$$\Theta_{a,M}(z) := \sum_{n \equiv a \mod M} q^{n^2}.$$

In particular for all but a finite number of square-free positive integers t, it is the case that $a(tn^2) = 0$ for every integer n. Therefore the number of integers $n \leq x$ for which $a(n) \neq 0$ is $O(\sqrt{x})$. However if $r \geq 1$, then the situation is very different and is of significant interest. A thorough understanding of the divisibility properties of Fourier coefficients when $r = 1$ will shed some light on the divisors of class numbers of imaginary quadratic fields and the Shafarevich-Tate groups of twists of certain modular elliptic curves. Therefore it is worth examining any analogs of Serre's divisibility result which may hold for half-integer weight forms.

From the works of Carlitz and Leopoldt we find that the modular forms $F_r(z)$ provide us with an infinite family of interesting modular forms, which are not trivially zero modulo an integer M, for which we find obvious analogs of Serre's divisibility theorem. Both proved that if χ is a Dirichlet character with conductor f that is not a power of a prime p, then $L(1-r,\chi)$ is an algebraic integer. However if χ is a character with a conductor that is a power of a prime p, then the prime ideal divisors of the denominator of $L(1-r,\chi)$ are prime ideal divisors of p. However if $r \geq 2$ fixed, it is known that the denominators of $L(1-r,\chi_D)$ are bounded which implies that there are at most finitely many D for which $L(1-r,\chi_D)$ is not an integer. Therefore since the modular form $F_r(z)$ may be written as

$$F_r(z) := \zeta(1-2r)\sum_{n=0}^{\infty} a_r(n)q^n = -\frac{B_{2r}}{2r}\sum_{n=0}^{\infty} a_r(n)q^n$$

where the coefficients $a_r(n)$ are rational with denominators bounded by D_r, the least common multiple of all the denominators occuring in the $a_r(n)$, it follows that the numerator of almost every $a_r(n)$ is a multiple of the denominator of $\zeta(1-2r) = -\dfrac{B_{2r}}{2r}$. By Von Staudt-Clausen and the Voronoi congruences (see [15.2.4, 10]), $\prod_{(p-1)|2r} p$ divides the denominator of $\frac{B_{2r}}{2r}$.
We have proved:

Proposition 8. *Let $r \geq 2$ be a positive integer. Then for all but finitely many square-free integers t we find that*

$$a_r(tn^2) \equiv 0 \mod M$$

for every integer n where $M = \prod_{(p-1)|2r} p$. In particular, the number of non-negative integers $n \leq x$ for which $a_r(n) \not\equiv 0 \mod M$ is $O(\sqrt{x})$.

Using this proposition as a template we establish circumstances for which the Fourier coefficients of a half-integer weight modular form are almost always a multiple of a power of a prime p. From the discussion above it is clear that we only need to consider those half-integer weight forms with weight $\geq \frac{3}{2}$. First we note that the classical theta function $\Theta(z) = 1 + 2\sum_{n=1}^{\infty} q^{n^2} \equiv 1 \mod 2$. Therefore if $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ is a holomorphic half-integer weight modular form with integer coefficients, then $f(z)\cdot\Theta(z) \equiv f(z) \mod 2$ is an integer weight holomorphic modular form for which the Fourier coefficients are almost always even by Serre's theorem. Therefore the coefficients $a(n)$ are almost always even. Therefore we may assume that p is an odd prime.

Let $f_p(z)$ be the weight $\frac{p-1}{2}$ modular form defined by

$$f_p(z) = \frac{\eta^p(z)}{\eta(pz)}.$$

It is easy to verify that $f_p(z) \in M_{\frac{p-1}{2}}(p,\chi_D)$ where $D := (-1)^{\frac{p-1}{2}}p$. More importantly if s is a positive integer, then since $1 - X^p \equiv (1-X)^p \mod p$, we find that

$$f_p^{p^s}(z) \equiv 1 \mod p^{s+1}. \tag{7}$$

Using this notation we observe:

Proposition 9. *Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_{r+\frac{1}{2}}(N, \chi)$ with rational integer coefficients. Let p be an odd prime and let s and k be positive integers for which*

$$2r = kp^s(p-1).$$

If for every cusp $\frac{c}{d}$ of $\Gamma_0(Np)$

$$\mathrm{Ord}(f, \frac{c}{d}) \geq \frac{Nkp^{s+1}}{24 \cdot \gcd(d, Np/d)d}\left(p - \frac{\gcd(d,p)^2}{p}\right)$$

where $\mathrm{Ord}(f, \frac{c}{d})$ is the analytic order of $f(z)$ at the cusp $\frac{c}{d}$, then for all but finitely many square-free positive integers t

$$a(tn^2) \equiv 0 \mod p^{s+1}$$

for every integer n. In particular, the set of non-negative integers $n \leq x$ for which $a(n) \not\equiv 0 \mod p^{s+1}$ is $O(\sqrt{x})$.

Proof of Proposition 9. If $2r = kp^s(p-1)$, then by (7) the weight of $\left(f_p^{p^s}(z)\right)^k$ is exactly $\frac{1}{2}$ more than $r + \frac{1}{2}$, the weight of $f(z)$. The system of inequalities implies that the modular form

$$f(z) \cdot \left(\frac{\eta^{p^{s+1}}(z)}{\eta^{p^s}(pz)}\right)^{-k} \equiv f(z) \mod p^{s+1}$$

is holomorphic at all the cusps of $\Gamma_0(Np)$ since the order of $f_p^{p^s}(z)$ at a cusp $\frac{c}{d}$ is given by (see [2])

$$\frac{Np^{s+1}}{24 \cdot \gcd(d, Np/p)}\left(p - \frac{\gcd(d,p)^2}{p}\right).$$

Therefore this form is a holomorphic weight $\frac{1}{2}$ form, hence is a finite linear combination of theta functions by the Serre-Stark basis theorem. This completes the proof.

□

By following an argument similar to the one above, it is easy to see that there will be half integer weight modular forms which are congruent modulo an integer m to a linear combination of weight $\frac{3}{2}$ theta series of the form

$$\Theta_{3,a,M}(z) = \sum_{n \equiv a \mod M} nq^{n^2}.$$

Clearly all such forms will have the property that almost all of their Fourier coefficients will be a multiple of m. Using these as templates of the more general case, it seems reasonable to make the following conjectures.

Conjecture A. Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ be a holomorphic modular form of weight $r + \frac{1}{2}$ with integer coefficients. If p is an odd prime that divides almost all (but not all) of the Fourier coefficients $a(n)$, then either

- $$p-1 \mid 2r$$

or

- $$p-1 \mid 2r-2.$$

A stronger version of this conjecture is:

Conjecture B. Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ be a holomorphic modular form of weight $r + \frac{1}{2}$ with integer coefficients. If p is an odd prime and s is a non-negative integer for which

$$a(n) \equiv 0 \mod p^{s+1}$$

for almost (but not all) every non-negative integer n, then either

- $$p^s(p-1) \mid 2r$$

or

- $$p^s(p-1) \mid 2r-2.$$

Moreover if $a(N) \equiv 0 \mod p^{s+1}$ for almost all N, then for all but finitely many integers t the congruence

$$a(tn^2) \equiv 0 \mod p^{s+1}$$

holds for all n. In particular the set of non-negative integers $n \leq x$ for which $a(n) \not\equiv 0 \mod p^{s+1}$ is at most $O(\sqrt{x})$.

3. Special values of modular $L-$functions

In this section we investigate the the congruence properties of special values of quadratic twists of a modular $L-$function at the center of the critical strip on the real line. By the work of Kohnen, Shimura, Waldspurger, and Zagier, the Fourier coefficients of certain special half-integer weight forms are *essentially* (up to a transcendental factor) the square-root of these special values. We now present two simple examples for which congruences exist.

A congruence related to Δ: Let $L(\Delta, s)$ denote the modular $L-$function defined by

$$L(\Delta, s) := \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s},$$

where $\tau(n)$ is Ramanujan's τ-function giving the Fourier expansion

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n$$

at infinity of the unique cusp form Δ of weight 12 and level 1.

If D is the fundamental discriminant of $\mathbb{Q}(\sqrt{D})$, we let $L(\Delta, D, s)$ denote the *twisted* $L-$function defined by

$$L(\Delta, D, s) := \sum_{n=1}^{\infty} \frac{\chi_D(n)\tau(n)}{n^s}.$$

Let $g(z) = \sum_{n=1}^{\infty} a(n)q^n$ be the weight $\frac{13}{2}$ eigenform defined by

$$g(z) := \frac{\Theta^9(z)\eta^8(4z)}{\eta^4(2z)} - \frac{18\Theta^5(z)\eta^{16}(4z)}{\eta^8(2z)} + \frac{32\Theta(z)\eta^{24}(4z)}{\eta^{12}(2z)}.$$

Using the Shimura correspondence, Kohnen and Zagier [14] proved a general theorem which in this case implies that if D is the fundamental discriminant of a real quadratic field, then

$$L(\Delta, D, 6) = \left(\frac{\pi}{D}\right)^6 \frac{\sqrt{D}}{5!} \frac{\langle \Delta(z), \Delta(z)\rangle}{\langle g(z), g(z)\rangle} \cdot (a(D))^2 \tag{8}$$

where $\langle \Delta(z), \Delta(z)\rangle$ and $\langle g(z), g(z)\rangle$ are the relevant Peterson scalar products. Therefore we shall refer to $(a(D))^2$ as the rational factor of $L(\Delta, D, 6)$. With this notation we prove the following congruences for the rational factors of $L(\Delta, D, 6)$:

Theorem 10. *If D_0 is a positive integer satisfying $\left(\frac{-D_0}{11}\right) = 1$, then the Fourier coefficient $a(11D_0)$ satisfies*

$$a(11D_0) \equiv 0 \mod 11.$$

Proof of Theorem 10. It suffices to check that the Fourier coefficients $a(n)$ satisfy a quadratic congruence modulo 11 of type $(11, -1)$. Let $T(z) \in M_{12}(44, \chi_0)$ be defined by

$$T(z) := \sum_{n=1}^{\infty} c(n)q^n = g(z) \cdot \Theta(11z) \cdot \frac{\eta^{11}(z)}{\eta(11z)}.$$

Since the right hand factor is a modular form whose Fourier expansion is $\equiv 1 \mod 11$, it suffices to check that the Fourier expansion of $T(z)$ has a quadratic congruence modulo 11 of type $(11, -1)$. However by Proposition 2 it suffices to check that

$$c(11n) \equiv 0 \mod 11$$

for all $n \leq 95832$ that satisfy $\left(\frac{n}{11}\right) = -1$. This congruence has been verified by machine computation.

□

Therefore by (8) we obtain:

Corollary 11. *Using the notation above, if $D = 11D_0$ is the fundamental discriminant of $\mathbb{Q}(\sqrt{D})$ where D_0 is a positive integer satisfying $\left(\frac{-D_0}{11}\right) = 1$, then the rational factor of $L(\Delta, D, 6)$ is a multiple of* 121.

Galois representations: We now propose a conceptual explanation for corollary 11 in terms of the Galois representations associated to cusp forms. Let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$, and let

$$\rho_\Delta : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}_2(\mathbb{Z}_{11})$$

be the 11-adic representation associated by Deligne to the cusp form Δ. Let $\chi : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_{11}^\times$ be the 11-adic cyclotomic character giving the action of $G_{\mathbb{Q}}$ on the 11-power roots of unity. Finally we identify χ_D with the character $G_{\mathbb{Q}} \longrightarrow \pm 1 \subset \mathbb{Z}_{11}^\times$ corresponding to the field $\mathbb{Q}(\sqrt{D})$.

Let E_{11} be the elliptic curve $X_0(11)$. It is the (unique, up to isogeny) elliptic curve of conductor 11, and its associated eigenform $f_{11} \in S_2(\Gamma_0(11))$ is

$$f_{11} = \eta(z)^2\eta(11z)^2 = q\prod(1-q^n)^2(1-q^{11n})^2 = \sum a_n(E_{11})q^n.$$

Denote by $\rho_{E_{11}}$ the Galois representation attached to this cusp form. (Equivalently, this is the Galois representation describing the action of $G_{\mathbb{Q}}$ on the 11-adic Tate module of E_{11}.) Then we have:

Lemma 12. *The* 11*-adic Galois representations* $\rho_1 = \rho_\Delta \otimes \chi_D \otimes \chi^{-5}$ *and* $\rho_2 = \rho_{E_{11}} \otimes \chi_{-D_0}$ *are residually absolutely irreducible, and their associated mod* 11 *representations are isomorphic.*

Proof: We have

$$\Delta = q\prod(1-q^n)^{24} \equiv q\prod(1-q^n)^2(1-q^{11n})^2 \equiv f_{11} \pmod{11},$$

so that $\tau(n) \equiv a_n(E_{11}) \pmod{11}$ for all n. Moreover, we have

$$\chi_D(p)p^{-5} \equiv \chi_{-D_0}(p) \pmod{11},$$

and the lemma follows directly from this.

Lemma 13. *If* 11 *is split in the field* $\mathbb{Q}(\sqrt{-D_0})$*, then*

$$L(E_{11}, \chi_{-D_0}, 1) = 0.$$

Proof: This follows from the calculation of the sign in the functional equation for $L(E_{11}, \chi_{-D_0}, s)$, which can be shown to be -1 when the conductor of E_{11} splits in the quadratic field $\mathbb{Q}(\sqrt{-D_0})$. (See for example [9].) Since 1 is the symmetry point for the functional equation, it follows that $L(E_{11}, \chi_{-D_0}, 1) = 0$, as was to be shown.

In some sense, lemmas 12 and 13 provide a conceptual explanation (although not a proof!) for the congruences of corollary 11. Indeed, lemma 12 leads us to expect that the special values of the L-functions $L(\Delta, D, 6+s)$ and $L(E_{11}, -D_0, 1+s)$, which are associated to the Galois representations $\rho_1 = \rho_\Delta \otimes \chi_D \otimes \chi^{-5}$ and $\rho_2 = \rho_{E_{11}} \otimes \chi_{-D_0}$, might be congruent modulo 11. This follows a philosophy suggested by Mazur. (Cf. [16], in particular the discussion on p. 208.) Lemma 13 states that $L(E_{11}, -D_0, 1) = 0$, so that one is led to expect that the rational factor of $L(\Delta, D, 6)$ is divisible by 11 (and hence, 121, since it is a square).

A congruence related to $\eta^8(z)\eta^8(2z)$ We present a second example of such congruences. In this example let $f(z) := \sum_{n=1}^{\infty} c(n)q^n = \eta^8(z)\eta^8(2z)$; hence $f(z)$ is the unique normalized weight 8 eigenform of level 2. Let $L(f,s)$ denote the modular $L-$function

$$L(f,s) := \sum_{n=1}^{\infty} \frac{c(n)}{n^s},$$

and let $L(f, D, s)$ be the twisted modular $L-$function defined as above.
Now let $h(z)$ denote the weight $\frac{9}{2}$ eigenform

$$h(z) := \sum_{n=1}^{\infty} d(n)q^n = \frac{\Theta^5(z)\eta^8(4z)}{\eta^4(2z)} - \frac{16\Theta(z)\eta^{16}(4z)}{\eta^8(2z)}.$$

The Shimura lift of $h(z)$ is $f(z)$, hence by [27] it turns out that if $N_1 \equiv N_2 \not\equiv 5 \bmod 8$ are two positive square-free integers with corresponding quadratic characters χ_{D_1} and χ_{D_2} where $d(N_1) \neq 0$, then

$$L(f, D_2, 4) = \frac{d^2(N_2)L(f, D_1, 4)N_1^{\frac{7}{2}}}{d^2(N_1)N_2^{\frac{7}{2}}}. \tag{9}$$

With this notation we prove:

Theorem 14. *If D_0 is a positive integer satisfying $\left(\frac{-D_0}{7}\right) = 1$, then the Fourier coefficient $d(7D_0)$ satisfies the congruence*

$$d(7D_0) \equiv 0 \mod 7.$$

Proof of Theorem 14. It suffices to check that the Fourier coefficients $d(n)$ satisfy a quadratic congruence modulo 7 of type $(7, -1)$. Let $S(z) \in M_8(28, \chi_0)$ be the modular form defined by

$$S(z) := \sum_{n=1}^{\infty} b(n)q^n := h(z) \cdot \Theta(7z) \cdot \frac{\eta^7(z)}{\eta(7z)}.$$

Since the right hand factor is a modular form whose Fourier expansion is $\equiv 1 \mod 7$, by Proposition 1 it suffices to check that

$$b(7n) \equiv 0 \mod 7$$

for all $n \leq 10976$ where $\left(\frac{n}{7}\right) = -1$. This has been verified by machine computation. □

By (9) we obtain:

Corollary 15. *Let D_0 be a positive square-free integer for which $7D_0 \not\equiv 5 \mod 8$ and $\left(\frac{-D_0}{7}\right) = 1$, and let $D = 7D_0$. Then the rational factor of $L(f, D, 4)$ is a multiple of* 49.

Galois representations: We now propose as before an interpretation in terms of Galois representations. Suppose that $D = 7D_0$ with 7 not dividing D_0. Let E_{14} be the elliptic curve $X_0(14)$. It is the (unique) modular elliptic curve of conductor 14, and its associated eigenform $f_{14} \in S_2(\Gamma_0(14))$ is

$$f_{14} = \eta(z)\eta(2z)\eta(7z)\eta(14z) = q \prod (1 - q^n)(1 - q^{2n})(1 - q^{7n})(1 - q^{14n}).$$

Let ρ_f be the 7-adic Galois representation associated to f, and let $\rho_{E_{14}}$ be the 7-adic representation associated to f_{14}. Then we have:

Lemma 16. *The 7-adic representations $\rho_f \otimes \chi_D \otimes \chi^{-3}$ and $\rho_{E_{14}} \otimes \chi_{-D_0}$ are both residually irreducible, and their mod 7 reductions are isomorphic.*

Proof: We have

$$f = q \prod (1-q^n)^8(1-q^{2n})^8 \equiv q \prod (1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n}) = f_{14} \pmod{14}.$$

The lemma follows directly from this, and from the fact that $\chi_D(p)p^{-3} \equiv \chi_{-D_0}(p) \pmod 7$.

Lemma 17. *If 2 and 7 are both split or both inert in the field $\mathbb{Q}(\sqrt{-D_0})$, then $L(E_{14}, -D_0, 1) = 0$.*

Proof: This follows from the calculation of the sign in the functional equation for $L(E_{14}, \chi_{-D_0}, s)$, which can be shown to be -1 when $\chi_{-D_0}(14) = 1$. (See for example [9].) Since 1 is the symmetry point for the functional equation, it follows that $L(E_{14}, -D_0, 1) = 0$.

As in the case of Δ, lemmas 16 and 17 suggest a conceptual explanation (although again not a proof!) for the congruences of corollary 15.

4. Some remarks on the Bloch-Kato Conjectures

This section contains a few general remarks and questions, motivated by the examples of sec. 3, about the Bloch-Kato conjecture on special values of L-functions associated to arithmetic objects of a very general type (the "motives" in the sense of Grothendieck and Deligne, as defined for example in [6]).

Motives: It is beyond our scope to give a detailed account of motives. For the purpose of our discussion, a motive M (over $\mathbb{Q}$, with rational coefficients, of rank r) can be thought of as a piece of the cohomology of an algebraic variety over $\mathbb{Q}$, giving rise to:

• For each prime ℓ, an ℓ-adic representation M_ℓ of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, arising from ℓ-adic étale cohomology. The object M_ℓ is an r-dimensional $\mathbb{Q}_\ell$-vector space equipped with an action of $G_{\mathbb{Q}}$. Since $G_{\mathbb{Q}}$ acts through a compact quotient, it leaves stable a $\mathbb{Z}_\ell$- sublattice T_ℓ of M_ℓ, and one can define the mod ℓ representation associated to M_ℓ to be the $\mathbf{F}_\ell$-vector space $\bar{M}_\ell = T_\ell/\ell T_\ell$. This space depends on the choice of T_ℓ in general, but its semi-simplification does not, by the Brauer-Nesbitt theorem. To obtain a canonical object we simply define $\bar{M}_\ell$ to be the semi-simplification of $T_\ell/\ell T_\ell$.

• The system $\{M_\ell\}$ should form a compatible system of rational ℓ-adic representations in the sense of [20], §I.11. More precisely, the action of $G_{\mathbb{Q}}$ is unramified outside $S \cup \{\ell\}$, where S is a fixed finite set of primes not depending on ℓ. Let D_p be a decomposition group at p in $G_{\mathbb{Q}}$ and let I_p denote an inertia subgroup of D_p. Let Frob_p be the canonical ("frobenius") generator of D_p/I_p which gives the map $x \mapsto x^p$ on residue fields. If $p \neq \ell$ is a prime, then the characteristic polynomial $Z_p(M,T)$ of Frob_p acting on $M_\ell^{I_p}$

$$Z_p(M,T) = \det((1 - \mathrm{Frob}_p T)|M_\ell^{I_p})$$

has integer coefficients and should not depend on the choice of $\ell \neq p$.

• A rational vector space M_B: the so called "Betti realization", arising from singular cohomology.

• A rational vector space M_{DR} coming from the algebraic DeRham cohomology, equipped with its natural Hodge structure.

The structures M_B and M_{DR} will not play an explicit role in our discussion, but are used in defining certain (possibly transcendental) periods associated to M as in [6].

The L-function: One defines the local L-function at p by $L_p(M,s) = Z_p(M,p^{-s})^{-1}$. By the compatibility axiom, $L_p(M,s)$ does not depend in the choice of the prime ℓ used to define it. One then defines the global L-function as a product over all primes p:

$$L(M,s) = \prod_p L_p(M,s).$$

This Euler product converges in a right half plane, by the Weil conjectures. It is conjectured that $L(M,s)$ has an analytic continuation and a functional equation (cf. [6], §1.2.) We will assume this. In the cases where M arises from a classical modular form, this is known to be true.

The Bloch-Kato conjectures: Under the asumption that the motive is "'critical" (in the sense of [6], Def. 1.3), Deligne has given a very general conjectural formula for the special value $L(M,0)$, modulo rational multiples, in terms of a certain period integral defined in terms of the structures M_B and M_{DR}. This conjecture has been refined by Bloch and Kato, and predicts that the "rational part" $L_{rat}(M,0)$ of $L(M,0)$ (i.e., the special value $L(M,0)$ divided by the Deligne period) can be interpreted as the order of a certain Selmer group $\mathrm{Sel}(M) = \oplus_\ell \mathrm{Sel}_\ell(M)$, where

$$\mathrm{Sel}_\ell(M) := \ker\left(H^1(\mathbb{Q}, M_\ell \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell) \longrightarrow \oplus_v H^1_f(\mathbb{Q}_v, M_\ell \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)\right).$$

The groups $H^1_f(\mathbb{Q}_v, M_\ell \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ are certain subgroups of the local Galois cohomology groups $H^1(\mathbb{Q}_v, M_\ell \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)$. When $v \notin S \cup \{\ell\}$ then these are exactly the unramified cohomology classes. When $v = \ell$, the definition of H^1_f is more subtle and relies on the crystalline cohomology theory developed by Fontaine and Messing. See [3] for details.

The module $\mathrm{Sel}(M)$ is a torsion $\hat{\mathbb{Z}}$-module which is cofinitely generated over $\hat{\mathbb{Z}}$. In general it need not be finite. If it is infinite, one conjectures that $L_{rat}(M,0) = 0$.

Congruences between motives: We say that two motives M and N are congruent modulo ℓ if the local L-factors $Z_p(M,T)$ and $Z_p(N,T)$ are congruent mod ℓ for all primes $p \neq \ell$. In particular, it follows from the Chebotarev density theorem that the mod ℓ Galois representations $\bar{M}_\ell$ and $\bar{N}_\ell$ associated to M and N are isomorphic. For example, modular forms whose Fourier coefficients are congruent modulo ℓ give rise to congruent motives. (See, for example, the discussion in the introduction to [16].) Generally speaking, motivated by the philosophy expressed in [16], one might expect a mod ℓ congruence between two motives to translate into a congruence modulo ℓ between the special values of their associated L-functions, at least when one ignores the possible complications arising from the bad factors in the Euler product decomposition.

Question 18. *If two motives M and N are congruent modulo ℓ, when can one predict a mod ℓ congruence between the associated L-values $L_{rat}(M,0)$ and $L_{rat}(N,0)$?*

It would be interesting to formulate a precise, convincing conjecture along these lines, and to compare it with the conjectures of Bloch and Kato.

Acknowledgements

The authors thank Will Galway (University of Illinois) for his assistance regarding the machine computations which were required for this paper.

References

1. G. Andrews, *The theory of partitions*, Addison-Wesley, 1976.
2. A. Biagioli, *The construction of modular forms as products of transforms of the Dedekind Eta function*, Acta. Arith. **54** (1990), 273-300.
3. S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck festschrift, vol. 1, Birkhäuser, 1990.
4. L. Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. Reine und Angew. Math. **201-202** (1959), 173-182.
5. H. Cohen, *Sums involving the values at negative integers of L−functions of quadratic characters*, Math. Ann. **217** (1975), 271-285.

6. P. Deligne, *Valeurs speciales de fonctions L et periodes d'integrales*, Proc. Symp. Pure Math., Corvallis Proceedings, 33 **2** (1979), 313-346.
7. D. Eichhorn and K. Ono, *Partition function congruences*, appearing in this volume.
8. B. Gordon, *private communication.*
9. B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Inv. Math. **84** (1986), 225-320.
10. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, 1982.
11. K. Iwasawa, *Lectures on $p-$adic $L-$functions*, Princeton Univ. Press, 1972.
12. M. Knopp, *Modular functions in analytic number theory*, Markham, 1970.
13. N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, 1984.
14. 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.
15. H. Leopoldt, *Eine verallgemeinerung der Bernoullischen zahlen*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 131-140.
16. B. Mazur, *On the arithmetic of special values of L-functions*, Invent. Math. **55** (1979), 207-240.
17. S. Ramanujan, *Congruence properties of partitions*, Proc. London Math. Soc. (2) **18** (1920), 19-20.
18. K. Rubin, *Congruences for special values of $L-$functions of elliptic curves with complex multiplication*, Invent. Math. **71** (1983), 339-364.
19. J.-P. Serre and H. Stark, *Modular forms of weight $\frac{1}{2}$*, Springer Lect. Notes Math. **627** (1977), 27-68.
20. J-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Addison-Wesley, 1988.
21. ———, *Congruences ét formes modulaires (d'aprés H.P.F. Swinnerton-Dyer)*, Seminaire Bourbaki **416** (1971).
22. ———, *Divisibilité des coefficients des formes modulaires*, C.R. Acad. Sci. Paris (A) **279** (1974), 679-682.
23. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, 1971.
24. ——— On modular forms of half-integral weight, Ann. Math. **97** (1973), 440-481.
25. J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes Math. **1240** (1984).
26. H.P.F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Springer Lect. Notes Math. **350** (1973).
27. J.L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.
28. L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, 1980.

Mathematical Institute of the Hungarian Academy of Sciences, P.O. Box 127, Budapest 1364, Hungary
E-mail address: h1165bal@ella.hu

Deaprtment of Mathematics, McGill University, Montréal, Canada PQ H3A 2K6
Current address: Department of Mathematics, Princeton University, Princeton, New Jersey 08540
E-mail address: darmon@math.princeton.edu

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

Department of Mathematics, Penn State University, University Park, Pennsylvania 16802
E-mail address: ono@math.psu.edu