RAMANUJAN-STYLE CONGRUENCES OF LOCAL ORIGIN

NEIL DUMMIGAN AND DANIEL FRETWELL

ABSTRACT. We prove that if a prime $\ell > 3$ divides $p^k - 1$, where p is prime, then there is a congruence modulo ℓ, like Ramanujan's mod 691 congruence, for the Hecke eigenvalues of some cusp form of weight k and level p. We relate ℓ to primes like 691 by viewing it as a divisor of a partial zeta value, and see how a construction of Ribet links the congruence with the Bloch-Kato conjecture (theorem in this case). This viewpoint allows us to give a new proof of a recent theorem of Billerey and Menares. We end with some examples, including where $p = 2$ and ℓ is a Mersenne prime.

1. INTRODUCTION

Let $\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n = q - 24q^2 + 252q^3 - 1472q^4 + \ldots$, where $q = e^{2\pi iz}$. Let $\sigma_r(n) = \sum_{d|n,\ d>0} d^r$. It was discovered by Ramanujan that, for all $n \geq 1$, $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$. The significance of Δ is that it is the unique normalised cusp form of weight 12 for the full modular group $\mathrm{SL}_2(\mathbb{Z})$, while 691 is a prime dividing the numerator of $\zeta(12)/\pi^{12}$, where $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$ is the Riemann zeta function. The congruence for general n follows from the special case that for all primes q, $\tau(q) \equiv 1 + q^{11} \pmod{691}$, using the multiplicative relations for τ implied by Δ being a Hecke eigenform. There are several proofs of this congruence, and of its generalisations to weights other than 12. The proof we give of the main theorem below is an adaptation of one such proof.

Theorem 1.1. *Let p be prime and let $k \geq 4$ be an even integer. Suppose that $\ell > 3$ is a prime such that $\mathrm{ord}_\ell((p^k-1)(B_k/2k)) > 0$, where B_k is the k^{th} Bernoulli number. Then there exists a normalised eigenform (for all T_q for primes $q \neq p$) $f = \sum_{n=1}^{\infty} a_n q^n \in S_k(\Gamma_0(p))$, and some prime ideal $\lambda|\ell$ in the field of definition $\mathbb{Q}_f = \mathbb{Q}(\{a_n\})$ such that*

$$a_q \equiv 1 + q^{k-1} \bmod \lambda$$

for all primes $q \neq p$.

If $\mathrm{ord}_\ell(B_k/2k) > 0$ then f may be taken to be a normalised eigenform in $S_k(\mathrm{SL}_2(\mathbb{Z}))$, and this is the straightforward generalisation of Ramanujan's congruence. Here we are more concerned with the case that $\mathrm{ord}_\ell(B_k/2k) = 0$ but $\ell \mid (p^k - 1)$, and this is where it becomes necessary, in general, to increase the level.

G. Harder was led to believe that such congruences (and others) exist, via reasoning involving Eisenstein cohomology [H]. In Section 2 we give a proof, mildly generalising a well-known proof of Ramanujan's congruence and its analogues. (We construct an Eisenstein series of weight k for $\Gamma_0(p)$, vanishing mod ℓ at both cusps.

Date: April 1st, 2014.
1991 *Mathematics Subject Classification.* 11F33.
Key words and phrases. Congruences of modular forms.

We lift it to a cusp form in characteristic 0, then show that this may be replaced by a Hecke eigenform, using the Deligne-Serre lemma.) In Section 3 we view such congruences from a direction different from Harder's, as connected with the Bloch-Kato conjecture for a partial Riemann zeta function with the Euler factor at p missing. An ℓ as in the previous paragraph occurs in the value at $s = k$ of this partial zeta value only because of the missing Euler factor, so we still follow Harder in describing these congruences as being of local origin. In Section 4 we use this (and Theorem 1.1 to give new proofs of theorems of Billerey and Menares, after reformulating their conjecture on level-raising for reducible Galois representations. (We are grateful to an anonymous referee for directing us to the preprint of Billerey and Menares.) In Section 5 we look at some numerical examples, in particular the case in which $p = 2$ and ℓ is a Mersenne prime.

2. Proof of Theorem 1.1

2.1. **Definitions and notation.** Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$, where $q = e^{2\pi i z}$, be an element of the space $M_k(\mathrm{SL}_2(\mathbb{Z}))$ of modular forms of weight k for the full modular group. The subspace $S_k(\mathrm{SL}_2(\mathbb{Z}))$ of cusp forms is the kernel of the map $f \mapsto f([\infty]) = a_0$. It has a complement spanned by the weight k Eisenstein series, which can be scaled to have the following q-expansion: $F_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$. The Bernoulli numbers B_n are defined by $\sum_{n=0}^{\infty} B_n x^n/n! = \frac{x}{e^x-1}$. For any positive even integer k we have $\zeta(k) = (-1)^{(k/2)-1} \frac{(2\pi)^k}{2(k!)} B_k$ and $\zeta(1-k) = -B_k/k$.

For any prime number p we have the congruence subgroup $\Gamma_0(p)$ of $\mathrm{SL}_2(\mathbb{Z})$ defined by the condition $p \mid c$. The action of $\Gamma_0(p)$ on $\mathbb{P}^1(\mathbb{Q})$ has two orbits, represented by 0 and ∞, so $\Gamma_0(p)\backslash\mathfrak{H}$ (the complex points of the open modular curve $Y_0(p)$) is compactified to $\Gamma_0(p)\backslash\mathfrak{H}^*$ (i.e. $X_0(p)(\mathbb{C})$) by the addition of the two cusps $[0]$ and $[\infty]$. The subspace $S_k(\Gamma_0(p))$ of $M_k(\Gamma_0(p))$ is the kernel of $f \mapsto (f([\infty]), f([0]))$, and has a 2-dimensional complement spanned by F_k and $H_k(z) := F_k(pz)$. Since $M_k(\mathrm{SL}_2(\mathbb{Z})) \subseteq M_k(\Gamma_0(p))$, it is clear that $F_k(z) \in M_k(\Gamma_0(p))$, but it is also easy to check that $H_k \in M_k(\Gamma_0(p))$. Of course, $H_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^{pn}$.

Associated with the matrix $\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$ we have the operator W_p defined by $W_p f(z) = z^{-k} f(-1/pz)$, and it is easy to check that W_p maps $M_k(\Gamma_0(p))$ to itself. We would also scale by $p^{-k/2}$ if we wanted an involution (the Fricke involution). Note that $z \mapsto -1/pz$ exchanges the cusps $[0]$ and $[\infty]$.

For any prime q let $T_q f(z) = q^{(k/2)-1} \left(\sum_{b=0}^{q-1} f(\frac{z+b}{q}) + f(qz) \right)$. This Hecke operator preserves $M_k(\mathrm{SL}_2(\mathbb{Z}))$ and $S_k(\mathrm{SL}_2(\mathbb{Z}))$, and for $q \neq p$ it preserves $M_k(\Gamma_0(p))$ and $S_k(\Gamma_0(p))$. The Eisenstein series F_k is an eigenfunction for each T_q, with eigenvalue $1 + q^{k-1}$, and the same can be said of H_k if we restrict to $q \neq p$. The space $S_k(\mathrm{SL}_2(\mathbb{Z}))$ has a basis of simultaneous eigenforms for all the T_q. If $f = \sum_{n=1}^{\infty} a_n q^n$ is such an eigenform then necessarily $a_1 \neq 0$, and if f is scaled such that $a_1 = 1$ then it is said to be normalised. If $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ then (abusing notation) $f(pz) \in S_k(\Gamma_0(p))$. If $f(z)$ is an eigenform for all the T_q then $f(pz)$ is an eigenform for all the T_q with $q \neq p$. The space of *old forms* is spanned by the $f(z)$ and $f(pz)$ for $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$. It has a complement in $S_k(\Gamma_0(p))$, the new subspace, spanned by normalised simultaneous eigenforms, for all $q \neq p$, which are also eigenfunctions for the operator U_p such that $U_p f(z) = p^{(k/2)-1} \left(\sum_{b=0}^{p-1} f(\frac{z+b}{p}) \right)$.

Above we have considered complex vector spaces of modular forms and cusp forms, defined as spaces of certain holomorphic functions on the upper half plane, but for arithmetic purposes it is useful to adopt Katz's definition of a modular form over a ring R as a certain functor on a category of elliptic curves over R-algebras, with level structure [K]. A convenient reference for the definition is Section 1 of [E]. Let $S_k(\Gamma_0(p), \overline{\mathbb{Z}}_\ell)$ be the $\overline{\mathbb{Z}}_\ell$-module of cusp forms over $\overline{\mathbb{Z}}_\ell$ of weight k. In the notation of [E], this is $M^0(p, k, \epsilon)_{\overline{\mathbb{Z}}_\ell}$ with the character ϵ chosen to be trivial. Likewise we consider $S_k(\Gamma_0(p), \overline{\mathbb{F}}_\ell)$.

2.2. **The proof.** Recall the normalised Eisenstein series F_k, and $H_k(z) := F_k(pz)$, both in $M_k(\Gamma_0(p))$. They have the same constant term at $[\infty]$, so $F_k - H_k$ is 0 at $[\infty]$. Our aim is to construct a cusp form modulo ℓ, so we need the constant terms at both cusps to be divisible by ℓ. For $F_k - H_k$ we do not know what is happening at $[0]$. Since W_p swaps the cusps, $W_p(F_k - H_k)$ is 0 at $[0]$. To see what happens now at $[\infty]$,

$$W_p F_k(z) = z^{-k} F_k(-1/pz) = z^{-k}(pz)^k F_k(pz) = p^k H_k(z);$$

$$W_p H_k(z) = z^{-k} H_k(-1/pz) = z^{-k} F_k(-1/z) = z^{-k} z^k F_k(z) = F_k(z).$$

Hence $W_p(F_k - H_k) = p^k H_k(z) - F_k(z)$, and its constant term at $[\infty]$ is $(p^k - 1)(-B_k/2k)$, which *is* 0 (mod ℓ). It follows from the q-expansion principle that the reduction of $W_p(F_k - H_k)$ gives rise to an element $\overline{g}$ of $S_k(\Gamma_0(p), \mathbb{F}_\ell)$. By [E, Proposition 1.10], the reduction map from $S_k(\Gamma_0(p), \overline{\mathbb{Z}}_\ell)$ to $S_k(\Gamma_0(p), \overline{\mathbb{F}}_\ell)$ is surjective. (This is where we use $\ell > 3$.) Hence $\overline{g}$ is the reduction of some element $g \in S_k(\Gamma_0(p), O'_{\lambda'})$, with $O'_{\lambda'}$ the ring of integers in some finite extension $K'_{\lambda'}$ of $\mathbb{Q}_\ell$. Let $\mathbb{F}'$ be the residue field of $O'_{\lambda'}$. The Hecke operators T_q for primes $q \neq p$ commute and act on $S_k(\Gamma_0(p), \mathbb{F}')$, with $\overline{g}$ a common eigenvector, eigenvalue $1 + q^{k-1}$ for T_q. By the Deligne-Serre lemma [DeSe, Lemme 6.11], there exists a common eigenvector $f' \in S_k(\Gamma_0(p), O_\lambda)$, with O_λ the ring of integers in some finite extension K_λ of $K'_{\lambda'}$, with eigenvalues $a_q \equiv 1 + q^{k-1} \pmod{\lambda}$. It is easy now to see that f' arises from an f as in the theorem, via an embedding of $\mathbb{Q}_f$ into K_λ.

2.3. **A remark on the case $k = 2$.** It is natural to wonder whether Theorem 1.1 remains true in the case $k = 2$. In general it does not, for the following reason. By a famous theorem of Mazur [M, Prop. 5.12(ii)], such a congruence holds for some cuspidal Hecke eigenform $f \in S_2(\Gamma_0(p))$ if and only if ℓ divides the numerator of $(p-1)/12$. But $p^2 - 1 = (p-1)(p+1)$, so it is possible for ℓ to divide $p^2 - 1$ (by dividing $(p+1)$) without there being such a congruence, for example when $p = 19$ and $\ell = 5$.

2.4. **A remark on the cases $\ell = 2$ and 3.** We are grateful to A. Ghitza for pointing out that, by [E, Lemma 1.9(1)], the reduction map from $S_k(\Gamma_1(p), \overline{\mathbb{Z}}_\ell)$ to $S_k(\Gamma_1(p), \overline{\mathbb{F}}_\ell)$ is surjective. Hence in the above proof, $\overline{g}$ is the reduction of some element $g \in S_k(\Gamma_1(p), O'_{\lambda'})$, even when $\ell = 2$ or 3. Since $\overline{g}$ has trivial character, it is to be expected that often g will also have trivial character, and Ghitza showed us several examples where Theorem 1.1 seems to work even for $\ell = 2$ and 3. But, whether or not it ever happens, we are in general unable to exclude the possibility that g has non-trivial character (with trivial reduction, hence of ℓ-power order), and cannot be replaced by another g with trivial character. However, in the case that $\ell = 3$ and $p \equiv 2 \pmod 3$, there is no such non-trivial character of 3-power

order, so we can extend the theorem to that case, at least. Note that Carayol's Lemma [E, Proposition 1.10] requires the irreducibility of the 2-dimensional Galois representation attached to $\overline{g}$, which does not hold here.

3. Comparison with the Bloch-Kato formula for a partial zeta function

Let k, p, ℓ, λ and $f = \sum_{n=1}^{\infty} a_n q^n$ be as in Theorem 1.1, with also $\ell \neq p$, and let $K = \mathbb{Q}_f$. By a well-known theorem of Deligne [De], there exists a continuous representation

$$\rho_f = \rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_\lambda),$$

unramified outside ℓp, such that if $q \nmid \ell p$ is a prime, and Frob_q is an arithmetic Frobenius element, then

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_q^{-1})) = a_q, \ \det(\rho_f(\mathrm{Frob}_q^{-1})) = q^{k-1}.$$

One can conjugate so that ρ_f takes values in $\mathrm{GL}_2(O_\lambda)$, then reduce $\pmod{\lambda}$ to get a continuous representation $\overline{\rho}_f = \overline{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$. This is in general dependent on a choice of invariant O_λ-lattice, but its irreducible composition factors are well-defined.

$\mathrm{Tr}(\overline{\rho}_f(\mathrm{Frob}_q^{-1})) = \overline{a_q} = 1 + q^{k-1}$ in $\mathbb{F}_\lambda$. It follows then, from the Brauer-Nesbitt theorem (and $\ell > 2$) and the Cebotarev density theorem, that the composition factors of $\overline{\rho}_f$ are the trivial one-dimensional module $\mathbb{F}_\lambda$ and its Tate twist $\mathbb{F}_\lambda(1-k)$.

By a well-known argument of Ribet [R1, Proposition 2.1], it is possible to choose the invariant O_λ-lattice in such a way that $\overline{\rho}_f$ is realised on a space V such that

$$0 \longrightarrow \mathbb{F}_\lambda(1-k) \longrightarrow V \xrightarrow{\pi} \mathbb{F}_\lambda \longrightarrow 0$$

is a non-split extension of $\mathbb{F}_\lambda[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-modules. Note that ρ_f is irreducible, by [R1, Proposition 4.1]. Let $v \in V$ be any element such that $\pi(v) = 1$, and define a cocycle $C : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\lambda(1-k)$ by $C(g) := g(v) - v$. The class $c := [C] \in H^1(\mathbb{Q}, \mathbb{F}_\lambda(1-k))$ is independent of the choice of v, and is non-zero because the extension is non-split. Let $i : \mathbb{F}_\lambda(1-k) \hookrightarrow (K_\lambda/O_\lambda)(1-k)$ be the inclusion (which depends on a choice of uniformiser in the case that λ is ramified), and let $d := i_*(c) \in H^1(\mathbb{Q}, (K_\lambda/O_\lambda)(1-k))$. If $(\ell-1) \nmid (k-1)$ (for example, if $\ell > k$) then $H^0(\mathbb{Q}, (K_\lambda/O_\lambda)(1-k))$ is trivial, so that i_* is injective and $d \neq 0$.

We would like to say that d belongs to a Bloch-Kato Selmer group, which we therefore now define. Following [BK, Section 3], for $q \neq \ell$ let

$$H^1_f(\mathbb{Q}_q, K_\lambda(1-k)) := \ker\big(H^1(D_q, K_\lambda(1-k)) \to H^1(I_q, K_\lambda(1-k))\big).$$

Here D_q is a decomposition subgroup at a prime above q, I_q is the inertia subgroup, and the cohomology is for continuous cocycles and coboundaries. For $q = \ell$ let

$$H^1_f(\mathbb{Q}_\ell, K_\lambda(1-k)) := \ker\big(H^1(D_\ell, K_\lambda(1-k)) \to H^1(D_\ell, K_\lambda(1-k) \otimes_{\mathbb{Q}_\ell} B_{\mathrm{crys}})\big).$$

(See [BK, Section 1], or [Fo, §2], for the definition of Fontaine's ring B_{crys}.) Let $H^1_f(\mathbb{Q}, K_\lambda(1-k))$ be the subspace of those elements of $H^1(\mathbb{Q}, K_\lambda(1-k))$ which, for all primes q, have local restriction lying in $H^1_f(\mathbb{Q}_q, K_\lambda(1-k))$. There is a natural exact sequence

$$0 \longrightarrow O_\lambda(1-k) \longrightarrow K_\lambda(1-k) \xrightarrow{\pi} (K_\lambda/O_\lambda)(1-k) \longrightarrow 0.$$

Let $H^1_f(\mathbb{Q}_q, (K_\lambda/O_\lambda)(1-k)) = \pi_* H^1_f(\mathbb{Q}_q, K_\lambda(1-k))$. Define the Selmer group $H^1_f(\mathbb{Q}, (K_\lambda/O_\lambda)(1-k))$ to be the subgroup of elements of $H^1(\mathbb{Q}, (K_\lambda/O_\lambda)(1-k))$

whose local restrictions lie in $H^1_f(\mathbb{Q}_q,(K_\lambda/O_\lambda)(1-k))$ for all primes q. Note that since $\ell\neq 2$ we may omit $q=\infty$. More generally, given a finite set Σ of primes with $\ell\notin\Sigma$, we define $H^1_\Sigma(\mathbb{Q},(K_\lambda/O_\lambda)(1-k))$ to be the subgroup of elements of $H^1(\mathbb{Q},(K_\lambda/O_\lambda)(1-k))$ whose local restrictions lie in $H^1_f(\mathbb{Q}_q,(K_\lambda/O_\lambda)(1-k))$ for all primes $q\notin\Sigma$.

Proposition 3.1. $d\in H^1_{\{p\}}(\mathbb{Q},(K_\lambda/O_\lambda)(1-k))$

Recall that $\rho_{f,\lambda}$ is unramified at all $q\nmid p\ell$. It is immediate that the restriction of d to $H^1(I_q,(K_\lambda/O_\lambda)(1-k))$ is 0, for all such q, then one deduces from [Br, Lemma 7.4] that $d\in H^1_f(\mathbb{Q}_q,(K_\lambda/O_\lambda)(1-k))$. Likewise, from the fact that $\rho_{f,\lambda}$ is crystalline at ℓ (recall $\ell\neq p$), one may deduce that $d\in H^1_f(\mathbb{Q}_\ell,(K_\lambda/O_\lambda)(1-k))$, in fact this is a direct consequence of the second part of [DFG, Proposition 2.2]. As a $\mathbb{Q}_\ell$-module for $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $K_\lambda(1-k)$ is simply a direct sum of copies of $\mathbb{Q}_\ell(1-k)$, in fact following through the definitions shows that $H^1_{\{p\}}(\mathbb{Q},(K_\lambda/O_\lambda)(1-k))$ is just a direct sum of copies of $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$, so projection to some factor gives us a non-zero element of $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$.

Now we start again, to arrive a different way at a non-zero element in $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$. Let $\zeta_\Sigma(s)$ be the partial Riemann zeta function, with the Euler factors at primes $q\in\Sigma$ omitted. The following is a reformulation of the ℓ-part of the Bloch-Kato conjecture, as in (59) of [DFG], similarly using the exact sequence in their Lemma 2.1.

Conjecture 3.2 (Case of ℓ-part of Bloch-Kato)**.** *If $\Sigma\neq\emptyset$ then*

$$\mathrm{ord}_\ell\left(\frac{\zeta_\Sigma(k)}{(2\pi i)^k}\right)=\mathrm{ord}_\ell\left(\frac{\mathrm{Tam}^0_\ell((\mathbb{Q}_\ell/\mathbb{Z}_\ell)(k))\ \#H^1_\Sigma(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))}{\#H^0(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))}\right). \tag{1}$$

We omit the definition of the Tamagawa factor $\mathrm{Tam}^0_\ell((\mathbb{Q}_\ell/\mathbb{Z}_\ell)(k))$, but note that (assuming $\ell>k$), its triviality is a direct consequence of [BK, Theorem 4.1(iii)]. The above instance of the Bloch-Kato conjecture is actually known to be true, by [BK, Theorem 6.1(i)]. Letting $\Sigma=\{p\}$ (again, recall $\ell\neq p$), $\zeta_{\{p\}}(k)=(1-p^{-k})\zeta(k)$, so if $\ell>k$ and $\ell\mid(p^k-1)$ then $\mathrm{ord}_\ell\left(\frac{\zeta_{\{p\}}(k)}{(2\pi i)^k}\right)>0$. So the formula implies that $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$ contains a non-zero element. (For this we do not even need to note that for $\ell>k$ we have $H^0(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$ trivial.)

This argument produces a non-zero element of $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$ for any prime $\ell>k$, $\ell\neq p$, such that $\mathrm{ord}_\ell\left(\frac{\zeta_{\{p\}}(k)}{(2\pi i)^k}\right)>0$. But for those with $\ell\mid(p^k-1)$ (the main concern of this paper), the existence of a non-zero element in $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$ may seem a little simpler. There is an exact sequence

$$0\to H^1_f(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))\to H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))\to H^1_f(\mathbb{Q}_p,\mathbb{Z}_\ell(k))^*\to 0.$$

(Here, $H^1_f(\mathbb{Q}_p,\mathbb{Z}_\ell(k))$ is the inverse image of $H^1_f(\mathbb{Q}_p,\mathbb{Q}_\ell(k))$.) This follows from [DFG, Lemma 2.1], given that $H^0(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(k))$ and $H^1_f(\mathbb{Q},\mathbb{Q}_\ell(k))$ are trivial. Then $\ell\mid(p^k-1)\implies\ell\mid\#H^0(\mathbb{Q}_p,(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(k))$, which is the torsion part of $H^1_f(\mathbb{Q}_p,\mathbb{Z}_\ell(k))$, whence the exact sequence implies that $\ell\mid\#H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$. But while the triviality of $H^0(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(k))$ is a simple consequence of $\ell>k$ (which implies $(\ell-1)\nmid k$), that of $H^1_f(\mathbb{Q},\mathbb{Q}_\ell(k))$, a consequence of the finiteness of $H^1_f(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(k))$, is much deeper.

What Proposition 3.1 shows is that such an element (of $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$) can also be obtained, via Ribet's construction, from the congruence in Theorem 1.1. If this were a case of the Bloch-Kato conjecture that was not already known to be true, this construction would provide some evidence. (This is exactly what happens in some other cases, e.g. the work of Brown on congruences between Saito-Kurokawa lifts and non-lifts [Br].) In some sense then the Bloch-Kato formula makes sense of the existence of the congruence.

Thinking back to §2.3, we should observe that when $k=2$ it is possible for there to be a non-zero element in $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$, whose existence is guaranteed by (1), but which does not arise from a congruence as above, for example when $p=19$ and $\ell=5$. If $k\geq 4$ and $\ell>k$, then (1) shows at least that if $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))\neq\{0\}$ then $\mathrm{ord}_\ell\left(\frac{\zeta_{\{p\}}(k)}{(2\pi i)^k}\right)>0$, so that by Theorem 1.1 there is a congruence, though if $\#H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))>\ell$ it does not imply that the classes arising from such congruences span the whole of $H^1_{\{p\}}(\mathbb{Q},(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$.

4. Alternative proofs of theorems of Billerey and Menares

The following is a reformulation of [BM, Conjecture 0.3]. We have also weakened their condition $\ell>k+1$ to $\ell>k$, and included an extra condition that $\ell\nmid N$. Condition (2) automatically excludes the possibility that $\ell\mid N$, but this seems difficult to justify, in fact Example 5.8 below suggests that we should not exclude $\ell\mid N$ (though in that example $\ell<k$).

Conjecture 4.1. *Consider an even integer $k\geq 4$, a square-free positive integer N (with set Σ_N of prime divisors) and a prime $\ell>k$, with $\ell\nmid N$. There exists a weight k* newform *$f=q+\sum_{n\geq 2}a_nq^n$ for $\Gamma_0(N)$, satisfying the congruence*

$$a_q\equiv 1+q^{k-1}\pmod{\lambda}\ \text{for all primes } q\nmid N\ell\ ,$$

where $\lambda\mid\ell$ in $\mathbb{Q}(\{a_n\})$, if and only if

(1) $\mathrm{ord}_\ell\left(\frac{\zeta_{\Sigma_N}(k)}{(2\pi i)^k}\right)>0$ *and*
(2) *for all primes p dividing N, $\ell\mid(p^k-1)(p^{k-2}-1)$.*

The necessity of these conditions (under the assumption $\ell\nmid N$) is Theorem 4.1 of [BM]. Condition (2) may be written in the form $(1+p^{k-1})^2\equiv(p^{k/2}+p^{(k/2)-1})^2 \pmod{\ell}$, and thereby viewed as an analogue of Ribet's level-raising condition. Its necessity is proved in the same way as in [R2, (2.2)], by considering the characters occurring in the $\pmod{\ell}$ Galois representation attached to f, restricted to a decomposition group at p. The proof in [BM] of the necessity of Condition (1) (assuming Condition (2)) is by an argument of Swinnerton-Dyer [SD, Lemma 8], applied to a certain Eisenstein series of level N, rather than level 1 as in [SD].

We offer now a completely different proof of the necessity of Condition (1) (independent of Condition (2)).

Proposition 4.2. *Given an even integer $k\geq 4$, a square-free positive integer N (with set Σ_N of prime divisors) and a prime $\ell>k$ such that $\ell\nmid N$, suppose that there exists a weight k newform $f=q+\sum_{n\geq 2}a_nq^n$ for $\Gamma_0(N)$, satisfying the congruence*

$$a_q\equiv 1+q^{k-1}\pmod{\lambda}\ \text{for all primes } q\nmid N\ell\ ,$$

where $\lambda\mid\ell$ in $\mathbb{Q}(\{a_n\})$. Then $\mathrm{ord}_\ell\left(\frac{\zeta_{\Sigma_N}(k)}{(2\pi i)^k}\right)>0$.

Proof. Let $K = \mathbb{Q}(\{a_n\})$. Let K_λ be the completion at λ, with ring of integers O_λ. Assuming the congruence, we may apply Ribet's construction to get a non-zero element of $H^1_{\Sigma_N}(\mathbb{Q}, (K_\lambda/O_\lambda)(1-k))$, just as in Proposition 3.1. Since $(K_\lambda/O_\lambda)(1-k)$ is isomorphic to a direct sum of a number of copies of $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k)$, we therefore have a non-zero element of $H^1_{\Sigma_N}(\mathbb{Q}, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))$. Looking back at Conjecture 3.2, and the discussion following it, we see that for $\ell > k$ it is a consequence of a theorem of Bloch and Kato that

$$\mathrm{ord}_\ell\left(\frac{\zeta_{\Sigma_N}(k)}{(2\pi i)^k}\right) = \mathrm{ord}_\ell\left(\#H^1_{\Sigma_N}(\mathbb{Q}, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-k))\right).$$

Hence $\mathrm{ord}_\ell\left(\frac{\zeta_{\Sigma_N}(k)}{(2\pi i)^k}\right) > 0$. Note that the condition $\ell \nmid N$ ensures that $\ell \notin \Sigma_N$, which is required. □

The sufficiency of Conditions (1) and (2) in Conjecture 4.1 is not known. (Again the case $k = 2$ is different, as discussed in [BM, Section 4] following Ribet [R3].) Billerey and Menares [BM, Theorem 4.3] prove a result in which "newform" is replaced by "eigenform" (for all T_q for primes $q \nmid N$ and U_p for primes $p \mid N$). Their proof is similar to our proof of Theorem 1.1, except that whereas we use an Eisenstein series of level p, they use one of level N, arranged to have constant terms divisible by ℓ at all cusps. This is quite a bit more difficult at composite level than at prime level, so we offer a different proof, starting from our Theorem 1.1. That we actually do not need to use Condition (2) is an indication of how far this falls short of proving Conjecture 4.1.

Proposition 4.3. *Given an even integer $k \geq 4$, a square-free positive integer N and a prime $\ell > k$, suppose that $\mathrm{ord}_\ell\left(\frac{\zeta_{\Sigma_N}(k)}{(2\pi i)^k}\right) > 0$. Then there exists a weight k eigenform $g = q + \sum_{n\geq 2} b_n q^n$ for $\Gamma_0(N)$, satisfying the congruence*

$$b_q \equiv 1 + q^{k-1} \pmod{\lambda} \text{ for all primes } q \nmid N\ell\ ,$$

where $\lambda \mid \ell$ in $\mathbb{Q}(\{b_n\})$.

Proof. Thanks to Condition (1), we may choose a prime $p_0 \mid N$ such that $\mathrm{ord}_\ell((p_0^k - 1)(B_k/2k)) > 0$. Now take f as in the conclusion of Theorem 1.1 (with $p = p_0$). The only problem with f is that it might not be an eigenvector for the U_p with $p \mid N$. First we replace f by the normalised newform f' in the same class. This f' is of level either 1 or p_0. In the latter case, f' is already an eigenvector for U_{p_0}. In either case, let $p \mid N$ be a prime such that f' is not an eigenvector for U_p (if such a p exists). If $f' = \sum c_n q^n$ then $\sum_{n=1}^\infty c_n n^{-s}$ has an Euler product. The factor at p is $(1 - c_p p^{-s} + p^{k-1-2s})^{-1}$. (Note that f' is an eigenvector for T_p.) In some suitable extension, $(1 - c_p X + p^{k-1}X^2) = (1 - \alpha X)(1 - \beta X)$. If we replace $f'(z)$ by $g(z) := f'(z) - \alpha f'(pz)$, the effect on the Dirichlet series is to multiply it by $(1 - \alpha p^{-s})$. By considering the effect of U_p on q-expansions, we see that g is an eigenvector for U_p, with eigenvalue β. It is still an eigenvector for those $U_{p'}$ and those T_q ($q \neq p$) for which f' was an eigenvector. This g may not yet be an eigenvector of U_p for all primes $p \mid N$, but we repeat the process until it is. □

As already noted, it is not necessary to assume Condition (2) for the above proposition. For a newform (which is what we really want) the eigenvalue of U_p would be $\pm p^{(k/2)-1}$. Examination of Billerey and Menares's proof (which uses Condition (2)) reveals that their eigenform actually has eigenvalue of U_p congruent

to $\pm p^{(k/2)-1} \pmod{\lambda}$. We can get the same if we assume Condition (2), which is equivalent to $(1-X)(1-p^{k-1}X) \equiv (1-\epsilon p^{k/2}X)(1-\epsilon p^{(k/2)-1}X) \pmod{\ell}$, for $\epsilon = \pm 1$. We simply choose α, in the above proof, to be whichever root is congruent to $\epsilon p^{k/2}$, noting that $c_p \equiv 1 + p^{k-1} \pmod{\lambda} \implies 1 - c_p X + p^{k-1}X^2 \equiv (1-X)(1-p^{k-1}X) \pmod{\lambda}$.

We are grateful to an anonymous referee for pointing out that in Proposition 4.3 $\Gamma_0(N)$ may be replaced by any congruence subgroup of $\Gamma_0(p)$, and essentially the same proof applies.

5. Examples

5.1. **Mersenne primes.** In seeking numerical examples, it is natural to consider first the smallest possible choice of p, namely $p = 2$. Moreover, if $\ell = 2^{p_0} - 1$ is a Mersenne prime then $\ell \mid 2^k - 1$ for any k that is a multiple of p_0, hopefully leading to some examples with relatively small k.

Theorem 5.1. *Let $M_{p_0} = 2^{p_0} - 1$ be a Mersenne prime for some odd prime p_0. For any integer $m \geq 1$, there exists a normalised eigenform $f \in S_{2mp_0}(\Gamma_0(2))$, and some prime ideal $\lambda | M_{p_0}$ in the field of coefficients $\mathbb{Q}_f$, such that*

$$a_q \equiv 1 + q^{2mp_0-1} \bmod \lambda$$

for all odd primes q, if and only if $\frac{M_{p_0}-1}{2p_0} \nmid m$.

Proof. First suppose that $\frac{M_{p_0}-1}{2p_0} \nmid m$. Let $k = 2mp_0$. Then $(M_{p_0} - 1) \nmid k$, which implies the M_{p_0}-integrality of $B_k/(2k)$, by direct application of [IR, Proposition 15.2.4]. (They describe this proposition as "often attributed to J. C. Adams". It seems to be part of the statement of Kummer's congruences.) Since $\ell \mid 2^k - 1$, as noted above, we have $\mathrm{ord}_\ell((2^k-1)(B_k/2k)) > 0$, hence the congruence, by Theorem 1.1.

Now suppose that $\frac{M_{p_0}-1}{2p_0} \mid m$.

$$2^k - 1 = (1+\ell)^{2m} - 1 = 2m\ell + \binom{2m}{2}\ell^2 + \ldots + \ell^{2m}.$$

It follows that $\mathrm{ord}_\ell(2^k - 1) = \mathrm{ord}_\ell(m) + 1$. If $(\ell - 1) \mid k$ (i.e. if $\frac{M_{p_0}-1}{2p_0} \mid m$) then $\mathrm{ord}_\ell(B_k) = -1$, by the von Staudt-Clausen Theorem, so $\mathrm{ord}_\ell((2^k - 1)(B_{2mp_0}/4mp_0)) = 0$. Now the existence of the congruence would contradict Proposition 4.2. □

Corollary 5.2. *With $p_0 > 3$ and M_{p_0} prime, there exists a form f, satisfying the required congruences, lying in $S_{2p_0}(\Gamma_0(2))$.*

Proof. The quantity $\frac{M_{p_0}-1}{2p_0}$ is clearly greater than 1 when $p_0 > 3$, so that $m = 1$ is always a valid choice. □

Notice that if $p_0 = 3$ then $\frac{M_3-1}{6} = 1$ and so no possible value for m exists. We shall exclude this case from now on. We consider only weights of the form $2mp_0$, since the weight must be even. Also note that $\frac{M_{p_0}-1}{2p_0}$ is necessarily an integer, by Fermat's Little Theorem.

Example 5.3. Take $p_0 = 5$ (giving the Mersenne prime $M_5 = 31$). Then $\frac{M_5-1}{10} = 3$, so as long as $m \not\equiv 0 \bmod 3$ we are guaranteed the existence of a normalised eigenform $f \in S_{10m}(\Gamma_0(2))$ such that (for all odd primes q)

$$a_q \equiv 1 + q^{10m-1} \bmod 31.$$

In particular take $m = 1$. Then one checks easily that $\dim(S_{10}(\Gamma_0(2))) = 1$, so there is a unique normalised eigenform contained in this space. It has q-expansion:

$$q + 16q^2 - 156q^3 + 256q^4 + 870q^5 + \cdots$$

and one verifies immediately that:

$$-156 \equiv 1 + 3^9 \bmod 31$$

$$870 \equiv 1 + 5^9 \bmod 31$$

and so on, observing directly the congruences $a_q \equiv 1 + q^9 \bmod 31$, guaranteed by the above corollary, for as many odd primes q as one cares to check.

For the choice $m = 2$ we find that $\dim(S_{20}(\Gamma_0(2))) = 2$, and there are two normalized eigenforms with q-expansions:

$$q - 512q^2 - 13092q^3 + 262144q^4 + 6546750q^5 + \cdots$$

$$q + 512q^2 - 53028q^3 + 262144q^4 - 5556930q^5 + \cdots$$

The second of these visibly satisfies the congruence $a_q \equiv 1 + q^{19} \bmod 31$ for the first few odd primes q.

For the case $m = 3$ we find that none of the normalised eigenforms in $S_{30}(\Gamma_0(2))$ satisfies the congruence, in accord with Theorem 5.1.

Example 5.4. Take $p_0 = 7$ (giving the Mersenne prime $M_7 = 127$). We easily see that $\frac{M_7-1}{14} = 9$, so as long as $m \not\equiv 0 \bmod 9$, we are guaranteed the existence of a normalised eigenform $f \in S_{14m}(\Gamma_0(2))$ such that (for all odd primes q)

$$a_q \equiv 1 + q^{14m-1} \bmod 127.$$

In particular, take $m = 1$. Then $\dim(S_{14}(\Gamma_0(2))) = 2$ and we have two normalised eigenforms with q-expansions:

$$q - 64q^2 - 1836q^3 + 4096q^4 + 3990q^5 + \cdots$$

$$q + 64q^2 + 1236q^3 + 4096q^4 - 57450q^5 + \cdots$$

It is the second of these that satisfies the congruence $a_q \equiv 1 + q^{13} \bmod 127$ for all odd primes q.

5.2. $\mathbf{p > 2.}$.

Harder gives an example with $p = 3$, $k = 10$ and $\ell = 61$ [H, Section 2.9]. We are grateful to an anonymous referee for encouraging us to present further examples with $p \neq 2$.

Example 5.5. Take $p = 13, k = 4$. We find $B_k/2k = -119 = -7 \cdot 17$, so $\ell = 7$ or 17. The computer package Magma tells us that $S_4(\Gamma_0(13))$ is 3-dimensional, spanned by newforms

$$f = q - 5q^2 - 7q^3 + 17q^4 - 7q^5 + 35q^6 - 13q^7 - 45q^8 + 22q^9 + 35q^{10} - 26q^{11} + \cdots$$

and

$$g = q + aq^2 + (-3a+4)q^3 + (a-4)q^4 + (a-2)q^5 + (a-12)q^6 + (11a-10)q^7 + (-11a+4)q^8 + (-15a+25)q^9 + (-a+4)q^{10} + (12a+34)q^{11} + \cdots,$$

where $a = (1 \pm \sqrt{17})/2$. If $f = \sum_{n=1}^{\infty} a_n q^n$ and $g = \sum_{n=1}^{\infty} b_n q^n$ then one easily checks that $a_n \equiv \sigma_3(n) \pmod 7$ for all $n \leq 11$, and $b_n \equiv \sigma_3(n) \pmod \lambda$ for all $n \leq 11$, where $(17) = \lambda^2$ in $\mathbb{Q}(a)$. Note that $a \equiv 9 \pmod \lambda$.

Example 5.6. Take $p = 7, k = 6$. Now $(7^6 - 1)B_6/12 = 1634/7 = 2 \cdot 19 \cdot 43/7$. Then $S_6(\Gamma_0(7))$ is 3-dimensional, spanned by newforms

$$f = q - 10q^2 - 14q^3 + 68q^4 - 56q^5 + 140q^6 - 49q^7 - 360q^8 - 47q^9 + 560q^{10} + 232q^{11} + \cdots$$

and

$$g = q + aq^2 + (-6a + 24)q^3 + (9a - 38)q^4 + (10a - 54)q^5 + (-30a + 36)q^6 + 49q^7 + (11a - 54)q^8 + (36a + 117)q^9 + (36a - 60)q^{10} + (-124a + 756)q^{11} + \cdots,$$

where $a = (9 \pm \sqrt{57})/2$. If $f = \sum_{n=1}^{\infty} a_n q^n$ and $g = \sum_{n=1}^{\infty} b_n q^n$ then one easily checks that $a_q \equiv 1 + q^5 \pmod{43}$ for all primes $q \leq 23$, except for $q = 7$, which divides the level. Also, $b_q \equiv 1 + q^5 \pmod \lambda$ for all primes $q \leq 23$, except for $q = 7$, where $(19) = \lambda^2$ in $\mathbb{Q}(a)$. Note that $a \equiv 14 \pmod \lambda$. Further, one may check that for all primes $q \leq 101$ except $q = 7$ and $q = 2$, we have $b_q \equiv 1 + q^5 \pmod{2 = \lambda\lambda'}$, even though 2 does not satisfy the condition $\ell > 3$. In fact, if we let λ be the divisor of (2) such that $a \equiv 0 \pmod \lambda$ then we have $b_q \equiv 1 + q^5 \pmod{\mathfrak{q}}$ for all primes $q \leq 101$, except $q = 7$. Since g is a Hecke eigenform, it follows from this (or can be checked directly) that $b_n \equiv \sigma_5(n)$ for all integers $1 \leq n \leq 101$ such that $7 \nmid n$. Since in this case the existence of the congruence is not guaranteed by Theorem 1.1, we would like to prove it by applying Sturm's theorem [St], which shows that two modular forms with all Fourier coefficients up to some bound satisfying a congruence, satisfy it for all Fourier coefficients. The condition $7 \nmid n$ may appear to be a problem, but, as pointed out by a referee, this can be fixed by a trick involving a character twist. Let χ be the quadratic character of conductor 7. Then $\chi(n)b_n \equiv \chi(n)\sigma_5(n)$ for em all integers $1 \leq n \leq 101$. These are Fourier coefficients for forms g_χ and $E_6^{\chi,\chi,1}$, both of which belong to $M_6(\Gamma_0(49))$, [DiSh, Theorem 4.5.2]. Since the constant term of $E_6^{\chi,\chi,1}$ (at ∞) is 0 [DiSh, Theorem 4.5.1], we have the congruence also for $n = 0$. Sturm's bound is $\frac{6}{12} \cdot 49 \cdot \left(1 + \frac{1}{7}\right) = 28$, so we can comfortably deduce the congruence between the Fourier coefficients of g_χ and $E_6^{\chi,\chi,1}$ for all n, hence between b_q and $1 + q^5$ for all primes $q \neq 7$.

Example 5.7. Take $p = 19, k = 4$. Now $(19^4 - 1)B_4/8 = -3 \cdot 181$. Then $S_4(\Gamma_0(19))$ is 4-dimensional, spanned by newforms

$$f = q - 3q^2 - 5q^3 + q^4 - 12q^5 + 15q^6 + 11q^7 + 21q^8 - 2q^9 + 36q^{10} - 54q^{11} + \cdots$$

and

$$g = q + aq^2 + (1/3)(-a^2 - 4a + 20)q^3 + (a^2 - 8)q^4 + (1/3)(a^2 - 8a + 7)q^5 + (1/3)(-7a^2 + 2a + 38)q^6 + (1/3)(-4a^2 + 8a + 17)q^7 + (3a^2 + 2a - 38)q^8 + (3a^2 - 29)q^9 + (1/3)(-5a^2 + 25a - 38)q^{10} + (1/3)(-a^2 + 8a + 23)q^{11} + \cdots,$$

where $a^3 - 3a^2 - 18a + 38 = 0$. If $f = \sum_{n=1}^{\infty} a_n q^n$ and $g = \sum_{n=1}^{\infty} b_n q^n$ then one easily checks that $a_q \equiv 1 + q^3 \pmod 3$ for all primes $q \leq 101$, except for $q = 19$, the level. Note that $19 \equiv 1 \pmod 3$, so this is not covered by the extension of Theorem 1.1 noted in §2.4. We found similar examples of apparent $\pmod 3$ congruences also at levels 37 and 73 (in weight 4). One checks also that $b_q \equiv 1 + q^5 \pmod \lambda$ for all primes $q \leq 11$, where λ is a degree-1 divisor of (181) such that $a \equiv 9 \pmod \lambda$.

Example 5.8. We modify the previous example by putting a factor of 3 in the level. We find that in $S_4(\Gamma_0(57))$ there is a newform

$$f = \sum_{n=1}^{\infty} a_n q^n = q + aq^2 - 3q^3 + (a^2 - 8)q^4 + (-3a^2 - 14a + 15)q^5 + \cdots ,$$

where $a^3 + 3a^2 - 12a + 6 = 0$, such that $a_q \equiv 1 + q^3 \pmod{\lambda}$, for all primes $q \leq 101$ except 3 and 19, where $(3) = \lambda^3$.

References

[BM] N. Billerey, R. Menares, On the modularity of reducible mod ℓ Galois representations, arXiv:1309.3717v2 [math.NT] 1 Oct. 2013.

[BK] S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift Volume I, 333–400, Progress in Mathematics, 86, Birkhäuser, Boston, 1990.

[Br] J. Brown, Saito-Kurokawa lifts and applications to the Bloch-Kato conjecture, *Compos. Math.* **143** (2007), 290–322.

[De] P. Deligne: *Formes modulaires et représentations l-adiques.* Sém. Bourbaki, éxp. 355, Lect. Notes Math., Vol. 179, 139–172, Springer, Berlin, 1969.

[DeSe] P. Deligne, J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. Ec. Norm. Sup.* **7** (1974), 507–530.

[DFG] F. Diamond, M. Flach, L. Guo, The Tamagawa number conjecture of adjoint motives of modular forms, *Ann. Sci. École Norm. Sup. (4)* **37** (2004), 663–727.

[DiSh] F. Diamond, J. Shurman, *A First Course in Modular Forms,* Graduate Texts in Mathematics 228, Springer, New York, 2005.

[E] B. Edixhoven, Serre's Conjecture, *in* Modular Forms and Fermat's Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.), 209–242, Springer-Verlag, New York, 1997.

[Fo] J.-M. Fontaine, Valeurs spéciales des fonctions L des motifs, Séminaire Bourbaki, Vol. 1991/92. *Astérisque* **206** (1992), Exp. No. 751, 4, 205–249.

[H] G. Harder, Secondary Operations in the Cohomology of Harish-Chandra Modules, http://www.math.uni-bonn.de/people/harder/Manuscripts/Eisenstein/SecOPs.pdf.

[IR] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory,* Second Edition, Springer-Verlag, New York, 1990.

[K] N. M. Katz, p-adic properties of modular schemes and modular forms, in *Modular Functions of One Variable III,* Lect. Notes Math. **350,** 69–190, Springer-Verlag, 1973.

[M] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33–186.

[R1] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162.

[R2] K. Ribet, Congruence relations between modular forms, *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, 503–514, PWN, Warsaw, 1984.

[R3] K. Ribet, Non-optimal levels of reducible mod ℓ Galois representations *or* Modularity of residually reducible representations, notes of a talk at C.R.M. Barcelona, 2010, http://math.berkeley.edu/ ribet/crm.pdf.

[St] J. Sturm, On the congruence of modular forms, in *Number theory (New York 1984–1985),* 275–280, Lect. Notes Math. **1240,** Springer-Verlag, 1987.

[SD] H. P. F. Swinnerton-Dyer: On l-adic representations and congruences for coefficients of modular forms. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 1–55. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

University of Sheffield, School of Mathematics and Statistics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.

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

E-mail address: daniel.fretwell@shef.ac.uk