ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 126 (2007) 193–199

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Congruences for modular forms of weights two and four

Scott Ahlgren [a,*,1], Mugurel Barcau [b]

[a] Department of Mathematics, University of Illinois, Urbana, IL 61801, USA

[b] Institute of Mathematics of the Romanian Academy, PO Box 1-764, RO-70700, Bucharest, Romania

Received 20 June 2006; revised 21 November 2006

Available online 6 February 2007

Communicated by David Goss

Abstract

We prove a conjecture of Calegari and Stein regarding mod p congruences between modular forms of weight four and the derivatives of modular forms of weight two.

MSC: 11F33; 11F11

1. Introduction

Suppose that $p \geqslant 5$ is prime, and let $M_k(\Gamma_0(p))$ (respectively $S_k(\Gamma_0(p))$) denote the usual complex vector space of modular forms (respectively cusp forms) of weight k on $\Gamma_0(p)$. Let $S_k(\Gamma_0(p), \mathbb{Z}) \subseteq S_k(\Gamma_0(p))$ consist of those forms whose Fourier expansion at ∞ has integral coefficients; this is a free $\mathbb{Z}$-module which contains a basis for $S_k(\Gamma_0(p))$ over $\mathbb{C}$ (see, for example, Theorem 3.5.2 of [6]).

If R is a ring, then define

$$S_k\big(\Gamma_0(p), R\big) := S_k\big(\Gamma_0(p), \mathbb{Z}\big) \otimes R. \tag{1.1}$$

* Corresponding author.

E-mail addresses: ahlgren@math.uiuc.edu (S. Ahlgren), mugurel.barcau@imar.ro (M. Barcau).

1 The first author thanks the National Science Foundation for its support through grant DMS 01-34577.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.11.012

The q-expansion principle guarantees that the natural map

$$S_k(\Gamma_0(p), R) \to R[[q]]$$

is injective. If f and g are two elements of $S_k(\Gamma_0(p), R)$ and I is an ideal of R, then by $f \equiv g \pmod{I}$ we will mean a term-by-term congruence between the q-expansions of f and g. Sections 12 and 13 of the survey article of Diamond and Im [3] contain further details on these issues.

We define operators Θ, U_p, and V_p via their actions on q-expansions:

$$\Theta\Big(\sum a(n)q^n\Big) := \sum na(n)q^n,$$
$$\sum a(n)q^n \mid U_p := \sum a(pn)q^n,$$
$$\sum a(n)q^n \mid V_p := \sum a(n)q^{pn}.$$

If $\gamma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$, $k \in \mathbb{N}$, and f is a function on the upper half-plane, then define the slash operator via

$$f(z)\big|_k \gamma := \det(\gamma)^{k/2}(cz+d)^{-k} f(\gamma z).$$

Then the Fricke involution on $S_k(\Gamma_0(p))$ is given by

$$f \mapsto f|_k w_p,$$

where $w_p := \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)$. The fields of rationality of f and $f \mid w_p$ are the same (see, for example, Section 3.1 of [5]). The action of w_p on those forms which lie in the new subspace of $S_k(\Gamma_0(p))$ is described by

$$w_p = -p^{1-k/2} U_p. \tag{1.2}$$

It follows that any newform is also an eigenform of w_p, with eigenvalue ± 1.

In a recent paper [2], Calegari and Stein formulate a number of conjectures related to their study of discriminants of Hecke algebras of prime level. Here we address one of these conjectures; in particular we recall

Conjecture 1. *(See [2, Conjecture 4].) Let $\mathcal{P}$ be the maximal ideal of $\overline{\mathbb{Z}}_p$. Suppose that $f \in S_2(\Gamma_0(p), \overline{\mathbb{Z}}_p)$ and $g \in S_4(\Gamma_0(p), \overline{\mathbb{Z}}_p)$ are eigenforms (for all of the Hecke operators) which satisfy $\Theta f \equiv g \pmod{\mathcal{P}}$. Then the eigenvalues of w_p for f and g have opposite signs.*

Our goal is to prove the following.

Theorem 1.1. *Conjecture* 1 *is true.*

Frank Calegari has pointed out that the truth of this conjecture can also be deduced from a deep theorem of Breuil and Mezard (Theorem 1.2 of [1]). Our proof uses only standard tools from the theory of modular forms modulo p.

2. Proof of Theorem 1.1

Suppose that f and g are as given in Conjecture 1. We may assume that each is normalized to have leading Fourier coefficient equal to 1. Let $K \subseteq \overline{\mathbb{Q}}_p$ be the field generated over $\mathbb{Q}$ by all of the coefficients of f and g; then K is a finite extension of $\mathbb{Q}$. Letting $\mathfrak{p}$ be the prime ideal of K corresponding to the inclusion $K \subseteq \overline{\mathbb{Q}}_p$, and letting $\mathcal{O}_\mathfrak{p} \subseteq K$ be the corresponding valuation ring, we see that

$$\Theta f \equiv g \pmod{\mathfrak{p}\mathcal{O}_\mathfrak{p}}.$$

Viewing K as embedded in $\mathbb{C}$, it will suffice to prove the following.

Theorem 2.1. *Suppose that K is a number field, that $p \geqslant 5$ is prime, that $\mathfrak{p}$ is a prime ideal of K over p, and that $\mathcal{O}_\mathfrak{p} \subseteq K$ is the corresponding valuation ring. Suppose that $f \in S_2(\Gamma_0(p)) \cap \mathcal{O}_\mathfrak{p}[\![q]\!]$ and $g \in S_4(\Gamma_0(p)) \cap \mathcal{O}_\mathfrak{p}[\![q]\!]$ are eigenforms of w_p, are not identically zero modulo $\mathfrak{p}$, and satisfy*

$$\Theta f \equiv g \pmod{\mathfrak{p}\mathcal{O}_\mathfrak{p}}.$$

Then the eigenvalues of f and g under w_p have opposite signs.

To begin the proof, we define, for even integers $k \geqslant 2$, the Eisenstein series

$$E_k(z) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

For $k \geqslant 4$ we have $E_k \in M_k(\mathrm{SL}_2(\mathbb{Z}))$, while for $k = 2$ the quasimodular form E_2 satisfies

$$E_2(-1/z) = z^2 E_2(z) + \frac{6z}{\pi i}. \tag{2.1}$$

Define

$$E_2^* := E_2 - pE_2 \mid V_p;$$

it is well known that $E_2^* \in M_2(\Gamma_0(p))$. We begin with an easy lemma.

Lemma 2.2. $E_2^*|_2 w_p = -E_2^*$.

Proof. We have

$$E_2^*|_2 w_p = \frac{1}{pz^2}\big(E_2(-1/pz) - pE_2(-1/z)\big).$$

The lemma now follows from a computation using (2.1). □

We require the operator $\partial : S_2(\Gamma_0(p)) \to S_4(\Gamma_0(p))$ defined by

$$\partial f := \Theta f - \frac{E_2 f}{6}. \tag{2.2}$$

We have the following result.

Lemma 2.3. *Suppose that $f \in S_2(\Gamma_0(p))$ has $f|_2 w_p = \epsilon f$, with $\epsilon \in \{\pm 1\}$. Then*

$$\partial f|_4 w_p = \epsilon\left(\partial f + \frac{E_2^* f}{6}\right).$$

Proof. On the space $S_k(\Gamma_0(p))$ we have

$$\Theta = \frac{1}{2\pi i}\frac{d}{dz}.$$

Using this fact together with a computation, we find that

$$\big(\Theta f(z)\big)\big|_4 w_p = \epsilon \Theta f(z) + \frac{\epsilon f(z)}{\pi i z}.$$

From (2.1) we find that

$$E_2(z)\big|_2 w_p = p E_2(pz) + \frac{6}{\pi i z}.$$

The lemma follows from a computation involving these facts together with (2.2). □

Suppose now that f and g satisfy the hypotheses of Theorem 2.1. In particular, we have

$$\Theta f \equiv g \pmod{\mathfrak{p}}. \tag{2.3}$$

Define ϵ by

$$f|_2 w_p = \epsilon f. \tag{2.4}$$

Our goal is to prove that $g|_4 w_p = -\epsilon g$. To this end, we assume by way of contradiction that

$$g|_4 w_p = \epsilon g. \tag{2.5}$$

Note that

$$E_2 \equiv E_2^* \pmod{p}$$

it follows from this fact together with (2.3) and (2.2) that

$$\partial f + \frac{E_2^* f}{6} \equiv g \pmod{\mathfrak{p}}.$$

Let π be a uniformizer for the local ring $\mathcal{O}_{\mathfrak{p}}$. We conclude that there exists a modular form $h \in S_4(\Gamma_0(p)) \cap \mathcal{O}_{\mathfrak{p}}[\![q]\!]$ such that

$$g - \partial f - \frac{E_2^* f}{6} = \pi h. \tag{2.6}$$

We now apply w_p to the equality (2.6). By (2.5), (2.4), Lemma 2.2 and Lemma 2.3, we obtain

$$\left(g - \partial f - \frac{E_2^* f}{6}\right)\bigg|_4 w_p = \epsilon g - \epsilon\left(\partial f + \frac{E_2^* f}{6}\right) + \epsilon \frac{E_2^* f}{6} = \epsilon(g - \partial f). \tag{2.7}$$

Combining (2.6) and (2.7) gives

$$g - \partial f = \epsilon \pi h|_4 w_p. \tag{2.8}$$

Combining (2.6) and (2.8), we conclude that

$$\frac{E_2^* f}{6} = \epsilon \pi h|_4 w_p - \pi h. \tag{2.9}$$

In other words, we have $\pi h|_4 w_p \in \mathcal{O}_{\mathfrak{p}}[\![q]\!]$ and

$$\frac{E_2^* f}{6} \equiv \epsilon \pi h|_4 w_p \pmod{\mathfrak{p}}. \tag{2.10}$$

We will derive a contradiction from (2.10) by showing that the two forms are of different filtration (we show below that the right side of (2.10) can be found at level one and weight $p+3$ modulo $\mathfrak{p}$, while the left side cannot).

For convenience, we will denote by M_k and S_k the spaces of modular forms and cusp forms of weight k on $\mathrm{SL}_2(\mathbb{Z})$ with coefficients in $\mathcal{O}_{\mathfrak{p}}$. Using an argument of Serre [5, Section 3.3], we see that there exists a cusp form $F \in S_{p+1}$ such that

$$F \equiv \frac{f}{6} \pmod{\mathfrak{p}}. \tag{2.11}$$

We next derive a similar result for the right side of (2.10).

Lemma 2.4. *If h, π, and ϵ are as in* (2.10)*, then there exists $H \in S_{p+3}$ such that*

$$H \equiv \epsilon \pi h|_4 w_p \pmod{\mathfrak{p}}. \tag{2.12}$$

Proof. We follow the argument of Serre mentioned above. We define

$$E(z) := E_{p-1}(z) - p^{p-1} E_{p-1}(z)\big|V_p. \tag{2.13}$$

Then we have $E(z) \equiv 1 \pmod{p}$ and

$$E(z)\big|_{p-1} w_p \equiv 0 \pmod{p^{\frac{p+1}{2}}}. \tag{2.14}$$

We define the usual trace map from $S_k(\Gamma_0(p))$ to $S_k(\Gamma_0(1))$ by

$$\mathrm{Tr}(f) := f + p^{1-k/2}(f|_k w_p)\big|U_p.$$

Then by (2.14) we obtain

$$\begin{aligned}\mathrm{Tr}\big(\epsilon\pi(h|_4 w_p)E\big) - \epsilon\pi(h|_4 w_p)E &= p^{1-(p+3)/2}\big(\big(\epsilon\pi(h|_4 w_p)E\big)\big|_{p+3} w_p\big)\big|U_p \\ &= \epsilon\pi p^{-(p+1)/2} h(E|_{p-1} w_p)\big|U_p \\ &\equiv 0 \pmod{\mathfrak{p}}.\end{aligned}$$

The form $H := \mathrm{Tr}(\epsilon\pi(h|_4 w_p)E) \in S_{p+3}$ satisfies the conclusions of the lemma. □

Letting $F \in S_{p+1}$ and $H \in S_{p+3}$ be defined by (2.11) and Lemma 2.4, and recalling that

$$E_2^* \equiv E_2 \equiv E_{p+1} \pmod{p},$$

we obtain the following congruence involving modular forms on $\mathrm{SL}_2(\mathbb{Z})$ with coefficients in $\mathcal{O}_{\mathfrak{p}}$:

$$H \equiv E_{p+1} F \pmod{\mathfrak{p}}. \tag{2.15}$$

We now require some elements of the theory of modular forms modulo $\mathfrak{p}$ as developed by Serre and Swinnerton-Dyer [7]; the book of Lang ([4], Chapter X) is also a good reference. As usual, define $Q := E_4$ and $R := E_6$. Then M_k can be identified with the set of isobaric polynomials of weight k in Q and R, and with coefficients in $\mathcal{O}_{\mathfrak{p}}$. Let A and B be the isobaric polynomials such that

$$E_{p-1} = A(Q, R), \qquad E_{p+1} = B(Q, R).$$

Let $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$, and denote the reduction map to $\mathbb{F}_{\mathfrak{p}}$ by $\bar{\ }$. By a standard abuse of notation, let $\overline{A}(Q, R)$ and $\overline{B}(Q, R)$ denote the polynomials in $\mathbb{F}_{\mathfrak{p}}[Q, R]$ (where Q and R are now regarded as indeterminates) obtained via reducing the coefficients of A and B.

If $f \in M_k$, then define the *filtration* $w(\overline{f})$ by

$$w(\overline{f}) := \inf\{k' \colon \text{ there exists } g \in M_{k'} \text{ with } \overline{f} = \overline{g}\}. \tag{2.16}$$

Here we record some basic properties (see, for example, [4, Chapter X, Theorem 7.5]).

Theorem 2.5. *Suppose that $f \in M_k$, and that $f = C(Q, R)$, where C is an isobaric polynomial of weight k.*

(1) *If $\overline{f} \neq 0$, then $w(\overline{f}) \equiv k \pmod{p-1}$.*
(2) *We have $w(\overline{f}) < k$ if and only if $\overline{A}(Q, R)$ divides $\overline{C}(Q, R)$.*

We now return to (2.15). Since $M_2 = \{0\}$, it follows from the first assertion of the theorem that $w(\overline{F}) = p+1$. By Theorem 7.3 of [4], Chapter X, we know that $\overline{B}(Q, R)$ is coprime to $\overline{A}(Q, R)$. Therefore we conclude from the second assertion of the theorem that

$$w(\overline{E_{p+1}F}) = 2p + 2. \tag{2.17}$$

However, this contradicts the fact that $H \in S_{p+3}$, and the theorem follows.

Acknowledgments

The authors thank Frank Calegari, Alex Ghitza and Steve Ullom for their helpful comments on a previous version of this paper.

References

[1] C. Breuil, A. Mézard, Multiplicités modulaires et représentations de $\mathrm{GL}_2(\mathbf{Z}_p)$ et de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ en $l = p$, Duke Math. J. 115 (2) (2002) 205–310, MR1944572 (2004i:11052).
[2] F. Calegari, W.A. Stein, Conjectures about discriminants of Hecke algebras of prime level, in: Algorithmic Number Theory, in: Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 140–152, MR2137350.
[3] F. Diamond, J. Im, Modular forms and modular curves, in: Seminar on Fermat's Last Theorem, Toronto, ON, 1993–1994, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133, MR1357209 (97g:11044).
[4] S. Lang, Introduction to Modular Forms, Springer, Berlin, 1995, Corrected reprint of the 1976 original, MR1363488 (96g:11037).
[5] J.-P. Serre, Formes modulaires et fonctions zêta p-adiques, in: Modular Functions of One Variable, III, Proc. Internat. Summer School, Univ. Antwerp, 1972, in: Lecture Notes in Math., vol. 350, Springer, Berlin, 1973, pp. 191–268, MR0404145 (53 #7949a).
[6] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton Univ. Press, Princeton, NJ, 1994, Reprint of the 1971 original, MR1291394 (95e:11048).
[7] H.P.F. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms, in: Modular Functions of One Variable, III, Proc. Internat. Summer School, Univ. Antwerp, 1972, in: Lecture Notes in Math., vol. 350, Springer, Berlin, 1973, pp. 1–55, MR0406931 (53 #10717a).