PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 142, Number 12, December 2014, Pages 4029–4038
S 0002-9939(2014)12162-9
Article electronically published on July 28, 2014

ON ATKIN AND SWINNERTON-DYER CONGRUENCES FOR NONCONGRUENCE MODULAR FORMS

JONAS KIBELBEK

(Communicated by Kathrin Bringmann)

Abstract. In 1985, Scholl showed that Fourier coefficients of noncongruence cusp forms satisfy an infinite family of congruences modulo powers of p, providing a framework for understanding the Atkin and Swinnerton-Dyer congruences. We show that solutions to the weight-k Scholl congruences can be rewritten, modulo the appropriate powers of p, as p-adic solutions of the corresponding linear recurrence relation. Finally, we show that there are spaces of cusp forms that do not admit any basis satisfying 3-term Atkin and Swinnerton-Dyer type congruences at supersingular places, settling a question raised by Atkin and Swinnerton-Dyer.

1. Introduction

For a finite-index congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$ and integer $k \geq 1$, any space $S_k(\Gamma)$ of weight k cusp forms admits a basis consisting of common eigenforms of the Hecke operators T_p for almost all primes p. A normalized Hecke newform has q-expansion $f = \sum_{n=1}^{\infty} a_n q^{n/M}$, where $q = e^{2\pi i z}$ and $a_1 = 1$. All a_n are algebraic integers, the sequence $\{a_n\}$ is multiplicative, and for each $p \nmid M$ and any m,

$$a_{pm} - A_p a_m + B_p a_{m/p} = 0, \tag{1.1}$$

where $A_p = a_p$ satisfies the Ramanujan conjecture $|A_p| \leq 2p^{(k-1)/2}$ and $B_p = p^{k-1}\zeta$, where ζ is a root of unity [1], [7]. As is conventional, we define $a_{m/p}$ to be 0 if m/p is not an integer.

In other words, the Dirichlet series $L(s, f) = \sum_{n=1}^{\infty} a_n n^{-s}$ has an Euler product

$$L(s, f) = \prod_{p \nmid M} \frac{1}{1 - A_p p^{-s} + B_p p^{-2s}} \prod_{p | M} \frac{1}{1 - a_p p^{-s}}.$$

Most subgroups of $SL_2(\mathbb{Z})$, however, are noncongruence; i.e., they do not contain any principle congruence subgroup $\Gamma(N)$. For each nonnegative integer g, there are only finitely many congruence subgroups with genus g, but there are infinitely many genus g noncongruence subgroups [5], [11]. While Hecke operators give us

Received by the editors February 2, 2012 and, in revised form, December 28, 2012.

2010 *Mathematics Subject Classification.* Primary 11F33; Secondary 11S31, 15A03, 11B37.

Key words and phrases. Atkin and Swinnerton-Dyer congruences, p-adic congruences, noncongruence modular forms.

This research was supported in part by NSF grant DMS-0801096 and NSA grant H98230-10-1-0195. Part of the research was done when the author was visiting the National Center for Theoretical Sciences in Hsinchu, Taiwan, and he thanks the NCTS for its hospitality. The author would like to thank Dr. Li for her encouragement and helpful suggestions, and is grateful for the referee's helpful comments, suggestions, and patience.

the rich theory of newforms in the congruence case, Hecke operators defined using double cosets yield no new information about noncongruence cusp forms, sending all genuinely noncongruence cusp forms to 0 [3].

For any finite-index noncongruence subgroup Γ of $SL_2(\mathbb{Z})$, the modular curve X_Γ has a model over a number field K with the cusp at infinity K-rational; we denote by μ the cusp width of $i\infty$. There are algebraic integers M and γ_∞, with M, ${\gamma_\infty}^\mu$, and $(M/\gamma_\infty)^\mu$ in A, the ring of integers of K, such that for any k, the d-dimensional space of noncongruence cusp forms $S_k(\Gamma)$ has a basis $\{f_i = \sum a_{i,n}q^{n/\mu}\}_{1\leq i\leq d}$ where each Fourier coefficient, for any n and i, satisfies $a_{i,n}{\gamma_\infty}^{-n} \in A[1/M]$. In other words, the coefficients $a_{i,n}$ are integral at all places $\mathfrak{p}$ not dividing the principal ideal (M), since the denominators involve only factors of M. In computed examples of noncongruence forms, the denominators of $a_{i,n}$ grow exponentially with n. (See examples in [8].) A folklore conjecture states that any cusp form f with algebraic Fourier coefficients is a cusp form for a congruence subgroup Γ if and only if its Fourier coefficients have bounded denominators.

In 1971, Atkin and Swinnerton-Dyer computed q-expansions for bases of several spaces of noncongruence cusp forms $S_k(\Gamma)$, with k even and with X_Γ defined over $\mathbb{Q}$ [2]. In their examples, they noted a remarkable fact reminiscent of equation (1.1). For each prime $p \nmid M$, they found a p-adic basis of forms such that for each basis form $f_i = \sum_{n=1}^{\infty} a_n q^{n/\mu}$ there is an algebriac integer A_p such that for all $m \geq 1$ and $n \geq 0$,

$$a_{mp^{n+1}} - A_p a_{mp^n} + p^{k-1}a_{mp^{n-1}} \equiv 0 \pmod{p^{(n+1)(k-1)}}, \tag{1.2}$$

where $|A_p| \leq 2p^{(k-1)/2}$.

The most significant progress towards understanding these congruences was Scholl's proof in [10] of long congruence relations for cusp forms in $S_k(\Gamma)$ for even $k \geq 4$; the case $k = 2$ was done by Katz in [6]. These proofs assume that X_Γ is defined over $\mathbb{Q}$, but similar arguments should apply to the general case.

Scholl defines a compatible family of $2d$-dimensional ℓ-adic Galois representations ρ_ℓ attached to $S_k(\Gamma)$, where each ρ_ℓ is unramified outside ℓM. For primes $p \nmid M$, the characteristic polynomial $H_p(T) \in \mathbb{Z}[T]$ of the Frobenius at p is independent of ℓ and has integral coefficients. Further, it can be factored as $H_p(T) = \prod_{i=1}^{2d}(T-\alpha_i)$, where all roots have absolute value $p^{(k-1)/2}$. We label the coefficients of $H_p(T)$ from C_{-d} to C_d by the equation $H_p(T) = \sum_{i=-d}^{d} C_i T^{d+i}$ to make Scholl's congruences easier to state and work with.

Scholl showed that any form $f = \sum a_n q^{n/\mu} \in S_k(\Gamma)$ with algebraic Fourier coefficients integral at p satisfies, for all $n \geq 0$ and $m \geq 1$,

$$S_{f,m,n} := \sum_{i=-d}^{d} C_i a_{mp^{n+i}} \equiv 0 \pmod{p^{(n+1)(k-1)}}. \tag{1.3}$$

(We denote by $S_{f,m,n}$ the expression on the left side in congruence (1.3).) If $d = 1$, this is precisely the 3-term ASD congruence (1.2). As above, we define a_n to be 0 if n is not an integer. Since the Fourier coefficients $a_{mp^{n+i}}$ are algebraic numbers, the congruence (1.3) is interpreted to mean

$$S_{f,m,n} \in p^{(n+1)(k-1)}\mathbb{A}[1/M],$$

where $\mathbb{A}$ denotes the ring of all algebraic integers.

For fixed f and m, the Scholl congruence (1.3) describes an infinite family of congruences on the sequence $\{a_{mp^n}\}_{n\geq 0}$. If instead of a family of congruences, we consider the linear recurrence relation corresponding to $S_{f,m,n}=0$,

$$\sum_{i=-d}^{d} C_i b_{n+i} = 0 \text{ for } n \geq d, \tag{1.4}$$

then it is well-known which sequences $\{b_n\}_{n\geq 0}$ satisfy this linear recursion. Writing $H_p(T)=\prod_{i=1}^{2d}(T-\alpha_i)$ and letting m_i count the number of $\alpha_j=\alpha_i$ with $j<i$, the general solution is $b_n=\sum_{i=1}^{2d}\kappa_i n^{m_i}{\alpha_i}^n$ for some constants κ_i. This motivates the following theorem describing solutions to the Scholl congruence.

Theorem 1.1 (Main Theorem). *Suppose all roots of*

$$H_p(T)=\prod_{i=1}^{2d}(T-\alpha_i)=\sum_{i=-d}^{d} C_i T^{i+d}\in\mathbb{Z}[T]$$

have size $p^{(k-1)/2}$, and let $\{b_n\}_{n\geq 0}$ be a sequence in some extension K_p of $\mathbb{Q}_p$. Denote by $\mathcal{Q}_p$ the splitting field of $H_p(T)$ over K_p. Let s be the number of roots of $H_p(T)$ with p-adic valuation less than $k-1$, and label these roots $\alpha_1,\dots,\alpha_s$. (So $d\leq s\leq 2d$, since the constant term C_{-d} of $H_p(T)$ is $\pm p^{d(k-1)}$.) We count multiplicities by defining m_i to be the number of $\alpha_j=\alpha_i$ with $j<i$. Then the following are equivalent:

- *The sequence $\{b_n\}_{n\geq 0}$ satisfies, for all $n\geq 0$,*

$$S_n := \sum_{i=-d}^{d} C_i b_{n+i}\equiv 0 \pmod{p^{(n+1)(k-1)}}.$$

- *The congruences $S_n\equiv 0 \pmod{p^{(n+1)(k-1)}}$ hold for $0\leq n<s$, and there exist constants $\kappa_i\in\mathcal{Q}_p$ such that*

$$b_n\equiv\sum_{i=1}^{s}\kappa_i n^{m_i}{\alpha_i}^n \pmod{p^{(n+1)(k-1)}}.$$

Our primary interest is to apply this theorem to sequences $b_n=a_{mp^n}$ of cusp form Fourier coefficients.

The p-adic valuations of the roots of $H_p(T)$ can be read directly from the Newton polygon of $H_p(T)$. This theorem shows that when we view the ASD or Scholl congruences p-adically, the roots of $H_p(T)$ with valuation $k-1$ have no effect on the congruences. Typically, half of the roots will be p-adic units and the other half will have valuation $k-1$; this is called the *ordinary* case (with $s=d$). If all roots are also distinct, we call the case *strongly ordinary.* Otherwise (for $s>d$), we have the *supersingular* case.

In the strongly ordinary case, Scholl notes ([10], Theorem 5.6) that by diagonalizing the action of the Frobenius, we obtain a p-adic basis of forms which satisfy the 3-term ASD congruences (1.2) and which actually satisfy two-term congruences; this corresponds precisely to the change of basis given by a matrix of the κ-coefficients of Theorem 1.1.[1] However, no method for constructing such a basis

[1] While Theorem 1.1 applies directly only to the mp^n-th Fourier coefficients for fixed m, numerical evidence suggests that the matrices of κ-coefficients are compatible for different m, so that in the strongly ordinary case, the same basis satisfies 3-term ASD congruences independent of m.

has been found in general. In fact, we give an example (developed in the final section) for which no 3-term congruences exist at supersingular places; this appears to be typical for the supersingular case.

Theorem 1.2. *For the (unique, up to conjugacy) finite index subgroup $\Gamma \subset SL_2(\mathbb{Z})$ with model $X_\Gamma : y^2 = x^5+2$, there is no basis of forms in $S_2(\Gamma)$ satisfying three-term ASD congruences at any odd prime $p \equiv 2, 3 \pmod 5$.*

Theorem 1.1 also has implications for the unbounded denominator conjecture (that every genuinely noncongruence cusp form with algebraic Fourier coefficients has unbounded denominators):

Proposition 1.3. *If f is a cusp form with algebraic Fourier coefficients a_n whose denominators are bounded, then the κ-coefficients described in Theorem* 1.1 *corresponding to the sequence $\{b_n\}$, where $b_n = a_{mp^n}$, are algebraic over $\mathbb{Q}$.*

Proof. Given any cusp form f with algebraic Fourier coefficients coming from a degree d Galois extension K of $\mathbb{Q}$ and having bounded denominators, we can obtain d cusp forms with integer Fourier coefficients whose span contains f. (Take an algebraically integral basis for K as a vector space over $\mathbb{Q}$ and write f in terms of this basis. By taking linear combinations of f and its Galois conjugates, we can obtain the d cusp forms which are the components of f with respect to the basis of K over $\mathbb{Q}$. Multiplying by a sufficiently large integer clears all denominators, giving us forms with integer Fourier coefficients.)

These cusp forms with integer Fourier coefficients will satisfy a long Scholl congruence (1.3), and they also must satisfy the Rankin bound $a_n = \mathcal{O}(n^{k/2-1/5})$ [9]. Thus, for sufficiently large n, the Scholl congruence on Fourier coefficients a_{mp^n} becomes a linear recurrence (just as is the case for congruence cusp forms) because it determines a_{mp^n} modulo p^{nk-C} for some fixed integer C, while the Rankin bound will eventually leave room for only one integer solution a_{mp^n} to this congruence. Solving this linear recurrence yields algebraic κ-coefficients; the κ-coefficients for our original form f will just be an algebraic linear combination of the κ-coefficients from its component forms, and thus are also algebraic numbers. □

Thus, if it can be shown that some κ-coefficient for a sequence of Fourier coefficients a_{mp^n} is transcendental over $\mathbb{Q}$, the corresponding cusp form must have unbounded denominators. Indeed, we expect the κ-coefficients coming from genuinely noncongruence forms to be transcendental, but new ideas or information would be needed for a proof. Even the knowledge that a cusp form f has unbounded denominators is by itself not enough to conclude that any of its κ-coefficients are transcendental.

2. Proof of the Main Theorem

Given a polynomial $H_p(T) = \prod_{i=1}^{2d}(T-\alpha_i) = \sum_{i=-d}^{d} C_i T^{d+i} \in \mathbb{Z}[T]$ with each root α_i having size $p^{(k-1)/2}$, we consider sequences $\{b_i\}_{i\geq 0}$ in an extension K_p of $\mathbb{Q}_p$ that satisfy Scholl congruences for all $n \geq 0$:

$$S_n := \sum_{i=-d}^{d} C_i b_{n+i} \equiv 0 \pmod{p^{(n+1)(k-1)}}.$$

This independence of m would be implied by the integrality at p of a formal group law associated to $S_k(\Gamma)$, as is discussed briefly in section 3.

We begin with the simple observation that the Scholl congruences are only sensitive to b_i modulo $p^{(i+1)(k-1)}$.

Proposition 2.1. *If the sequence* $\{b_i\}$ *satisfies the Scholl congruences, then so does any sequence* $\{c_i\}$ *with* $c_i \equiv b_i \pmod{p^{(i+1)(k-1)}}$.

Proof. Since all coefficients C_i are in $\mathbb{Z}$ and all roots of $H_p(T)$ have absolute value $p^{(k-1)/2}$, we must have $C_{-i} \equiv 0 \pmod{p^{i(k-1)}}$ for $1 \le i \le d$. The proposition immediately follows. □

We denote by $\mathcal{Q}_p$ the splitting field of $H_p(T)$ over K_p and write $H_p(T) = \prod_{i=1}^{2d}(T-\alpha_i) \in \mathcal{Q}_p[T]$, where the first s roots have p-adic valuation less than $k-1$. We have $d \le s \le 2d$ because there are at most d roots with valuation $k-1$. Let $H_p^*(T) = \prod_{i=1}^{s}(T-\alpha_i)$; we label the coefficients of $H_p^*(T)$ by

$$H_p^*(T) = \sum_{i=d-s}^{d} C_i^* T^{s-d+i}$$

and define linear combinations of entries in the sequence $\{b_i\}$:

$$S_n^* := \sum_{i=d-s}^{d} C_i^* b_{n+i}. \tag{2.1}$$

Lemma 2.2. *If a sequence* $\{b_i\}$ *is integral at* p *and satisfies all congruences* $S_n \equiv 0 \pmod{p^{(n+1)(k-1)}}$*, then it also satisfies all congruences* $S_n^* \equiv 0 \pmod{p^{(n+1)(k-1)}}$.

Proof. The proof is by induction on n.

Define coefficients B_i by $H_p(T)/H_p^*(T) = \prod_{i=s+1}^{2d}(T-\alpha_i) = \sum_{i=0}^{2d-s} B_i T^{2d-s-i}$. Since the roots of this polynomial are precisely those α_i such that $p^{k-1}|\alpha_i$, we have $p^{i(k-1)} \mid B_i$. In particular, $B_0 = 1$ and $H_p(T) \equiv T^{2d-s}H_p^*(T) \pmod{p^{k-1}}$, which implies $C_i \equiv C_i^* \pmod{p^{k-1}}$ for $0 \le i \le d$, establishing the base case of induction $S_0^* \equiv S_0 \equiv 0 \pmod{p^{k-1}}$.

Now we suppose that $S_n^* \equiv 0 \pmod{p^{(n+1)(k-1)}}$ for all $n < N$. Then $S_N \equiv 0 \pmod{p^{(N+1)(k-1)}}$ implies that $S_N^* \equiv 0 \pmod{p^{(N+1)(k-1)}}$ because

$$S_N \equiv \sum_{j=0}^{2d-s} B_j S_{N-j}^* \equiv S_N^* \pmod{p^{(N+1)(k-1)}}.$$ □

We can now prove the main result.

Proof of the Main Theorem. It is clear by Proposition 2.1 that if

$$b_n \equiv \sum_{i=1}^{s} \kappa_i n^{m_i} {\alpha_i}^n \pmod{p^{(n+1)(k-1)}}$$

for some constants $\kappa_i \in \mathcal{Q}_p$, and $S_n \equiv 0 \pmod{p^{(n+1)(k-1)}}$ for $0 \le n < s$, then $S_n \equiv 0 \pmod{p^{(n+1)(k-1)}}$ for all n.

To show the converse, we consider the linear recursion relation over $\mathcal{Q}_p$ given by

$$c_{n+d} = -\sum_{i=d-s}^{d-1} C_i^* c_{n+i}.$$

For any s initial conditions, this determines a unique sequence $\{c_n\}$; the vector space of such sequences is s-dimensional over $\mathcal{Q}_p$. It is well-known that a basis of the space is given by $\{n^{m_i}{\alpha_i}^n\}_{1\leq i\leq s}$. (This can be seen by taking the partial fraction decomposition of the generating function of this linear recursion, which has the form $\sum_{n=0}^{\infty} c_n x^n = \frac{f(x)}{H_p^*(x)}$, with $f(x)$ a polynomial of degree $< s$ determined by the initial conditions.)

The confluent Vandermonde matrix associated with this linear recurrence is $\mathcal{A} := ((i-1)^{m_j}{\alpha_j}^{i-1})_{1\leq i,j\leq s}$. We denote by $\boldsymbol{\alpha}$ the upper-triangular matrix with (i,j)-th entry $\binom{m_j}{m_i}\alpha_i$ if $\alpha_i = \alpha_j$ with $i < j$, and 0 otherwise. So a typical example, with $\alpha_1 = \alpha_2 = \alpha_3$ and $m_4, m_s = 0$ (i.e., α_4 and α_s are not repeated roots), is

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & 0 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_1 & \alpha_1 & \alpha_4 & \cdots & \alpha_s \\ {\alpha_1}^2 & 2{\alpha_1}^2 & 4{\alpha_1}^2 & {\alpha_4}^2 & \cdots & {\alpha_s}^2 \\ {\alpha_1}^3 & 3{\alpha_1}^3 & 9{\alpha_1}^3 & {\alpha_4}^3 & \cdots & {\alpha_s}^3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ {\alpha_1}^{s-1} & (s-1){\alpha_1}^{s-1} & (s-1)^2{\alpha_1}^{s-1} & {\alpha_4}^{s-1} & \cdots & {\alpha_s}^{s-1} \end{pmatrix}$$

and

$$\boldsymbol{\alpha} = \begin{pmatrix} \alpha_1 & \alpha_1 & \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_1 & 2\alpha_1 & 0 & \cdots & 0 \\ 0 & 0 & \alpha_1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \alpha_4 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \alpha_s \end{pmatrix}.$$

These matrices allow us to concisely describe solutions to the linear recurrence above because

$$\mathcal{A}\boldsymbol{\alpha}^n = ((n+i-1)^{m_j}{\alpha_j}^{n+i-1})_{1\leq i,j\leq s}.$$

We will use this to find the solution to the linear recurrence that matches the sequence $\{b_j\}_{j\geq 0}$ in s consecutive terms, starting with the n-th term b_n, and we compare these solutions for different values of n. We must find the unique constants $\kappa_{i,n}$ such that

$$b_{n+j} = \sum_{i=1}^{s} \kappa_{i,n}(n+j)^{m_i}{\alpha_i}^{n+j} \tag{2.2}$$

for $0 \leq j \leq s-1$.

If we define the column vectors $\vec{\kappa}_n := \langle \kappa_{i,n}\rangle_{1\leq i\leq s}$ and $\vec{b}_n := \langle b_{n+j}\rangle_{0\leq j\leq s-1}$, then the system of equations can be rewritten in matrix form as

$$\vec{b}_n = \mathcal{A}\boldsymbol{\alpha}^n\vec{\kappa}_n.$$

Since $\mathcal{A}$ and $\boldsymbol{\alpha}$ are invertible, we have $\vec{\kappa}_n = \boldsymbol{\alpha}^{-n}\mathcal{A}^{-1}\vec{b}_n$.

This gives us the unique vector $\vec{k}_n$ such that equation (2.2) is satisfied for $0 \leq j \leq s-1$. If we compare the following term b_{n+s} from our Scholl congruence sequence with the corresponding term $\sum_{i=1}^{s} \kappa_{i,n}(n+s)^{m_i}\alpha^{n+s}$ in the linear recurrence sequence defined by $\vec{\kappa}_n$, then the congruence S^*_{n+s-d} is precisely the statement that these terms are congruent modulo $p^{(n+s-d+1)(k-1)}$. In fact, working modulo $p^{(n+s-d+1)(k-1)}$, we see from S^*_{N+s-d} for each $N \geq n$ that

$$b_{N+s} \equiv \sum_{i=1}^{s} \kappa_{i,n}(N+s)^{m_i}\alpha^{N+s} \pmod{p^{(n+s-d+1)(k-1)}}.$$

In particular, this shows that

$$\vec{b}_{n+1} = \mathcal{A}\boldsymbol{\alpha}^{n+1}\vec{\kappa}_{n+1} \equiv \mathcal{A}\boldsymbol{\alpha}^{n+1}\vec{\kappa}_n \pmod{p^{(n-d+1)(k-1)}}.$$

From this congruence, we will see that the vectors $\vec{\kappa}_n$ converge p-adically as $n \to \infty$. Denote the p-adic valuation of the determinant of $\mathcal{A}$ by $\delta := v_p(\det(\mathcal{A}))$. If we multiply the congruence on the left by $\mathcal{A}^{-1}$, we get

$$\boldsymbol{\alpha}^{n+1}\vec{\kappa}_{n+1} \equiv \boldsymbol{\alpha}^{n+1}\vec{\kappa}_n \pmod{p^{(n-d+1)(k-1)-\delta}}.$$

If all roots are distinct, this immediately gives us

$$\alpha_i^{n+1}\kappa_{i,n+1} \equiv \alpha_i^{n+1}\kappa_{i,n} \pmod{p^{(n-d+1)(k-1)-\delta}}.$$

If there are repeated roots, we get the same result after some straightforward row reduction. In any case, we have

$$\kappa_{i,n+1} \equiv \kappa_{i,n} \pmod{p^{(n-d+1)(k-1)-(n+1)v_p(\alpha_i)-\delta}}. \tag{2.3}$$

Recall that for $1 \leq i \leq s$, we have $v_p(\alpha_i) < k-1$. The power of congruence in (2.3) is, up to constant terms, just $n(k-1-v_p(\alpha_i))$, which grows arbitrarily large as n approaches infinity; thus the sequence $\kappa_{i,n}$ converges p-adically. We define $\kappa_i := \lim_{n\to\infty}\kappa_{i,n}$ and $\vec{\kappa} := \langle\kappa_i\rangle_{1\leq i\leq s}$.

We now claim that for all n,

$$b_n \equiv \sum_{i=1}^{s} \kappa_i n^{m_i}\alpha_i^n \pmod{p^{(n+1)(k-1)}}.$$

To show this for any particular n, we first choose N_n large enough so that $\vec{\kappa}_{N_n} \equiv \vec{\kappa} \pmod{p^{(n+1)(k-1)}}$; then it suffices to show that $\vec{b}_n \equiv \mathcal{A}\boldsymbol{\alpha}^n\vec{\kappa}_{N_n} \pmod{p^{(n+1)(k-1)}}$.

Notice that C^*_{d-s} has valuation $v_p(C^*_{d-s}) = (s-d)(k-1)$ since

$$C^*_{d-s}\left(\prod_{i=1}^{2d-s}\alpha_{s+i}\right) = p^{d(k-1)},$$

and each of the α_{s+i} appearing in the product has valuation $v_p(\alpha_{s+i}) = k-1$.

If we solve the congruence S^*_n for the lowest term, b_{n+d-s}, we get

$$b_{n+d-s} \equiv \frac{-\left(b_{n+d} + \ldots + C^*_{d-s-1}b_{n+d-s+1}\right)}{C^*_{d-s}} \pmod{p^{(n+1)(k-1)}},$$

which determines b_{n-d+s} modulo $p^{(n-d+s+1)(k-1)}$; and it suffices to know b_i modulo $p^{(i+1)(k-1)}$ for $n+d-s+1 \leq i \leq n+d$ to solve this congruence.

Since we know that $\vec{b}_{N_n} = \mathcal{A}\boldsymbol{\alpha}^{N_n}\vec{\kappa}_{N_n}$, the congruence $S^*_{N_n+s-d-1}$ is precisely the statement that

$$b_{N_n-1} \equiv \sum_{i=1}^{s} \kappa_{N_n}(N_n-1)^{m_i}\alpha_i^{N_n-1} \pmod{p^{(N_n)(k-1)}}.$$

Using the congruence S^*_{j+s-d}, we obtain $b_j \equiv \sum_{i=1}^{s} \kappa_{N_n} j^{m_i} \alpha_i^j \pmod{p^{(j+1)(k-1)}}$ for all $0 \le j < N_n$ by descending induction. In particular,

$$\vec{b}_n \equiv \mathcal{A}\boldsymbol{\alpha}^n \vec{\kappa}_{N_n} \equiv \mathcal{A}\boldsymbol{\alpha}^n \vec{\kappa} \pmod{p^{(n+1)(k-1)}},$$

which completes the proof of the theorem. □

3. Three-term congruences

For a d-dimensional space $S_k(\Gamma)$ of weight k forms, where X_Γ has a model defined over $\mathbb{Q}$ with the cusp at infinity $\mathbb{Q}$-rational, we choose a basis of d forms f_i with rational Fourier coefficients. For almost all primes p, the Fourier coefficients of each f_i satisfy $2d+1$-term Scholl congruences. We consider the sequence of mp^n-th Fourier coefficients a_{i,mp^n} of f_i, where m is coprime to p. In the strongly ordinary case there are d distinct unit roots α_j of $H_p(T)$. The remaining d roots are divisible by p^{k-1} and play no role in the Scholl congruences, and so we can find p-adic numbers $\kappa_{m,i,j}$ giving the coefficient of ${\alpha_j}^n$ in a_{i,mp^n} modulo $p^{(n+1)(k-1)}$. Thus, in the strongly ordinary case we have a $d \times d$ matrix $\boldsymbol{\kappa}_m := (\kappa_{m,i,j})_{1\le i,j\le d}$ of p-adic numbers, and the j-th row of $\boldsymbol{\kappa}_m^{-1}$ gives precisely the linear combination of our original basis $\{f_i\}$ such that the mp^n-th Fourier coefficient of the linear combination is simply ${\alpha_j}^n$ modulo $p^{(n+1)(k-1)}$.[2]

Consequently, considering only the mp^n-th Fourier coefficients, the basis of $S_k(\Gamma)$ given by the rows of $\boldsymbol{\kappa}_m^{-1}$ satisfies the 3-term ASD congruences associated with the polynomials $(T-\alpha_j)(T-p^{k-1}/\alpha_j)$.[3] To show that this basis satisfying 3-term ASD congruences at mp^n-th coefficients is independent of m, we would need to check that corresponding columns of $\boldsymbol{\kappa}_m$ for varying m are scalar multiples of each other, i.e., that there is some p-adic matrix $\boldsymbol{\kappa}$ such that for each m coprime to p, we have $\boldsymbol{\kappa}_m = \boldsymbol{\kappa}\boldsymbol{D}_m$ for some diagonal matrix $\boldsymbol{D}_m$. Numerical evidence suggests this is indeed the case at all strongly ordinary primes, and this can be proved for certain examples by constructing a formal group law out of Fourier coefficients for a basis of $S_k(\Gamma)$ that is integral at p (see Corollary 2.5 in [4]). In the case that $k = 2$, this is just the formal group of the Jacobian of X_Γ. The existence of these formal groups is hinted at by Scholl (note ii on p. 51 in [10]), and the author expects that such integral formal group laws can be constructed for any such $S_k(\Gamma)$, though this construction has never been carried out in general.

Outside the strongly ordinary case, we have two potential obstacles to obtaining a basis of 3-term congruences: repeated roots and supersingular reduction. Terms of the form $n^{m_j}\alpha_j^n$ with $m_j > 0$ coming from repeated roots of $H_p(T)$ will obstruct 3-term congruences, but these terms cannot be present if the action of the Frobenius on the corresponding Galois representation is semi-simple. It is expected that the action of the Frobenius is always semi-simple; for weight $k = 2$ forms, the semi-simplicity of the Frobenius operator follows from the theory of abelian varieties [6].

[2] If $\kappa_{\mathbf{m}}$ is not invertible, the situation is actually simpler; we can find forms whose mp^n-th Fourier coefficients are 0 modulo $p^{(n+1)(k-1)}$.

[3] In fact, they satisfy the 2-term congruences associated with the polynomial $(T - \alpha_j)$ or the 3-term congruences associated with $(T - \alpha_j)(T - \beta_j)$, where β_j is any number divisible by p^{k-1}, because as we have seen, these congruences are independent of any roots with p-adic valuation $k - 1$.

If the reduction at p is supersingular ($s > d$), then we have s roots α_j that affect the congruences. For a basis of d forms, this gives us a $d \times s$ matrix $(\kappa_{i,j})$, and we have no guarantee that row reduction of this matrix can yield rows with only one or two nonzero entries, as 3-term congruences require.

In the following example, there are no 3-term ASD congruences at supersingular primes. From computations on other examples, this appears to be typical; at places of supersingular reduction, we often do not find 3-term congruences.

We denote by q_μ the standard variable $q^{1/\mu} = e^{\frac{2\pi i z}{\mu}}$ at the cusp $i\infty$ of width μ. The modular function $\lambda = \frac{{\theta_2}^4}{{\theta_3}^4} = 16q_2 - 128{q_2}^2 + 704{q_2}^3 + \ldots$ is a Hauptmodul of the genus 0 congruence subgroup $\Gamma(2)$.[4] We define Hauptmoduln $x := -\sqrt[5]{2\lambda}$ and $y := \sqrt{2-2\lambda}$, which determine finite index genus 0 subgroups Γ_x and Γ_y. Then $\Gamma := \Gamma_x \cap \Gamma_y$ is a genus 2 subgroup with model $X_\Gamma : y^2 = x^5 + 2$. A basis for $S_2(\Gamma)$, corresponding to holomorphic differential forms $\omega_1 = \frac{xdx}{2y}$ and $\omega_2 = \frac{dx}{2y}$, is

$$f_1 = \sum_{n=1}^{\infty} a_{1,n}{q_{10}}^n = q_{10} - \frac{8}{5}{q_{10}}^6 - \frac{108}{5^2}{q_{10}}^{11} + \frac{768}{5^3}{q_{10}}^{16} + \frac{3374}{5^4}{q_{10}}^{21} + \ldots,$$

$$f_2 = \sum_{n=1}^{\infty} a_{2,n}{q_{10}}^n = {q_{10}}^2 - \frac{16}{5}{q_{10}}^7 + \frac{48}{5^2}{q_{10}}^{12} + \frac{64}{5^3}{q_{10}}^{17} + \frac{724}{5^4}{q_{10}}^{22} + \ldots.$$

The powers of q_{10} present in the expansions of x and y dictate that f_1 only has powers of q_{10} congruent to 1 (mod 5) and f_2 only has powers congruent to 2 (mod 5). The curve X_Γ has supersingular reduction at odd primes $p \equiv 2$, 3 (mod 5) with $H_p(T) = T^4 + p^2$, so the Scholl congruence on $S_2(\Gamma)$ at these places is

$$a_{i,mp^{n+2}} + p^2 a_{i,mp^{n-2}} \equiv 0 \pmod{p^{n+1}}.$$

However, there is no linear combination of f_1 and f_2 that will satisfy a 3-term congruence, since there are not enough nonzero terms in the q-expansions of f_1 and f_2.

Theorem 3.1. *For the finite index subgroup $\Gamma \subset SL_2(\mathbb{Z})$ defined above, there is no basis of forms in $S_2(\Gamma)$ satisfying three-term ASD congruences at any odd prime $p \equiv 2, 3 \pmod 5$.*

Proof. Let p be any odd prime congruent to 2 or 3 modulo 5. Since $a_{1,1} = 1$ and $H_p(T) = T^4 + p^2$, we have $v_p(a_{1,p^{4n}}) = 2n$. For any basis of forms satisfying 3-term congruences at p, at least one of the forms must be $c_1 f_1 + c_2 f_2$ with c_1 nonzero; the p^n-th Fourier coefficient of this form is $a_{p^n} = c_1 a_{1,p^n} + c_2 a_{2,p^n}$.

Then $a_{p^{4n}} = c_1 a_{1,p^{4n}}$, since $a_{2,p^{4n}} = 0$. If $p \equiv 2 \pmod 5$, we have $a_{p^{4n}+2} = a_{p^{4n}+3} = 0$. For $p \equiv 3 \pmod 5$, we have $a_{p^{4n}+1} = a_{p^{4n}+2} = 0$. In both cases, there is no possibility of 3-term congruences; $v_p(a_{p^{4n}}) = 2n + v_p(c_1)$ while 3-term congruences involving $a_{p^{4n}}$ depend on $a_{p^{4n}}$ modulo at least p^{4n}. So, if n is chosen large enough, $a_{p^{4n}}$ is nonzero modulo the relevant power of p, but the two adjacent terms, $a_{p^{4n}\pm 1}$ and $a_{p^{4n}\pm 2}$ (± depending on $p \pmod 5$), are both 0. Thus, there is no possibility of finding a basis of $S_2(\Gamma)$ satisfying 3-term congruences. □

[4] That is, it is invariant under the action of $\Gamma(2)$ by fractional linear transformation and parametrizes the genus 0 modular surface $X_{\Gamma(2)} = \Gamma(2)\backslash\mathcal{H} \cup \{0, 1, i\infty\}$.

References

[1] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160. MR0268123 (42 #3022)

[2] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*, Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I., 1971, pp. 1–25. MR0337781 (49 #2550)

[3] Gabriel Berger, *Hecke operators on noncongruence subgroups* (English, with English and French summaries), C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 9, 915–919. MR1302789 (95k:11063)

[4] E. J. Ditters, *Hilbert functions and Witt functions. An identity for congruences of Atkin and of Swinnerton-Dyer type*, Math. Z. **205** (1990), no. 2, 247–278, DOI 10.1007/BF02571239. MR1076132 (92b:14025)

[5] Gareth A. Jones, *Triangular maps and noncongruence subgroups of the modular group*, Bull. London Math. Soc. **11** (1979), no. 2, 117–123, DOI 10.1112/blms/11.2.117. MR541962 (83a:10039)

[6] Nicholas M. Katz, *Crystalline cohomology, Dieudonné modules, and Jacobi sums*, Automorphic forms, representation theory and arithmetic (Bombay, 1979), Tata Inst. Fund. Res. Studies in Math., vol. 10, Tata Inst. Fundamental Res., Bombay, 1981, pp. 165–246. MR633662 (83a:14022)

[7] Wen Ch'ing Winnie Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315. MR0369263 (51 #5498)

[8] Ling Long, *Finite index subgroups of the modular group and their modular forms*, Modular forms and string duality, Fields Inst. Commun., vol. 54, Amer. Math. Soc., Providence, RI, 2008, pp. 83–102. MR2454321 (2009k:11069)

[9] R. A. Rankin. *Contributions to the theory of Ramanujan's function* $\tau(n)$ *and similar functions II. The order of the Fourier coefficients of integral modular forms*, Proc. Cambridge Philos. Soc. **35** (1939), 357–373. MR0000411 (1,69d)

[10] A. J. Scholl, *Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences*, Invent. Math. **79** (1985), no. 1, 49–77, DOI 10.1007/BF01388656. MR774529 (86j:11045)

[11] J. G. Thompson, *A finiteness theorem for subgroups of* $\mathrm{PSL}(2, \mathbf{R})$ *which are commensurable with* $\mathrm{PSL}(2, \mathbf{Z})$, The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, R.I., 1980, pp. 533–555. MR604632 (82b:20067)

Department of Mathematics, Iowa State University, Ames, Iowa 50011
Current address: 3505 Sharonwood Road, Apt. 2D, Laurel, Maryland 20724
E-mail address: jckibelbek@gmail.com