Contemporary Mathematics
Volume 166, 1994

Congruences on the Fourier coefficients of modular forms on $\Gamma_0(N)$

KEN ONO

Dedicated to the memory of Hans Rademacher

ABSTRACT. Swinnerton-Dyer used ℓ-adic Galois representations to classify congruences satisfied by Ramanujan's τ(n) function. He proved the classical Ramanujan congruence $\tau(n) \equiv \sigma_{11}(n) \mod 691$ by applying modern techniques from modular form theory. By classifying subgroups of $GL_2(F_\ell)$, he identified congruences which arise when the image of a certain Galois group is 'small' under an ℓ-adic representation. The methodology given by Swinnerton-Dyer applies to normalized simultaneous eigenforms on the full modular group $SL_2(Z)$ with integer coefficients . Here these methods are generalized to include modular forms on $\Gamma_0(N)$ with character ϵ.

1. Introduction

In 1969, Deligne [D] proved Serre's conjecture on the existence of ℓ-adic Galois representations ρ_ℓ attached to modular forms on $\Gamma_0(N)$. Then, in 1972, Swinnerton-Dyer [S-D] determined the possible images of $\tilde{\rho}_\ell$, the reduction mod ℓ of ρ_ℓ, and showed that 'small' images imply certain congruences among modular forms of level one. In this paper we shall show that Swinnerton-Dyer's method and proof go through for eigenforms of level N : The novelty here is that certain possibilities for the images of ρ_ℓ, which are ruled out in the level one setting, do occur in the level N case. These cases are analyzed in Theorems 3.2 and 3.3 (cf. $(iv), (v)$).

We will use the notation adopted by Swinnerton-Dyer [S-D],[S-D2]. Let ℓ be a rational prime. Denote by K_ℓ the maximal algebraic extension of Q ramified only at ℓ. Let K_ℓ^{ab} be the maximal subfield of K_ℓ abelian over Q. If $p \neq \ell$ is a rational prime, we denote by Frob(p) the conjugacy class of Frobenius elements for p in Gal(K_ℓ/Q). Let Z_ℓ be the ring of ℓ-adic integers, and $F_\ell = Z/\ell Z$ its

1991 *Mathematics Subject Classification.* Primary 11F11, 11F30, 11F33 ;Secondary 11F20.
This paper is in final form and no version of it will be submitted for publication elsewhere.

residue class field. The canonical isomorphism χ_ℓ of $\mathrm{Gal}(K_\ell^{ab}/Q) \to Z_\ell^*$ induces a canonical character $\chi_\ell : \mathrm{Gal}(K_\ell/Q) \to Z_\ell^*$. For all $p \neq \ell$ this character satisfies $\chi_\ell(\mathrm{Frob}(p)) = p$.

In Section 2 we recall basic definitions and the theorems of Deligne and Serre [D], [D,S] concerning the existence of the desired Galois representations. When the image of $\mathrm{Gal}(\bar{Q}/Q)$ is small, congruences satisfied by the coefficients of a modular form arise from relations between the trace and determinant of the matrices representing Frobenius elements. This is discussed in Section 3. In Section 4, facts about modular forms mod ℓ are presented. Examples of congruences are given in Section 5.

2. Preliminaries

Let $N \geq 1$ be a rational integer. Then we define the following congruence subgroups of $SL_2(Z)$. Let A denote the matrix below with integer entries:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

i) $A \in \Gamma_0(N) \iff c \equiv 0 \mod N$.

ii) $A \in \Gamma_1(N) \iff a \equiv d \equiv 1 \mod N$ and $c \equiv 0 \mod N$.

iii) $A \in \Gamma(N) \iff a \equiv d \equiv 1 \mod N$ and $b \equiv c \equiv 0 \mod N$.

Let ϵ be a Dirichlet character mod N. This means that $\epsilon : (Z/NZ)^* \to C^*$ is a homomorphism. Let $k \in Z$ where $\epsilon(-1) = (-1)^k$. If f is a modular form of weight k with respect to $\Gamma_1(N)$ satisfying $f(A\tau) = \epsilon(d)(c\tau + d)^k f(\tau)$ for all $\tau \in H$ (where H is the upper half complex plane) and for all $A \in \Gamma_0(N)$ we say that f is a modular form of type (k, ϵ) on $\Gamma_0(N)$. The character ϵ is called the Nebentypus character of f.

Let $f = \sum a(n)q^n$ be the Fourier expansion of a modular form of type (k, ϵ) on $\Gamma_0(N)$ at $\tau = i\infty$. Here $q = e^{2\pi i\tau}$ is the uniformizing variable at infinity. If p is a rational prime , we define the Hecke operator T_p by

$$f|T_p = \sum a(pn)q^n + \epsilon(p)p^{k-1}\sum a(n)q^{pn}.$$

Note that if $p \mid N$ then $\epsilon(p) = 0$, so T_p reduces to the dissection operator U_p defined by:

$$f \mid U_p = \sum a(pn)q^n$$

This paper classifies congruences satisfied by $a(n)$ for a particular class of modular forms of type (k, ϵ) on $\Gamma_0(N)$. This class consists of cusp forms f that satisfy the following:

a) f is an eigenform of the Hecke operators T_p for all primes $p \in Z$

b) the Fourier coefficients $a(n)$ of f are rational integers, and $a(1) = 1$.

THEOREM 2.1. *(Deligne-Serre)*

Let f be a modular form of type (k, ϵ) on $\Gamma_0(N)$ satisfying a) and b) above. If $k \geq 1$ then for every rational prime ℓ there is a continuous linear representation

$$\rho_\ell : \mathrm{Gal}(\bar{Q}/Q) \to GL_2(Z_\ell)$$

which is unramified outside $N\ell$ *such that for all primes* p *with* $p \not| \ell N$ *we have:*

$$\mathrm{tr}(\rho_\ell(\mathrm{Frob}(p)) = a(p)$$

$$\det(\rho_\ell(\mathrm{Frob}(p)) = \epsilon(p)p^{k-1}.$$

REMARK 2.1. If p is a prime with $p \not| \ell N$ then the theorem implies that the characteristic polynomial of $\rho_\ell(Frob(p))$ is congruent to

$$x^2 - a(p)x + \epsilon(p)p^{k-1} \mod \ell.$$

3. Congruences induced by Galois representations

The search for congruences depends on the classification of subgroups of $GL_2(F_\ell)$. Given a modular form f and its associated representation ρ_ℓ, congruences hold when the image $\rho_\ell(\mathrm{Gal}(\bar{Q}/Q))$ does not contain $SL_2(Z_\ell)$. For $\ell > 3$, this happens only if $\tilde{\rho}_\ell(Gal(\bar{Q}/Q))$ does not contains $SL_2(F_\ell)$, where $\tilde{\rho}_\ell$ is the reduction of ρ_ℓ modulo ℓ. In this case we say that ℓ is an '*exceptional prime*' for f and we call the image $\tilde{\rho}_\ell(\mathrm{Gal}(\bar{Q}/Q))$ '*small.*' It will now be shown that identifying certain congruences reduces to a search for exceptional primes for f.

A Borel subgroup of $GL_2(F_\ell)$ is any subgroup which is conjugate to the group of nonsingular upper-triangular matrices. There are two types of Cartan subgroups of $GL_2(F_\ell)$. A *split* Cartan subgroup is any subgroup conjugate to the group of nonsingular diagonal matrices. Hence a *split* Cartan subgroup is the direct product of two cyclic groups of order $\ell - 1$.

A *nonsplit* Cartan subgroup is defined as follows. Let V be a 2 dimensional vector space over F_ℓ, and W its extension by scalars in F_{ℓ^2} :

$$W = V \otimes_{F_\ell} F_{\ell^2}$$

The nontrivial automorphism σ of F_{ℓ^2}/F_ℓ acts on W in the natural way.

Let U be a one-dimensional subspace of W with $U \neq \sigma(U)$. The nonsplit Cartan subgroup associated with U consists of those elements of $GL_2(F_\ell)$ that have U and $\sigma(U)$ as eigenspaces. Each element of a nonsplit Cartan subgroup is uniquely determined by its eigenvalue on U, since the eigenvalue for $\sigma(U)$ is its conjugate. In particular a nonsplit Cartan subgroup is isomorphic to $F^*_{\ell^2}$.

REMARK 3.1. Since each element of the normalizer of a Cartan subgroup either fixes or interchanges the associated eigenspaces, it follows that a Cartan subgroup is of index 2 in its normalizer.

LEMMA 3.1. *Let* G *be a subgroup of* $GL_2(F_\ell)$. *If* $\ell \mid |G|$, *then* G *is either contained in a Borel subgroup of* $GL_2(F_\ell)$ *or contains* $SL_2(F_\ell)$. *If* $\ell \not| |G|$, *let* H *be the image of* G *in* $PGL_2(F_\ell)$. *In this case either*
A. H *is cyclic and* G *is contained in a Cartan subgroup of* $GL_2(F_\ell)$

or

B. H is dihedral and G is in the normalizer of a Cartan subgroup of $GL_2(F_\ell)$, but not in the Cartan subgroup itself (This can occur only if $\ell > 2$.)

or

C. H is isomorphic to A_4 S_4, or A_5. (The first two cases here can only occur if $\ell > 3$ and the third case can occur only if $\ell > 5$.

For the proof of this lemma see [S-D].

The Deligne-Serre representation ρ_ℓ is unramified outside $N\ell$. In general it is ramified at the prime divisors of $N\ell$. Recall that an $\ell-$adic representation is unramified at a prime p if it is trivial on the inertia group of p. When a normalized cusp eigen-form is on $\Gamma_0(\ell)$, then the representation ρ_l factors through $\mathrm{Gal}(K_\ell/Q)$ [Se, p.I-7]. We discuss the congruences of such forms in Theorem 3.2. Before proceeding to congruences we make the following observation.

THEOREM 3.1. *If $\ell = N$ then ρ_ℓ factors through K_ℓ. In this case, $\tilde{\rho}_\ell(\mathrm{Gal}(K_\ell/Q))$ cannot be contained in a nonsplit Cartan subgroup of $GL_2(F_\ell)$ without being contained in a Borel subgroup.*

PROOF. Suppose the image $\tilde{\rho}_\ell(\mathrm{Gal}(K_\ell/Q))$ under $\tilde{\rho}_\ell$ is contained in a nonsplit Cartan subgroup C. Since C is abelian, we have the following commutative diagram:

$$\begin{array}{ccc} & \overset{\tilde{\rho}_\ell}{} & \\ \mathrm{Gal}(K_\ell/Q) & \to & C \\ \nu \downarrow & \nearrow & \\ \mathrm{Gal}(K_\ell^{ab}/Q) & & \end{array}$$

(where ν is the natural projection map). Since all finite factor groups of $\mathrm{Gal}(K_\ell^{ab}/Q)$ have order dividing $\ell^n(\ell-1)$ for some n, it follows that $|\tilde{\rho}_\ell(\mathrm{Gal}(K_\ell/Q)| \mid (\ell-1)$. Hence the matrices in $\tilde{\rho}_\ell(\mathrm{Gal}(K_\ell/Q))$ have eigenvalues in F_ℓ since their minimal polynomials divide $x^{\ell-1} - 1$. Since they commute, they can be simultaneously diagonalized so $\mathrm{Gal}(K_\ell/Q)$ is contained in a Borel subgroup. □

COROLLARY 3.1. *Let f be a modular form of type (k,ϵ) on $\Gamma_0(\ell)$ satisfying a) and b). Let ℓ be an exceptional prime for f and let $\tilde{\rho}_\ell$ be the associated Galois representation*

$$\tilde{\rho}_\ell : \mathrm{Gal}(K_\ell/Q) \to GL_2(F_\ell)$$

given by Serre and Deligne. Let $G = \tilde{\rho}_\ell(\mathrm{Gal}(K_\ell/Q))$ and let H be the image of G in $PGL_2(F_\ell)$. Then one of the following is true:

(i) $G \subseteq$ a Borel subgroup of $GL_2(F_\ell)$.

or

(ii) $G \subseteq$ the normalizer of a Cartan subgroup but not in the Cartan subgroup itself. (This can occur only if $\ell > 2$.)

or
(iii) $H \cong S_4$ *(This can occur only if* $\ell > 3$. *)*
or
(iv) $H \cong A_4$ *(This can occur only if* $\ell > 3$.*)*
or
(v) $H \cong A_5$ *(This can occur only if* $\ell > 5$. *)*

Now Swinnerton-Dyer type congruences on the Fourier coefficients of the form f can be classified by investigating the structure of the groups given in this corollary.

THEOREM 3.2. *Let* f *be a modular form of type* (k, ϵ) *on* $\Gamma_0(\ell)$ *satisfying a) and b). If* ℓ *is an exceptional prime for* f *then we have the following congruences: (i) If* $G \subseteq$ *a Borel subgroup of* $GL_2(F_\ell)$ *and* ϵ *is trivial, then* $\exists$ *an integer* m *such that if* $(n, \ell) = 1$ *then*

$$a(n) \equiv n^m \sigma_{k-1-2m}(n) \mod \ell$$

(ii) If $G \subseteq$ *the normalizer of a Cartan subgroup but not in the Cartan subgroup itself, then:*

$$a(n) \equiv 0 \mod \ell \qquad \text{when } (n, \ell) = 1 \text{ and } \left(\frac{n}{\ell}\right) = -1$$

(iii) If $H \cong S_4$ *then*

$$\epsilon^{-1}(p)p^{1-k}a^2(p) \equiv 0, 1, 2, 4 \mod \ell \qquad \text{when } p \not| \ell$$

(iv) If $H \cong A_4$ *then*

$$\epsilon^{-1}(p)p^{1-k}a^2(p) \equiv 0, 1, 4 \mod \ell \qquad \text{when } p \not| \ell$$

(v) If $H \cong A_5$ *then*

$$\left\{\epsilon^{-1}(p)p^{1-k}a^2(p) - \frac{3}{2}\right\}^2 \equiv \frac{1}{4}, \frac{5}{4}, \frac{9}{4}, \frac{25}{4} \mod \ell \qquad \text{when } p \not| \ell$$

Note: (ii) can occur only if $\ell > 2$. (iii), and (iv) can occur only if $\ell > 3$. (v) can occur only if $\ell > 5$.

PROOF. (i) We know that if $p \not| \ell N$, then $a(p) \equiv p^m + p^{k-1-m} \mod \ell$, since the only character representations of $\mathrm{Gal}(K_\ell/Q)$ into F_ℓ^* are powers of $\tilde{\chi}_\ell$. The general case now follows from the multiplicativity of the Fourier coefficients of f.

(ii) Let N be the normalizer of the Cartan subgroup C. The natural projection map $\gamma : G \to N/C \cong Z/2Z$ yields the following commutative diagram:

$$\begin{array}{ccccc} & & & & \gamma \\ \mathrm{Gal}(K_\ell/Q) & \to & G & \to & Z/2Z \\ \downarrow & & & \nearrow & \\ \mathrm{Gal}(K_\ell^{ab}/Q) & \tilde{\to} & Z_\ell^* & & \end{array}.$$

The only nontrivial homomorphism of Z_ℓ^* to $Z/2Z$ is the one whose kernel consists of the squares of Z_ℓ^*. Any element $\alpha \in \mathrm{Gal}(K_\ell/Q)$ with $\tilde{\rho}_\ell(\alpha) \notin C$ interchanges the associated eigenspaces. Using the eigenspaces associated with C over F_{ℓ^2}, we see that $\tilde{\rho}_\ell(\alpha)$ has the form:

$$\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}.$$

If $p \not| \ell N$ then $\tilde{\rho}_\ell(\mathrm{Frob}(p)) \in C$ if and only if p is a quadratic residue mod ℓ. Hence if p is a quadratic nonresidue mod ℓ it follows that:

$$\mathrm{tr}(\tilde{\rho}_\ell(\mathrm{Frob}(p)) \equiv a(p) \equiv 0 \mod \ell.$$

(iii), (iv) These congruences are identical to the type 3 congruence given by Swinnerton-Dyer. The proof of this congruence follows from the fact that an element of S_4 has order 1,2,3 or 4 and that an element of A_4 has order 1,2 or 3. Hence the eigenvalues of $\tilde{\rho}_\ell(\mathrm{Frob}(p))$ can be determined, and the trace and determinant of $\tilde{\rho}_\ell(\mathrm{Frob}(p))$ give the desired congruence.
For details see [SW].

(v) For this congruence we need only to consider the element of order 5 in A_5. Suppose that A is an element of order five in $PGL_2(F_\ell)$ and let A'' be a representative of A in $GL_2(F_\ell)$. Then

$$\det((A'')^5) \in (F_\ell^*)^2,$$

and it follows that there is a representative A' for A'' with $\det(A') = 1$ whose characteristic polynomial divides $t^4 + t^3 + t^2 + t + 1$. This polynomial factors in F_{ℓ^2} as $(t^2 + at + 1)(t^2 + bt + 1)$ with $a = \frac{1-\sqrt{5}}{2}$ and $b = \frac{1+\sqrt{5}}{2}$. The congruence now follows by relating the trace and determinant. □

The methods which constructed the congruences above also define congruences for level N forms. Some of these congruences are contained in the following theorem.

THEOREM 3.3. *Let f be a modular form of type (k, ϵ) on $\Gamma_0(N)$ satisfying a) and b). If ℓ is an exceptional prime for f then let $G = \tilde{\rho}_\ell(\mathrm{Gal}(\bar{Q}/Q)$ and let H be the image of G in $PGL_2(F_\ell)$.*
(ii) If $G \subseteq$ the normalizer of a Cartan subgroup but not in the Cartan subgroup itself, then

$$a(p) \equiv 0 \mod \ell \quad \text{for a set of primes with density} \geq 1/2.$$

(iii) If $H \cong S_4$ *then*

$$\epsilon^{-1}(p)p^{1-k}a^2(p) \equiv 0, 1, 2, 4 \mod \ell \qquad \text{when } p \nmid \ell N.$$

(iv) If $H \cong A_4$ *then*

$$\epsilon^{-1}(p)p^{1-k}a^2(p) \equiv 0, 1, 4 \mod \ell \qquad \text{when } p \nmid \ell N.$$

(v) If $H \cong A_5$ *then*

$$\left\{\epsilon^{-1}(p)p^{1-k}a^2(p) - \frac{3}{2}\right\} \equiv \frac{1}{4}, \frac{5}{4}, \frac{9}{4}, \frac{25}{4} \mod \ell \qquad \text{when } p \nmid \ell N.$$

4. Modular forms of level $N \mod \ell$

In [SD], Swinnerton-Dyer proved that there are only finitely many exceptional primes ℓ for a given f by studying modular forms mod ℓ. Here we state results of Katz [Ka] and Sturm [St] which are used in proving congruences. In particular, emphasis will be placed on the Ramanujan θ-operator, a function on formal power series.

DEFINITION 4.1. *Given a formal power series* $\sum a(n)q^n$, *the Ramanujan* θ-*operator is defined to be the map which acts on formal power series in the following way:*

$$\theta : \sum a(n)q^n \to \sum na(n)q^n$$

DEFINITION 4.2. *Fix a prime* $\ell \geq 5$ *with* $\ell \nmid N$. *Define* $M_k(N)$ *to be the subset of modular forms of weight* k *on* $\Gamma_0(N)$ *whose Fourier coefficients at* $i\infty$ *are* ℓ-*integral.*

DEFINITION 4.3. *We define* $\tilde{M}_k(N)$ *to be:*

$$\tilde{M}_k(N) = \left\{\tilde{f} = \sum \tilde{a}(n)q^n \mid f = \sum a(n)q^n \in M_k(N)\right\}$$

REMARK 4.1. If $\ell \geq 5$ is a prime and k is an integer then:

$$\tilde{M}_k(N) \subseteq \tilde{M}_{k+\ell-1}(N).$$

DEFINITION 4.4. *Given* $\tilde{f} \in \tilde{M}_k(N)$, *define the filtration of* $\tilde{f}$, *denoted* $\omega(\tilde{f})$, *to be:*

$$\omega(\tilde{f}) = inf\left\{j \mid \tilde{f} \in \tilde{M}_j(N)\right\}$$

THEOREM 4.1. ***(Katz)***
The Ramanujan θ-*operator maps* $\tilde{M}_k(N) \to \tilde{M}_{k+\ell+1}(N)$. *In fact,*

$$\omega(\theta(\tilde{f})) \leq \omega(\tilde{f}) + \ell + 1$$

with equality if and only if $\omega(\tilde{f}) \not\equiv 0 \mod \ell$.

DEFINITION 4.5. *Let ℓ be a prime. Let f be a formal power series $f = \Sigma a(n)q^n$ with rational integer coefficients. The $Ord_\ell(f)$ is defined by:*

$$Ord_\ell(f) = inf\{n \mid \ell \not| a(n)\}$$

THEOREM 4.2. ***(Sturm)***

Let f and g be modular forms of weight k on Γ where Γ contains a principal congruence subgroup $\Gamma(N)$ for some N. If f and g have integer Fourier coefficients and there exists a prime ℓ such that

$$Ord_\ell(f-g) > k[\Gamma(1):\Gamma]/12$$

then $Ord_\ell(f-g) = \infty$. (i.e. $f \equiv g \mod \ell$).

5. Examples

EXAMPLE 5.1. In this discussion we shall assume that f is a normalized simultaneous eigenform of type (k, ϵ) on $\Gamma_0(N)$. For notational purposes we take $f = \Sigma a(n)q^n$. Note that the congruences given in Theorem 2 only pertain to those coefficients $a(n)$ when $(n, \ell N) = 1$.

We can retrieve some congruences for those Fourier coefficients whose indices are not relatively prime to the level N. Let p be a prime dividing the level N. The eigenvalue of f with respect to the Hecke operator T_p is easily shown to be $a(p)$. Since $\epsilon(p) = 0$ we know then that the Fourier coefficients of f satisfy $a(pn) = a(p)a(n)$. So a congruence satisfied by $a(p)$, provides congruences for $a(pn)$.

The space of cusp forms on $\Gamma_0(5)$ of weight 4 is one dimensional. Using the theory developed by Newman and Gordon [Go] we see that a basis for this space is $\eta^4(\tau)\eta^4(5\tau)$.

$$\eta^4(\tau)\eta^4(5\tau) = q - 4q^2 + 2q^3 + 8q^4 - 5q^5 - 8q^6 \ldots$$

Since $a(5) = -5$ we see then that $a(5n) \equiv 0 \mod 5$ for all n.

EXAMPLE 5.2. In this example we consider $\eta^{12}(2\tau)$. This form is the unique normalized cuspform of weight 6 on $\Gamma_0(4)$. The first few terms of its Fourier expansion are:

$$\eta^{12}(2\tau) = q - 12q^3 + 54q^5 + 88q^7 - 99q^9 + 540q^{11} - 418q^{13} - 648q^{15} + 594q^{17} \ldots$$

By observation it appears that this form satisfies a type (ii) congruence; the first few terms satisfy $a(n) \equiv 0 \mod 11$ when $\left(\frac{n}{11}\right) = -1$. Notice that we do not worry about those Fourier coefficients with even indices because $a(2n) = 0$ for all n. Let $f(\tau) = \eta^{12}(2\tau)$. Consider the equation

$$\theta\tilde{f} = \theta^{(\ell+1)/2}\tilde{f}.$$

If a form f satisfies this equation then we formally have:

$$\Sigma n a(n) q^n \equiv \Sigma n^{(\ell+1)/2} a(n) q^n \mod \ell.$$

It follows that $a(n) \equiv a(n) n^{(\ell-1)/2} \mod \ell$ if $\ell \not| n$ and it follows that

$$a(n) \equiv 0 \mod \ell \quad \text{when} \quad \left(\frac{n}{\ell}\right) = -1.$$

Proving this last equation proves the type (ii) congruence.

Here we choose $\ell = 11$. By Katz's Theorem it is known that $\theta \tilde{f} \in \tilde{M}_{18}(4)$ and $\theta^6 \tilde{f} \in \tilde{M}_{78}(4)$. By Remark 4 we know that $\tilde{M}_{18}(4) \subseteq \tilde{M}_{78}(4)$. Sturm's Theorem indicates that we only need to show that:

$$n a(n) \equiv n^6 a(n) \mod 11$$

for $n = 1, 2, 3 \ldots 39$. Recall that $[\Gamma(1) : \Gamma_0(N)] = N \prod_{p|N}(1 + 1/p)$. These congruences are indeed satisfied for $n = 1, 2, 3, \ldots 39$ thus verifying our Type (ii) congruence.

There are several other examples of type (ii) congruences which are proven using the same techniques. Here are other examples of Type (ii) congruences.

1. $\eta^8(3\tau)$ satisfies $a(n) \equiv 0 \mod 5$ if $\left(\frac{n}{5}\right) = -1$.
2. $\eta^8(3\tau)$ satisfies $a(n) \equiv 0 \mod 7$ if $\left(\frac{n}{7}\right) = -1$.

EXAMPLE 5.3. In this example we verify a Type (ii) equality involving the cusp form $\eta^3(\tau)\eta^3(7\tau)$ on $\Gamma_0(7)$. This form is the unique cusp form of weight 3 and character $\epsilon(d) = \left(\frac{-7}{d}\right)$ on $\Gamma_0(7)$.

Let $\Sigma a(n) q^n$ be the Fourier expansion of this form at $i\infty$. The following Type (ii) equality occurs.

$$a(n) = 0 \quad \text{if} \left(\frac{n}{7}\right) = -1$$

This equality follows from the Jacobi product formula:

$$\prod_{n=1}^{\infty}(1 - q^n)^3 = \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{n(n+1)/2}$$

The equality follows from the fact that $n(n+1) \equiv 0, 2, 5$ or $6 \mod 7$. For all $\ell \neq 7$, experimental evidence suggests that the projective image of the Deligne-Serre representation is dihedral.

EXAMPLE 5.4. Now I want to suggest a Type (iii) congruence. Again we will consider the form $\eta^{12}(2\tau)$, the unique normalized eigenform of weight 6 on $\Gamma_0(4)$. Basil Gordon has found that the following congruence holds for the first fourteen hundred primes:

$$a^2(p) p^{-5} \equiv 0, 1, 2 \text{ or } 4 \mod 19.$$

Although this congruence is undoubtedly true, I have no proof of it.

This congruence has some interesting consequences. Consider the classical theta function, $\theta(\tau) = \Sigma q^{n^2}$, a modular form of weight $1/2$ on $\Gamma_0(4)$ in the sense of Shimura. Hence given a positive integer k, $\theta^{2k}(\tau)$ is a modular form of weight k on $\Gamma_0(4)$. If k is even then $\theta^{2k}(\tau)$ is a modular form with the trivial Nebentypus character.

Consider $\theta^{12}(\tau)$ as a modular form of weight 6 on $\Gamma_0(4)$. As is true with any modular form, we can write $\theta^{12}(\tau)$ as a linear combination of Eisenstein series and cusp forms. The Eisenstein series used here are denoted by $E_{6,1/4}(\tau)$ and $E_{6,1}(\tau)$. The 6 in each subscript means that these Eisenstein series are weight 6 forms. $\Gamma_0(4)$ has three inequivalent cusps, $\tau = 1, 1/2$ and $1/4$. Here $E_{6,1/4}(\tau)$ is constructed as to vanish at $1/2$ and 1 but not at $1/4$. Similarly $E_{6,1}(\tau)$ is the Eisenstein series which vanishes at $1/4$ and $1/2$, but not at 1.Using the methods outlined in [Sch] it is easily verified that these Eisenstein series have the following Fourier expansions at $i\infty$.

$$E_{6,1/4}(\tau) = 4 - \frac{1}{2}\sum_{n\geq 1}\left(\sum_{\substack{m|4n \\ 4n/m \equiv 0 \mod 4}} m^5 sgn(m) i^m\right) q^n$$

$$E_{6,1}(\tau) = -\frac{1}{2}\sum_{n\geq 1}\left(\sum_{\substack{m|4n \\ m \equiv 0 \mod 4 \\ 4n/m \equiv 3 \mod 4}} m^5 sgn(m)\right) q^n$$

For completeness, here are the first few terms of the Fourier expansions of each of these Eisenstein series.

$$E_{6,1/4}(\tau) = 4 + 32q^2 - 992q^4 + 7808q^6 - 33760q^8 + 100032q^{10} + \ldots$$

$$E_{6,1}(\tau) = -512q - 16384q^2 - 124928q^3 - 524288q^4 - 1600512q^5 + \ldots$$

It should be noted that $E_{6,1/4}(\tau)$ only contains terms with even exponents. Moreover for n odd, the coefficient of q^n in $E_{6,1}(\tau)$ is $-512\sigma_5(n)$.

Using linear algebra it can be shown that

$$\theta^{12}(\tau) = 16\eta^{12}(2\tau) - \frac{E_{6,1}(\tau)}{64} + \frac{E_{6,1/4}(\tau)}{4}$$

Put $\theta^{12}(\tau) = \Sigma r_{12}(n)q^n$ and $\eta^{12}(2\tau) = \Sigma a(n)q^n$. For any prime $p \neq 2$, we get:

$$r_{12}(p) = 16a(p) + 8(1 + p^5)$$

by using the formula for $E_{6,1}(\tau)$. Using the Type (iii) congruence we find that

$$r_{12}^2(p)p^{-5} - 16r_{12}(p)(1 + p^{-5}) + 7(p^5 + p^{-5} + 2) \equiv 0, 9, 17, \text{ or } 18 \mod 19.$$

With some computation, this congruence can be rewritten as:

$$r_{12}(p) - 8(1 + p^5) \equiv p^{5/2}(0, \pm 3, \pm 6) \mod 19 \quad \text{if } \left(\frac{p}{19}\right) = 1$$

$$r_{12}(p) - 8(1 + p^5) \equiv (-p)^{5/2} \mod 19 \quad \text{if } \left(\frac{p}{19}\right) = -1$$

It is a well known fact that the Fourier coefficient $r_s(p)$ of q^n in $\theta^s(\tau)$ is the number of ways that n is represented as a sum of s squares [Ko]. Hence the congruential relation above leads to an interesting arithmetic property involving the number of ways an odd prime is represented as a sum of 12 squares.

EXAMPLE 5.5. Type (i) congruences can be constructed by using the decomposition of integral modular forms into Eisenstein series and cusp forms. In the last example this decomposition was demonstrated for $\theta^{12}(\tau)$. Define $F(\tau)$ to be the modular form of weight 6 on $\Gamma_0(4)$ equal to $\frac{\theta^{12}(\tau)}{8} - 2\eta^{12}(\tau)$. It is easily verified that

$$F(\tau) = \frac{\theta^{12}(\tau)}{8} - 2\eta^{12}(2\tau) = \frac{E_{6,1/4}(\tau)}{32} - \frac{E_{6,1}(\tau)}{512}.$$

By the remarks made in Example 4, we have:

$$a(n) = \sigma_5(n)$$

for n odd. This is an equality of Fourier coefficients.

Infinitely many Type (i) congruences can be constructed using this equality. $F(\tau)$ is ℓ-integral for all primes $\ell \neq 2$. We may use the theory developed by Katz [K] to produce infiinitely many Type (i) congruences. Given any $\ell \geq 5$ and any positive integer m we know there exists a modular form $F_{\ell,m} \in M_{6+m(\ell+1)}(4)$ such that

$$\theta^m(\tilde{F}) \equiv \tilde{F}_{\ell,m} \mod \ell.$$

Let $F_{\ell,m} = \Sigma a_{\ell,m}(n)q^n$ for notational convenience. If n is odd then the following Type (i) congruence holds:

$$a_{\ell,m}(n) \equiv n^m \sigma_5(n) \mod \ell$$

EXAMPLE 5.6. Here an explicit Type (iv) congruence is demonstrated. In 1952, van der Blij explicitly described the behavior of $\eta(\tau)\eta(23\tau)$ [vdB]. This eta product is an eigenform of weight 1 on $\Gamma_0(23)$ with Nebentypus character $(\frac{-23}{d})$.

Denote its Fourier expansion at $i\infty$ by $\eta(\tau)\eta(23\tau) = \Sigma a(n)q^n$. The results of van der Blij include:

$$a(p) = 0 \quad \text{if } \left(\frac{p}{23}\right) = -1$$

$$a(p) = -1 \text{ or } 2 \quad \text{if } \left(\frac{p}{23}\right) = 1$$

The expression occurring in the congruence is $\epsilon^{-1}(p)a^2(p)$. By Quadratic Reciprocity it follows that for all primes p we have:

$$\epsilon^{-1}(p)a^2(p) = \left(\frac{p}{23}\right)a^2(p) = 0, 1, \text{ or } 4.$$

So $\eta(\tau)\eta(23\tau)$ satisfies the Type (iv) congruence for all primes ℓ.

Acknowledgements

I am grateful to Professor Basil Gordon, my thesis advisor, for his encouragement during my graduate study at the University of California, Los Angeles. I wish to thank the referee for providing the historical paragraph which appears at the beginning of the paper, and Professor R. Bruggeman who pointed out misprints in an early version of the paper.

REFERENCES

[Co] H. Cohen and J. Oesterle. *Dimensions des éspaces de formes modulaires. Springer Lecture Notes in Math. 601, Springer-Verlag (1976),Berlin*

[D] P. Deligne, *Formes modulaires et répresentations ℓ-adiques, Seminaire Bourbaki (1969) No.355*

[D,S] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1, Ann. Scient. École Normale Sup, 4^e série t.7, (1974)*

[Go] B. Gordon and D. Sinor, *Multiplicative properties of η-products Springer Lecture Notes in Math. 1395 Springer-Verlag (1987),Berlin*

[K] N. Katz, *A result on modular forms in characteristic p, Springer Lecture Notes in Math. 601 Springer-Verlag (1976),Berlin*

[Ko] N. Koblitz, *Introduction to elliptic curves and modular forms, Springer-Verlag (1984),Berlin*

[Sch] B. Schoeneberg, *Elliptic modular functions- an introduction, Springer-Verlag (1970),Berlin*

[S] J.-P. Serre, *Congruences et formes modulaires (d'aprés H.P.F. Swinnerton- Dyer), Seminaire Bourbaki (1971) No.416*

[Se] J.-P. Serre, *Abelian $\ell-$adic representations and elliptic curves, Addison-Wesyley Publ. Co. (1989)*

[Shi] G. Shimura, *Introduction to the arithmetic theory of automorphic functions, Publ. Math. Society of Japan, No. 11 (1971)*

[St Sturm, *On the congruence of modular forms, Springer Lecture Notes in Math. 1240, Springer-Verlag (1984),Berlin*

[S-D] H.P.F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms, Springer Lecture Notes in Math. 350 Springer-Verlag (1973),Berlin*

[S-D2] H.P.F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms II, Springer Lecture Notes in Math. 601, Springer-Verlag (1976),Berlin*

[vdB] F. van der Blij, *Binary quadratic forms of discriminant -23, Nederl. Akad. Wetensch. Proc. Ser A. 55 = Indagationes Math. 14,(1952)*

DEPARTMENT OF GENERAL EDUCATION, WOODBURY UNIVERSITY, BURBANK, CALIFORNIA 91510

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT LOS ANGELES, LOS ANGELES, CALIFORNIA 90024,

Current address: Department of Mathematics,The University of Georgia, Athens, Georgia 30602

E-mail address: ono@joe.math.uga.edu